

F A C U L D A D E   D A M A S   D A   I N S T R U Ç Ã O   C R I S T Ã

CURSO DE BACHARELADO EM ADMINISTRAÇÃO

PEDRO HENRIQUE SILVA AGUIAR BARBOSA

**UMA ABORDAGEM SOBRE A LEI GERAL DE PROTEÇÃO DE DADOS NO  
SETOR DE RECURSOS HUMANOS**

Recife

2025

PEDRO HENRIQUE SILVA AGUIAR BARBOSA

**UMA ABORDAGEM SOBRE A LEI GERAL DE PROTEÇÃO DE DADOS NO  
SETOR DE RECURSOS HUMANOS**

Trabalho de conclusão de curso apresentado à  
Faculdade Damas da Instrução Cristã, como  
requisito parcial para obtenção ao título de  
Bacharel em Administração, sob orientação da  
Professora Ms. Andrea Karla Travassos de  
Lima.

Recife

2025

**Catalogação na fonte**  
**Bibliotecário Ricardo Luiz Lopes CRB-4/2116**

Barbosa, Pedro Henrique Silva Aguiar.

B238u      Uma abordagem sobre a Lei Geral de Proteção de Dados no setor de recurso humanos / Pedro Henrique Silva Aguiar Barbosa. - Recife, 2025.

47 f. : il.

Orientador: Prof.<sup>a</sup> Ms. Andrea Karla Travassos de Lima.

Trabalho de Conclusão de Curso (Monografia - Administração) – Faculdade Damas da Instrução Cristã, 2025.

Inclui bibliografia.

1. Lei geral de proteção de dados. 2. Proteção de dados. 3. Recurso humanos. 4. Governança de dados. 5. Segurança da informação. I. Lima, Andrea Karla Travassos de. II. Faculdade Damas da Instrução Cristã. III. Título

658 CDU (22. ed.)

FADIC(2025.1- 019)

PEDRO HENRIQUE SILVA AGUIAR BARBOSA

**UMA ABORDAGEM SOBRE A LEI GERAL DE PROTEÇÃO DE DADOS NO  
SETOR DE RECURSOS HUMANOS**

Defesa Pública em Recife, 03 de Junho de 2025.

BANCA EXAMINADORA

---

Orientador: Professor Ms. Andrea Karla Travassos de Lima

---

Professor Convidado: Profa. Dra. Ana Lúcia Neves de Moura

## **AGRADECIMENTOS**

Agradeço este trabalho primeiramente a Deus, pela força, sabedoria e perseverança que me guiou em cada etapa deste processo. Agradeço também a mim, por toda a dedicação, esforço e resiliência demonstrados ao longo de toda a pesquisa. A minha orientadora, Andrea Karla Travassos de Lima, merece um agradecimento especial pela paciência, apoio constante e orientações valiosas que foram fundamentais para a realização deste trabalho. Por fim, deixo meu agradecimento a todas as pessoas que estiveram ao meu lado durante este percurso, oferecendo suporte, incentivo e palavras de encorajamento. Sem a ajuda e compreensão de cada um de vocês, este trabalho não teria sido possível.

## RESUMO

Este trabalho teve como objetivo analisar os desafios e implicações da implementação da Lei Geral de Proteção de Dados Pessoais (LGPD) no tratamento de dados, com foco específico no setor de Recursos Humanos (RH). A pesquisa abordou as dimensões legais e práticas da LGPD, destacando a necessidade de adaptação das organizações à nova legislação, em especial no que se refere à proteção e ao tratamento de dados pessoais. O problema de pesquisa concentrou-se nas dificuldades enfrentadas pelas empresas para implementar as políticas estabelecidas pela LGPD, especialmente no que diz respeito à governança de dados e à segurança das informações no contexto de Recursos Humanos. O método adotado incluiu uma análise qualitativa, com a revisão de literatura e a coleta de dados por meio de estudos de caso em empresas do setor. A discussão envolveu os principais aspectos da LGPD, como a transparência, a finalidade e a eliminação de dados, evidenciando como estes princípios impactam diretamente o setor de RH. Os resultados mostraram que, embora a LGPD traga avanços significativos na proteção de dados pessoais, ainda existem desafios relacionados à implementação efetiva da legislação, especialmente em pequenas e médias empresas, que enfrentam dificuldades financeiras e técnicas. Constatou-se também que a capacitação dos profissionais e o investimento em tecnologia são fundamentais para garantir a conformidade com a LGPD. Por fim, sugeriu-se que futuras pesquisas abordem a eficácia da fiscalização da Autoridade Nacional de Proteção de Dados (ANPD) e explorem como as empresas podem superar as barreiras impostas pela nova legislação.

**Palavras-chave:** lei geral de proteção de dados; proteção de dados; recursos humanos; governança de dados; segurança da informação.

## **ABSTRACT**

This study aimed to analyze the challenges and implications of implementing the General Data Protection Law (LGPD) in data processing, with a specific focus on the Human Resources (HR) sector. The research addressed both the legal and practical dimensions of the LGPD, highlighting the need for organizations to adapt to the new legislation, especially regarding the protection and handling of personal data. The research problem focused on the difficulties faced by companies in implementing the policies established by the LGPD, particularly in relation to data governance and information security in the HR context. The methodology included a qualitative analysis, with a literature review and case studies from companies in the sector. The discussion covered the main aspects of the LGPD, such as transparency, purpose, and data deletion, demonstrating how these principles directly impact the HR sector. The results revealed that, although the LGPD brings significant advances in personal data protection, challenges remain in effectively implementing the legislation, especially for small and medium-sized enterprises that face financial and technical difficulties. It was also found that training professionals and investing in technology are essential to ensure compliance with the LGPD. Finally, the study suggested future research on the effectiveness of the National Data Protection Authority (ANPD) oversight and how companies can overcome the barriers posed by the new legislation.

**Keywords:** LGPD; data protection; human resources; data governance; information security.

## **LISTA DE ABREVIATURAS E SIGLAS**

ANPD - Autoridade Nacional de Proteção de Dados

CISA- *Cybersecurity & Infrastructure Security Agency*

COVID-19 - *Coronavírus Disease 2019*

CPF- Cadastro de Pessoa Física

GDPR - *General Data Protection Regulation*

LGPD - Lei Geral de Proteção de Dados

OMS - Organização Mundial da Saúde

RH - Recursos Humanos

SARS-CoV-2 - *Severe Acute Respiratory Syndrome Coronavirus 2*

## SUMÁRIO

<b>1</b>	<b>INTRODUÇÃO .....</b>	<b>9</b>
<b>1.1</b>	<b>Justificativa .....</b>	<b>10</b>
<b>1.2</b>	<b>Objetivos .....</b>	<b>11</b>
1.2.1	Objetivo geral .....	11
1.2.2	Objetivos específicos .....	11
<b>1.3</b>	<b>Estrutura do trabalho .....</b>	<b>11</b>
<b>2</b>	<b>REFERENCIAL TEORICO .....</b>	<b>12</b>
<b>2.1</b>	<b>A Lei Geral de Proteção de Dados.....</b>	<b>12</b>
2.1.1	Fundamentos da Lei Geral de Proteção de Dados .....	13
2.1.2	Princípios da Lei Geral de Proteção de Dados .....	15
2.1.3	O Processamento dos Dados.....	17
2.1.4	Término de Tratamento dos Dados.....	19
<b>2.2</b>	<b>Processos de Recursos Humanos .....</b>	<b>20</b>
2.2.1	Agregação de Pessoas.....	20
2.2.2	Aplicação de Pessoas.....	22
2.2.3	Recompensar Pessoas.....	24
2.2.4	Desenvolvimento de Pessoas.....	25
2.2.5	Manutenção de Pessoas.....	27
2.2.6	Monitoramento de Pessoas.....	29
2.2.7	Setor de Recursos Humanos.....	31
2.2.8	Dados Pessoais e Dados Sensíveis.....	33
2.2.9	Penalidades e Multas Administrativas.....	35
<b>3</b>	<b>MÉTODO .....</b>	<b>36</b>
<b>3.1</b>	<b>Natureza da Pesquisa .....</b>	<b>36</b>
<b>3.2</b>	<b>Abordagem .....</b>	<b>36</b>
<b>3.3</b>	<b>Objetivos da Pesquisa .....</b>	<b>37</b>
<b>3.4</b>	<b>Procedimentos Metodológicos .....</b>	<b>37</b>
<b>3.5</b>	<b>Instrumentos de Coleta de Dados .....</b>	<b>37</b>
<b>3.6</b>	<b>Análise dos Dados .....</b>	<b>37</b>
<b>3.7</b>	<b>Limitações do Estudo .....</b>	<b>38</b>

<b>4</b>	<b>RESULTADOS E ANÁLISE DOS DADOS .....</b>	<b>39</b>
<b>4.1</b>	<b>Os Impactos da LGPD no Setor de Recursos Humanos .....</b>	<b>39</b>
4.1.1	Recrutamento e Seleção .....	39
4.1.2	Controle dos Termos de Autorização e Consentimento.....	40
4.1.3	Proteção dos Dados Pessoais .....	40
4.1.4	Dados Biométricos no Recursos Humanos .....	41
<b>5</b>	<b>CONSIDERAÇÕES FINAIS .....</b>	<b>42</b>
	<b>REFERÊNCIAS .....</b>	<b>44</b>

## 1 INTRODUÇÃO

A influência da tecnologia na vida dos indivíduos torna-se mais evidente a cada dia. O avanço tecnológico tem proporcionado o surgimento de novos meios de comunicação e, ao mesmo tempo, desenvolvido desafios no manuseio de dados, tanto para Estados quanto para organizações (Brasil, 2018). Com o volume crescente de dados pessoais circulando na internet, o direito busca definir mecanismos para garantir a preservação das informações dos indivíduos. Nesse contexto, a Lei Geral de Proteção de Dados (LGPD) emerge como uma resposta necessária para regulamentar a forma como as instituições tratam dados pessoais, estabelecendo diretrizes para garantir a privacidade e segurança (Brasil, 2018).

Os dados pessoais representam um grande desafio, pois informações sensíveis, como endereço, Cadastro de Pessoa Física (CPF), senhas e até preferências pessoais, têm sido alvo de vazamentos e acessos indevidos. Raminelli e Rodegheri (2016, p. 92), se expressaram sobre esses dados da seguinte forma:

[...] O grande desafio que se coloca à frente dos cidadãos é o controle dos dados pessoais que pode ser feito por empresas ou, até mesmo, pelos governos. Há possibilidade de verificação, por meio de um monitoramento online, de preferências artísticas, musicais, hábitos de vida, de viagens, operações financeiras, orientação sexual, crenças religiosas, entre outros.

Esses desafios são ainda mais evidentes no setor de Recursos Humanos (RH) das organizações, que lida diariamente com uma quantidade significativa de informações sensíveis de seus colaboradores, como dados de produtividade, registros financeiros e informações pessoais (Chiavenato, 2010). A adequação do setor de RH à LGPD é essencial para mitigar riscos de vazamento de dados e proteger a privacidade dos funcionários. Profissionais de RH têm a responsabilidade de garantir que os dados sob sua gestão sejam tratados de forma segura, evitando que tais informações sejam interceptadas por cibercriminosos e utilizadas para fins maliciosos, como fraude e extorsão (Bioni, 2021).

A criação da LGPD, que regula a relação entre os titulares de dados e os responsáveis pelo tratamento das informações, representa um marco na proteção dos direitos dos indivíduos no Brasil. Além de estabelecer as obrigações e penalidades para casos de violação, a Lei (Brasil, 2018). Como destaca Peck (2020), a LGPD afeta tanto instituições públicas quanto privadas, ao tratar da proteção de dados pessoais em diversas esferas da sociedade.

Diante desse contexto, este estudo foi orientado pela seguinte pergunta de pesquisa: Qual o impacto da Lei Geral de Proteção de Dados na gestão de informações no setor de Recursos Humanos? O estudo focou nas transformações que essa Lei tem imposto às práticas organizacionais, principalmente na proteção de dados dos colaboradores.

### **1.1 Justificativa**

A implementação da Lei Geral de Proteção de Dados em práticas organizacionais, especialmente no setor de Recursos Humanos, é de grande relevância, considerando o crescente volume de dados pessoais coletados e armazenados pelas empresas. Em um cenário marcado por um aumento alarmante de vazamentos de dados, a conformidade com a LGPD torna-se um fator crucial para garantir a privacidade dos colaboradores e evitar riscos legais e reputacionais (Carvalho, 2020).

De acordo com a *Cybersecurity & Infrastructure Security Agency* (CISA), o número de vazamentos de dados aumentou em 300% durante a pandemia, o que reforça a urgência de medidas rigorosas de proteção de dados (CISA, 2021). A LGPD, sancionada em 2018, estabelece diretrizes para o tratamento de dados pessoais, promovendo não apenas a privacidade, mas também uma cultura de responsabilidade nas organizações (Brasil, 2018). Este estudo pode contribuir para a prática dos gestores e profissionais de RH ao oferecer um entendimento detalhado das exigências legais impostas pela LGPD e de como estas impactam diretamente a gestão de pessoas. Além disso, conforme Mendes (2020) aponta, a conformidade com a LGPD pode se tornar um diferencial competitivo para empresas que adotam uma postura proativa em relação à proteção de dados.

Teoricamente, a pesquisa pode ampliar a compreensão sobre a intersecção entre a LGPD e o setor de Recursos Humanos, e pode fornecer *insights* para futuros estudos e debates acadêmicos sobre a proteção de dados no ambiente organizacional.

## 1.2 Objetivos

### 1.2.1 Objetivo geral

Analisar o impacto da Lei Geral de Proteção de Dados na gestão de informações no setor de Recursos Humanos.

### 1.2.2 Objetivos específicos

- a) Identificar as implicações práticas da LGPD.
- b) Descrever os processos de Recursos Humanos que envolvem o manuseio de dados pessoais.
- c) Investigar correspondência entre as exigências legais da LGPD e os processos do setor de RH.

## 1.3 Estrutura do trabalho

Este trabalho está dividido em cinco capítulos, estruturados de forma a facilitar a compreensão sobre os impactos da Lei Geral de Proteção de Dados (LGPD) no setor de Recursos Humanos:

- A. Capítulo 1 – Introdução: Apresenta o contexto do tema, a justificativa da pesquisa, os objetivos gerais e específicos e a relevância do estudo para as áreas de proteção de dados e gestão de pessoas.
- B. Capítulo 2 – Referencial Teórico: Aborda os principais conceitos relacionados à LGPD, dados pessoais, dados sensíveis e suas implicações no setor de Recursos Humanos, além de discutir os processos e desafios associados à gestão de informações no ambiente organizacional.
- C. Capítulo 3 – Método: Descreve os métodos e técnicas utilizados para a realização da pesquisa, incluindo a abordagem, os procedimentos de coleta e análise de dados, e a delimitação do estudo.
- D. Capítulo 4 – Resultados e Análise do Dados: apresenta os impactos e desafios da LGPD nos processos da área de Recursos Humanos.
- E. Capítulo 5 – Conclusão: Oferece uma síntese das principais contribuições do estudo, destacando as conclusões e sugestões para futuras pesquisas e práticas organizacionais relacionadas à proteção de dados no RH.

## 2 REFERENCIAL TEÓRICO

Neste capítulo serão conceituados a Lei Geral de Proteção de Dados, seus reflexos no Direito do Trabalho e os impactos da LGPD no setor de Recursos Humanos.

### 2.1 A Lei Geral de Proteção de Dados

A Lei Geral de Proteção de Dados é um meio de fazer cumprir os direitos pessoais, protegendo-os contra abusos relacionados ao tratamento inadequado de informações sensíveis (Coelho, 2019). A LGPD regula o tratamento de dados a nível nacional, assegurando que as atividades realizadas por empresas e órgãos públicos não comprometam a privacidade e os direitos fundamentais dos indivíduos. Trata-se de uma legislação eficiente, que, embora compacta, aborda de forma clara e prática os principais elementos relacionados à proteção de dados, promovendo maior segurança jurídica no Brasil (Bioni, 2021).

A LGPD (Lei nº 13.709/2018) unificou um conjunto de normas que, anteriormente, estavam dispersas, exigindo interpretações complexas e metódicas do ordenamento jurídico. Esse processo de unificação trouxe maior consistência à proteção de dados no país. Além disso, a LGPD incorpora direitos que estavam presentes em legislações anteriores, como a qualidade dos dados, a transparência e o livre acesso, estabelecendo um padrão legal mais robusto e abrangente (Brasil, 2018). De acordo com Peck (2021), essa unificação é essencial para garantir maior coerência e segurança no tratamento das informações pessoais, sobretudo em um cenário de digitalização acelerada.

Dentre as normas que antecedem a LGPD, destacam-se as seguintes:

A. Constituição Federal Brasileira de 1988, artigo 5º, incisos X e XII (Brasil, 1988):

X - São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação; [...] XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

Esses dispositivos asseguram o direito à privacidade como um dos fundamentos dos direitos fundamentais.

- B. Decreto nº 6.135/2007: Regula o Cadastro Único para Programas Sociais do Governo Federal, estabelecendo que os dados de identificação das famílias são sigilosos e somente podem ser utilizados para fins específicos, como formulação de políticas públicas e estudos (Brasil, 2007).
- C. Lei do Marco Civil da Internet (Lei nº 12.965/2014): Considerada um marco na regulamentação do uso da internet no Brasil, essa lei estabelece direitos e responsabilidades dos usuários e provedores, além de consolidar princípios como a proteção de dados pessoais, a liberdade de expressão e a privacidade no ambiente digital (Brasil, 2014). Segundo Bioni (2021), muitos dos conceitos e diretrizes do Marco Civil serviram de base para a LGPD.

Em síntese, a proteção dos direitos fundamentais do cidadão tende a ser reforçada por normas técnicas e categóricas que proporcionam maior segurança e resguardam os indivíduos contra abusos relacionados à sensibilidade dos dados pessoais. Essa abordagem contribui para fortalecer a privacidade em tempos de rápida evolução digital, criando um equilíbrio entre inovação tecnológica e responsabilidade legal (Doneda, 2021). Esses direitos dos titulares estão fundamentados nos princípios estabelecidos pela LGPD, que orientam todas as práticas de tratamento de dados pessoais no Brasil, garantindo transparência, segurança e respeito à privacidade.

### 2.1.1 Fundamentos da Lei Geral de Proteção de Dados

A Lei Geral de Proteção de Dados, estabelecida pela Lei nº 13.709/2018 e influenciada pelo Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia, veio como uma resposta ao aumento de vazamentos e ao uso inadequado de dados pessoais no Brasil. De acordo com Doneda (2021), a LGPD reflete um esforço significativo para adaptar os direitos fundamentais ao contexto digital, padronizando o tratamento de dados pessoais no território nacional e estabelecendo regras claras para garantir que os dados sejam manipulados com respeito aos direitos de seus titulares e com responsabilidade por parte de controladores e operadores.

Originalmente sancionada para entrar em vigor em agosto de 2020, a implementação da LGPD teve sua aplicação de penalidades adiada para agosto de 2021, devido à pandemia do *Coronavírus Disease 2019 (COVID-19)* (Brasil, 2018). Desde então, tornou-se um marco para a proteção de dados no Brasil, influenciando diretamente empresas e instituições públicas no tratamento das informações pessoais (Bioni, 2021).

A COVID-19 é uma doença infecciosa causada pelo vírus *Severe Acute Respiratory Syndrome Coronavirus 2* detectado inicialmente em Wuhan, na China, em dezembro de 2019. Declarada pandemia pela Organização Mundial da Saúde (OMS) em março de 2020, a COVID-19 causou impactos profundos na saúde pública, nas economias e nas rotinas sociais em todo o mundo. Segundo Peck (2021), a crise acelerou a transformação digital e o uso intensivo de dados pessoais, ampliando a relevância de regulamentações como a LGPD para garantir a privacidade e segurança das informações.

A LGPD se estrutura sobre sete fundamentos, declarados no seu artigo 2º, que norteiam todas as práticas e políticas de tratamento de dados no país (Brasil, 2018):

- a) Respeito à privacidade: Os dados pessoais devem ser tratados de forma a preservar a privacidade dos indivíduos, garantindo que não sejam utilizados sem consentimento ou por finalidade justificada.
- b) Autodeterminação informativa: Este princípio assegura ao titular o controle sobre seus dados, demandando que organizações informem detalhadamente os processos e objetivos do tratamento (Doneda, 2021).
- c) Liberdade de expressão, de informação e opinião: A LGPD respeita os direitos fundamentais de expressão e acesso à informação, equilibrando-os com a proteção da privacidade.
- d) Inviolabilidade da intimidade, da honra e da imagem: Protege dados sensíveis de usos que possam prejudicar os titulares.
- e) Desenvolvimento econômico e inovação: Promove a proteção de dados como parte do avanço tecnológico, incentivando soluções que respeitem os direitos fundamentais (Bioni, 2021).
- f) Livre iniciativa e defesa do consumidor: Assegura transparência no tratamento de dados, conferindo maior segurança aos consumidores e responsabilidade às empresas.

- g) Direitos humanos e cidadania: Fundamenta-se em valores éticos, assegurando que o tratamento de dados respeite a dignidade humana e a cidadania.

Esses princípios orientam o cumprimento e a interpretação da LGPD, definindo limites claros para o uso de dados pessoais e protegendo os direitos dos titulares (Doneda, 2021). Além disso, a Lei incorpora o princípio da minimização de dados, exigindo que apenas informações essenciais sejam coletadas e processadas, bem como a transparência, garantindo que as operações sejam comunicadas de forma clara aos titulares.

A LGPD também introduz um conjunto de direitos do titular de dados, como acesso, retificação, anonimização e eliminação de informações pessoais, além da revogação de consentimento previamente concedido. Esses direitos fortalecem a autonomia dos titulares, promovendo a segurança e privacidade em um cenário digital cada vez mais desafiador (Peck, 2021).

Com base nisso, é importante compreender os princípios da LGPD que regula as operações práticas de tratamento de dados, definindo processos, atores e responsabilidades envolvidas, como será abordado na seção seguinte.

### 2.1.2 Princípios da Lei Geral de Proteção de Dados

Os princípios que fundamentam a Lei Geral de Proteção de Dados representam diretrizes essenciais para que o tratamento de dados pessoais no Brasil ocorra com transparência, segurança e respeito aos direitos dos titulares. Esses princípios, listados no Artigo 6º da LGPD, estabelecem os valores centrais que devem nortear as práticas de processamento de dados em todas as organizações, sejam elas públicas ou privadas. Eles promovem a boa-fé nas operações e garantem que o uso dos dados pessoais seja legítimo, ético e seguro (Doneda, 2021).

A conformidade com esses princípios é essencial para evitar abusos e assegurar que o tratamento de dados ocorra de maneira adequada e proporcional aos objetivos propostos. Cada princípio cumpre uma função específica e serve para guiar os agentes de tratamento nas boas práticas de proteção de dados. Abaixo, são descritos detalhadamente os princípios estabelecidos pela LGPD, no seu artigo 6º (Brasil, 2018):

- a) Finalidade: O tratamento de dados deve ocorrer para propósitos legítimos, específicos, explícitos e informados ao titular. Segundo Sarlet e Schertel Mendes (2021), esse princípio é fundamental para evitar a "função aberta" do uso de dados,

garantindo que sua aplicação seja vinculada às finalidades previamente informadas ao titular.

- b) Adequação: Este princípio assegura que o tratamento de dados seja compatível com as finalidades comunicadas. Doneda (2021) destaca que a adequação é um elemento-chave para alinhar as expectativas dos titulares com as práticas das organizações, promovendo confiança mútua.
- c) Necessidade: Introduz o conceito de "minimização de dados", limitando o tratamento ao mínimo necessário para a finalidade. Conforme Peck (2021), esse princípio não apenas reduz os riscos associados ao uso excessivo de informações, mas também incentiva uma revisão constante das práticas de coleta e armazenamento.
- d) Livre Acesso: Esse princípio garante que o titular possa consultar, gratuitamente, o uso e o armazenamento de seus dados. Como apontam Sarlet e Schertel Mendes (2021), essa medida reforça a transparência e a confiança entre agentes de tratamento e titulares.
- e) Qualidade dos Dados: Assegura que as informações sejam exatas, claras, relevantes e atualizadas. Segundo Bioni (2021), a qualidade dos dados é essencial para evitar decisões baseadas em informações equivocadas, o que poderia prejudicar tanto os titulares quanto as organizações.
- f) Transparência: Determina que os titulares tenham acesso a informações claras e detalhadas sobre o tratamento de seus dados. De acordo com Doneda (2021), a transparência é um dos pilares da autodeterminação informativa, permitindo que os titulares exerçam maior controle sobre suas informações pessoais.
- g) Segurança: Esse princípio exige a implementação de medidas técnicas e administrativas que protejam os dados contra acessos não autorizados e eventos acidentais. Como Peck (2021) ressalta, a segurança deve ser vista como uma responsabilidade contínua, que inclui a adoção de tecnologias avançadas e treinamentos regulares.
- h) Prevenção: Os agentes de tratamento devem adotar precauções para evitar danos ao titular dos dados. Doneda (2021) afirma que a prevenção deve ser proativa, promovendo o planejamento e a mitigação de riscos em todos os níveis organizacionais.

- i) Não Discriminação: Proíbe o uso de dados para práticas discriminatórias, assegurando que o tratamento respeite os direitos fundamentais dos titulares. Esse princípio é destacado por Sarlet e Schertel Mendes (2021) como crucial para preservar a dignidade e a igualdade.
- j) Responsabilização e Prestação de Contas: Impõe que os agentes de tratamento demonstrem a conformidade com a LGPD, adotando práticas verificáveis e efetivas. Segundo Bioni (2021), a responsabilidade é uma das características mais inovadoras da LGPD, pois transforma a proteção de dados em um compromisso ativo e mensurável.

Além disso, o tripé composto pelos princípios de finalidade, adequação e necessidade estabelece um 'núcleo de legitimidade' para o tratamento de dados. Esse tripé funciona como uma referência central que orienta as operações de coleta e uso dos dados, exigindo que cada processo seja justificado por um propósito claro, ajustado ao contexto e limitado ao mínimo necessário. Conforme Bioni (2021, p. 98), esses princípios operam como uma base sólida que "serve para limitar o tratamento a um escopo claramente definido, reduzindo excessos e promovendo um uso mais ético dos dados pessoais." Dessa forma, a LGPD estrutura um sistema de proteção que confere aos titulares maior controle e segurança sobre suas informações pessoais, consolidando um padrão elevado para o tratamento ético de dados no Brasil.

### 2.1.3 O Processamento dos Dados

A operação da Lei Geral de Proteção de Dados (LGPD) visa implementar diretrizes claras para o tratamento de dados pessoais, utilizando o verbo "tratar" para descrever o processamento de dados de forma ampla. O item X do Art. 5º (Brasil, 2018) define tratamento como:

todas as operações realizadas em dados pessoais, tais como relacionadas à coleta, produção, recepção, classificação, uso, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle de informações, modificação, comunicação, transferência, disseminação ou extração.

Essa definição abrange uma série de atividades que buscam garantir que os dados sejam processados de maneira ética e em conformidade com os direitos dos titulares. Além das operações de processamento, a LGPD destaca quatro figuras principais envolvidas no tratamento dos dados:

- a) Titular dos Dados Pessoais: De acordo com o inciso V do Art. 5º, o titular é “a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento”. O titular é o detentor dos dados e tem direitos específicos sobre o uso e o acesso a essas informações. Para Bioni (2021), o titular dos dados é um dos pilares da LGPD, sendo essencial para garantir o controle das informações pessoais. A autora também destaca que ele deve ser informado de maneira clara e objetiva sobre como seus dados são usados.
- A. Controlador: Conforme o inciso VI, o controlador é a “pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais”. O controlador é responsável por determinar a finalidade e os meios do tratamento de dados, sendo a principal autoridade na organização em relação à proteção desses dados. De acordo com Maldonado e Blum (2019), o controlador deve tomar decisões estratégicas sobre como tratar as informações pessoais, sempre respeitando os direitos dos titulares.
- B. Operador: Definido no inciso VII do Art. 5º, o operador é a “pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador”. Este agente executa o tratamento sob as instruções do controlador, sendo responsável também por adotar medidas de segurança para a proteção dos dados. Para Francoski e Tasso (2021), o operador deve seguir as orientações do controlador e estar em conformidade com as exigências legais da LGPD.
- C. Encarregado: O encarregado é a pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). A Lei nº 13.853/2019 ampliou essa função, permitindo que o encarregado fosse uma pessoa jurídica, podendo ser terceirizado. Segundo Pinheiro (2021), o encarregado tem um papel fundamental na implementação da LGPD dentro das organizações, garantindo a transparência e o diálogo entre a empresa e os titulares dos dados.

Além de entender as figuras envolvidas no tratamento, a LGPD também especifica as condições para o término do processamento de dados. A lei determina que o término deve ocorrer quando a finalidade for alcançada ou quando o titular solicitar a eliminação dos dados, exceto nos casos em que a retenção seja permitida por motivos legítimos, como cumprimento de obrigações legais ou execução de contratos. Gomes (2019) destaca que a eliminação de dados pessoais deve ser realizada de forma transparente e respeitando os direitos dos titulares, sendo um dos direitos fundamentais garantidos pela LGPD.

#### 2.1.4. Término do Tratamento de Dados

Por fim, vale ressaltar a importância do término do tratamento destes dados no Art. 15 da LGPD (Brasil, 2018), onde é destacado o término do tratamento de dados pessoais, que ocorrerá nas seguintes hipóteses:

- I - Verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
- II - Fim do período de tratamento;
- III - Comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público;
- IV - Determinação da autoridade nacional, quando houver violação ao disposto nesta.

O Art. 16 da LGPD (Brasil, 2018), determina que os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

- I - Cumprimento de obrigação legal ou regulatória pelo controlador;
- II - Estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- III - Transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
- IV - Uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

O inciso I, conclui que após a finalidade ser alcançada ou não, o controlador deve iniciar o processo de encerramento e o descarte destes dados. Por exemplo, no setor de Recursos Humanos, onde os dados pessoais são utilizados para entrevistas. E, caso o entrevistado não seja contratado, os dados devem ser devidamente descartados pelo controlador. Nesse sentido, é importante analisar os instrumentos utilizados para reforçar as medidas de proteção dos dados pessoais dentro das organizações, direcionando tais medidas para o setor de RH.

## 2.2 Processos de Recursos Humanos

A gestão de Recursos Humanos desempenha um papel essencial nas organizações modernas, alinhando as práticas de gestão de pessoas com as estratégias empresariais para alcançar resultados mais eficazes. Segundo Ivancevich (2008), a importância estratégica do setor de RH é vista em práticas como a análise de problemas, a avaliação de custos e benefícios, e a adoção de modelos de planejamento, que garantem a eficiência da organização em suas funções diárias e na adaptação a novos desafios.

Para garantir que essas práticas de gestão de pessoas sejam eficazes, Chiavenato (2010) define seis processos principais (Figura 1).

Figura 1 - Seis processos da gestão de pessoas



Fonte: Chiavenato (2010, p. 14).

### 2.2.1 Agregação de Pessoas

É um dos primeiros e mais importantes processos na gestão de Recursos Humanos, responsável por atrair e recrutar talentos para a organização. Chiavenato (2010) afirma que a qualidade da organização está diretamente ligada à qualidade das pessoas que a compõem, pois são elas que garantem o bom desempenho das operações e a realização das metas estabelecidas. Este processo envolve etapas essenciais como o recrutamento, a seleção e a coleta de dados relacionados aos candidatos, com o objetivo de escolher aqueles que não apenas atendem aos requisitos técnicos da vaga, mas também se alinham à cultura organizacional da empresa. A seleção de novos colaboradores precisa ser estratégica, visando não apenas preencher uma posição, mas atrair profissionais que tragam consigo competências e características que atendam às necessidades de longo prazo da organização.

Durante a fase de recrutamento, o RH deve utilizar diferentes canais de comunicação, como anúncios de vagas, redes sociais, parcerias com universidades, e programas de estágio, para atrair uma gama diversificada de candidatos. Uma vez atraídos, é necessário realizar uma análise criteriosa durante a seleção, por meio de entrevistas, testes e dinâmicas de grupo, com o intuito de garantir que o perfil do candidato esteja alinhado com o perfil desejado pela organização. Além disso, Chiavenato (2010) enfatiza que a entrevista deve ser um espaço para compreender não só as habilidades técnicas do candidato, mas também suas motivações, valores e expectativas em relação ao ambiente de trabalho e à cultura da empresa.

No entanto, um aspecto crucial que deve ser observado durante este processo é a gestão dos dados pessoais dos candidatos. A Lei Geral de Proteção de Dados (LGPD) impõe que as organizações tratem essas informações de maneira ética e transparente, garantindo que o consentimento para a coleta de dados seja obtido de forma clara e informada. A coleta de dados pessoais, como currículos, históricos profissionais, informações de contato e outros dados sensíveis, deve ser feita com o devido cuidado para não violar a privacidade dos candidatos. Além disso, Chiavenato (2010) alerta que a gestão desses dados deve seguir rigorosamente os princípios da LGPD, incluindo o armazenamento adequado e o tempo limitado de retenção das informações, que deve ser exclusivo para o processo seletivo. Após a conclusão do processo de recrutamento e seleção, é imprescindível que os dados dos candidatos que não foram contratados sejam eliminados ou anonimizados, de acordo com a legislação.

A proteção dos dados no processo de agregação de pessoas não se limita à questão do armazenamento seguro, mas também envolve o uso responsável dessas informações. A organização deve ser transparente quanto ao uso dos dados, informando aos candidatos como suas informações serão tratadas e por quanto tempo serão mantidas em posse da empresa. Caso a empresa decida utilizar os dados para futuras vagas, o candidato deve ser informado sobre isso e seu consentimento deve ser renovado. Além disso, é importante que os dados dos candidatos não sejam compartilhados com terceiros sem a autorização expressa deles, o que reforça a responsabilidade do RH na gestão dessas informações de maneira ética e segura.

A aplicação rigorosa dos princípios da LGPD no processo de agregação de pessoas é fundamental para garantir que a organização atue de maneira ética e responsável, preservando a confiança dos candidatos e evitando possíveis sanções legais. Chiavenato (2010) salienta que, para além da eficiência e da eficácia do processo seletivo, as práticas de recrutamento e seleção devem ser realizadas de forma a preservar a privacidade dos indivíduos e a assegurar a transparência no tratamento dos dados pessoais. Portanto, o processo de agregação de pessoas não envolve apenas a escolha de candidatos qualificados para a organização, mas também a

responsabilidade de garantir que as informações coletadas sejam tratadas com o máximo respeito, conforme os preceitos legais estabelecidos pela LGPD.

### 2.2.2 Aplicação de Pessoas

Este processo está intimamente relacionado à definição de papéis, responsabilidades e à avaliação de desempenho dos colaboradores dentro da organização. Segundo Chiavenato (2010), esse processo visa garantir que cada indivíduo esteja no cargo mais adequado às suas habilidades e potencial, além de assegurar que as funções e responsabilidades estejam bem delineadas, promovendo um desempenho eficaz e alinhado às metas organizacionais. A aplicação das pessoas, portanto, não se limita à simples alocação de tarefas, mas envolve um profundo entendimento sobre as competências e as necessidades da equipe e da organização como um todo. Chiavenato (2010) argumenta que a clareza nas atribuições de cargos é fundamental para evitar ambiguidades e conflitos, além de ser essencial para a maximização do potencial dos colaboradores.

Nesse contexto, o RH desempenha um papel crucial ao definir as descrições e especificações dos cargos. A descrição de cargos deve detalhar claramente as responsabilidades, os requisitos e as expectativas para cada função, proporcionando um entendimento preciso tanto para os gestores quanto para os colaboradores. Isso ajuda a evitar sobrecarga de trabalho e a garantir que as competências de cada membro da equipe sejam adequadamente aproveitadas. Além disso, Chiavenato (2010) aponta que, ao alocar as pessoas de forma estratégica, é possível otimizar o funcionamento da organização, promovendo um ambiente de trabalho mais produtivo e harmonioso.

Outro aspecto central na "Aplicação de Pessoas" é a avaliação de desempenho. O RH deve estabelecer critérios claros e justos para a avaliação do desempenho dos colaboradores, de modo a garantir que os objetivos da organização sejam alcançados e que os colaboradores recebam feedbacks construtivos e oportunos. A avaliação de desempenho é um processo contínuo e essencial para o desenvolvimento da equipe, pois permite que o RH identifique as forças e as áreas de melhoria de cada colaborador, ajustando suas responsabilidades e ações de acordo com essas observações. Chiavenato (2010) destaca que, para ser eficaz, a avaliação de desempenho deve ser baseada em objetivos claros, metas específicas e indicadores de desempenho que sejam mensuráveis e justos, possibilitando o crescimento contínuo do indivíduo e da organização.

No entanto, a aplicação desse processo também envolve uma gestão cuidadosa dos dados relacionados ao desempenho e às atribuições dos colaboradores. Cada avaliação de desempenho gera um grande volume de informações pessoais e sensíveis, que precisam ser tratadas com responsabilidade, especialmente no contexto da LGPD. A conformidade com a Lei Geral de Proteção de Dados é essencial para garantir a segurança e a privacidade das informações, tanto durante o processo de avaliação quanto no armazenamento e uso dessas informações no futuro. De acordo com a LGPD, as organizações devem garantir que os dados dos colaboradores sejam coletados, armazenados e processados de maneira ética e transparente, com o consentimento explícito dos indivíduos e por um tempo limitado, exclusivamente para as finalidades determinadas. Além disso, Chiavenato (2010) reforça que a privacidade e a transparência devem ser princípios norteadores em todos os processos de gestão de pessoas, incluindo a aplicação das pessoas nos cargos e a avaliação de seu desempenho.

A avaliação de desempenho, ao gerar informações sobre a produtividade e os resultados dos colaboradores, também envolve dados sensíveis, como feedbacks sobre o comportamento e a interação com os colegas. Esses dados devem ser tratados com cuidado para evitar discriminação ou uso indevido das informações. A organização precisa garantir que esses dados não sejam utilizados de forma a prejudicar os colaboradores, mas sim como uma ferramenta para seu desenvolvimento profissional. Além disso, é necessário que a utilização dessas informações seja feita de maneira transparente, com a devida comunicação aos colaboradores sobre como seus dados serão utilizados e protegidos.

Portanto, o processo de aplicação de pessoas, além de envolver a definição de papéis e a avaliação de desempenho, exige um gerenciamento cuidadoso dos dados pessoais e sensíveis dos colaboradores. A conformidade com a LGPD é fundamental para garantir que as informações sejam tratadas com ética, transparência e segurança, assegurando que os direitos dos colaboradores sejam respeitados ao longo de todo o ciclo de vida profissional dentro da organização. Chiavenato (2010) reforça que, para que a aplicação de pessoas seja eficaz, deve-se criar um ambiente de confiança, onde os colaboradores se sintam seguros em relação à forma como seus dados são tratados e como suas avaliações impactam seu desenvolvimento na organização.

### 2.2.3 Recompensar Pessoas

Refere-se à administração das compensações financeiras e benefícios oferecidos aos colaboradores, um dos pilares da gestão de Recursos Humanos. Chiavenato (2010) destaca que a recompensa é uma das principais formas de motivar os funcionários, influenciando diretamente no seu engajamento, satisfação e desempenho dentro da organização. A gestão de recompensas abrange não apenas o salário, mas também bônus, benefícios, reconhecimento e outros incentivos que contribuem para a valorização do trabalho do colaborador. Para Chiavenato (2010), a recompensa deve ser vista como uma ferramenta estratégica para atrair, reter e motivar talentos, alinhando as expectativas dos colaboradores com os objetivos organizacionais.

O processo de recompensa é complexo e envolve uma série de decisões, como a definição de políticas salariais, o ajuste de benefícios e a criação de programas de reconhecimento. A definição do salário e dos bônus deve ser feita com base em critérios objetivos e transparentes, levando em consideração a competitividade do mercado de trabalho e a performance dos colaboradores. Chiavenato (2010) argumenta que as recompensas devem ser justas e equitativas, considerando o desempenho individual e coletivo, além de serem competitivas em relação aos padrões do mercado. Quando bem estruturado, o sistema de recompensas pode impulsionar a produtividade, pois os colaboradores tendem a se sentir mais motivados quando sabem que seu esforço será reconhecido e recompensado de maneira justa.

Além disso, Chiavenato (2010) destaca que a gestão de recompensas deve ser abrangente, incluindo tanto recompensas financeiras, como salários e bônus, quanto recompensas não financeiras, como reconhecimento público, oportunidades de desenvolvimento e benefícios como planos de saúde, vale-alimentação, entre outros. As recompensas não financeiras são especialmente importantes, pois contribuem para a satisfação e o bem-estar dos colaboradores, criando um ambiente de trabalho mais positivo e saudável. Programas de reconhecimento, como premiações de funcionário do mês ou elogios em reuniões, ajudam a fortalecer a cultura organizacional e reforçam comportamentos desejáveis, como a colaboração e a inovação.

Entretanto, o processo de recompensar pessoas também envolve a gestão cuidadosa de dados financeiros e pessoais, que são coletados e processados no momento de definição e pagamento das recompensas. A proteção dessas informações é de extrema importância, não apenas pela necessidade de atender aos requisitos legais, mas também para preservar a privacidade dos colaboradores. A Lei Geral de Proteção de Dados (LGPD) exige que as

organizações tratem com segurança e responsabilidade os dados pessoais e financeiros de seus funcionários, garantindo que as informações sejam utilizadas exclusivamente para as finalidades para as quais foram coletadas e de acordo com o consentimento dos colaboradores.

A gestão de dados financeiros e pessoais relacionados às recompensas deve ser feita com transparência e segurança, assegurando que as informações não sejam compartilhadas de forma inadequada e que os colaboradores estejam cientes de como seus dados estão sendo utilizados. A empresa deve ter políticas claras para o tratamento desses dados, incluindo o armazenamento seguro e a eliminação das informações após o término do ciclo de uso. Além disso, é fundamental que as organizações forneçam informações detalhadas e claras sobre as recompensas oferecidas, para que os colaboradores compreendam os critérios que influenciam a determinação de salários e bônus, aumentando a transparência e a confiança no processo.

Em suma, a recompensa das pessoas é um componente crítico da gestão de Recursos Humanos, pois impacta diretamente na motivação e no engajamento dos colaboradores. A criação de um sistema de recompensas bem estruturado e transparente contribui para o sucesso da organização, atraiendo e retendo talentos, além de estimular um ambiente de trabalho positivo. No entanto, é essencial que a gestão das recompensas seja acompanhada de uma gestão ética e segura dos dados pessoais e financeiros dos colaboradores, em conformidade com a LGPD, para garantir a proteção da privacidade e a confiança no processo de recompensa.

#### 2.2.4 Desenvolvimento de Pessoas

É fundamental para garantir que os colaboradores da organização se mantenham atualizados, capacitados e preparados para lidar com as mudanças e desafios do ambiente de trabalho. Chiavenato (2010) destaca que o desenvolvimento das pessoas deve ser visto como um investimento contínuo, pois as competências dos colaboradores têm um impacto direto no desempenho organizacional. Esse processo envolve atividades de treinamento, educação e aprimoramento profissional, com o objetivo de melhorar as habilidades e conhecimentos dos funcionários, alinhando-os às necessidades estratégicas da organização. Para Chiavenato (2010), um programa de desenvolvimento bem-estruturado contribui para o crescimento tanto individual quanto coletivo, criando uma cultura organizacional focada no aprendizado contínuo.

O desenvolvimento de pessoas engloba diferentes tipos de programas, desde treinamentos técnicos e específicos até programas de liderança e gestão. Esses programas podem ser realizados internamente, com recursos próprios da organização, ou externamente, por meio de parcerias com instituições de ensino, empresas especializadas ou consultorias. O RH desempenha um papel central na identificação das necessidades de desenvolvimento, realizando diagnósticos sobre as lacunas de habilidades e conhecimentos dos colaboradores e da organização como um todo. Chiavenato (2010) argumenta que é essencial que o desenvolvimento das pessoas esteja alinhado com as estratégias da organização, para que os colaboradores adquiram as competências necessárias para enfrentar os desafios futuros e contribuir para o sucesso da empresa.

Ulrich (2018) defende que as organizações devem investir continuamente na capacitação de seus colaboradores, visando não apenas o aprimoramento individual, mas também o fortalecimento da cultura organizacional. A criação de programas contínuos de desenvolvimento, como workshops e mentorias, contribui para a atualização constante dos colaboradores em relação às novas demandas do mercado e às tendências da sua área de atuação.

Chiavenato (2010) destaca a importância de programas contínuos de desenvolvimento, como *workshops*, cursos de especialização, mentorias e *coaching*. Esses programas não apenas aprimoram as competências técnicas dos colaboradores, mas também contribuem para o desenvolvimento de habilidades interpessoais, como comunicação, liderança, trabalho em equipe e gestão de conflitos. O desenvolvimento de habilidades interpessoais é especialmente importante, pois, no ambiente corporativo, os resultados não dependem apenas das habilidades técnicas, mas também da capacidade de trabalhar em grupo e de se relacionar com diferentes pessoas e situações. A promoção de um ambiente que valorize o desenvolvimento das competências interpessoais fortalece a cultura organizacional e a colaboração entre as equipes.

No entanto, o processo de desenvolvimento de pessoas também exige a gestão cuidadosa de dados sensíveis dos colaboradores. Informações sobre o histórico educacional, treinamentos realizados, avaliações de desempenho e feedbacks devem ser coletadas e armazenadas de maneira ética e transparente, respeitando a privacidade e a segurança das informações. A conformidade com a Lei Geral de Proteção de Dados (LGPD) é essencial para garantir que as informações dos colaboradores sejam tratadas de forma adequada, com o consentimento expresso dos indivíduos. Os dados relacionados ao desenvolvimento devem ser usados exclusivamente para a finalidade de planejamento e execução de programas de capacitação, sendo armazenados apenas pelo tempo necessário para esses fins.

A LGPD também estabelece que os dados pessoais sensíveis, como informações sobre saúde ou origem racial, que podem ser coletados em programas de desenvolvimento, devem ser tratados com cuidado redobrado. A organização deve garantir que esses dados sejam armazenados de maneira segura e que sejam utilizados de forma ética, com a devida transparência sobre como esses dados serão utilizados e por quanto tempo serão mantidos. Os colaboradores devem ser informados sobre a coleta e o uso de seus dados, além de poderem exercer seus direitos, como a revogação do consentimento ou o pedido de exclusão das informações.

Portanto, o desenvolvimento de pessoas não é apenas uma prática que visa melhorar as competências dos colaboradores, mas também um processo que deve ser conduzido com responsabilidade no que diz respeito ao tratamento e à proteção de dados. A implementação de programas de desenvolvimento bem estruturados e a gestão cuidadosa dos dados pessoais são essenciais para criar um ambiente de aprendizagem eficaz e ético, alinhado com as necessidades organizacionais e com os direitos dos colaboradores. Chiavenato (2010) reforça que o desenvolvimento das pessoas deve ser um processo contínuo, que acompanhe as transformações do mercado e as mudanças nas necessidades da organização, garantindo que os colaboradores permaneçam preparados e motivados para contribuir para o sucesso a longo prazo.

## 2.2.5 Manutenção de Pessoas

Tem como objetivo garantir o bem-estar, a saúde e a segurança dos colaboradores dentro da organização, além de promover um ambiente de trabalho saudável e motivador. Segundo Chiavenato (2010), a manutenção das pessoas envolve ações que visam não apenas a prevenção de problemas, mas também a promoção de condições que favoreçam o equilíbrio entre vida pessoal e profissional, garantindo a satisfação dos colaboradores e a redução de riscos ocupacionais. O RH desempenha um papel essencial na criação de políticas e práticas que atendam às necessidades físicas, psicológicas e sociais dos trabalhadores, contribuindo para um ambiente organizacional mais saudável e produtivo.

A manutenção de pessoas envolve uma série de ações voltadas para a preservação da saúde física e mental dos colaboradores. A organização deve adotar práticas de prevenção, como a promoção de programas de saúde ocupacional, a oferta de exames periódicos, a implementação de medidas para evitar acidentes de trabalho, além de ações que promovam o bem-estar emocional, como a criação de ambientes que favoreçam o equilíbrio entre as

demandas profissionais e pessoais. Chiavenato (2010) argumenta que a prevenção de problemas de saúde e a promoção do bem-estar não só reduzem custos relacionados a afastamentos e licenças, mas também contribuem para um clima organizacional mais positivo, onde os colaboradores se sentem valorizados e cuidados.

Além disso, a manutenção de pessoas também envolve o cuidado com o ambiente de trabalho, que deve ser adequado às necessidades dos colaboradores. Chiavenato (2010) ressalta que um ambiente de trabalho saudável e seguro é fundamental para que os colaboradores possam desempenhar suas funções com eficácia. Isso inclui a adequação das condições físicas do local de trabalho, como a qualidade do ar, a iluminação e a ergonomia dos equipamentos. A segurança no ambiente de trabalho deve ser garantida por meio da implementação de normas e procedimentos de segurança, treinamento para prevenção de acidentes e o fornecimento de equipamentos de proteção individual (EPIs), quando necessário.

A gestão do bem-estar emocional também é um aspecto central da manutenção de pessoas. O RH deve estar atento às necessidades psicológicas dos colaboradores, promovendo ações que favoreçam a saúde mental, como programas de apoio psicológico, gestão do estresse e práticas de *mindfulness*. Chiavenato (2010) enfatiza que o cuidado com o lado emocional dos colaboradores é essencial, pois questões como o estresse e a ansiedade podem afetar diretamente a produtividade e o ambiente de trabalho. Programas de apoio psicológico, como terapia ocupacional ou apoio a funcionários que enfrentam questões pessoais e profissionais, ajudam a manter a saúde mental dos colaboradores e, consequentemente, o bom funcionamento da organização.

Outro aspecto importante da manutenção de pessoas está relacionado ao tratamento de dados sensíveis, especialmente aqueles vinculados à saúde e ao bem-estar dos colaboradores. A Lei Geral de Proteção de Dados (LGPD) estabelece que os dados relacionados à saúde dos colaboradores devem ser tratados com o máximo de cuidado e sigilo. Informações sobre doenças, histórico médico ou condições psicológicas precisam ser gerenciadas de maneira ética e responsável, garantindo que o acesso a esses dados seja restrito e que sua utilização esteja de acordo com as finalidades legais e com o consentimento do colaborador. A LGPD também exige que os dados relacionados à saúde e segurança no trabalho sejam armazenados de maneira segura e mantidos por tempo limitado, conforme a necessidade de cumprimento das obrigações legais.

A conformidade com a LGPD é crucial para garantir a transparência e a segurança no tratamento dessas informações. Os colaboradores devem ser informados sobre a coleta e uso dos seus dados, bem como ter a opção de revogar o consentimento, quando necessário. A organização deve adotar políticas claras e rigorosas para o gerenciamento de dados sensíveis, assegurando que essas informações sejam tratadas de maneira ética, transparente e em conformidade com a legislação vigente.

Em resumo, a manutenção de pessoas vai além da simples gestão de saúde e segurança no trabalho. Trata-se de um processo abrangente que envolve a criação de um ambiente de trabalho seguro, saudável e motivador, onde os colaboradores se sintam valorizados e cuidados. A gestão do bem-estar físico e emocional, aliada ao cumprimento das exigências da LGPD, é essencial para garantir a sustentabilidade do ambiente organizacional e o sucesso a longo prazo da empresa. Chiavenato (2010) reforça que as organizações que investem na manutenção das pessoas tendem a observar benefícios não apenas na redução de custos com saúde, mas também no aumento da produtividade e na retenção de talentos, criando uma cultura organizacional de confiança e respeito.

## 2.2.6 Monitoramento de Pessoas

O processo de monitoramento está vinculado à prática de acompanhar o desempenho e as atividades dos colaboradores dentro da organização, com o objetivo de garantir que as metas e os resultados esperados sejam atingidos. Chiavenato (2010) destaca que o monitoramento é uma ferramenta essencial para a gestão de Recursos Humanos, pois permite a identificação de áreas de melhoria, o ajuste de estratégias e o fornecimento de feedbacks construtivos aos colaboradores. A avaliação contínua do desempenho dos funcionários é crucial para o desenvolvimento organizacional e para a implementação de ações corretivas quando necessário, contribuindo para a manutenção de altos níveis de produtividade e eficiência.

O monitoramento de pessoas envolve a coleta e análise de dados sobre o comportamento e o desempenho dos colaboradores, por meio de diversos instrumentos de avaliação, como feedbacks, indicadores de performance, avaliações de 360 graus, pesquisas de clima organizacional e outras ferramentas. Chiavenato (2010) afirma que a utilização de sistemas de monitoramento é uma maneira eficaz de obter informações precisas sobre a atuação dos colaboradores, possibilitando uma análise detalhada de sua produtividade e do cumprimento de metas. A partir desses dados, a organização pode identificar pontos fortes e áreas de desenvolvimento de cada colaborador, implementando estratégias de melhoria e

proporcionando o suporte necessário para o seu crescimento.

No entanto, o monitoramento de pessoas deve ser realizado de maneira ética e transparente, respeitando a privacidade dos colaboradores e assegurando que os dados coletados sejam usados para fins legítimos e específicos. A Lei Geral de Proteção de Dados (LGPD) estabelece que as informações pessoais e profissionais dos colaboradores devem ser tratadas com segurança, sendo necessárias medidas adequadas para proteger esses dados contra vazamentos, acessos não autorizados e usos indevidos. É fundamental que os colaboradores sejam informados sobre os tipos de dados que estão sendo coletados, a finalidade do monitoramento e o tempo pelo qual as informações serão armazenadas (Brasil, 2018).

Chiavenato (2010) também enfatiza que o monitoramento não deve ser confundido com vigilância excessiva ou invasão da privacidade dos colaboradores. O objetivo do monitoramento é fornecer dados que possam ser usados para melhorar o desempenho, identificar necessidades de treinamento e reconhecer os esforços dos colaboradores, e não para controlar de forma rígida e excessiva. A utilização de tecnologias de monitoramento, como softwares de rastreamento de atividades ou sistemas de gestão de desempenho, deve ser feita com respeito à dignidade do colaborador, garantindo que essas ferramentas sejam usadas de maneira justa e equilibrada.

Além disso, o monitoramento de pessoas também envolve a análise dos resultados e a interpretação dos dados coletados. Chiavenato (2010) ressalta que, para que o monitoramento seja eficaz, os resultados obtidos devem ser utilizados de maneira construtiva. A organização deve fornecer feedbacks claros e objetivos, destacando as áreas que precisam de melhorias e oferecendo sugestões para o desenvolvimento do colaborador. O feedback é uma ferramenta essencial para o crescimento e a motivação dos funcionários, pois permite que eles compreendam suas fortalezas e as oportunidades de aprimoramento.

O uso de dados de monitoramento também pode ser aliado ao planejamento de sucessão e à gestão de talentos dentro da organização. Ao acompanhar o desempenho dos colaboradores, o RH pode identificar aqueles com maior potencial para assumir cargos de liderança ou outras posições estratégicas na organização, ajudando no processo de desenvolvimento e retenção de talentos. Além disso, a coleta de dados sobre a performance dos colaboradores pode ser uma fonte importante para a definição de estratégias de reconhecimento, promoção e recompensa, garantindo que os esforços dos funcionários sejam devidamente valorizados.

Em síntese, o monitoramento de pessoas é um processo fundamental para a gestão de recursos humanos, permitindo a coleta de dados valiosos sobre o desempenho e o

comportamento dos colaboradores. No entanto, é essencial que esse processo seja conduzido de forma ética, transparente e em conformidade com a LGPD, respeitando a privacidade dos colaboradores e garantindo que as informações sejam usadas para melhorar o desempenho e o bem-estar organizacional. Chiavenato (2010) enfatiza que, quando realizado corretamente, o monitoramento de pessoas pode ser uma ferramenta poderosa para o desenvolvimento individual e organizacional, contribuindo para a criação de um ambiente de trabalho mais produtivo, colaborativo e motivador.

No contexto atual, em que a transformação digital é cada vez mais presente, a gestão de dados pessoais se tornou um aspecto crucial no setor de RH. As organizações não apenas precisam recrutar e treinar talentos, mas também devem lidar com grandes volumes de dados dos colaboradores, que são fundamentais para diversas funções de gestão. Lima (2017) destaca que o conhecimento profundo sobre o colaborador, assim como sobre os dados que são gerenciados, é crucial para que o RH desenvolva uma estratégia bem-sucedida de gestão de pessoas.

A gestão dos dados pessoais e sensíveis é, portanto, um componente crítico dentro de cada um desses processos de RH. A conformidade com a LGPD não se limita à simples coleta e armazenamento de informações; ela também envolve a proteção e o uso ético dos dados dos colaboradores ao longo de todo o ciclo de vida do empregado dentro da organização. Esse cuidado e a transparência no tratamento dos dados são fundamentais para a construção de um ambiente organizacional ético e seguro.

## 2.2.7 Setor de Recursos Humanos

O setor de Recursos Humanos (RH) tem se consolidado ao longo do tempo como uma área fundamental dentro das organizações, transcendendo sua função administrativa para se tornar um parceiro estratégico. Tradicionalmente, o RH era visto apenas como um setor de apoio, com funções limitadas à contratação, gestão de folha de pagamento e cuidados com a legislação trabalhista. Contudo, com o avanço das práticas empresariais e a crescente valorização do capital humano, o papel do RH foi se transformando, sendo reconhecido como essencial para o sucesso das organizações (Chiavenato, 2014).

A gestão de pessoas passou a ser vista como um dos maiores ativos estratégicos das empresas, pois são as pessoas que criam, inovam e possibilitam a implementação de estratégias organizacionais. Nesse sentido, o RH é responsável por alinhar os objetivos da organização com o desenvolvimento das pessoas, assegurando que a estrutura humana da empresa esteja em

sintonia com suas metas e desafios. Como Dessler (2020) enfatiza, um setor de RH bem estruturado deve garantir que a organização tenha as pessoas certas, nos lugares certos, e com as competências adequadas para atingir os objetivos estratégicos da empresa.

O RH desempenha diversas funções essenciais para o bom funcionamento da organização. Um exemplo crucial é o recrutamento e seleção, processo inicial que permite à empresa identificar e atrair profissionais com as competências necessárias para seu crescimento. Como Dessler (2020) destaca, um processo de seleção bem feito não só melhora a qualidade da contratação, mas também alinha os colaboradores à cultura organizacional, promovendo o desempenho eficiente e o fortalecimento do time.

Outro aspecto relevante do RH é a gestão de benefícios e remuneração, que abrange não apenas as políticas salariais, mas também benefícios como planos de saúde, previdência privada, bônus e outros incentivos. Sarlet e Schertel Mendes (2021) argumentam que a oferta de benefícios competitivos é fundamental para atrair e reter talentos, proporcionando bem-estar e motivação para os colaboradores.

O RH também assume um papel significativo na gestão de dados sensíveis e confidenciais dos colaboradores. Essas informações, que incluem dados sobre saúde, desempenho, salários e histórico educacional, são frequentemente armazenadas em plataformas digitais para otimizar os processos e garantir a eficiência da gestão de pessoas. No entanto, a digitalização e o uso crescente de dados impõem uma responsabilidade enorme ao RH, que deve proteger essas informações contra vazamentos e acessos não autorizados. Peck (2021) destaca que o RH deve garantir que o tratamento desses dados esteja em conformidade com a Lei Geral de Proteção de Dados (LGPD), assegurando a coleta, o armazenamento e o uso adequado das informações de forma ética e legal.

Além de cumprir com as exigências legais, o RH precisa adotar práticas de governança de dados, como sublinha Chiavenato (2014), garantindo a transparência das operações e esclarecendo para os colaboradores como suas informações estão sendo utilizadas. Isso fortalece a confiança interna, pois a organização demonstra seu compromisso com a segurança e a privacidade. Dessler (2020) também acrescenta que, com a implementação de tecnologias no setor de RH, a segurança da informação deve ser tratada com prioridade, utilizando ferramentas adequadas de proteção e garantindo que os profissionais da área estejam capacitados para lidar com os desafios legais e tecnológicos.

Os princípios éticos são a base das práticas de RH. O princípio da justiça e igualdade visa assegurar que todos os colaboradores sejam tratados de forma justa, sem discriminação de qualquer tipo, seja por gênero, raça ou qualquer outra característica. Segundo Doneda (2021),

garantir a equidade no tratamento dos colaboradores é fundamental para a criação de um ambiente de confiança e respeito.

A transparência também desempenha papel essencial no RH. Esse princípio assegura que todos os processos, como recrutamento, seleção, avaliação de desempenho e políticas de remuneração, sejam conduzidos de maneira clara, permitindo que os colaboradores compreendam as decisões da empresa e como elas impactam seu trabalho e desenvolvimento dentro da organização. A transparência é um dos pilares para a construção de um ambiente organizacional ético e saudável.

Historicamente, o setor de RH era considerado um departamento de apoio, responsável principalmente por funções operacionais, como contratação e folha de pagamento. No entanto, com o tempo, o papel do RH evoluiu para uma função estratégica. Hoje, o RH influencia diretamente a cultura organizacional, o desenvolvimento de competências e a melhoria da performance organizacional (Ulrich, 2018).

De acordo com Ulrich (2018), o RH deve ser visto não apenas como um "gestor de pessoas", mas como um "gestor de desempenho". Isso significa que, além de administrar os recursos humanos, o RH tem um papel central na formulação e execução das estratégias organizacionais, garantindo que o capital humano esteja alinhado aos objetivos de longo prazo da empresa.

Essa transformação é ainda mais evidente em tempos de transformação digital e globalização. O RH precisa não apenas atrair e reter talentos, mas também desenvolver competências específicas para enfrentar os desafios tecnológicos e a inovação constante. Como apontado por Sarlet e Schertel Mendes (2021), a digitalização trouxe novas exigências para o setor de RH, tornando-o cada vez mais responsável por garantir que a organização esteja preparada para o futuro, com uma força de trabalho qualificada e adaptável.

Nesse contexto, o setor de RH também precisa fortalecer as medidas de proteção dos dados pessoais dos colaboradores, assegurando que a conformidade com a LGPD seja cumprida em todas as suas operações. Nesse sentido, é importante analisar os instrumentos utilizados para reforçar as medidas de proteção dos dados pessoais dentro das organizações, direcionando tais medidas para o setor de RH.

## 2.2.8 Dados Pessoais e Dados Sensíveis

A Lei Geral de Proteção de Dados (LGPD), que entrou em vigor em 2020, estabelece regras rigorosas sobre o tratamento de dados pessoais e dados pessoais sensíveis, ambos essenciais para a atuação do setor de Recursos Humanos (RH). A compreensão da distinção entre esses tipos de dados é fundamental para a gestão ética e legal das informações dentro das organizações.

O Artigo 5º da LGPD define dados pessoais como qualquer informação relacionada a uma pessoa natural identificada ou identificável, como nome, endereço, idade, CPF, e até mesmo dados financeiros, como a carteira de bitcoin (Brasil, 2018). Esses dados são frequentemente utilizados pelo setor de RH para uma série de processos operacionais e estratégicos, incluindo recrutamento, gestão de desempenho e monitoramento de benefícios.

Por outro lado, os dados pessoais sensíveis incluem informações que, devido à sua natureza, podem levar a discriminação, estigmatização ou impactos negativos significativos na privacidade do indivíduo. Esses dados envolvem categorias como: origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas, dados sobre saúde, biometria e vida sexual (Brasil, 2018). O tratamento de dados sensíveis exige cuidados ainda mais rigorosos, sendo necessário o consentimento explícito do titular, especialmente quando esses dados são usados para finalidades que envolvem a vulnerabilidade do indivíduo.

A coleta e o uso desses dados devem ser feitos com base em princípios da LGPD, que incluem a finalidade específica e a necessidade, ou seja, os dados devem ser coletados apenas para fins legítimos e de forma proporcional às necessidades da organização (Peck, 2021). Além disso, o setor de RH deve garantir que as informações sensíveis sejam tratadas de maneira segura, utilizando tecnologias de proteção de dados, como criptografia e controle de acessos (Dessler, 2020).

Em casos específicos, como o tratamento de dados de menores de idade, a LGPD exige o consentimento explícito dos pais ou responsáveis legais. Importante destacar que, em situações emergenciais ou relacionadas à proteção de crianças e adolescentes, é permitido coletar apenas os dados estritamente necessários, sem o compartilhamento com terceiros (Brasil, 2018).

No setor de RH, o manuseio de dados pessoais e sensíveis acontece em diversas situações, como no desenvolvimento de planos de carreira, na gestão estratégica de talentos, e no monitoramento do clima organizacional. O uso desses dados deve ser pautado pela

transparência, comunicação clara com os colaboradores sobre o uso de suas informações e um processo contínuo de auditoria para assegurar que as práticas de proteção estejam sendo seguidas (Sarlet; Schertel Mendes, 2021).

A relação entre dados pessoais e as práticas de RH não se limita à simples coleta e armazenamento. A segurança desses dados deve ser uma prioridade constante, com a implementação de processos claros de governança de dados, que protejam as informações sensíveis contra acesso não autorizado, vazamentos ou uso indevido (Chiavenato, 2010). Dessa forma, a próxima etapa é compreender como a LGPD impacta especificamente as operações cotidianas de RH, como o controle de consentimento dos dados dos colaboradores e a necessidade de implementação de medidas de proteção de dados.

## 2.2.9 Penalidades e Multas Administrativas

O Artigo 52, da Lei Geral de Proteção de Dados (Brasil, 2018), prevê penalidade e multas administrativa para o descumprimento do disposto na Lei:

- I - Advertência, com indicação de prazo para adoção de medidas corretivas;
- II - Multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração;
- III - Multa diária, observado o limite total a que se refere o inciso II;
- IV - Publicização da infração após devidamente apurada e confirmada a sua ocorrência;
- V - Bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
- VI - Eliminação dos dados pessoais a que se refere a infração;
- X - Suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
- XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
- XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Conforme explicado acima, podem ser aplicadas penalidades e multas muito pesadas, que têm impacto significativo sobre o governo, como multa de até R\$50.000.000,00 (cinquenta milhões de reais). Contudo, o impacto financeiro não é única sanção. Segundo Peck (2021), o maior dano causado por essas penalidades pode ser à reputação da empresa. A publicização da infração compromete a credibilidade da organização no mercado e a confiança de seus colaboradores, parceiros e clientes.

Francoski e Tasso (2021) ressaltam que a conformidade com a LGPD não é apenas uma questão legal, mas também estratégica. Empresas que investem em boas práticas de governança

de dados, com a implementação de ferramentas de segurança e políticas claras de proteção de informações, conseguem mitigar os riscos de infrações e, consequentemente, evitar penalidades severas.

### **3. MÉTODO**

Este estudo foi desenvolvido com o objetivo de compreender os impactos da Lei Geral de Proteção de Dados no setor de Recursos Humanos, seguindo uma abordagem metodológica fundamentada em conceitos teóricos e práticos. A seguir, são apresentados os detalhes do percurso metodológico.

#### **3.1 Natureza da Pesquisa**

A pesquisa realizada se caracteriza como aplicada, uma vez que tem como objetivo principal contribuir com soluções práticas para os desafios enfrentados pelos gestores de Recursos Humanos no contexto da Lei Geral de Proteção de Dados (LGPD). Diferentemente da pesquisa básica, que busca expandir o conhecimento teórico sem foco imediato em aplicações práticas, a pesquisa aplicada visa oferecer orientações e ferramentas que possam ser utilizadas diretamente no ambiente organizacional.

Conforme Barros e Lehfeld (2014), a pesquisa aplicada busca não apenas ampliar o conhecimento, mas também propor soluções para problemas reais, visando à implementação de ações concretas. No presente estudo, a investigação explora as implicações práticas da LGPD no setor de RH, com o intuito de orientar as organizações na adequação à legislação e na adoção de medidas efetivas de proteção de dados. Nesse sentido, o estudo não apenas contribui para o debate acadêmico, mas também para a melhoria das práticas organizacionais no âmbito da LGPD, fortalecendo a governança corporativa e promovendo um ambiente de trabalho mais seguro e transparente.

#### **3.2 Abordagem**

Adotou-se uma abordagem qualitativa, que se caracteriza pela análise detalhada e interpretativa de fenômenos complexos. Conforme Oliveira (2007), a pesquisa qualitativa é apropriada para descrever a complexidade de suposições e problemas, permitindo uma melhor compreensão dos processos dinâmicos vivenciados pelas organizações. No presente estudo, a abordagem qualitativa foi empregada para explorar como a LGPD influencia os processos de gestão de dados no RH.

### **3.3 Objetivos da Pesquisa**

A pesquisa foi classificada como exploratória e descritiva:

- a) Exploratória, por buscar identificar os principais impactos da LGPD no setor de RH e propor uma análise inicial sobre o tema. Segundo Gil (2019), pesquisas exploratórias são apropriadas quando o objetivo é proporcionar maior familiaridade com o problema, tornando-o mais explícito.
- b) Descritiva, pois se dedicou a caracterizar os processos do RH que envolvem o tratamento de dados pessoais e analisar as implicações legais da LGPD nessas atividades. Gerhardt e Silveira (2009) reforçam que a pesquisa descritiva busca observar, registrar e analisar fatos sem interferir diretamente neles.

### **3.4 Procedimentos Metodológicos**

A investigação utilizou os seguintes procedimentos:

- a) Pesquisa bibliográfica: Baseou-se em obras, artigos científicos e legislação relevante. Segundo Fonseca (2002), a pesquisa bibliográfica é realizada a partir de material previamente publicado, seja em formato impresso ou eletrônico.
- b) Pesquisa documental: Incluiu a análise de documentos legislativos, como o texto da Lei nº 13.709/2018 (LGPD), além de pareceres e relatórios técnicos que abordam a aplicação prática da legislação.

### **3.5 Instrumentos de Coleta de Dados**

Os dados foram coletados por meio de uma revisão sistemática de literatura, que envolveu a seleção criteriosa de fontes confiáveis e pertinentes ao tema. A utilização de bancos de dados acadêmicos, como Google Scholar e Scielo, garantiu a qualidade das informações analisadas.

### **3.6 Análise dos Dados**

Os dados coletados foram analisados utilizando o método interpretativo, que, segundo Gerhardt e Silveira (2009), permite a triangulação entre diferentes fontes de informação para identificar padrões, tendências e implicações práticas. Essa análise foi realizada com o objetivo de relacionar o referencial teórico às práticas observadas no setor de RH.

### **3.7 Limitações do Estudo**

Entre as limitações do estudo, destaca-se a ausência de dados empíricos oriundos de entrevistas ou questionários. Embora a pesquisa tenha se concentrado em fontes bibliográficas e documentais, a inclusão de dados primários poderia fornecer uma visão mais prática sobre os desafios enfrentados pelas organizações no cumprimento da LGPD. Recomenda-se que futuros estudos combinem abordagens teóricas e empíricas para aprofundar a análise.

## **4 RESULTADOS E ANÁLISE DOS DADOS**

### **4.1 Os Impactos da LGPD no Setor de Recursos Humanos**

A implementação da Lei Geral de Proteção de Dados (LGPD) trouxe profundas transformações na forma como as organizações, especialmente o setor de Recursos Humanos (RH), devem tratar os dados pessoais de seus colaboradores e candidatos. Com a vigência desta Lei, a proteção de dados pessoais se tornou uma prioridade, e as empresas passaram a ter que adotar novas práticas para garantir que seus processos de recrutamento, seleção e gestão de informações estejam em conformidade com a legislação.

Segundo Peck (2021), a chegada da LGPD exige um novo olhar sobre a natureza dos dados pessoais e sobre os procedimentos de sua coleta, armazenamento e utilização dentro das empresas. O não cumprimento das obrigações da lei pode acarretar penalidades severas, incluindo multas significativas. Diante disso, a LGPD obriga que as empresas, especialmente os departamentos de RH, se adaptem e implementem medidas de segurança e transparência em todas as fases do tratamento de dados pessoais.

#### **4.1.1 Recrutamento e Seleção**

No contexto do recrutamento e seleção, o RH deve ser particularmente cuidadoso ao solicitar informações de candidatos. Com a LGPD, é necessário revisar a necessidade de cada dado coletado e garantir que a solicitação de dados seja limitada às informações essenciais para a avaliação profissional. Sarlet e Schertel Mendes (2021) salientam que, por exemplo, dados como posição política, crenças religiosas, filiação sindical, dados de saúde, e origem racial ou étnica são considerados dados pessoais sensíveis pela LGPD (Brasil, 2018). A coleta e o tratamento desses dados devem ser evitados ou, ao menos, tratados com extrema cautela, pois o uso inadequado pode resultar em discriminação e violação dos direitos do indivíduo.

Além disso, muitas informações solicitadas durante o processo de seleção podem ser irrelevantes para a empresa, e, após a coleta, o armazenamento dessas informações em bancos de dados precisa ser justificado de acordo com a finalidade específica do tratamento. Dados pessoais devem ser mantidos somente pelo tempo necessário para atingir a finalidade para a qual foram coletados (BRASIL, 2018). Chiavenato (2010) destaca que a coleta excessiva de dados pode resultar em uma sobrecarga de informações, o que não só aumenta os riscos de violação de dados, mas também pode afetar a percepção dos candidatos sobre a transparência da organização.

#### 4.1.2 Controle dos Termos de Autorização e Consentimento

A LGPD exige que as empresas obtenham o consentimento explícito dos titulares dos dados antes de coletar ou processar suas informações pessoais. Isso inclui não apenas os dados dos candidatos durante o recrutamento, mas também os dados dos colaboradores ao longo de sua permanência na empresa. Sarlet (2021) enfatiza que o consentimento deve ser livre, informado e específico, com o candidato ou colaborador tendo pleno conhecimento do que está sendo coletado e para que finalidade.

No caso de candidatos a uma vaga, a empresa deve garantir que o consentimento para armazenar as informações no banco de talentos seja solicitado de maneira transparente, deixando claro que esses dados serão utilizados apenas para futuras oportunidades de emprego. Se o titular dos dados se recusar a fornecer esse consentimento, a empresa deverá excluir as informações imediatamente após o uso (Brasil, 2018). Sarlet e Schertel Mendes (2021) destacam a importância de garantir que os dados não sejam mantidos além do necessário, como forma de assegurar a conformidade com a LGPD e a proteção da privacidade do titular.

Da mesma forma, os colaboradores que já fazem parte da organização devem assinar contratos e termos de autorização para o uso e armazenamento de seus dados pessoais, especialmente no que diz respeito ao tratamento de dados sensíveis. Isso ajuda a evitar potenciais litígios ou problemas jurídicos relacionados ao tratamento indevido de informações pessoais (Brasil, 2018).

#### 4.1.3 Proteção dos Dados Pessoais

A proteção dos dados pessoais é um dos pilares da LGPD. Não basta que os dados sejam coletados de forma legal; as empresas devem garantir que os dados sejam armazenados de maneira segura, prevenindo vazamentos e acessos não autorizados. A Segurança da Informação deve ser uma prioridade dentro do RH, principalmente no que diz respeito ao armazenamento e uso de dados sensíveis. Peck (2021) reforça que, quando um colaborador deixa a empresa, os dados pessoais, especialmente as sensíveis, devem ser excluídos ou anonimizados, salvo em situações excepcionais, como em obrigações legais.

Dessler (2020) sugere que o RH deve adotar tecnologias de criptografia e controle de acesso para garantir que somente pessoas autorizadas possam acessar dados pessoais. É fundamental, também, que os dados sejam armazenados em softwares seguros, que possuam recursos de backup e monitoramento contínuo para detectar e prevenir vazamentos.

Além disso, o RH deve estar ciente de que outras empresas não podem acessar as informações dos seus colaboradores sem o devido consentimento, o que inclui consultorias externas ou fornecedores de serviços. A transparência sobre como os dados são utilizados e quem tem acesso a eles é essencial para criar um ambiente de confiança dentro da organização (Sarlet, Schertel Mendes, 2021).

#### 4.1.4 Dados Biométricos no Recursos Humanos

Um dos procedimentos mais impactados pela LGPD no setor de RH é o uso de dados biométricos, como a biometria facial e as impressões digitais para o controle de ponto. Esses dados são frequentemente utilizados para registrar a jornada de trabalho dos colaboradores, mas sua coleta e armazenamento exigem cuidados especiais devido ao seu caráter sensível.

A LGPD impõe que a coleta de dados biométricos seja feita com o consentimento explícito do colaborador e que o uso desses dados seja justificado pela necessidade de controle de ponto e segurança. Peck (2021) alerta que a coleta indiscriminada de dados biométricos pode ser vista como uma violação da privacidade, sendo necessário garantir que esses dados sejam armazenados em sistemas seguros, com acesso restrito apenas aos profissionais autorizados.

Portanto, o uso de biometria no RH deve ser feito de forma equilibrada, com a devida proteção das informações e em conformidade com a LGPD. Qualquer abuso ou falha no gerenciamento desses dados pode resultar em penalidades severas para a organização, além de prejudicar a confiança dos colaboradores (BRASIL, 2018).

No setor de Recursos Humanos, o vazamento de dados pessoais ou sensíveis dos colaboradores pode criar um ambiente de desconfiança interna, dificultando o engajamento e a retenção de talentos. Além disso, empresas que têm seus processos suspensos ou que enfrentam restrições no tratamento de dados podem sofrer atrasos em atividades essenciais, como o pagamento de salários ou a gestão de benefícios.

## 5 CONSIDERAÇÕES FINAIS

O presente trabalho teve como objetivo investigar os desafios e implicações da implementação da Lei Geral de Proteção de Dados Pessoais, com foco no setor de Recursos Humanos. A pesquisa buscou compreender como a legislação influencia o tratamento de dados pessoais, destacando as implicações práticas e éticas para as organizações. Esses objetivos permitiram estruturar uma análise crítica e fundamentada sobre os impactos da LGPD na governança corporativa e na proteção de dados sensíveis no ambiente empresarial.

Ao longo do estudo, foram abordados elementos fundamentais da LGPD, como os princípios da transparência, finalidade e segurança. Tais princípios não apenas norteiam a conformidade legal, mas também refletem uma mudança paradigmática na maneira como os dados pessoais são tratados. Sabe-se que o sucesso da implementação da LGPD está diretamente relacionado à conscientização e ao compromisso ético das organizações. Esse ponto foi amplamente explorado na pesquisa, especialmente no contexto do RH, onde o uso e o armazenamento de dados pessoais exigem maior responsabilidade devido à sua sensibilidade e impacto direto sobre os indivíduos.

A análise dos desafios práticos revelou que a adaptação à LGPD não é apenas uma questão de ajustar processos tecnológicos, mas também de transformar a cultura organizacional. Estudos indicam que o alinhamento entre tecnologia e gestão é essencial para uma governança de dados eficiente. No setor de RH, isso implica a implementação de políticas claras para o término do tratamento de dados, como a eliminação de informações de candidatos não contratados, conforme previsto nos artigos 15 e 16 da LGPD. Contudo, observou-se que a literatura aponta desafios significativos enfrentados pelas empresas para aplicar as diretrizes da LGPD em suas rotinas diárias. Esses desafios estão relacionados à falta de recursos tecnológicos, que dificultam a implementação de sistemas adequados à governança de dados, e à necessidade de maior capacitação dos profissionais para compreenderem e aplicarem corretamente os requisitos da legislação. O presente estudo não buscou constatar empiricamente esses aspectos, mas baseia-se em evidências teóricas revisadas que sugerem que esses fatores são frequentemente apontados como barreiras para a conformidade com a LGPD.

Além disso, a pesquisa destacou que a LGPD não é apenas uma norma regulatória, mas um marco civilizatório que busca equilibrar os avanços da economia digital com a proteção de direitos fundamentais, como a privacidade. Nesse sentido, a proteção de dados vai além da conformidade técnica, sendo um elemento indispensável para a construção de confiança entre empresas e titulares de dados. Essa perspectiva é particularmente relevante no contexto do RH,

onde a relação de confiança é essencial para o desenvolvimento de um ambiente de trabalho ético e produtivo.

Sob uma perspectiva crítica, foi evidenciado que a eficácia da LGPD depende não apenas da adesão por parte das empresas, mas também de uma atuação consistente da Autoridade Nacional de Proteção de Dados. A ANPD desempenha um papel crucial na orientação e fiscalização, especialmente em setores como saúde e educação, onde o tratamento de dados sensíveis exige regulamentações específicas. A pesquisa reforçou que, sem uma fiscalização eficaz e sem incentivos para a conformidade, a aplicação da LGPD corre o risco de se tornar apenas uma formalidade burocrática, sem gerar os avanços esperados em termos de proteção de dados.

Por fim, com base nos resultados obtidos, conclui-se que a LGPD representa um desafio significativo, mas também uma oportunidade para promover práticas organizacionais mais éticas e transparentes. No entanto, para que a legislação alcance seu pleno potencial, é necessário um esforço contínuo de educação, investimento em tecnologias adequadas e fortalecimento das políticas públicas de fiscalização. Estudos futuros poderão aprofundar a análise de como pequenas e médias empresas podem superar barreiras de conformidade, além de investigar o impacto da LGPD em setores específicos, ampliando o entendimento sobre sua aplicação prática e efetividade

. Assim, a LGPD não apenas regula o tratamento de dados, mas também provoca uma reflexão sobre o papel da ética, da governança e da cidadania no contexto digital. Mais do que um conjunto de normas técnicas, ela se apresenta como um marco transformador, essencial para a construção de uma sociedade mais justa, transparente e alinhada aos princípios democráticos.

## REFERÊNCIAS

APPOLINÁRIO, Fábio. **Metodologia da ciência:** filosofia e prática da pesquisa. São Paulo: Cengage Learning, 2011.

BARROS, Aidil Jesus da Silveira; LEHFELD, Neide Aparecida de Souza. **Fundamentos de Metodologia Científica.** 3<sup>a</sup> ed. São Paulo: Pearson Universidades, 2007.

BONI, Bruno Ricardo, **Proteção de Dados Pessoais:** a função e os limites do consentimento - 3. ed - Rio de Janeiro: Forense. 2021.

BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/L13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm)>. Acesso em: 30.maio.2024

BRASIL. **DECRETO-LEI No 5.452, de 1º de maio de 1943.** Aprova a Consolidação das Leis do Trabalho. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/decretolei/del5452.htm](http://www.planalto.gov.br/ccivil_03/decretolei/del5452.htm)>. Acesso em: 24. agosto.2024

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Disponível em:<[http://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm)>. Acesso em: 24. agosto. 2024.

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, edição 157, seção 1, p. 59, 15 ago. 2018. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/L13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm). Acesso em: 28 ago. 2024

BRASIL. Decreto nº 6.135, de 26 de junho de 2007. Disponível em: <http://www.planalto.gov.br>. Acesso em: 20 nov. 2024.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Marco Civil da Internet.** Disponível em: <http://www.planalto.gov.br>. Acesso em: 20 nov. 2024.

CARVALHO, Adriana Cristina França Leite de. **Da segurança e das boas práticas LGPD na educação.** In: SANTOS, Regiane Martins dos;

CARVALHO, Adriana Cristina França Leite de. **Comentários à Lei Geral de Proteção de Dados.** São Paulo: OAB, 2020.

CHIAVENATO I, **Gestão de Pessoas:** o novo papel dos recursos humanos nas organizações. 3<sup>a</sup>ed. Rio de Janeiro: Elsevier, 2010.

CISA. Cybersecurity & Infrastructure Security Agency. **Report:** Cybersecurity risks and vulnerabilities. Washington, D.C.: CISA, 2021. Disponível em: <https://www.cisa.gov> . Acesso em: 27 agosto. 2024.

COELHO, A. C. B. **A Lei Geral de Proteção de Dados Pessoais Brasileira como meio de efetivação dos direitos da personalidade.** João Pessoa: [s.n.], 2019.

COUTINHO, Eduardo Dias; FREITAS, André Souza. **Public value through technologies developed with open government data:** The Love Serenade Operation case. *Revista de Administração Mackenzie*, São Paulo, v. 22, 2021. Disponível em: <https://www.scielo.br>. Acesso em: 4 dez. 2024.

DONEDA, Danilo. **Direitos Fundamentais e Sociedade Tecnológica:** Estudos sobre Proteção de Dados Pessoais. São Paulo: Saraiva Educação, 2021.

DESSLER, Gary. **Administração de Recursos Humanos.** 13. ed. São Paulo: Pearson, 2020.

FONSECA, João José Saraiva. **Metodologia da pesquisa científica.** São Paulo: EPU, 2002.

FRANCOSKI, Denise de Souza; TASSO, Fernando Antonio. **A Lei geral de proteção de dados pessoais:** aspectos práticos e teóricos relevantes no setor público e privado. São Paulo: Revista dos Tribunais, 2021.

GERHARDT, Tatiana Engel; SILVEIRA, Denise Tolfo. **Métodos de pesquisa.** Porto Alegre: Editora da UFRGS, 2009.

GIL, Antônio Carlos. **Métodos e técnicas de pesquisa social.** 6<sup>a</sup> ed. São Paulo: Atlas, 2019.

GOMES, Rodrigo Dias de Pinho. **Big data:** desafios à tutela da pessoa humana na sociedade da informação. 2. ed. Rio de Janeiro: Lumen Juris, 2019.

IVANCEVICH, John M. **Gestão de Recursos Humanos.** 10. ed. São Paulo: McGraw-Hill, 2008.

LEGGE, Karen. **Human Resource Management:** Rhetorics and Realities. London: Macmillan, 2005.

LIMA, Humberto. **Gestão de Pessoas:** Teoria e Prática. São Paulo: Pearson, 2017.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD: Lei Geral de Proteção de Dados:** comentada. 2. ed. rev. atual. e ampl. São Paulo: Revista dos Tribunais, 2019.

MEDEIROS, Maurício M.; MAÇADA, Antônio Carlos G.; HOPPEN, Norberto. **O papel da administração e análise de big data como habilitadoras da gestão do desempenho corporativo.** *Revista de Administração Mackenzie*, São Paulo, v. 22, 2021. Disponível em: <https://www.scielo.br>. Acesso em: 4 dez. 2024.

MENDES, Ana Clara. **A conformidade com a LGPD como diferencial competitivo.** São Paulo: Editora Jurídica, 2020. 245 p.

OLIVEIRA, Maria Cecília de Souza Minayo. **O desafio do conhecimento: pesquisa qualitativa em saúde.** São Paulo: Hucitec, 2007.

PECK, Patrícia Pinheiro. **Proteção de dados pessoais:** comentários à Lei n. 13.709/2018 (LGPD) /– 2. ed. – São Paulo: Saraiva Educação, 2021

RAMINELLI, Francieli Puntel; RODEGHERI, Letícia Bodanese. **A Proteção de Dados Pessoais na Internet no Brasil:** Análise de decisões proferidas pelo Supremo Tribunal Federal. In: Revista Cadernos do Programa de Pós-Graduação em Direito PPGDir./UFRGS. Disponível em: <http://seer.ufrgs.br/ppgdir/article/view/61960/39936> Acesso em: 15. maio. 2024

SARLET, Ingo Wolfgang; SCHERTEL MENDES, Laura. **Estudos sobre Proteção de Dados Pessoais.** Porto Alegre: Livraria do Advogado, 2021.

ULRICH, Dave. **Human Resource Champions.** Boston: Harvard Business Press, 2018.