Organização : Tauanne Andrade

MANUAL LGPD

PARA RECRUTAMENTO E SELEÇÃO

Um Guia Prático para Profissional de RH

1ª Edição

Ela Jurista

MANUAL LGPD PARA RECRUTAMENTO E SELEÇÃO

Um Guia Prático para Profissionais de RH

Organização: Tauanne Andrade

1ª Edição

Ela Jurista

Ana Carolina da Costa

Andressa Lourenço Gonçalves

Daniele Ozorio

Giuliana Visconte

Juliana Cristina da Silva

Régia D. Freitas da Silva

Silvia Aparecida Celestino

Sarah Carolina de Sales Gobo

MANUAL LGPD PARA RECRUTAMENTO E SELEÇÃO

Um Guia Prático para Profissionais de RH

1ª Edição

Organização: Tauanne Andrade

Ela Jurista

Belo Horizonte 2025

Coordenação: Tauanne Andrade

Autores: Ana Carolina da Costa

Andressa Lourenço Gonçalves

Daniele Ozorio Giuliana Visconte

Juliana Cristina da Silva

Régia D. Freitas da Silva

Silvia Aparecida Celestino

Sarah Carolina de Sales Gobo

Revisão: Juliana Cristina da Silva

Ela Jurista

Belo Horizonte 2025

ACESSO O GUIA ONLINE

Explore a versão web, um Guia estruturado e interativo do Manual para consulta rápida em qualquer dispositivo.

👉**CLIQUE AQUI PARA ACESSAR**

Para todas as mulheres da comunidade Ela Jurista, que transformam conhecimento em colaboração e expertise em ferramenta de mudança.

Que este manual seja a prova da nossa potência coletiva.

Por que este Manual foi Criado?

Este manual é um reflexo da missão da **Ela Jurista**: um negócio de impacto social que promove a diversidade, equidade e inclusão no setor jurídico. Nossa missão é clara: capacitar e conectar mulheres a oportunidades de carreira, construindo um ambiente de trabalho mais justo para todas.

A ideia de criar este guia sobre a Lei Geral de Proteção de Dados (LGPD) para o RH surgiu diretamente de nossa comunidade de "membras". Mulheres que são estudantes de Direito, advogadas, empreendedoras e líderes do setor. Ao participarem de processos seletivos, elas frequentemente notavam uma lacuna: a falta de conhecimento sobre como tratar dados pessoais de forma segura e ética. Percebemos que, mais do que uma

intenção de invadir a privacidade, a maioria dessas práticas vinha da falta de informação sobre as novas exigências da lei.

Reconhecendo essa necessidade,fizemos uma provocação a algumas de nossas membras, especialistas em LGPD, para que juntas criássemos um material que preenchesse essa lacuna. Elas prontamente aceitaram o desafio de conscientizar o mercado. Este manual, portanto, é um Este manual é um reflexo da missão da **Ela Jurista**: um negócio de impacto social que promove a diversidade, equidade e inclusão no setor jurídico. Nossa missão é clara: capacitar e conectar mulheres a oportunidades de carreira, construindo um ambiente de trabalho mais justo para todas.

A ideia de criar este guia sobre a Lei Geral de Proteção de Dados (LGPD) para o RH guia feito por profissionais, para profissionais.

É com orgulho que apresentamos este trabalho, fruto do talento e da expertise das mulheres que compõem nossa comunidade. Este manual é a prova de que, ao se conectar à Ela Jurista, empresas se conectam a talentos potentes e mulheres acessam oportunidades, em uma parceria que capacita e valoriza o talento feminino.

Nosso objetivo é fornecer a você, profissional de RH ou do setor jurídico, as ferramentas necessárias para:

- **Compreender e aplicar** os princípios da LGPD em cada etapa do processo seletivo.
- **Adotar práticas éticas e seguras** que protejam os dados de candidatos e colaboradores.
- **Transformar a LGPD** de uma obrigação legal em um pilar de confiança e credibilidade para sua empresa.

Com este manual, esperamos que a proteção de dados seja vista como um caminho para construir processos

mais seguros, justos e alinhados com a nova realidade do mercado, valorizando o respeito e a privacidade de todos.

Tauanne Andrade

Fundadora da Ela Jurista

Sobre a Ela Jurista

A Ela Jurista promove inclusão produtiva de mulheres no setor jurídico, conectando talentos qualificados a oportunidades reais de trabalho e desenvolvimento.

Atendemos empresas que buscam profissionais jurídicas preparadas, de destaque e capazes de gerar resultados reais, enquanto geram impacto social ao fortalecer a presença de mulheres diversas no mercado jurídico.

Mais do que uma plataforma, somos uma comunidade que transforma carreiras e organizações, onde competência, propósito e resultados caminham juntos.

Sobre as Autoras

Ana Carolina da Costa

Advogada especialista em Direito Digital e Proteção de Dados e Presidente da Comissão de Privacidade, Proteção de Dados e IA de Matão/SP.

Andressa Lourenço Gonçalves

Bacharel em Direito pelo Centro Universitário Augusto Motta, com pós-graduação em Direito Digital, Direito do Consumidor e Direito Médico e da Saúde. Atualmente, atua como residente jurídica no Ministério Público do Estado do Rio de Janeiro. Sua trajetória inclui experiências no Tribunal de Justiça do Rio de Janeiro, na Junta Comercial (Procuradoria Jurídica) e em escritório de advocacia, com forte atuação em direito médico e da saúde, direito do consumidor e direito processual.

Daniele Ozorio

Advogada trabalhista especialista em Direito do Trabalho, Direito Social, LGPD e Gestão de Negócios com experiência em assessoria jurídica estratégica para empresas, departamento pessoal, compliance e recursos humanos de grandes corporações, além de uma sólida experiência como docente em cursos profissionalizantes. Atua diretamente junto a Tribunais Regionais e Superiores, Ministério do Trabalho e Emprego, INSS e Ministério Público do Trabalho, sempre com foco na conformidade legal e na prevenção de litígios.

Giuliana Visconte

Advogada consultiva com atuação em instituição financeira, formada pela Universidade Presbiteriana Mackenzie (2015) e regularmente inscrita na OAB/SP, com experiência consolidada em Direito Contratual, Direito Societário e, especialmente, em temas relacionados à privacidade e proteção de dados pessoais, com enfoque na conformidade à Lei Geral de Proteção de Dados (Lei nº 13.709/2018 – LGPD).

Juliana Cristina da Silva

Advogada e jornalista, pós-graduada em Proteção e Privacidade de Dados, com MBA em Gestão de Negócios e Negociação. Atua como monitora convidada em cursos da Data Privacy Brasil e possui experiência em Direito Civil e do Consumidor.

Régia D. Freitas da Silva

Advogada, especializada em Direito do Trabalho e pós-graduanda em Direito Previdenciário e Proteção de Dados. Membro da Comissão Nacional da Advocacia Jovem (CEAJ) da OAB/PE, possui formações específicas em GDPR (Regulamento Geral de Proteção de Dados da UE) e na certificação EXIN PDPE (Privacy and Data Protection Essentials). Dedica-se ao estudo da regulação do ambiente digital, analisando temas como LGPD, ética em IA e a governança de tecnologias emergentes sob a perspectiva jurídica.

Sarah Carolina de Sales Gobo

Advogada autônoma, especialista em Advocacia Civil pela FMP e em Lei Geral de Proteção de Dados Pessoais pela Legale Educacional. Vice-presidência da

Comissão de Privacidade e Proteção de Dados da OAB Uberlândia/MG (gestão 2025-) e integra o Comitê Público da APDADOS – Associação Nacional dos Profissionais de Privacidade de Dados. Atua em consultoria e contencioso estratégico, com foco em Direito do Consumidor, proteção de dados e responsabilidade digital.

Silvia Aparecida Celestino

Professora de Direito Processual Cível, mediadora extrajudicial e especialista em Direito Processual Civil e Direito das Mulheres.

Tauanne Andrade

Advogada, Pós graduada em Direito Empresarial e Direito Digital. Fundadora e Head de Operações da Ela Jurista, responsável pelo desenvolvimento de processos, tecnologias e soluções para inclusão produtiva de mulheres no setor jurídico. Organizou este manual, reunindo práticas alinhadas à LGPD e à gestão de talentos jurídicos.

Sumário

Parte I – Fundamentos e Práticas Essenciais

Capítulo 1: Entendendo a LGPD e seu Impacto no RH

O que é a LGPD?

Autora: Daniele Ozorio

O avanço tecnológico, impulsionado pela globalização e pelo amplo acesso à informação, tornou a privacidade e a segurança dos dados temas essenciais na sociedade, em virtude do reflexo direto dessas mudanças no comportamento das pessoas(físicas ou jurídicas) exigindo, assim, maior proteção das informações pessoais. Diante desse cenário, o Brasil sancionou, em 2018, a Lei Geral de Proteção de Dados (LGPD), inspirada no Regulamento Geral de Proteção de Dados (GDPR) da União Europeia.

Instituída pela Lei nº 13.709/2018, marcando uma nova era na proteção de dados pessoais no Brasil, a LGPD

estabelece diretrizes para a coleta, armazenamento, processamento, compartilhamento e até exclusão de dados pessoais, regulando seu uso por indivíduos e empresas, públicas ou privadas, em formatos digitais ou físicos, garantindo transparência e equilíbrio entre inovação e privacidade.

Seu objetivo é proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade, conforme disposto no artigo 1º da lei.

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre

> desenvolvimento da personalidade da pessoa natural.

A relevância do tratamento de dados foi ratificada através da Emenda Constitucional nº 115, de 10 de fevereiro de 2002, que acrescentou à Constitucional a proteção de dados pessoais como um direito fundamental, conforme art. 5º, LXXIX:

> Art. 5º é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

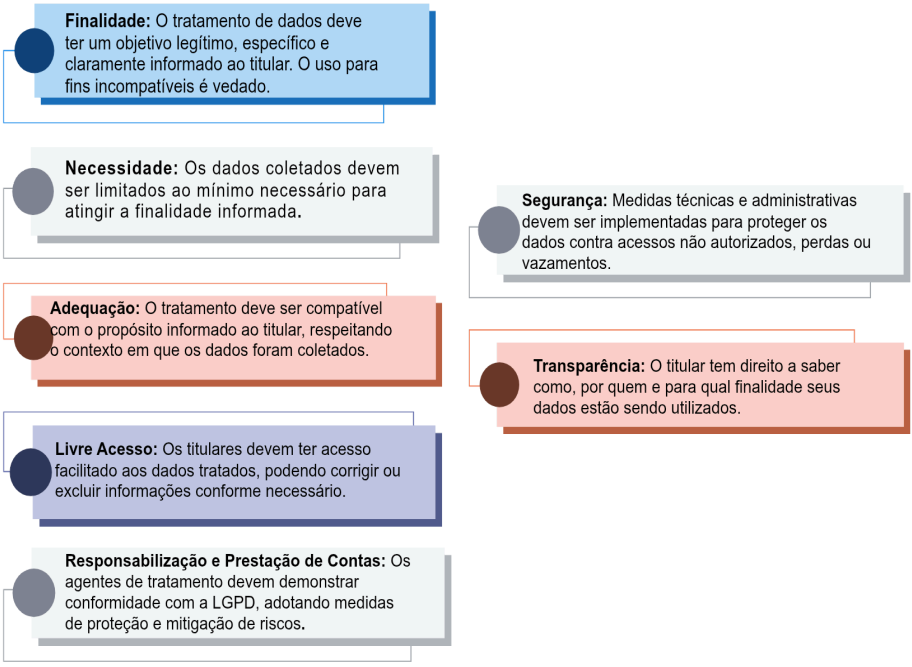
Aliado a esse fato, a LGPD possui princípios que são diretrizes fundamentais que orientam o tratamento de dados pessoais, sendo indispensáveis para garantir sua aplicação adequada. Podemos destacar uma tríade básica aliada aos demais e que orientam a sua aplicação no cotidiano das relações:

FINALIDADE	NECESSIDADE	ADEQUAÇÃO

ADEQUAÇÃO	LIVRE ACESSO	RESPONSABILIDADE	SEGURANÇA	TRANSPARÊNCIA

Importante destacar que a LGPD se aplica a qualquer operação de tratamento de dados pessoais realizada no território nacional, independentemente do meio utilizado (físico ou digital).

A lei traz importante definição acerca dos papéis e destaca dois agentes principais no tratamento de dados: O Controlador e o Operador.


Finalidade: O tratamento de dados deve ter um objetivo legítimo, específico e claramente informado ao titular. O uso para fins incompatíveis é vedado.
Necessidade: Os dados coletados devem ser limitados ao mínimo necessário para atingir a finalidade informada.
Adequação: O tratamento deve ser compatível com o propósito informado ao titular, respeitando o contexto em que os dados foram coletados.
Livre Acesso: Os titulares devem ter acesso facilitado aos dados tratados, podendo corrigir ou excluir informações conforme necessário.
Responsabilização e Prestação de Contas: Os agentes de tratamento devem demonstrar conformidade com a LGPD, adotando medidas de proteção e mitigação de riscos.
Segurança: Medidas técnicas e administrativas devem ser implementadas para proteger os dados contra acessos não autorizados, perdas ou vazamentos.
Transparência: O titular tem direito a saber como, por quem e para qual finalidade seus dados estão sendo utilizados.

A LGPD representa um marco e relevância não apenas para a privacidade dos indivíduos, mas também para a governança e ética nas organizações. Empresas que tratam dados pessoais precisam adotar práticas que garantam segurança, transparência e respeito aos direitos dos titulares.

Nesse cenário destaca-se o consentimento do titular dos dados com fator preponderante para o tratamento dos dados, cabendo exceção somente para: cumprir exigências legais; implementar políticas públicas

previstas em lei; conduzir pesquisas por órgãos especializados; executar contratos; resguardar direitos em processos judiciais ou administrativos; proteger a vida e a integridade física de alguém; viabilizar a atuação de profissionais da saúde ou da área sanitária; prevenir fraudes contra o titular; garantir a proteção do crédito; ou atender a interesses legítimos, desde que não violem os direitos fundamentais do cidadão.

Consentimento	Autorização do titular dos dados para que seus dados pessoais (sensíveis ou não) sejam tratados. Deve ser prévia, explícita, inequívoca, requerida de forma clara, transparente e livre e para finalidade determinada

Podemos citar os processos de Recursos Humanos (RH), onde a coleta e o processamento de dados pessoais e

sensíveis são rotineiros, a LGPD desempenha um papel fundamental na proteção dos direitos dos trabalhadores e candidatos. Podemos destacar que um dos principais impactos da LGPD no RH é a necessidade de consentimento para o tratamento de dados pessoais. Por exemplo, ao coletar currículos em processos seletivos, as empresas devem informar aos candidatos a finalidade do uso dessas informações e obter autorização explícita. Além disso, dados sensíveis, como informações sobre saúde para benefícios médicos, precisam de proteção reforçada para evitar usos indevidos ou vazamentos.

Outro ponto relevante é a restrição no compartilhamento de dados. Empresas frequentemente terceirizam serviços de folha de pagamento e benefícios, exigindo a transmissão de informações pessoais a terceiros. Com a LGPD, é imprescindível que esse compartilhamento ocorra de forma segura, mediante contratos que garantam a confidencialidade e a integridade dos dados.

No exemplo acima vemos que os impactos da LGPD incluem:

1. **Confiança:** A proteção de dados promove maior transparência e fortalece o relacionamento entre o titular dos dados e o controlador/operador.
2. **Evita Penalidades:** A não conformidade pode resultar em multas.
3. **Competitividade:** Empresas que demonstram conformidade com a LGPD têm vantagem competitiva.

Por isso, a LGPD não é apenas uma exigência legal; é um reflexo das demandas sociais por maior proteção e responsabilidade no uso de dados pessoais. Com seus princípios bem delineados e um escopo amplo de aplicação, a lei estabelece um novo paradigma de governança e transparência.

Adotar as diretrizes da LGPD é essencial não apenas para evitar sanções, mas também para promover práticas éticas e construir relações de confiança com titulares de dados.

Impacto da LGPD no Recrutamento e Seleção

A Lei Geral de Proteção de Dados (LGPD) trouxe uma nova realidade para empresas que realizam processos seletivos, considerando as regras estabelecidas sobre a coleta, armazenamento, uso e descarte de dados pessoais de candidatos. Com o objetivo de proteger a privacidade e garantir transparência, a LGPD impacta todas as etapas do recrutamento e seleção, desde a captação de currículos até a retenção de informações para futuras oportunidades.

No recrutamento e seleção, isso significa que qualquer empresa que colete currículos, realize entrevistas ou

processe dados de candidatos está sujeita às disposições da lei. Podemos citar como exemplo de aplicação no recrutamento e seleção:

- Coleta de dados pessoais por meio de formulários online, plataformas de recrutamento ou entrega de currículos físicos.
- Armazenamento de informações de candidatos em bancos de dados.
- Compartilhamento de dados com gestores ou terceiros envolvidos no processo seletivo.
- Uso de ferramentas de inteligência artificial ou algoritmos para análise de currículos.

Sendo assim, os princípios da LGPD que orientam o tratamento de dados pessoais são cabíveis no processo de recrutamento e seleção, pois devem ser observados

por todos os agentes que lidam com dados pessoais, como vemos abaixo:

1. **Finalidade**: Os dados coletados devem ter um propósito específico e legítimo relacionado ao processo seletivo. As empresas devem informar claramente como essas informações serão utilizadas.

2. **Necessidade**: Apenas os dados estritamente necessários para a seleção devem ser coletados, evitando excessos e minimizando riscos.

3. **Transparência**: Os candidatos devem ser informados sobre o tratamento de seus dados de forma clara e acessível, incluindo detalhes sobre armazenamento, compartilhamento e exclusão.

4. **Segurança**: Medidas técnicas e organizacionais devem ser adotadas para proteger os dados contra acessos não autorizados, vazamentos e uso indevido.

5. **Livre acesso**: Os candidatos devem ter o direito de acessar suas informações, verificar como estão sendo tratadas e solicitar correções ou exclusão, se necessário.

6. **Qualidade dos dados**: As empresas devem garantir que os dados armazenados sejam precisos, atualizados e pertinentes ao processo seletivo.

7. **Responsabilização e prestação de contas**: As empresas devem adotar práticas de governança e manter registros que comprovem o cumprimento das diretrizes da LGPD.

Essa observância é essencial para garantir conformidade legal e proteção dos dados dos candidatos.

Ciclo de Vida no Tratamento de Dados - Etapas do Recrutamento e Seleção

A transparência deve ser um princípio fundamental no processo seletivo. O candidato tem o direito de saber quais informações estão sendo usadas e para qual finalidade, especialmente quanto ao tempo na base de dados para tratamento indefinido, sem qualquer justificativa ante a vedação legal.

Assim, o ciclo de vida de tratamento de vida, via de regra, possui início e fim, lastreado pela finalidade e alcance do objetivo, excepcionando a previsão contida no art. 16 da LGPD.

Lembrando que o art. 15 da LGPD elenca quais são as hipóteses em que ocorrerá o encerramento do tratamento de dados.

Coleta de Dados	No momento da inscrição do candidato em um processo seletivo, as empresas devem ter um propósito legítimo e explícito para coletar seus dados pessoais. É essencial obter o consentimento do candidato de forma clara, garantindo que ele saiba como suas informações serão utilizadas. Dados excessivos ou irrelevantes para a seleção não devem ser coletados, minimizando riscos e garantindo conformidade com a lei. Exemplo: Uma empresa pode solicitar nome, contato, formação acadêmica e experiências profissionais, mas não deve pedir informações sobre religião ou

	orientação política, pois esses dados não são necessários para a seleção e podem representar um risco jurídico. Além disso, informações sensíveis, como origem étnica, religião ou condição de saúde, exigem um cuidado redobrado, pois possuem proteção especial na LGPD. Empresas devem garantir que a coleta dessas informações seja justificada e estritamente necessária para o processo seletivo.

Armazenamento e Segurança	Após a coleta, a empresa deve adotar medidas técnicas e organizacionais para proteger os dados dos candidatos contra acessos não autorizados, vazamentos e uso indevido. A segurança da informação é um dos pilares da LGPD, e descuidos nesse aspecto podem resultar em penalidades severas. Exemplo: Se uma empresa armazena currículos em um sistema online, deve garantir que ele tenha mecanismos de criptografia e acesso restrito apenas a recrutadores autorizados, evitando vazamentos de informações.

	Além disso, a retenção dos dados deve ser limitada ao período necessário para a seleção. Caso a empresa deseje manter currículos para futuras oportunidades, deve informar ao candidato e obter seu consentimento prévio. O candidato também tem o direito de solicitar a exclusão de seus dados a qualquer momento. A revogação do consentimento para uso dos seus dados, pode ser realizada a qualquer momento.

Uso de Dados e Compartilhamento	Os dados coletados devem ser utilizados estritamente para os fins informados no momento da coleta. O compartilhamento dessas informações com terceiros, como consultorias de RH ou plataformas de recrutamento, só pode ocorrer se houver uma base legal que o justifique, como consentimento do titular ou legítimo interesse, desde que respeitados os princípios da LGPD.

Dados de candidatos não selecionados	Os dados de candidatos não selecionados podem ser: Excluídos quando fornecidos para uma vaga específica, sem consentimento para armazenamento, devido à perda de finalidade. Mantidos com consentimento, caso o candidato autorize sua inclusão em um banco de currículos para futuras seleções. Nesse caso, é fundamental garantir transparência sobre quem terá acesso (1 ou mais controladores/operadores), qual prazo, utilização restrito em vagas alinhadas ao perfil do candidato e

	direito de requerer a exclusão dos dados a qualquer tempo.

Dica de Implementação

As diretrizes a seguir consideraram etapas básicas geralmente utilizadas no processo de recrutamento e seleção e que são impactadas pela LGPD, sendo que seus riscos e medidas preventivas servem como uma referência para análise e adaptação conforme a realidade da sua empresa. É essencial considerar as políticas de privacidade e segurança de dados já implementadas, garantindo conformidade com a legislação e proteção dos dados dos candidatos. Avalie os pontos apresentados e ajuste-os conforme as necessidades do seu processo seletivo e normas da sua empresa.

1. **Divulgação da Vaga e Captação de Currículos**

    - Impacto **da LGPD**: As empresas devem garantir que a divulgação da vaga informe como os dados dos candidatos serão tratados, além de coletar apenas as informações necessárias para a seleção.
    - **Risco**: Coletar dados excessivos ou não obter consentimento adequado pode resultar em infrações e penalidades.

Dica: Inserir uma cláusula de consentimento nos formulários de candidatura e informar claramente a política de privacidade.

2. **Triagem e Análise de Currículos**

- **Impacto da LGPD**: As empresas devem utilizar apenas os dados fornecidos com consentimento e garantir que não haja discriminação baseada em informações sensíveis.
- **Risco**: O uso de inteligência artificial sem transparência pode levar a práticas discriminatórias e contestação por parte dos candidatos.

Dica: Implementar processos auditáveis e garantir que o candidato tenha acesso às informações utilizadas na triagem.

3. **Entrevistas e Testes Seletivos**

- **Impacto da LGPD**: Informações coletadas durante entrevistas e testes devem ser registradas e

armazenadas com segurança, limitando o acesso apenas a pessoas autorizadas.

- **Risco**: O armazenamento inadequado ou compartilhamento indevido dessas informações pode comprometer a privacidade do candidato e resultará em sanções.

Dica: Utilizar plataformas seguras para armazenar dados e limitar o acesso aos responsáveis pelo processo seletivo.

4. **Decisão e Comunicação de Resultados**

- **Impacto da LGPD**: As empresas devem garantir que os dados sejam utilizados exclusivamente para a decisão do processo seletivo e

comunicar a decisão de maneira ética e transparente.

- **Risco**: O uso indevido de dados para outras finalidades pode gerar reclamações e ações legais por parte dos candidatos.

Dica: Criar um processo documentado para justificar decisões e garantir que informações pessoais não sejam compartilhadas com terceiros sem autorização.

5. **Armazenamento e Retenção de Dados**

- **Impacto da LGPD**: Os dados dos candidatos devem ser armazenados apenas pelo tempo necessário para a finalidade informada, sendo excluídos após o prazo estabelecido.

- **Risco**: A retenção prolongada de dados sem justificativa legal pode resultar em violações à LGPD e penalizações.

Dica: Definir prazos claros para retenção de dados e implementar processos de exclusão segura de informações.

6. **Uso Futuro de Dados para Novas Oportunidades**

- **Impacto da LGPD**: Caso a empresa deseje manter os currículos em um banco de talentos, deve obter consentimento explícito do candidato para essa finalidade.
- **Risco**: A utilização dos dados sem consentimento para futuras seleções

pode ser considerada uma infração grave.

Dica: Oferecer a opção para o candidato consentir explicitamente e permitir que ele revogue esse consentimento a qualquer momento.

A LGPD transformou a forma como as empresas lidam com dados pessoais nos processos seletivos, exigindo mais transparência, segurança e respeito aos direitos dos candidatos. Para profissionais de recrutamento e seleção, compreender e aplicar os princípios da LGPD é essencial para garantir a conformidade legal e promover um ambiente de confiança e respeito aos direitos dos candidatos.

Ao final, a LGPD deve ser vista como uma oportunidade para fortalecer as práticas de RH, alinhando-as aos

padrões modernos de proteção de dados e boas práticas empresariais

.

Referências

BRASIL. Lei 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 12/2024, 01/2025 e 02/2025.

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, DF. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 12/2024, 01/2025 e 02/2025

BRASIL. Lei n. 13.853, de 8 de julho de 2019. Brasília, DF. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a

Autoridade Nacional de Proteção de Dados; e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 01/2025 e 02/2025.

CARLOTO, Selma; GUERRA, Elaine. Manual Prático de Adequação à LGPD com Enfoque nas Relações de Trabalho. São Paulo. 1. Ed. Ltr, 2021.

SILVA, Fabricio Lima; PINHEIRO, Iuri; BOMFIM, Vólia. Manual do Compliance Trabalhista Teoria e Prática. Salvador. 2. Ed. Ver. Ed. JusPodivm, 2021.

SANTOS, Karina Menezes. Percepções acerca do consentimento na LGPD. Revista Jus Navigandi, Disponível em: https://jus.com.br/artigos/92195/percepcoes-acerca-do-consentimento-na-lgpd. Acesso em: 12/2024, 01/2025 e 02/2025.

ALBUQUERQUE JUNIOR, Carlos Cavalcanti. A garantia constitucional da privacidade nos processos de recrutamento e seleção com o advento da lei geral de proteção de dados. Disponível em: https://jus.com.br/artigos/85774/a-garantia-constitucional-da-privacidade-nos-processos-de-recrutamento-e-selecao-com-o-advento-da-lei-geral-de-protecao-de-dados. Acesso em: 12/2024, 01/2025 e 02/2025.

Capítulo 2. Coleta e Tratamento de Dados Pessoais

Autoras: Silvia Celestino e Redação da Ela Jurista

O que a LGPD exige do RH

A **Lei Geral de Proteção de Dados (Lei 13.709/2018)** trouxe mudanças importantes para todas as áreas que lidam com informações pessoais no Brasil. No setor de Recursos Humanos, essas mudanças impactam diretamente o modo como os processos seletivos são conduzidos, desde o momento em que o candidato envia um currículo até o descarte de informações após o fim da seleção.

O objetivo da lei é simples: garantir que todo cidadão tenha controle sobre seus próprios dados. Para o RH, isso significa adotar critérios claros de coleta, tratamento, armazenamento e exclusão de dados de

candidatos, sem excessos e sem práticas discriminatórias.

Quais dados podem ser coletados em processos seletivos

Um dos maiores erros de empresas e recrutadores é solicitar informações que **não têm relação com a vaga**. Sob a ótica da LGPD, isso gera risco de violação de direitos e pode até caracterizar discriminação.

Em um processo seletivo, o RH está autorizado a coletar apenas os dados **necessários para avaliar o perfil do candidato em relação à vaga**.

Exemplos de dados que podem ser coletados:

- Nome completo, CPF e dados de contato.
- Histórico acadêmico.
- Experiência profissional.
- Competências técnicas.

- Disponibilidade de horário.

Exemplos de dados que não devem ser coletados:

- Religião, crença ou filiação a grupos religiosos.
- Opinião política ou filiação partidária.
- Orientação sexual.
- Estado civil, número de filhos ou intenção de ter filhos.

Essas informações não são relevantes para o desempenho da função e podem gerar **tratamento discriminatório** se forem consideradas.

Consentimento para coleta e uso de dados

Para que os dados sejam tratados de forma legítima, é necessário obter o **consentimento claro do candidato**. Esse consentimento deve ser:

- **Livre:** sem pressão ou obrigatoriedade.

- **Informado:** o candidato deve saber exatamente para que seus dados serão usados.
- **Específico:** deve estar vinculado ao processo seletivo em questão.

Na prática, isso pode ser feito por meio de um **termo de consentimento** assinado ou de um **checkbox digital** em formulários de inscrição.

O consentimento não é definitivo. O candidato tem o direito de **retirar a autorização a qualquer momento**, o que exige que o RH tenha um canal de comunicação aberto para atender essas solicitações.

Dados de diversidade em processos seletivos afirmativos

Um ponto sensível e cada vez mais presente nos processos seletivos é o uso de dados relacionados à **diversidade e inclusão**. Muitas empresas adotam ações afirmativas para garantir representatividade de pessoas negras, indígenas, mulheres, pessoas com deficiência, pessoas LGBTQIA+ e outros grupos minorizados.

Nesses casos, o RH pode solicitar informações de diversidade, mas com regras claras:

1. O candidato deve fornecer esses dados de forma **voluntária**.
2. A pergunta deve ser feita de maneira **inclusiva e respeitosa**, sem qualquer viés discriminatório.
3. O consentimento deve ser **específico para dados sensíveis** (raça, etnia, saúde, deficiência etc.).
4. As informações só podem ser usadas para o fim declarado — como o cumprimento de cotas legais ou programas de diversidade interna.

Exemplo prático:

Em um processo seletivo com vagas afirmativas para pessoas com deficiência, o RH pode incluir no formulário uma pergunta como:

"Você deseja se candidatar na modalidade de vaga afirmativa para pessoas com deficiência? ( ) Sim ( ) Não".

Essa pergunta deve vir acompanhada de um aviso claro:

> "Esta informação é opcional, e será usada apenas para atender a políticas de inclusão e diversidade da empresa, conforme a LGPD."

Consentimento para dados sensíveis

Dados sensíveis exigem ainda mais cuidado, porque dizem respeito a aspectos íntimos e que podem expor o candidato a riscos de discriminação. A LGPD considera sensíveis informações como:

- Raça e etnia.

- Opinião política.
- Religião ou crença.
- Orientação sexual.
- Dados de saúde.
- Filiação sindical.

O tratamento desses dados só é permitido com **consentimento expresso** do titular. Ou seja, o candidato precisa declarar de forma clara que concorda com a coleta e o uso dessas informações para determinada finalidade.

Além disso, esses dados devem ser **armazenados com segurança** e descartados assim que não forem mais necessários.

Boas práticas para o RH

Para que a empresa esteja em conformidade com a LGPD e, ao mesmo tempo, promova um ambiente de

seleção inclusivo, o RH deve adotar algumas práticas essenciais:

1. **Coletar apenas o necessário:** não peça dados irrelevantes para a vaga.
2. **Explicar o uso dos dados:** sempre informe como as informações serão utilizadas.
3. **Respeitar a voluntariedade:** dados sensíveis nunca devem ser obrigatórios.
4. **Armazenar com segurança:** restrinja o acesso a dados sensíveis apenas a quem realmente precisa.
5. **Definir prazo de retenção:** descarte os dados após o término do processo seletivo, salvo quando a lei exigir retenção.
6. **Evitar compartilhamento desnecessário:** informações de diversidade não devem circular livremente entre áreas da empresa.

Conclusão

A coleta e o tratamento de dados pessoais em processos seletivos são inevitáveis, mas precisam ser feitos com responsabilidade. A LGPD não veio para burocratizar o trabalho do RH, e sim para garantir que candidatos sejam tratados com respeito, transparência e segurança.

Ao aplicar essas práticas, o RH não apenas cumpre a lei, mas também fortalece a imagem da empresa como um ambiente inclusivo e ético, capaz de atrair e reter os melhores talentos.

Referências

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Guia Orientativo sobre Agentes de Tratamento e Encarregado. Versão 2.0, Brasília, 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018.

PINHEIRO, Patrícia Peck. Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018 (LGPD). 4. ed. São Paulo: Saraiva Jur, 2024.

Capítulo 3: Armazenamento e Proteção de Dados

Autor: Redação Ela Jurista

Medidas de segurança para armazenamento de dados pessoais

Após a coleta, o próximo passo essencial é garantir que os dados pessoais dos candidatos estejam armazenados em um ambiente seguro. A LGPD exige que as empresas adotem medidas técnicas e administrativas para proteger as informações contra acessos não autorizados, vazamentos acidentais e uso indevido. O objetivo é criar um "escudo" para os dados, garantindo que apenas as pessoas certas tenham acesso às informações corretas.

Para isso, o RH pode adotar práticas como:

- **Controle de Acesso:** Certifique-se de que apenas os profissionais diretamente envolvidos no processo seletivo (como recrutadores e gestores da vaga) tenham acesso aos dados dos candidatos. Utilize senhas fortes e privilégios de acesso específicos para cada usuário.
- **Armazenamento Seguro:** Evite guardar currículos e informações em locais inseguros, como e-mails pessoais, computadores sem senha ou pastas compartilhadas. Prefira sistemas de gestão de recrutamento (ATS - *Applicant Tracking System*) que ofereçam funcionalidades de segurança, como criptografia.
- **Criptografia:** Trata-se de uma tecnologia que transforma os dados em códigos ilegíveis, impedindo que pessoas não autorizadas consigam ler as informações mesmo se houver um vazamento. A criptografia é uma medida essencial para proteger dados armazenados.

Proteção adicional para dados sensíveis e de diversidade

Dados sensíveis — como informações sobre origem racial ou étnica, opiniões políticas, dados de saúde e biometria — exigem uma camada extra de proteção. Se a sua empresa coleta este tipo de informação, por exemplo, em programas de diversidade e inclusão, é fundamental aplicar medidas de segurança mais rigorosas.

Para esses dados, o RH deve considerar:

- **Acesso Restrito:** Além do controle de acesso básico, garanta que apenas um grupo muito reduzido de pessoas tenha permissão para acessar dados sensíveis. O ideal é que o acesso seja feito por perfis de usuário específicos, com auditoria constante para monitorar quem acessou o quê.

- **Anonimização:** Sempre que possível, os dados de diversidade devem ser tratados de forma que não possam estar diretamente relacionados a um candidato específico. Isso pode ser feito usando códigos ou identificadores que separam a informação da identidade do titular, garantindo a privacidade e prevenindo vieses ou discriminação.
- **Criptografia Fortalecida:** Para dados sensíveis, utilize criptografia avançada tanto no armazenamento (dados "em repouso") quanto na transferência (dados "em trânsito") entre sistemas.

Prazos de retenção de dados

Um dos princípios da LGPD é a **limitação da finalidade e do tempo de armazenamento**. Isso significa que as empresas não podem reter dados pessoais indefinidamente. O RH deve ter uma política clara sobre por quanto tempo as informações dos candidatos serão mantidas.

Para definir o prazo, a regra é: os dados devem ser guardados apenas pelo tempo necessário para cumprir a sua finalidade original.

- **Candidatos não selecionados:** Se o candidato não consentiu em fazer parte de um banco de talentos para futuras oportunidades, seus dados devem ser excluídos logo após o término do processo seletivo.
- **Banco de talentos:** Se a empresa tem um banco de talentos, o consentimento para manter os dados deve ser explícito, e o prazo de retenção precisa ser comunicado ao candidato. É uma boa prática definir um período de, por exemplo, 1 ou 2 anos e, ao final, entrar em contato para perguntar se ele ainda deseja manter suas informações na base.

O descarte dos dados deve ser feito de forma segura. Em caso de informações físicas, a destruição deve ser

completa (ex.: por meio de trituradoras). Em caso de dados digitais, a exclusão deve ser permanente, sem a possibilidade de recuperação.

Referências

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Guia Orientativo de Segurança da Informação para Agentes de Tratamento de Pequeno Porte. Versão 1.0, Brasília, 2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018.

MONTEIRO, Renato Leite. LGPD - Lei Geral de Proteção de Dados: Teoria e Prática. 2. ed. Salvador: JusPodivm, 2023

Capítulo 4: Divisão de Papéis no Processo Seletivo

Autor: Redação Ela Jurista

LGPD para cada profissional: Recrutador, Gestor de Vagas e DP

A conformidade com a LGPD em um processo seletivo é uma responsabilidade compartilhada. Para que tudo funcione de forma fluida e segura, é essencial que cada profissional entenda seu papel e a importância de suas ações na proteção dos dados dos candidatos. O trabalho em equipe entre o RH, o gestor da vaga e o Departamento Pessoal (DP) é a chave para o sucesso.

O Recrutador: A primeira conexão com a LGPD

O recrutador é a ponte entre a empresa e os candidatos. Por ser o primeiro a lidar com os dados, ele é o ponto de partida para a conformidade.

Seu papel é garantir que:

- **A coleta seja transparente:** Quando divulgar uma vaga, deixe claro quais dados serão coletados e para qual finalidade.
- **O consentimento seja claro:** Obtenha o consentimento do candidato de forma explícita, especialmente se o currículo dele for para um banco de talentos.
- **A informação seja mínima:** Colete apenas os dados estritamente necessários para a vaga. Evite pedir informações que não são relevantes para a avaliação profissional.

- **O compartilhamento seja seguro:** Ao enviar currículos ao gestor, utilize canais seguros (como um sistema de recrutamento) e evite o envio por e-mail, que pode ser menos protegido.

O Gestor de Vagas: O avaliador cuidadoso

O gestor da vaga é o líder que irá tomar a decisão final. Ele recebe os dados dos candidatos e precisa tratá-los com a mesma responsabilidade que o RH.

Seu papel é:

- **Usar os dados com finalidade:** Utilizar as informações recebidas apenas para avaliar a qualificação do candidato para a posição.
- **Evitar a coleta indevida:** Durante a entrevista, foque no perfil profissional. Não solicite informações pessoais irrelevantes, como estado civil, orientação sexual ou filiação política.

- **Garantir o descarte seguro:** Se o candidato não for selecionado, apague ou devolva de forma segura qualquer cópia física ou digital dos documentos que recebeu.

O Departamento Pessoal (DP): O guardião dos dados do colaborador

Quando o candidato é contratado, a LGPD se torna responsabilidade do DP. Este setor lida com os dados mais sensíveis, como informações de saúde, dados bancários e documentos de identificação.

Seu papel é:

- **Usar as bases legais corretas:** Na maioria das vezes, o DP utiliza a **obrigação legal** (como a legislação trabalhista) ou a **execução de contrato** como justificativa para o tratamento dos dados.

- **Proteger os dados:** Armazenar todas as informações dos colaboradores em sistemas seguros, com acesso restrito e senhas fortes.
- **Respeitar os prazos:** Ter uma política clara sobre por quanto tempo os dados de ex-colaboradores serão mantidos e garantir que sejam descartados de forma segura após esse período.

Com uma divisão de papéis bem definida, a LGPD se torna um fluxo natural e integrado ao processo, fortalecendo a segurança e a confiança em todas as etapas.

Referências

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Guia Orientativo sobre Agentes de Tratamento e Encarregado. Versão 2.0, Brasília, 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018.

PINHEIRO, Patrícia Peck. Direito Digital. 8. ed. São Paulo: Saraiva Jur, 2024

Capítulo 5 – Transparência e Comunicação com Candidatos

Autora: Juliana Cristina da Silva e Redação Ela Jurista

5.1 Como informar os candidatos sobre o uso dos dados

Autora: Juliana Cristina da Silva

A transparência é um dos pilares centrais da **LGPD**. Para o candidato, isso significa ter clareza sobre **quais dados estão sendo coletados, como serão utilizados e por quanto tempo ficarão armazenados**. A comunicação clara evita dúvidas, reduz riscos de reclamações e fortalece a confiança do candidato em relação à empresa.

Melhores práticas para comunicação com candidatos:

- **Avisos no início do processo seletivo:** sempre inclua, já na divulgação da vaga, informações sobre como os dados do candidato serão tratados.
- **Linguagem simples e acessível:** evite juridiquês; explique de forma objetiva como as informações serão usadas.
- **Canais de contato abertos:** disponibilize e-mail ou telefone para que o candidato possa tirar dúvidas sobre o uso de seus dados.
- **Feedback transparente:** informe quando e por quanto tempo os dados ficarão armazenados após o término do processo seletivo.

Exemplo prático:

No anúncio da vaga, ao lado do formulário de inscrição, pode constar a seguinte mensagem:

> “Seus dados serão utilizados exclusivamente para este processo seletivo, armazenados de forma segura e descartados em até 12 meses, salvo se você autorizar o uso para futuras oportunidades.”

Essa comunicação direta mostra ao candidato que a empresa leva a sério a proteção de suas informações.

5.2 Políticas de privacidade para processos seletivos

Redação Ela Jurista

Ter uma **política de privacidade específica para recrutamento e seleção** é uma prática recomendada para qualquer empresa que queira alinhar-se à LGPD. Essa política não precisa ser um documento extenso ou

técnico, mas deve ser **objetiva e adaptada ao contexto do RH**.

Elementos essenciais de uma política de privacidade em processos seletivos:

1. **Finalidade:** explicar para que os dados serão usados (ex.: análise de perfil, contato com o candidato).
2. **Base legal:** indicar a hipótese legal (consentimento, obrigação legal, execução de contrato etc.).
3. **Tempo de retenção:** informar por quanto tempo os dados ficarão armazenados.
4. **Direitos do candidato:** explicar como ele pode solicitar exclusão, correção ou acesso aos seus dados.
5. **Segurança:** indicar como a empresa protege as informações coletadas.

A política deve estar **visível e acessível**, seja no site de carreiras da empresa, seja no próprio formulário de inscrição para a vaga.

5.3 Transparência no tratamento de dados sensíveis

Redação Ela Jurista

Dados sensíveis, como informações sobre saúde, deficiência, raça, etnia ou orientação sexual, exigem **maior cuidado e clareza** no tratamento. A LGPD determina que o uso desses dados só pode ocorrer com **consentimento expresso** e para finalidades específicas.

Boas práticas para transparência com dados sensíveis:

- **Informar sempre a finalidade:** deixe claro se o dado está sendo coletado para ações afirmativas

ou cumprimento de cotas.

- **Garantir voluntariedade:** a resposta do candidato deve ser opcional, sem impacto negativo na candidatura.

- **Dar visibilidade à escolha:** explique que o candidato pode retirar seu consentimento a qualquer momento.

- **Detalhar segurança:** informe como esses dados serão armazenados, quem terá acesso e quando serão descartados.

Exemplo prático:

> “Esta informação será utilizada apenas para atendimento à política de inclusão da empresa. Sua resposta é voluntária, não afeta

> sua participação no processo seletivo e pode ser retirada a qualquer momento.”

Com essa postura, a empresa mostra respeito à diversidade e reforça seu compromisso com a ética e a conformidade legal.

Conclusão

Transparência não é apenas uma exigência legal da LGPD, mas também um **diferencial competitivo**. Empresas que comunicam de forma clara como tratam os dados dos candidatos transmitem confiança e fortalecem sua reputação como empregadoras.

Ao adotar **políticas de privacidade bem estruturadas**, **linguagem acessível** e **boas práticas no tratamento de dados sensíveis**, o RH cumpre a legislação e cria uma experiência mais justa e respeitosa para todos os candidatos.

Referências

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Guia Orientativo sobre Agentes de Tratamento e Encarregado. Versão 2.0, Brasília, 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018.

PINHEIRO, Patrícia Peck. Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018 (LGPD). 4. ed. São Paulo: Saraiva Jur, 2024.

Capítulo 6. Compartilhamento de Dados Pessoais

Diretrizes para compartilhamento de dados com terceiros

Autor: Redação Ela Jurista

Em um processo seletivo, é comum o RH precisar compartilhar dados de candidatos com terceiros, como plataformas de recrutamento, consultorias de RH, empresas de *background check* ou até mesmo o gestor da vaga. A LGPD permite esse compartilhamento, mas estabelece regras claras para garantir que os dados não sejam usados de forma indevida.

A base para qualquer compartilhamento é a **finalidade**. O dado deve ser compartilhado apenas para um propósito

específico e legítimo, que esteja alinhado com o motivo original da coleta. O RH precisa ter clareza sobre:

- **Com quem está compartilhando:** É um fornecedor de confiança? Ele também cumpre a LGPD?
- **Quais dados estão sendo compartilhados:** É o mínimo necessário? Não se deve compartilhar mais informações do que o parceiro precisa.
- **Para qual finalidade:** O parceiro usará os dados apenas para a finalidade combinada?

Para assegurar a conformidade, a LGPD exige que a empresa tenha uma **base legal** para o compartilhamento, sendo a mais comum o **consentimento do candidato**. Outras bases, como o **legítimo interesse** ou o **cumprimento de um contrato**, também podem ser usadas, desde que bem documentadas.

Contratos de conformidade com a LGPD para fornecedores e parceiros

A responsabilidade pela proteção de dados não termina quando o dado é enviado a um terceiro. A empresa que coleta a informação é co-responsável por ela. Por isso, ter um contrato robusto com fornecedores e parceiros é fundamental.

Este contrato deve incluir cláusulas específicas que garantam que o parceiro também cumpre a LGPD. As cláusulas essenciais incluem:

- **Obrigação de sigilo:** O fornecedor deve se comprometer a manter a confidencialidade das informações.
- **Limitação do uso dos dados:** O contrato deve especificar que o fornecedor só pode usar os dados para a finalidade acordada e pelo tempo necessário.
- **Medidas de segurança:** O parceiro deve detalhar as medidas técnicas e administrativas que usa para proteger os dados.

- **Responsabilidade em caso de incidente:** O contrato deve prever as responsabilidades e sanções em caso de vazamento de dados ou falha de segurança.
- **Devolução ou exclusão dos dados:** Ao final do contrato, o parceiro deve se comprometer a devolver ou excluir todos os dados de forma segura.

Regras específicas para o compartilhamento de dados sensíveis e de diversidade

O compartilhamento de dados sensíveis (como os de saúde) ou de diversidade exige um cuidado extra. Se a empresa utiliza esses dados, por exemplo, em programas de inclusão, o compartilhamento só pode ocorrer com o **consentimento específico e destacado do titular**.

No contrato com o fornecedor, as cláusulas devem ser ainda mais rigorosas:

- O documento deve deixar claro que os dados são sensíveis e que o tratamento está alinhado a uma finalidade legítima.
- O acesso deve ser restrito a um grupo seleto de pessoas, mesmo dentro da equipe do fornecedor.

Seguindo essas diretrizes, o RH consegue garantir que o compartilhamento de dados seja feito com segurança e transparência, protegendo os candidatos e a própria empresa.

Referências

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Guia Orientativo sobre Agentes de Tratamento e Encarregado. Versão 2.0, Brasília, 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018.

PINHEIRO, Patrícia Peck. Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018 (LGPD). 4. ed. São Paulo: Saraiva Jur, 2024.

Capítulo 7. Direitos dos Candidatos

Autora: Régia Freitas

A Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, trouxe mudanças significativas na forma como as empresas tratam dados pessoais. No contexto de recrutamento e seleção, entender e aplicar as diretrizes da LGPD é fundamental para garantir segurança, transparência e conformidade legal.

Este manual tem o objetivo de orientar empresas e candidatos sobre boas práticas, direitos e procedimentos relacionados ao tratamento de dados pessoais, promovendo uma interação ética e segura no mercado de trabalho.

Benefícios da LGPD para Empresas.

- **Maior Confiança:** Demonstra compromisso com a privacidade e proteção de dados.
- **Redução de Riscos:** Diminui a exposição a sanções legais e prejuízos reputacionais.
- **Diferencial Competitivo:** Empresas alinhadas às práticas de proteção de dados são vistas como mais modernas e confiáveis.

Direitos dos Candidatos

1.1 - Direito de Acesso, Retificação e Exclusão dos Dados.

Todo candidato tem o direito garantido pela LGPD de acessar, corrigir e solicitar a exclusão de seus dados pessoais mantidos por uma empresa durante um processo seletivo.

- Acesso: Permite ao candidato saber quais dados pessoais a empresa tem sobre ele.
- Retificação: Possibilita a correção de dados incorretos ou desatualizados.
- Exclusão: Garante o direito de solicitar a exclusão de dados pessoais, salvo quando houver obrigação legal de armazenamento.

1.1.1 - Explicação dos Direitos dos Candidatos de Acessar, Corrigir e Excluir seus Dados Pessoais.

A proteção de dados pessoais é um direito fundamental garantido pela Constituição Federal e pela Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018. No contexto do recrutamento e seleção, os candidatos precisam compreender como seus dados pessoais são tratados pelas empresas, além de conhecer e exercer seus direitos. Garantir esses direitos não é

apenas uma obrigação legal, mas também uma prática que reforça a ética e a transparência nos processos seletivos.

A LGPD impacta diretamente as atividades de recrutamento, pois estabelece regras claras para a coleta, armazenamento, tratamento e exclusão de dados pessoais dos candidatos. Desde informações básicas, como nome e telefone, até dados sensíveis, como saúde e orientação sexual, a legislação busca assegurar que essas informações sejam tratadas com segurança e respeito.

É fundamental que tanto os candidatos quanto as empresas compreendam seus papéis nesse processo: os candidatos, como titulares dos dados, devem saber como proteger suas informações e exercer seus direitos; as empresas, como controladoras, precisam garantir que os

dados sejam tratados de forma ética, segura e conforme a legislação vigente.

Nas próximas seções, abordaremos os principais direitos dos candidatos e como as empresas podem assegurar o cumprimento dessas garantias, promovendo uma relação mais transparente e respeitosa durante os processos seletivos.

1.1.2 - Compreender os Direitos dos Candidatos e Como Garanti-los.

Conhecer seus direitos é fundamental para garantir uma participação segura e transparente nos processos seletivos. As empresas devem informar claramente como os dados são tratados e disponibilizar canais para que os candidatos possam exercer seus direitos.

Exemplo prático: Se você percebe que seu e-mail está incorreto, pode solicitar à empresa a correção desta informação. Caso desista de um processo seletivo, pode pedir a exclusão de seus dados.

Procedimento para os Candidatos Realizarem suas Solicitações.

2.1 - Passos e Práticas Recomendadas para que Candidatos Façam Solicitações de Acesso, Correção ou Exclusão de seus Dados.

1. **Identifique a empresa:** Certifique-se de ter os contatos corretos do setor de recursos humanos ou do encarregado de dados pessoais.

2. **Envie uma solicitação formal:** Inclua no e-mail ou documento:
    a. Nome completo
    b. Documento de identificação (quando solicitado)
    c. Pedido claro (acesso, correção ou exclusão)
3. **Aguarde a resposta:** A empresa deve responder dentro de um prazo razoável, geralmente até 15 dias úteis.
4. **Confirme a execução:** Verifique se a alteração ou exclusão foi efetivada.

Dica: Guarde registros de suas solicitações para evitar problemas futuros.

2.1.2 - Saber como Processar e Atender Adequadamente às Solicitações dos Candidatos.

Empresas devem ter um processo claro para receber, validar e responder às solicitações dos candidatos. Isso inclui:

- Confirmar o recebimento da solicitação.
- Validar a identidade do candidato.
- Garantir a segurança durante a comunicação e manuseio dos dados.

Exemplo prático: Uma empresa deve oferecer um canal direto para solicitações de dados, como um e-mail específico para privacidade ou um formulário seguro.

Referências

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Guia Orientativo sobre Agentes de Tratamento e o Encarregado. Versão 2.0, Brasília, 2024.

BRASIL. Constituição (1988). Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais. Diário Oficial da União, Brasília, DF, 11 fev. 2022.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018.

Parte II– Governança, Riscos e Tecnologia

Capítulo 8 Confidencialidade e Sigilo

Autora Régia Freitas

Garantindo o Sigilo das Informações dos Candidatos.

1.1 - Importância da Confidencialidade nos Processos Seletivos.

A confidencialidade é essencial para preservar a integridade e privacidade dos dados pessoais dos candidatos, garantindo segurança e respeito durante os processos seletivos.

1.2 - Medidas para Garantir que as Informações dos Candidatos sejam Mantidas em Sigilo.

As empresas devem adotar medidas para proteger os dados pessoais dos candidatos:

- Controle de acesso: Apenas pessoas autorizadas devem ter acesso aos dados.
- Criptografia: Proteção das informações por meio de códigos digitais.
- Treinamento de funcionários: Capacitação para manuseio seguro dos dado

1.3 - Conhecer as Práticas para Assegurar a Confidencialidade das Informações dos Candidatos.

Candidatos podem adotar algumas práticas para proteger suas informações:

- Certificar-se de que estão compartilhando dados apenas com empresas confiáveis.
- Perguntar sobre as políticas de segurança da informação.

Exemplo prático: Prefira enviar currículos para e-mails institucionais da empresa.

1.4 - Medidas de Confidencialidade para Dados Sensíveis.

Dados sensíveis incluem informações sobre saúde, origem étnica, opinião política ou crenças religiosas. Esses dados exigem um nível elevado de segurança.

1.5 - Estratégias Adicionais para Proteger a Confidencialidade de Dados Sensíveis

- Segregação de informações: Manter dados sensíveis separados.

- Consentimento específico: Solicitar autorização clara do candidato para coleta e uso desses dados.
- Armazenamento seguro: Utilização de plataformas com alto nível de segurança.

1.6 - Entender como Proteger a Confidencialidade dos Dados Sensíveis em Processos Seletivos.

Garantir a confidencialidade dos dados sensíveis significa:

- Manter essas informações restritas ao setor responsável.
- Adotar tecnologias seguras para armazenamento.
- Evitar a circulação desnecessária dos dados dentro da empresa.

Exemplo prático: Se você informar em seu currículo que possui uma deficiência física, a empresa deve tratar essa informação com o máximo sigilo.

Glossário

- **Dados Pessoais:** Qualquer informação relacionada a uma pessoa identificada ou identificável.
- **Dados Sensíveis:** Informações sobre origem racial, saúde, religião, orientação sexual, opinião política e outros dados protegidos pela LGPD.
- **Titular dos Dados:** Pessoa a quem os dados pessoais se referem.
- **Controlador:** Entidade que decide como e por que os dados pessoais são processados.

- **Consentimento:** Permissão dada pelo titular para o tratamento de seus dados pessoais.

Referências Normativas

- Lei Geral de Proteção de Dados (Lei nº 13.709/2018) - Texto Integral
- Autoridade Nacional de Proteção de Dados (ANPD) - Site Oficial

Modelos de Solicitação

Modelo 1: Solicitação de Acesso a Dados

Assunto: Solicitação de Acesso a Dados Pessoais Prezado(a) [Nome da empresa], Eu, [Nome completo], CPF [número], venho solicitar acesso aos meus dados pessoais tratados por esta empresa, conforme o artigo 18 da LGPD (Lei nº 13.709/2018).

Aguardo retorno dentro do prazo legal.
Atenciosamente,
[Nome]
[Telefone]

Modelo 2: Solicitação de Retificação de Dados

Assunto: Solicitação de Retificação de Dados Pessoais

Prezado(a) [Nome da empresa],

Eu, [Nome completo], CPF [número], venho solicitar a correção dos seguintes dados pessoais que se encontram incorretos/desatualizados:

- Dado atual: [Exemplo: e-mail incorreto]
- Correção solicitada: [Novo e-mail correto]

Aguardo confirmação da retificação.

Atenciosamente,
[Nome]
[Telefone]
[E-mail]

Checklist para Empresas

- Designar um encarregado de proteção de dados.
- Manter registros atualizados sobre o tratamento de dados.
- Realizar treinamentos periódicos para equipes de recrutamento.
- Disponibilizar canais claros para solicitações dos candidatos.
- Adotar tecnologias seguras para armazenamento e tratamento dos dados.

Conclusão

A implementação adequada da LGPD no processo de recrutamento e seleção é fundamental para garantir a transparência e a segurança no tratamento de dados

pessoais dos candidatos. Este manual não apenas orienta as empresas a adotarem práticas conforme à legislação, mas também capacita os candidatos a compreenderem e exercerem seus direitos. A construção de um ambiente ético e transparente contribui para processos seletivos mais seguros e confiáveis.

Com as informações aqui apresentadas, espera-se que as empresas possam desenvolver políticas robustas de proteção de dados e que os candidatos se sintam mais seguros ao participarem de processos seletivos, sabendo que seus dados estão protegidos.

O respeito à privacidade não é apenas uma obrigação legal, mas um diferencial que reforça a credibilidade e a reputação das empresas no mercado.

Referências

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Guia Orientativo de Segurança da Informação para Agentes de Tratamento de Pequeno Porte. Versão 1.0, Brasília, 2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018.

PINHEIRO, Patrícia Peck. Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018 (LGPD). 4. ed. São Paulo: Saraiva Jur, 2024.

Capítulo 9. Identificação de Riscos no Tratamento de Dados Pessoais e Avaliação de Impacto de Proteção de Dados para Processos Seletivos

Autora Giuliana Visconde

O processo de recrutamento e seleção envolve o tratamento de uma ampla variedade de dados pessoais, como: nome completo, idade, gênero, endereço, telefone, e-mail, CPF, RG, PIS, CNH, RNE, passaporte, carteira de trabalho, reservista, remuneração, dados bancários, título de eleitor, certidão de nascimento e casamento, raça, nacionalidade, naturalidade, sexo, estado civil, escolaridade, histórico profissional, cursos e treinamentos, idiomas e todas as informações que forem apresentadas no currículo, e até mesmo dados sensíveis,

como laudos médicos ou antecedentes criminais em casos específicos.

Considerando a quantidade de dados coletados e a consequente sensibilidade, é de extrema importância que essas atividades sejam devidamente estruturadas e mapeadas com o objetivo de reduzir riscos. Este capítulo aborda como o departamento de Recursos Humanos (RH) deve identificar e mitigar os riscos associados ao tratamento desses dados, alinhando-se à Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018), bem como a metodologia para a realização de uma Avaliação de Impacto de Proteção de Dados (RIPD), conforme o art. 38 da LGPD.

2. Finalidades do Tratamento de Dados no RH

O primeiro passo para realizar o tratamento de dados pessoais de forma segura é entender a legitimidade da coleta e suas finalidades, garantindo que as atividades

exercidas pela área que contenham o tratamento de dados pessoais, estejam sempre pautadas na legislação. Levando em consideração as atividades exercidas de maneira geral pela área, podemos listar:

1. **Recrutamento e seleção:** que compreendem as atividades de agendamento de entrevistas e realização de processos seletivos, possuindo como base legal o “legítimo interesse”.

2. **Admissão e Demissão:** que compreende as atividades de celebração do contrato de trabalho e organização de ficha, arquivos e registros do colaborador admitido, realização de exame admissional, bem como a rescisão contratual e exame demissional, possuindo como base legal a execução de contrato e cumprimento de obrigação legal.

3. **Armazenamento dos registros de ex-funcionários:** tratamento feito com base no cumprimento de obrigação legal e exercício regular de direito.

4. **Pagamentos:** que compreende o pagamento de salários, incentivos e/ou qualquer remuneração devida ao colaborador, pautado na execução de contrato.

5. **Prestação de contas:** que compreende compartilhamento de dados com autoridades públicas para, por exemplo, realização do DIRF, REINF e eSocial, pautado no cumprimento de obrigação legal ou regulatória.

3. Identificação de Riscos no Tratamento de Dados Pessoais

Importante pontuar que a LGPD trouxe para além dos direitos do titular como, por exemplo: (a) direito de obter

determinadas informações sobre quais dados pessoais nós obtemos e como estamos utilizando-os; (b) solicitar a correção de seus dados pessoais; (c) se opor a determinado tratamento, ou fazer uma requisição para anonimização, bloqueio ou exclusão de determinados dados; (d) solicitar a revogação do seu consentimento para determinadas atividades de tratamento opcionais; (e) obter uma cópia dos seus dados pessoais ou requisitar que eles sejam transferidos a um terceiro na medida autorizada pela Autoridade Nacional de Proteção de Dados (ANPD), a LGPD trouxe também, um conjunto de melhores práticas que visam garantir que os direitos sejam cumpridos e que os dados estejam submetidos aos menores riscos possíveis. Podemos listar algumas das melhores práticas sugeridas:

- Acesso à base de dados restrito às empresas e aos profissionais autorizados;
- Criptografia ponta a ponta;

- Monitoramento aos acessos e às ações realizadas em relação aos Dados Pessoais;
- Definição de uma clara distinção de funções e competências relativas às categorias de pessoas responsáveis ou envolvidas nos sistemas;
- Auditoria regular interna e externa de proteção de Dados Pessoais; e
- Adoção de procedimentos preventivos contra incidentes de segurança da informação.

No art. 46 da LGPD, há a obrigação dos agentes de tratamento adotarem medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas, ou seja, vulnerabilidades que podem expor os dados dos titulares a tratamento inadequado ou ilícito.

O gerenciamento de riscos no âmbito da segurança da informação consiste no processo de identificar, quantificar e gerenciar os riscos relacionados a fim de obter- se um equilíbrio eficiente entre a concretização de oportunidades de ganhos e a minimização de vulnerabilidades e perdas.

Neste sentido, para que sejam tomadas medidas aptas a prevenir a ocorrência de danos aos titulares em virtude de suas atividades, é necessário realizar a identificação de riscos para que se possa analisar todo o ciclo de vida dos dados pessoais durante o processo seletivo, desde a coleta até o descarte.

Os principais riscos associados ao tratamento de dados incluem:

- **Coleta excessiva de dados**: Solicitar informações não essenciais sem justificativa legal.

- **Armazenamento inadequado**: Falhas de segurança que levam ao acesso não autorizado ou perda de dados.
- **Compartilhamento indevido**: Divulgação não autorizada a terceiros, como empresas de recrutamento.
- **Retenção prolongada**: Manutenção de dados após o fim do processo seletivo sem consentimento ou base legal.
- **Falta de transparência**: Ausência de informações claras aos candidatos sobre o uso dos dados.

Para mitigar esses riscos, o RH deve mapear os fluxos de dados considerando:

- **Identificação de dados coletados**: Listar tipos de dados pessoais.
- **Definição de finalidades**: Garantir que cada dado seja coletado para uma finalidade específica, clara e legítima.

- **Mapeamento de envolvidos**: Identificar agentes de tratamento e terceiros com acesso aos dados.

Além disso, é de suma importância a criação de uma metodologia objetiva de avaliação para que possa mitigar os riscos associados ao tratamento de dados pessoais, principalmente em atividades que possam implicar alto risco aos direitos e liberdades dos titulares de dados. A adoção de medidas organizacionais para mitigação de riscos e redução de vulnerabilidades, transparência demonstrando o compromisso com a proteção de dados pessoais e a conformidade legal traz benefícios não somente para os titulares, mas também às empresas na medida em que reduz riscos de aplicações penalidades e sanções pela ANPD, bem como fortalece a relação com titulares de dados e parceiros comerciais.

Não existe uma metodologia específica obrigatória, sendo do controlador a responsabilidade

pela decisão da metodologia a ser adotada de forma que a gestão de risco pode ser feita por diferentes metodologias. Caberá então, ao controlador identificar o maior número possível de fatores, principalmente os mais relevantes, que possam afetar os dados pessoais que serão tratados e registrá-los de maneira justificada para que possa demonstrar que as decisões tomadas em relação à gestão de risco foram as mais adequadas com base nas informações disponíveis.

4. Documentos Necessários para Mitigação de Riscos

A LGPD exige que organizações e/ ou agentes de tratamentos adotem medidas para mitigar os riscos no tratamento de dados pessoais e demonstrem conformidade com a legislação, além de garantir a

transparência, segurança e a aplicação dos princípios da lei. Podemos citar diversos documentos que foram trazidos pelo legislador com o objetivo de assegurar tanto a proteção de direitos individuais, quanto direitos coletivos ao proteger os direitos fundamentais de liberdade e privacidade das pessoas, bem como o livre desenvolvimento da personalidade de cada indivíduo.

Os principais documentos que devem ser produzidos para tratar riscos relacionados ao tratamento de dados pessoais, são:

- **Política de Privacidade:** (Art. 6º da lei) Pautado na transparência e respeito aos princípios da LGPD visa comunicar aos titulares como os seus dados pessoais são tratados, incluindo as finalidades, bases legais, e direitos garantidos pela LGPD e como exercê-los Informações sobre compartilhamento e transferência

internacional de dados e detalhes sobre segurança da informação.

- **Registros de Atividades de Tratamento (ROPA):** Disposto no Artigo 37 da LGPD, possui como objetivo documentar todas as atividades de tratamento de dados realizadas por uma organização contendo as finalidades do tratamento; as categorias de dados e de titulares; informações acerca do compartilhamento de dados e transferências internacionais, bem como medidas de segurança adotadas. Funcionam, na prática, como um inventário detalhado que descreve todas as atividades de tratamento conduzidas por uma organização desde a coleta dos dados até a sua exclusão.

- **Políticas Internas de Segurança e Proteção de Dados:** Com fulcro no Art. 46 da LGPD, possui

como objetivo definir normas e práticas internas de uma organização para proteger dados pessoais e mitigar riscos de incidentes de segurança. São informações essenciais que devem constar dessas políticas o controle de acesso às informações, o gerenciamento de vulnerabilidades adotadas, os procedimentos em caso de vazamentos e informações relacionadas ao treinamento de colaboradores.

- **Plano de Resposta a Incidentes de Segurança:** com base legal no art. 48 da LGPD, tem como objetivo estabelecer um plano de ação em caso de vazamentos ou violações de dados pessoais, garantindo a notificação à ANPD e aos titulares, listando ações corretivas adotadas para reduzir o impacto e o registro detalhado de incidentes.

- **Relatório de Impacto à Proteção de Dados (RIPD):** O RIPD é o documento exigido pela LGPD para mitigar riscos ao tratar dados pessoais. Previsto no Art. 38 da LGPD, deve conter minimamente, a descrição dos tratamentos realizados, os riscos identificados e medidas de mitigação e a conformidade do tratamento com os princípios da LGPD. Eles correspondem a documentos que detalham os riscos e impactos de determinadas atividades de tratamento de dados pessoais, bem como as medidas adotadas para mitigá-los.

5. Avaliação de Impacto de Proteção de Dados (RIPD)

O RIPD deve ser produzido pelo controlador sempre que o tratamento envolve alto risco aos direitos e liberdades dos titulares e/ou quando solicitado pela Autoridade Nacional de Proteção de Dados (ANPD).

Além disso, a ANPD pode determinar situações específicas em que o RIPD será obrigatório, por meio de regulamentações adicionais.

O controlador dos dados pessoais é o responsável por elaborar o RIPD. Em muitos casos, o Encarregado de Dados (DPO) terá um papel fundamental na coordenação desse processo, junto com as áreas técnicas, jurídicas e de segurança da informação.

Um conceito que pode gerar confusão aos operadores do direito e/ou profissionais envolvidos no tratamento de dados pessoais é a diferença entre RIPD e ROPA. Enquanto o ROPA é um registro mais amplo, que documenta todas as atividades de tratamento realizadas por uma organização, o RIPD é focado na avaliação de riscos e impactos de atividades específicas de tratamento de dados.

Neste sentido, pela LGPD, o RIPD deverá ser gerado apenas para os tratamentos que puderem criar riscos para o titular a risco e conter, no mínimo, "a descrição dos tipos de dados coletados, a metodologia utilizada para coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mitigação de riscos adotados" (art. 38, parágrafo único, da LGPD). A LGPD lista, ainda, situações específicas em que o RIPD poderá ser exigido pela ANPD, como: (a) operações de tratamento efetuadas para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (art. 4º, § 3º); (b) quando o tratamento tiver como fundamento a hipótese de interesse legítimo (art. 10, § 3º); (c) para agentes do Poder Público, incluindo determinação quanto à publicação do RIPD (art. 32); e (d) para controladores em geral, quanto às suas operações de

tratamento, incluindo as que envolvam dados pessoais sensíveis (art. 38).

Veja um fluxograma disponibilizado pela ANPD para melhor compreensão:

Fonte: Autoridade Nacional de Proteção de Dados.

Assim, considerando especificamente as atividades envolvidas no processo de recrutamento e seleção de candidatos pela área de recursos humanos nas organizações, entendemos ser essencial o conhecimento e elaboração dos RIPDs pelos profissionais envolvidos nestas atividades.

Recomenda-se elaborar o RIPD antes de o controlador iniciar o tratamento dos dados pessoais para a finalidade desejada, justamente para que ele possa avaliar, de antemão, os possíveis riscos associados a esse tratamento.

Dessa forma, o controlador conseguirá, antes mesmo de usar os dados pessoais para aquela finalidade, identificar a probabilidade de ocorrência de cada fator de risco e o seu impacto sobre as liberdades e direitos fundamentais dos titulares e adotar as medidas, as

salvaguardas e os mecanismos de mitigação de risco apropriados à hipótese. Entretanto, caso não seja possível elaborar o RIPD antes do início do tratamento, recomenda-se elaborá-lo assim que se identificar um tratamento que possa gerar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD e às liberdades civis e aos direitos fundamentais do titular de dados. De todo modo, o controlador deverá, ainda, elaborar o RIPD caso seja solicitado pela ANPD.

6. Etapas para Elaboração do RIPD:

1. **Descrição dos tipos de dados coletados**:
    - Dados de identificação (ex.: nome, CPF, e-mail).
    - Dados sensíveis (ex.: informações de saúde ou antecedentes criminais, quando aplicável).
2. **Medidas de Mitigação de Riscos**:

    - Identificar e categorizar riscos de acordo com probabilidade e gravidade.
    - Implementar soluções como criptografia, anonimização e controles de acesso.
3. **Metodologia para Garantia de Segurança**:
    - Monitoramento e auditorias periódicas.
    - Transparência com os titulares sobre o ciclo de vida dos dados.

7. Exemplo Prático e modelo de RIPD:

Uma empresa coletou antecedentes criminais de todos os candidatos, independentemente do cargo. Isso levou a uma sanção pela ANPD por coleta excessiva e sem base legal. A solução foi implementar uma análise caso a caso, solicitando apenas quando justificável.

Contexto:

- Atividade de tratamento: Recrutamento e seleção de candidatos.

- Finalidade: Avaliar e selecionar profissionais qualificados, garantindo que os candidatos atendam aos requisitos técnicos e comportamentais necessários para os cargos disponíveis.
- Controlador: Empresa ABC Ltda, responsável pela decisão sobre o tratamento dos dados.
- Operador: Software de recrutamento XYZ, que processa os dados sob instruções do controlador.

Descrição dos Dados Coletados:

- Dados pessoais: Nome, e-mail, telefone, endereço, experiência profissional, formação acadêmica.
- Dados sensíveis: Informações de saúde (exclusivamente para candidatos a vagas destinadas a pessoas com deficiência – PCD) e Antecedentes criminais (somente para vagas que justifiquem a necessidade dessa informação).

Riscos Identificados:

- Coleta de Dados Não Essenciais: A coleta indiscriminada de antecedentes criminais, sem avaliação do cargo ou finalidade específica, representou um desrespeito aos princípios de minimização e adequação previstos na LGPD.

- Armazenamento Sem Criptografia Adequada: Dados sensíveis estavam suscetíveis a acessos não autorizados, expondo a empresa a riscos de vazamento.

- Compartilhamento Indevido de Currículos: Ausência de mecanismos que garantissem a autorização prévia para o compartilhamento de dados de candidatos com terceiros.

Medidas de Mitigação:

- Revisão de Campos no Sistema de Recrutamento: Redefinição dos dados obrigatórios solicitados, incluindo a exclusão de antecedentes criminais em casos sem justificativa. A coleta passou a ser feita apenas mediante análise prévia da necessidade, baseada na função a ser desempenhada.

- Implementação de Criptografia: Garantia de proteção dos dados armazenados com protocolos robustos de segurança.

- Contratos com Fornecedores: Estabelecimento de cláusulas contratuais específicas com operadores, assegurando a confidencialidade e o cumprimento da LGPD.

Metodologia:

- Auditorias Regulares: Realização de auditorias semestrais nos sistemas de tratamento de dados

para identificar vulnerabilidades e promover melhorias contínuas.

- Treinamento da Equipe de RH: Capacitação dos colaboradores para adoção de boas práticas de proteção de dados e conscientização sobre os riscos associados à coleta e ao tratamento inadequados.

- Autenticação Multifatorial: Uso de autenticação em dois fatores para acesso aos sistemas de recrutamento e armazenamento de dados, reduzindo o risco de acessos indevidos.

Conclusão do RIPD: A empresa adotou um modelo de análise caso a caso para a coleta de antecedentes criminais, solicitando essa informação apenas quando justificável e pertinente ao cargo em questão. Foram definidos critérios objetivos para tal análise, garantindo que a coleta ocorresse em conformidade com os princípios da finalidade e da minimização. Com as

medidas adotadas, a empresa conseguiu reduzir os riscos a níveis aceitáveis, garantindo a conformidade com a LGPD e evitando novas sanções. Além disso, o aprimoramento das práticas de proteção de dados fortaleceu a confiança de candidatos, colaboradores e parceiros comerciais, contribuindo para a sustentabilidade e a reputação positiva da organização.

8. Conclusão

A criação de um RIPD eficiente exige planejamento estratégico, profundo entendimento das exigências legais e a aplicação de práticas adequadas de proteção de dados. Além de assegurar a conformidade com a LGPD, é essencial adotar medidas preventivas, como a revisão contínua de processos e o treinamento dos colaboradores. Essas ações não apenas reforçam a segurança dos dados pessoais e reduzem a probabilidade de incidentes, como também protegem os direitos dos titulares e aprimoram a imagem da

organização perante colaboradores e parceiros de negócios.

Nesse contexto, o setor de Recursos Humanos desempenha um papel fundamental, sendo o responsável por garantir que todos os fluxos de dados estejam alinhados às exigências legais. Para isso, é indispensável que o RH seja devidamente capacitado, faça uso de ferramentas tecnológicas apropriadas, mantenha uma comunicação transparente com os titulares dos dados e fomente uma cultura organizacional que priorize a proteção de informações pessoais.

A implementação eficaz dessas práticas não só proporciona maior segurança jurídica e previne sanções regulatórias, mas também fortalece a confiança de candidatos e parceiros. Como resultado, contribui diretamente para a reputação, sustentabilidade e sucesso da organização.

6. Referências

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

ANPD. GUIA ORIENTATIVO SEGURANÇA DA INFORMAÇÃO PARA AGENTES DE TRATAMENTO DE PEQUENO PORTE. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-vf.pdf

ANPD. Guia orientativo para a elaboração de relatório de impacto à proteção de dados pessoais. Disponível em: https://www.gov.br/anpd.

PINHEIRO, Renato Monteiro. "LGPD – Lei Geral de Proteção de Dados: Teoria e Prática". Editora Revista dos Tribunais, 2021.

Banco Central do Brasil. Relatório de Impacto a Proteção de Dados Pessoais. Disponível em: ttps://www.bcb.gov.br/content/acessoinformacao/lgpd_docs/relatorio_de_impacto_a_protecao_de_dados_pessoais.pdf

LGPD: Você sabe o que ROPA e RIPD significam e quando prepará-los?. Disponível em https://www.machertecnologia.com.br/lgpd-ropa-ripd/#:~:text=O%20RIPD%20ser%C3%A1%20necess%C3%A1rio%20sempre,10%20da%20LGPD).

GET PRIVACY. O que é e como elaborar o Relatório de Impacto à Proteção de Dados Pessoais. Disponível em: https://getprivacy.com.br/relatorio-de-impacto-lgpd/#elementor-toc__heading-anchor-1

DPO.NET. Matriz de riscos. Disponível em: https://blog.dponet.com.br/matriz-de-risco-o-que-e-e-como-aplicar-na-sua-empresa/

Capítulo 10. Gerenciamento de Incidentes

Autora: Sarah Gobo

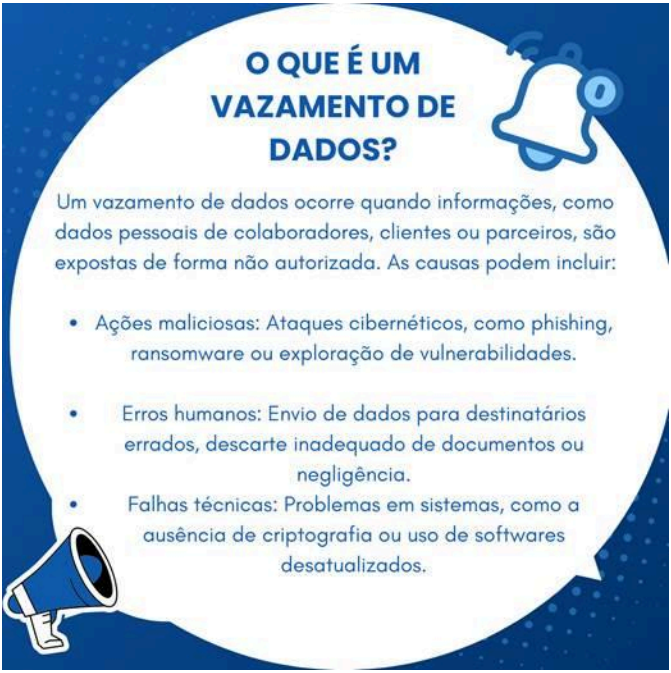
A Lei Geral de Proteção de Dados (LGPD) não define explicitamente o termo "incidente de segurança", mas seu significado pode ser inferido a partir do artigo 46. Esse artigo impõe ao controlador e ao operador a obrigação de adotar medidas técnicas e administrativas para proteger os dados pessoais contra acessos não autorizados e incidentes como destruição, perda, alteração, comunicação ou difusão indevida.

Um incidente de segurança abrange tanto o vazamento de informações quanto o acesso indevido a documentos físicos, como currículos e atestados, por pessoas não autorizadas. Já o artigo 48 estabelece a obrigatoriedade

de comunicar a Autoridade Nacional de Proteção de Dados (ANPD) sempre que o incidente representar risco ou dano relevante aos titulares.

DE MANEIRA RESUMIDA, PODE-SE DIZER QUE O INCIDENTE DE SEGURANÇA É QUALQUER EVENTO QUE COMPROMETA A SEGURANÇA DOS DADOS PESSOAIS EM MEIOS FÍSICOS OU DIGITAIS.

Outro ponto relevante a ser entendido é que a gravidade do incidente é avaliada considerando o potencial **risco ou dano** aos direitos dos titulares dos dados. Para isso, a ANPD pode determinar os critérios para essa avaliação, como o número de titulares afetados, o tipo de dados expostos e a possibilidade de prejuízos financeiros, reputacionais ou de outra natureza.



Como Lidar com Vazamentos de Dados: Procedimentos e Medidas Essenciais para Proteger Informações Comprometidas

A proteção de dados no setor de Recursos Humanos (RH) exige medidas preventivas rigorosas, pois a quantidade de informações pessoais e sensíveis

tratadas torna essa área especialmente vulnerável a incidentes de segurança. Mesmo com práticas de proteção bem implementadas, é impossível garantir 100% de segurança. Por isso, é essencial adotar uma abordagem ampla e detalhada para a gestão de incidentes, considerando tanto o meio digital quanto o físico.

Os dados pessoais tratados pelo RH incluem currículos, históricos trabalhistas e avaliações de desempenho, além de informações sensíveis, como exames médicos e atestados. A falta de proteção adequada pode levar a acessos não autorizados, vazamentos e prejuízos significativos.

Meios Físicos

Documentos em papel, como currículos, contratos e laudos médicos, ainda são comuns no RH e apresentam

riscos específicos, como perdas, furtos ou manuseio indevido. Para minimizar essas ameaças, é fundamental:

- Utilizar armários com trancas e restringir o acesso às áreas onde os documentos são armazenados.
- Implementar uma política de mesa limpa, evitando o acúmulo de papéis desnecessários.
- Adotar métodos seguros de descarte, como fragmentação ou shredding, para documentos que não são mais necessários.

Ambiente Digital

Os sistemas digitais do RH, como bancos de currículos e plataformas de gestão de talentos, também enfrentam riscos, como ataques cibernéticos, falhas de configuração e erros humanos. Para mitigar esses problemas, recomenda-se:

- Utilizar senhas fortes e autenticação multifator.
- Implementar monitoramento contínuo para identificar acessos suspeitos.
- Manter backups regulares para recuperação de dados em caso de falha.

Capacitação e Resposta a Incidentes

A capacitação da equipe é essencial para garantir um gerenciamento eficaz de incidentes. Os profissionais de RH devem estar preparados para identificar riscos, reconhecer ataques cibernéticos e lidar corretamente com documentos sensíveis. Além disso, devem ser treinados para agir rapidamente ao detectar um incidente, garantindo uma resposta estruturada e eficiente.

Ter um plano de resposta bem definido é crucial. Isso significa que, ao ocorrer um incidente, a equipe já sabe quais passos seguir, quais ações tomar e quem deve ser notificado. Uma resposta ágil e organizada minimiza os impactos do incidente e protege a empresa contra danos maiores.

Ao adotar essas medidas, o RH fortalece a proteção dos dados e reduz significativamente os riscos de segurança, demonstrando compromisso com a privacidade e conformidade legal.

Para isso, é importante ter em mente 3 passos simples ao se deparar com um incidente de segurança:

Além das medidas operacionais, a gestão de incidentes no RH deve considerar as implicações éticas e legais, especialmente a conformidade com a Lei Geral de Proteção de Dados (LGPD). Mais do que uma obrigação legal, a transparência e a responsabilidade no tratamento

das informações são fundamentais para manter a confiança dos titulares.

Para isso, é essencial que a coleta de dados seja limitada ao necessário para a finalidade pretendida e que a empresa adote práticas de accountability, demonstrando compromisso com a proteção das informações.

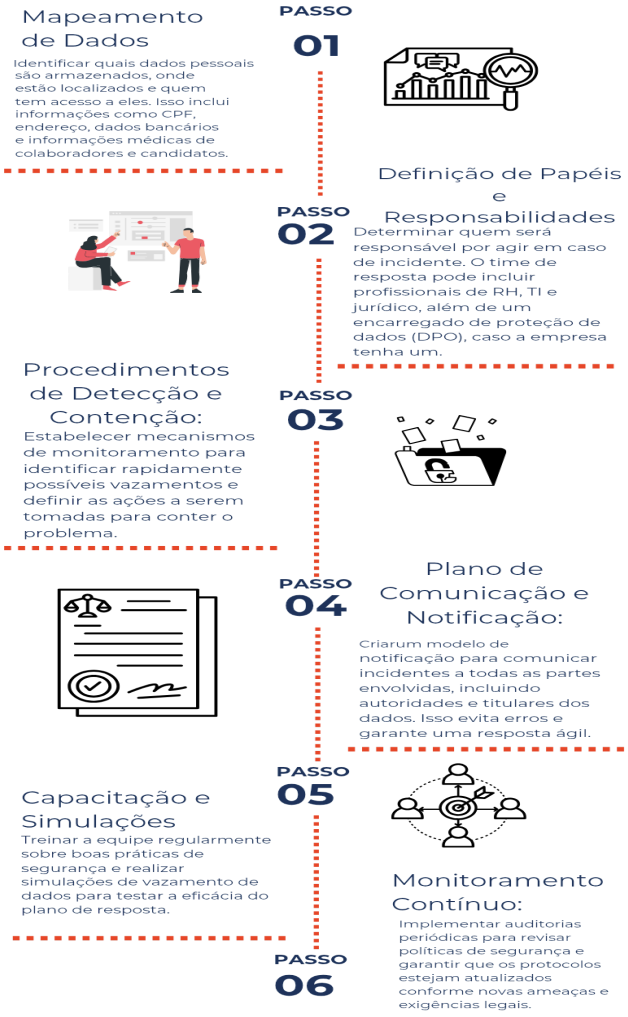
Uma gestão eficiente de incidentes exige atenção aos detalhes, integração de políticas de segurança robustas, capacitação contínua da equipe e uso estratégico da tecnologia. Com essas práticas, o RH fortalece a proteção dos dados e garante uma abordagem ética e segura no manuseio das informações.

Plano de Resposta a Incidentes Envolvendo Dados Pessoais e Dados Sensíveis

Diante da crescente digitalização das informações no setor de RH, a implementação de um plano de resposta a incidentes é essencial para lidar com situações críticas de maneira eficaz. Esse plano deve ser estruturado para garantir que a equipe saiba exatamente como agir em caso de vazamento de dados pessoais e sensíveis.

Como forma de facilitar a elaboração dele segue abaixo uma esquema-sugestão de como elaborá-lo em 6 passos:

Ainda, para casos em que seja necessário a comunicação do incidente de segurança, sugere-se os seguintes modelos:



Fonte: Criado pela autora

Assunto: Comunicação sobre Incidente de Segurança de Dados

Prezado(a) [Nome do Cliente],

Gostaríamos de informá-lo(a) sobre um incidente de segurança de dados ocorrido em [data do incidente], que pode ter impactado algumas informações relacionadas ao seu cadastro em nossa empresa.

Identificamos que houve um vazamento de dados envolvendo [descrever quais dados foram afetados, como nome, CPF, endereço, e-mail, etc.]. Assim que tomamos conhecimento da ocorrência, adotamos imediatamente as medidas necessárias para conter o incidente, mitigar possíveis impactos e reforçar nossas medidas de segurança.

Ressaltamos que nossa equipe de segurança da informação está conduzindo uma investigação detalhada para identificar a origem do incidente e implementar ações preventivas para evitar futuras ocorrências. Além disso, notificamos a Autoridade Nacional de Proteção de Dados (ANPD), conforme exigido pela legislação vigente.

Recomendamos que você fique atento a qualquer atividade suspeita relacionada aos seus dados e evite compartilhar informações sensíveis por meios não confiáveis. Caso tenha qualquer dúvida ou precise de mais

informações, nossa equipe de suporte está disponível pelo e-mail [contato] ou telefone [número].

Reiteramos nosso compromisso com a transparência e a proteção dos seus dados. Lamentamos pelo ocorrido e estamos à disposição para esclarecer quaisquer dúvidas.

Atenciosamente,
[Seu Nome]
[Cargo]
[Nome da Empresa]
[Contato]

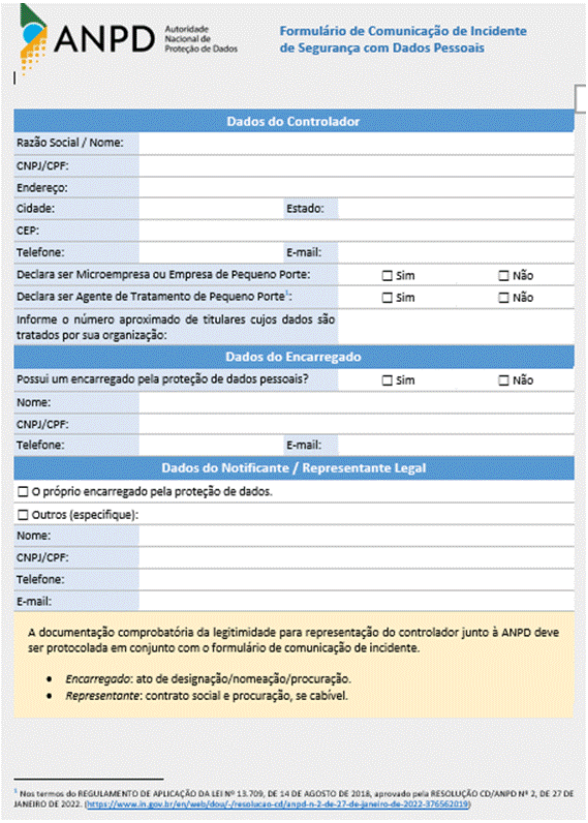
Para comunicar um incidente de segurança à Autoridade Nacional de Proteção de Dados (ANPD) por meio do Sistema Eletrônico de Informações (SEI), siga os seguintes passos:

1. **Cadastro no SEI**:
    - Caso ainda não possua um cadastro, acesse o SEI da ANPD e realize o cadastro como usuário externo. O cadastro é necessário para que pessoas físicas, vinculadas ou não a pessoas jurídicas, possam participar de processos administrativos junto à ANPD.
2. **Acesso ao SEI**:
    - Após a aprovação do cadastro, faça login no SEI utilizando suas credenciais.
3. **Início de um Novo Processo**:
    - No menu à esquerda, localize a seção "Peticionamento" e selecione "Processo Novo".

4. **Seleção do Tipo de Processo**:
    - Escolha o tipo de processo "ANPD – Comunicados de Incidentes à Autoridade Nacional de Proteção De Dados".
5. **Preenchimento do Formulário de Incidente de Segurança**:
    - No campo "Documento Principal", clique no formulário de incidente de segurança disponível (preliminar ou completo) e preencha todas as informações solicitadas.
    - O formulários próprio que deve ser preenchido e encaminhado pode ser encontrado em https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/com

unicado-de-incidente-de-seguranca-cis/formulario_cis_anpd1.docx

ele possui a seguinte aparência



ANPD Autoridade Nacional de Proteção de Dados

Formulário de Comunicação de Incidente de Segurança com Dados Pessoais

Dados do Controlador			
Razão Social / Nome:			
CNPJ/CPF:			
Endereço:			
Cidade:	Estado:		
CEP:			
Telefone:	E-mail:		
Declara ser Microempresa ou Empresa de Pequeno Porte:		☐ Sim	☐ Não
Declara ser Agente de Tratamento de Pequeno Porte[1]:		☐ Sim	☐ Não
Informe o número aproximado de titulares cujos dados são tratados por sua organização:			
Dados do Encarregado			
Possui um encarregado pela proteção de dados pessoais?		☐ Sim	☐ Não
Nome:			
CNPJ/CPF:			
Telefone:	E-mail:		
Dados do Notificante / Representante Legal			
☐ O próprio encarregado pela proteção de dados.			
☐ Outros (especifique):			
Nome:			
CNPJ/CPF:			
Telefone:			
E-mail:			

A documentação comprobatória da legitimidade para representação do controlador junto à ANPD deve ser protocolada em conjunto com o formulário de comunicação de incidente.

- *Encarregado*: ato de designação/nomeação/procuração.
- *Representante*: contrato social e procuração, se cabível.

[1] Nos termos do REGULAMENTO DE APLICAÇÃO DA LEI Nº 13.709, DE 14 DE AGOSTO DE 2018, aprovado pela RESOLUÇÃO CD/ANPD Nº 2, DE 27 DE JANEIRO DE 2022. (https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019)

6. **Anexação de Documentos Complementares**:
    - Em "Documentos Complementares", anexe documentos que comprovem a legitimidade para representar o controlador perante a ANPD, como o ato de designação do encarregado, procuração e atos constitutivos da empresa, se aplicável.
7. **Revisão e Protocolo**:
    - Revise todas as informações inseridas e, após verificar que estão corretas, protocole o processo no SEI para envio à ANPD.

Para mais detalhes sobre o procedimento de comunicação de incidentes de segurança, consulte o

Manual Externo do SEI disponível no site da ANPD. Em caso de dúvidas ou dificuldades durante o processo, entre em contato com o Protocolo da ANPD pelo e-mail protocolo@anpd.gov.br.

Lembre-se de que a comunicação de incidentes de segurança deve ser realizada pelo encarregado pela proteção de dados ou por um representante legalmente constituído do controlador.

Referências

Comunicação de incidente de segurança - Guia orientativo ANPD - https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis - Acesso em 05/01/2025

LEI Nº 13.709, DE 14 DE AGOSTO DE 2018 - disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Formulário de comunicaão de incidente de segurança ANPD - https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis/formulario_cis_anpd1.docx

RESOLUÇÃO CD/ANPD Nº 15, DE 24 DE ABRIL DE 2024 - disponível em https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024

Guia de Boas práticas e proteção de Dados pessoais - STF https://bibliotecadigital.stf.jus.br/xmlui/bitstream/handle

/123456789/7488/GUIA%20LGPD_13%202%20%281%29.pdf?sequence=1&isAllowed=y

Capítulo 11. Auditoria e Monitoramento de Conformidade

Autora: Andressa Lourenço Gonçalves

No setor de Recursos Humanos (RH), a proteção de dados pessoais é uma prioridade, pois envolve informações sensíveis de funcionários e candidatos. Para garantir a conformidade com as legislações de proteção de dados, como a Lei Geral de Proteção de Dados (LGPD), é fundamental estabelecer processos contínuos de auditoria e monitoramento. Este capítulo abordará como as auditorias podem avaliar o nível de conformidade da organização e como o monitoramento contínuo pode minimizar riscos, assegurando a privacidade e segurança das informações tratadas pelo RH.

Monitoramento de Políticas de Privacidade e Proteção de Dados

O monitoramento das políticas de privacidade e proteção de dados no RH deve ser uma prática contínua, já que o tratamento de dados pessoais está em constante evolução. Em muitos casos, o departamento de RH é o responsável por lidar com dados sensíveis, como informações de saúde, salários, avaliações de desempenho, entre outros. Para garantir a conformidade com as leis de proteção de dados, como a Lei Geral de Proteção de Dados (LGPD) ou legislações locais, deve-se adotar estratégias de monitoramento eficazes que incluam:

A) Ferramentas de Monitoramento em Tempo Real:

É essencial que as empresas implementem plataformas de gestão de conformidade que monitoram, em tempo real, o tratamento de dados pessoais no setor de RH. Essas ferramentas podem verificar acessos não autorizados, manipulação indevida de informações sensíveis ou compartilhamento inadequado de dados com terceiros. Elas ajudam a identificar rapidamente qualquer vulnerabilidade ou falha nas políticas de segurança.

b) Auditoria de Acessos e Logs de Dados:

Estabelecer uma estratégia de monitoramento de acessos aos dados é fundamental. Isso pode incluir a implementação de sistemas de gestão de logs que registram quem acessou ou modificou os dados pessoais, qual foi a ação realizada e em que momento. Monitorar os acessos e a manipulação de dados ajuda a identificar

atividades incomuns ou não conformes. Além disso, esses registros são cruciais para a realização de auditorias futuras e para comprovar a conformidade em caso de investigações externas.

c) **Monitoramento de Contratos e Terceirização:**

Em muitas organizações, o RH contrata fornecedores ou terceirizados que também têm acesso a dados pessoais. O monitoramento de contratos e acordos com fornecedores é vital para garantir que essas partes externas também sigam as políticas de proteção de dados e estejam em conformidade com as regulamentações pertinentes. Além disso, é importante que o RH realize auditorias de conformidade periódicas junto aos fornecedores para avaliar o tratamento adequado dos dados pessoais.

A auditoria de conformidade no setor de RH é um processo sistemático para revisar políticas, práticas e procedimentos relacionados ao tratamento de dados pessoais. O objetivo é garantir que a organização esteja aderindo às regulamentações aplicáveis e seguindo as melhores práticas de segurança da informação.

Principais Etapas da Auditoria

1. **Planejamento da Auditoria**

    - Definição dos objetivos e escopo da auditoria.
    - Identificação das legislações e normas aplicáveis.
    - Seleção da equipe responsável pelo processo.

2. **Coleta e Análise de Dados**

   - Levantamento das práticas adotadas no tratamento de dados.
   - Avaliação da conformidade com a LGPD e demais normas.
   - Identificação de riscos e pontos de melhoria.

3. **Elaboração do Relatório de Auditoria**

   - Registro dos achados da auditoria.
   - Recomendações para corrigir inconformidades.
   - Definição de prazos para implementação de melhorias.

4. **Implementação de Ações Corretivas**

   - Aplicação das recomendações sugeridas.
   - Revisão de políticas e treinamentos para os colaboradores.

- Monitoramento da eficácia das medidas adotadas.

Práticas de Auditoria Contínua

A auditoria contínua é um processo sistemático e contínuo de revisão das práticas de proteção de dados, para garantir que as políticas estejam sendo seguidas corretamente ao longo do tempo. Essa abordagem proativa ajuda a identificar problemas antes que eles se tornem crises e permite realizar ajustes nas políticas conforme necessário. Algumas práticas essenciais de auditoria incluem:

A. Auditorias Internas Regulares:

As auditorias internas devem ser realizadas de forma periódica, com a participação de uma equipe especializada em conformidade e

privacidade. A auditoria interna permite a verificação da aderência das práticas de RH às políticas estabelecidas pela organização e às legislações vigentes. Essa atividade deve se concentrar na análise de processos, como coleta, armazenamento, acesso e compartilhamento de dados pessoais, identificando possíveis brechas ou não conformidades.

b) **Auditorias Externas e Consultorias Especializadas:**

Além das auditorias internas, é aconselhável realizar auditorias externas com consultores especializados em proteção de dados. Esses auditores independentes podem oferecer uma visão imparcial sobre as práticas da empresa e identificar áreas de risco que possam ter sido negligenciadas pela equipe interna. A contratação de consultorias pode ser particularmente útil para

avaliar a conformidade com a legislação local de proteção de dados e para realizar avaliações de impacto à privacidade (DPIA).

c) Revisão de Políticas e Procedimentos de Proteção de Dados:

A auditoria contínua também envolve a revisão constante das políticas de privacidade e de segurança de dados do RH. Essa revisão deve ser feita pelo departamento de conformidade, garantindo que as políticas estejam sempre atualizadas conforme as mudanças legislativas e regulatórias. É importante que as políticas e procedimentos estejam adequados às necessidades da organização e refletem as práticas de mercado.

D) **Identificação de Deficiências e Ações Corretivas:**

Durante as auditorias, podem ser identificadas deficiências ou falhas no processo de tratamento de dados pessoais. Quando isso ocorrer, o RH deve tomar ações corretivas para corrigir as falhas imediatamente. Isso pode envolver a atualização de processos, tratamento de funções ou implementação de novas tecnologias de segurança. A documentação dessas ações corretivas é essencial para garantir a rastreabilidade das mudanças e demonstrar a conformidade com auditorias futuras.

Ferramentas e Técnicas para Garantir a Conformidade

O uso de ferramentas tecnológicas no monitoramento e auditoria de conformidade facilita a automação de processos complexos e permite um controle mais

eficiente sobre os dados pessoais tratados no RH. Algumas das principais ferramentas e técnicas incluem:

a) Sistemas de Gestão de Conformidade (GRC):

As ferramentas de Governança, Risco e Conformidade (GRC) são plataformas integradas que ajudam as organizações a gerenciar e mitigar os riscos associados ao tratamento de dados pessoais. Elas oferecem recursos como monitoramento de conformidade regulatória, auditorias de dados e gestão de incidentes de segurança. Essas plataformas podem ser configuradas para gerar alertas automáticos sempre que ocorrer um incidente ou violação de política de privacidade, ajudando o RH a agir rapidamente.

b) Ferramentas de Análise de Riscos e Avaliação de Impacto à Privacidade (DPIA):

As ferramentas de análise de riscos ajudam a identificar áreas de vulnerabilidade no processo de tratamento de dados pessoais. Elas são particularmente úteis durante a implementação de novos processos, sistemas ou tecnologias no RH, para garantir que o tratamento de dados seja realizado de forma compatível com a legislação. A realização de uma Avaliação de Impacto à Privacidade (DPIA) ajuda a prever os riscos envolvidos no tratamento de dados sensíveis, permitindo que medidas mitigadoras sejam aplicadas.

c) Softwares de Monitoramento de Segurança e Privacidade de Dados:

Existem diversos softwares específicos para monitoramento de segurança e privacidade de dados. Esses sistemas podem verificar e garantir que as medidas de segurança, como criptografia, autenticação multifatorial e controle de acesso, estejam sendo aplicadas corretamente. Também são capazes de gerar relatórios detalhados que ajudam o RH a identificar falhas nos controles de segurança e agir preventivamente.

D) Automação de Processos e Relatórios:

A automação pode ser uma ferramenta poderosa para garantir a conformidade contínua. Softwares que automatizam a coleta de dados, a criação de relatórios e a gestão de incidentes podem facilitar o monitoramento constante da conformidade com as políticas de proteção de dados. Esses sistemas também ajudam a garantir que a documentação

necessária esteja sempre disponível para auditorias externas ou investigações legais.

Conclusão

A conformidade com a legislação de proteção de dados no setor de RH exige um esforço contínuo, com auditorias regulares e monitoramento eficaz. Ao adotar essas práticas, as empresas garantem a segurança dos dados dos colaboradores, minimizam riscos jurídicos e demonstram comprometimento com a privacidade. Dessa forma, a auditoria e o monitoramento tornam-se ferramentas essenciais para fortalecer a governança corporativa e a cultura de proteção de dados dentro das organizações.

Referências

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Guia Orientativo sobre Agentes de Tratamento e o Encarregado. Versão 2.0, Brasília, 2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Guia Orientativo para Elaboração de Relatório de Impacto à Proteção de Dados Pessoais (RIPD). Brasília, [s.d.].

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Guia Orientativo de Segurança da Informação para Agentes de Tratamento de Pequeno Porte. Versão 1.0, Brasília, 2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018.

PINHEIRO, Patrícia Peck. Direito Digital. 8. ed. São Paulo: Saraiva Jur, 2024.

Capítulo 12. Treinamento e Conscientização

Treinamento e Conscientização: Como Preparar sua Equipe para a LGPD?

Autora: Sarah Gobo

Se você trabalha com RH, já deve saber que a LGPD não é só uma obrigação legal – é uma mudança de cultura. E para que isso aconteça de verdade, a equipe precisa estar bem treinada. Afinal, não adianta ter regras impecáveis se ninguém sabe como aplicá-las, certo?

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, determina que todas as empresas devem adotar medidas para proteger os dados pessoais dos candidatos e colaboradores. Mas essa responsabilidade não é só do setor jurídico ou do DPO

(Data Protection Officer). **Cada colaborador que lida com informações pessoais no dia a dia tem um papel essencial nessa missão.**

O Papel dos Colaboradores na Proteção de Dados

Todo profissional que lida com informações pessoais deve:

- Tratar os dados apenas para as finalidades específicas informadas ao titular;
- Seguir boas práticas de segurança, como o uso de senhas fortes e armazenamento adequado;
- Evitar o compartilhamento indevido de informações;
- Relatar imediatamente qualquer incidente de segurança.

Se essas medidas forem adotadas por todos, a empresa reduz riscos e garante um ambiente mais seguro para os dados.

Confidencialidade e Boas Práticas no RH

Manter sigilo sobre os dados dos candidatos e colaboradores não é apenas uma recomendação – é uma exigência da LGPD. Aqui estão algumas boas práticas para garantir a confidencialidade:

- **Privilégio mínimo!** Apenas pessoas autorizadas devem acessar os dados – Se um colaborador não precisa de determinada informação para realizar seu trabalho, ele não deve acessá-la.
- **Evite expor informações desnecessárias** – Nada de planilhas abertas na tela do computador ou currículos esquecidos na impressora!

- **Cuidado com e-mails e mensagens** – Um simples erro no envio pode causar um vazamento de dados.
- **Usar canais seguros para armazenar e compartilhar informações** – E-mails pessoais e pastas desprotegidas não são a melhor opção.

Gestão de Acessos: Quem Pode Ver o Quê?

Nem todo colaborador precisa ter acesso a todos os dados. Uma boa gestão de acessos garante que cada funcionário tenha permissão apenas para as informações necessárias ao seu trabalho. Para isso, as empresas devem:

· Criar políticas claras sobre quem pode acessar quais dados;

· Implementar autenticação multifator (MFA) para proteger o acesso a informações sensíveis;

· Monitorar e revisar acessos regularmente, evitando que ex-colaboradores ainda tenham credenciais ativas.

Treinamento: Como Ensinar a Equipe sobre a LGPD?

Treinar a equipe sobre a LGPD não precisa ser algo chato ou burocrático. Existem formas mais dinâmicas e eficazes de levar a mensagem:

- Vídeos curtos e interativos;
- Guias e folhetos ilustrados;
- Boletins informativos enviados por e-mail;
- Seminários e palestras com café da manhã;

- Simulações e estudos de caso para fixar o aprendizado na prática.

O ideal é combinar dois ou mais formatos para garantir que o aprendizado seja realmente absorvido e aplicado no dia a dia.

A implementação de um programa de treinamento estruturado permite que o RH atue com segurança, diminuindo riscos e assegurando a conformidade com a LGPD. E precisa ser contínuo, pois mudanças de comportamentos levam tempo!

A educação continuada da equipe é essencial para manter a cultura de proteção de dados dentro da organização.

Cultura de Proteção de Dados: Um Compromisso Contínuo

O treinamento não pode ser algo isolado. Para que a proteção de dados faça parte do DNA da empresa, é essencial:

✔ Reforçar a importância do tema em reuniões e comunicados internos;

✔ Disponibilizar um canal de dúvidas para que os colaboradores possam se informar sempre que precisarem;

✔ Garantir que a liderança esteja engajada e dê o exemplo.

A LGPD veio para ficar e, mais do que um conjunto de regras, é uma oportunidade para as empresas se tornarem mais organizadas, seguras e confiáveis.

Com colaboradores bem treinados e boas práticas implantadas, a conformidade com a LGPD deixa de ser um desafio e se torna um diferencial competitivo.

Referências

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Guia Orientativo de Segurança da Informação para Agentes de Tratamento de Pequeno Porte. Versão 1.0, Brasília, 2021.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Guia Orientativo para Elaboração de Relatório de Impacto à Proteção de Dados Pessoais (RIPD). Brasília, [s.d.].

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Guia Orientativo sobre Agentes de Tratamento e Encarregado. Versão 2.0, Brasília, 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018.

PINHEIRO, Patrícia Peck. Direito Digital. 8. ed. São Paulo: Saraiva Jur, 2024.

SUPREMO TRIBUNAL FEDERAL (STF). Guia de Boas Práticas e Proteção de Dados Pessoais. Brasília, 2023.

Parte III – Ferramentas e Práticas de Conformidade

Capítulo 13: Registro de Atividades de Tratamento

Autor: Redação Ela Jurista

O Registro de Atividades como seu diário de bordo

Para os profissionais de RH e Departamento Pessoal (DP), a LGPD é uma oportunidade de organizar e profissionalizar a gestão de dados. A chave para isso é o **Registro de Atividades de Tratamento**. Pense nele como o seu diário de bordo: um documento simples e prático que mapeia todas as ações que a sua equipe faz com os dados dos candidatos e colaboradores.

Manter este registro não é apenas uma obrigação legal, é uma **estratégia inteligente** que protege a empresa de forma proativa. Ele serve como sua prova oficial de conformidade, um recurso valioso em caso de auditoria

ou questionamento da **ANPD** (Autoridade Nacional de Proteção de Dados). Com ele, você consegue ter clareza total sobre o fluxo de dados e:

- **Saber exatamente quais dados são coletados, por que e para onde eles vão.** Isso garante que a informação certa chegue à pessoa certa, na hora certa.
- **Facilitar a gestão.** Se um candidato pedir para ter seus dados excluídos, você saberá exatamente onde encontrá-los. Se o RH for auditado, a documentação estará pronta.
- **Fortalecer a confiança.** Mostrar que sua empresa tem um processo organizado e transparente aumenta a credibilidade com candidatos e colaboradores, tornando-se um diferencial competitivo.

Um modelo prático de registro

Para auxiliar na documentação e garantir a conformidade com a LGPD, apresentamos um modelo prático de Registro de Atividades de Tratamento. Este modelo pode ser adaptado à realidade da sua empresa e utilizado como um guia para mapear o fluxo de dados no RH e DP.

Identificação do Processo	**Finalidade do Tratamento**	**Tipos de Dados Pessoais Coletados**	**Base Legal**	**Tempo de Retenção**	**Medidas de Segurança Adotadas**
Recrutamento e Seleção	Avaliar candidatos para preenchimento de vaga	Nome, telefone, e-mail, currículo, histórico profissional	Consentimento do Titular	2 anos (ou até revogação do consentimento)	Acesso restrito com login e senha; uso de sistemas criptografados; treinamento da equipe

Admissão de Colaboradores	Contratação e gestão de colaboradores	Nome, CPF, RG, endereço, dados bancários	Cumprimento de obrigação legal ou execução de contrato	Período de vigência do contrato e o que for exigido em lei	Acesso restrito a sistemas de folha de pagamento; uso de servidores seguros; auditorias internas
Gestão de Benefícios	Oferecer e gerir benefícios como plano de saúde e vale-transporte	Dados de saúde (com consentimento específico), endereço, dependentes	Consentimento ou Execução de contrato	Período de vigência do contrato de trabalho	Acesso restrito a profissionais do RH e DP; sistemas seguros; acordos de confidencialidade com fornecedores

Existem softwares que podem ajudar?

Sim, existem diversas ferramentas de software de **gestão de conformidade com a LGPD** (chamadas de GRC - *Governance, Risk and Compliance*) que podem

automatizar grande parte desse trabalho. Em vez de focar em um nome específico, o ideal é que você verifique se a sua empresa já utiliza ou se pode adquirir uma solução que ofereça:

- **Mapeamento de Dados:** Ferramentas que ajudam a visualizar e documentar o fluxo de dados em toda a organização.
- **Gestão de Consentimento:** Recursos para capturar, registrar e gerenciar o consentimento dos titulares de forma centralizada.
- **Relatórios Automatizados:** Funcionalidades que geram automaticamente os relatórios de registro de atividades, facilitando a auditoria e a prestação de contas.
- **Monitoramento em Tempo Real:** Sistemas que alertam a equipe sobre acessos indevidos ou atividades suspeitas, ajudando a prevenir incidentes.

O uso dessas ferramentas pode otimizar a rotina do RH e DP, garantindo que o registro de dados seja feito de forma consistente e segura, minimizando o risco de erros humanos.

Quem é o responsável pela LGPD na sua empresa?

Antes de iniciar qualquer registro ou alteração, é fundamental saber se sua empresa já tem um responsável pela LGPD. O primeiro passo é verificar se existe um **Encarregado de Dados (DPO - *Data Protection Officer*)** ou um comitê de privacidade.

Normalmente, a responsabilidade pela LGPD é compartilhada entre diferentes departamentos:

- **Departamento Jurídico:** Responsável por analisar as bases legais e garantir que as políticas de privacidade estejam em conformidade com a lei.
- **Tecnologia da Informação (TI):** Encarregado de implementar as medidas de segurança, como criptografia, controle de acesso e proteção de servidores.
- **Recursos Humanos (RH) e Departamento Pessoal (DP):** Responsáveis por aplicar as diretrizes da LGPD no dia a dia, desde a coleta de currículos até o descarte de informações de ex-colaboradores.

Se sua empresa ainda não tem um responsável formal, é essencial iniciar essa conversa com a liderança para que a responsabilidade pela LGPD seja atribuída de forma clara.

Referências

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Guia Orientativo sobre Agentes de Tratamento e Encarregado. Versão 2.0, Brasília, 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Art. 37. Diário Oficial da União, Brasília, DF, 15 ago. 2018.

MONTEIRO, Renato Leite. LGPD - Lei Geral de Proteção de Dados: Teoria e Prática. 2. ed. Salvador: JusPodivm, 2023

Capítulo 14. Processos Automatizados e Inteligência Artificial

Reconhecer como utilizar inteligência artificial em recrutamento e as responsabilidades associadas

Autor: Ana Carolina da Costa

QUADRO DIDÁTICO SOBRE INTELIGÊNCIA ARTIFICIAL

Inteligência Artificial (IA)

A Inteligência Artificial (IA) é uma tecnologia que permite que máquinas simulem a inteligência humana, aprendendo, raciocinando e tomando decisões para resolver problemas.

Principais Conceitos da IA

Conceito	Descrição
Dados	Base da IA. São coletados, organizados e analisados para treinar algoritmos.
Infraestrutura	Inclui servidores, nuvem e poder computacional necessário para processar dados.
Algoritmos	Sequências de instruções que guiam o aprendizado da máquina e fazem previsões.
Visualização de Dados	Apresenta os resultados de maneira compreensível por meio de gráficos e dashboards.

Aprendizado de Máquina (ML)	Computadores aprendem a partir de dados, identificam padrões e tomam decisões.
Redes Neurais Artificiais	Inspiradas no cérebro humano, ajudam no reconhecimento de padrões complexos.
Processamento de Linguagem Natural (PLN)	IA interpreta e responde a textos e falas humanas, como em assistentes virtuais.
Visão Computacional	Permite que máquinas "vejam" e interpretem imagens e vídeos.

Big Data	Enorme volume de dados usados pela IA para aprendizado e melhoria contínua.
***Chatbots* e Assistentes Virtuais**	Programas que interagem com usuários de forma automatizada.
***Deep Learning* (Aprendizado Profundo)**	Usa redes neurais profundas para reconhecer padrões em grandes volumes de dados.

Aplicações da IA no Dia a Dia

- **Saúde:** Diagnóstico de doenças e assistência a médicos.

- **Finanças:** Previsão de tendências e detecção de fraudes.
- **Transporte:** Carros autônomos e otimização de rotas.
- **Atendimento ao Cliente:** *Chatbots* para suporte 24h.
- **Entretenimento:** Recomendações personalizadas em *streaming*.

Benefícios e Desafios da IA

Benefícios	**Desafios**
Automatização de tarefas repetitivas	Questões éticas e de privacidade
Agilidade e precisão na análise de dados	Possíveis vieses nos algoritmos

Assistência na tomada de decisões	Impactos no mercado de trabalho

A **Inteligência Artificial (IA)** tenta imitar algumas capacidades humanas, como aprender, tomar decisões e resolver problemas. Existem dois tipos principais de IA:

- **A fraca (estreita)** – Faz apenas tarefas específicas, como reconhecer rostos ou recomendar filmes.
- **A forte (geral)** – Seria capaz de fazer tudo o que um ser humano faz, mas, por enquanto, só existe na ficção científica.

Atualmente, a IA que usamos no dia a dia é a **IA fraca**, ajudando em tarefas repetitivas, perigosas ou muito trabalhosas, como a automação em fábricas e os robôs que limpam casas. Mas à medida que a IA avança,

surgem novos desafios políticos, econômicos e sociais que precisamos debater.

Muita gente pensa que a IA é algo novo, mas sua ideia já existia desde o **século XVIII**, quando a matemática começou a ser usada para tomar decisões rápidas e eficientes. Hoje, usamos a IA em várias situações sem perceber, como:

📧**Filtros de spam** para evitar e-mails indesejados;
🗺️ **Mapas e rotas** que nos ajudam a chegar mais rápido ao destino;
💬 **Chatbots** que respondem mensagens automaticamente;

O termo **"Inteligência Artificial"** só foi criado nos anos **1950** por John McCarthy. Nessa mesma época, o cientista **Alan Turing** criou um teste para descobrir se uma máquina poderia "pensar" como um ser humano –

esse experimento ficou conhecido como **Teste de Turing**.

As **máquinas não aprendem sozinhas**. Elas precisam de um conjunto de dados que programamos para funcionar. No entanto, algumas tecnologias de IA já conseguem **aprender e melhorar com o tempo**. Isso acontece porque analisam muitos dados e identificam padrões automaticamente.

Machine Learning **(Aprendizado de Máquina)** é uma área da IA que melhora com o uso de grandes volumes de dados, o chamado ***Big Data***. Isso significa que quanto mais informações uma IA recebe, melhor ela se torna. Esse processo ajuda na análise de dados e na tomada de decisões, tornando nosso trabalho mais ágil e eficiente.

Mas como isso mudou nossa percepção de mundo tão rápido?

Foi um processo decorrente da 3ª Revolução Industrial, com computadores de alta capacidade de processamento de dados, a internet, o *cloud computing*, redes sociais, internet das coisas, e, também a coleta de dados massiva ("*big data*").

Como a IA pode nos ajudar?

Amplificando nossas capacidades, assim, aumentando nossa eficiência, tendo mais acurácia, e o trabalho com escalabilidade. Um exemplo disso: um médico que analisa imagens de raio x em busca de diagnóstico, com a IA, pode ver mais imagens em menos tempo, identificar padrões que podem levá-lo a concluir sobre determinada doença, sendo mais confiante em seu diagnóstico, podendo fazê-lo por mais exames, podendo até aperfeiçoar técnicas de realização de tratamento.

Assim, estamos certos de que as mudanças que a utilização de IA provoca em vários níveis: lógico, pessoal, organizacional e pessoal. Para o nível cultural, então, é o mais delicado. Por isso, precisamos pensar em usos éticos para a inteligência artificial.

Essa inteligência artificial deve ser **confiável**, resultando em **bem-estar** para as pessoas e a sociedade, precisa respeitar a **autonomia do indivíduo**, **privacidade, democracia, diversidade, não-discriminação, inclusão, bem como, a justiça social, os direitos fundamentais**.

O impacto da IA na sociedade:

A IA traz mudanças em vários níveis:

🔍 **Lógico** – Melhora nossa capacidade de analisar informações

👤 **Pessoal** – Afeta como interagimos com a

tecnologia no dia a dia

🏢 **Organizacional** – Transforma a forma como as empresas trabalham

🌍 **Cultural** – Esse é o impacto mais delicado, pois muda a forma como vivemos e pensamos

Por isso, é essencial discutir o **uso ético** da IA.

IA responsável e confiável

A Inteligência Artificial deve ser desenvolvida para trazer **bem-estar** à sociedade e respeitar valores fundamentais, como: **Autonomia do indivíduo**; **Privacidade e proteção de dados**; **Democracia e diversidade**; **Justiça social e direitos humanos.**

Assim, garantimos que a IA seja uma ferramenta que beneficie a todos, sem causar prejuízos ou discriminação.

Como a Inteligência Artificial pode ajudar o Setor de Recrutamento e Seleção em uma empresa?

A Inteligência Artificial (IA) está transformando o mundo do recrutamento e seleção, trazendo mais agilidade, eficiência e precisão aos processos. A seguir, explicamos como a IA pode beneficiar tanto empresas quanto candidatos, de forma simples e acessível.

Como a IA é eficiente e ágil?

A IA pode acelerar o processo de recrutamento, tornando-o mais eficiente. Ao automatizar tarefas repetitivas e específicas, como a triagem de currículos, a IA reduz o tempo gasto em etapas que antes demandavam esforço humano. Isso significa que as empresas podem encontrar os candidatos certos mais rapidamente.

Implementação de tecnologias nos processos organizacionais

A introdução de tecnologias como a IA nos processos organizacionais tem o objetivo de melhorar a produtividade e a qualidade das contratações. As empresas podem integrar ferramentas de IA nos sistemas de recrutamento para tornar o processo mais preciso e ágil, além de otimizar o tempo gasto com tarefas burocráticas.

Como a IA pode auxiliar em vagas com maior volume de inscrições?

Em situações em que há um grande número de inscrições, a IA ajuda a filtrar rapidamente os currículos, destacando os candidatos mais adequados para a vaga, de acordo com os requisitos necessários antecipadamente descritos para a vaga e perfil da empresa. Isso facilita a gestão de grandes volumes de

candidaturas e assegura que os recrutadores consigam focar nos candidatos mais alinhados com a posição.

- **Redução do tempo e custo na triagem de currículos**

  Ao automatizar a triagem de currículos, a IA pode reduzir significativamente o tempo e os custos com a seleção de candidatos. Ela consegue analisar rapidamente as qualificações e experiências dos candidatos, proporcionando uma visão mais clara sobre quem está mais preparado para a vaga, isto é, de acordo com os parâmetros que a IA apresenta, pois essa decisão não é fatal, definitiva, outras abordagens humanas são essenciais: a entrevista, a análise do perfil comportamental através de dinâmicas ou semelhantes, fases de testes que necessitam que sejam feitas pessoalmente ou através de videochamadas.

- **Quantidade de pessoas procurando emprego utilizando a web**

  Com o aumento da digitalização, mais pessoas estão buscando emprego através da internet. A IA se torna uma aliada essencial para gerenciar a grande quantidade de candidatos que se inscrevem pelas plataformas online, facilitando a busca por perfis mais qualificados de maneira rápida e eficaz.

O que é e-recruitment?

O e-recruitment é o uso de plataformas digitais e ferramentas online para recrutar candidatos. A IA pode ser integrada a essas plataformas, ajudando a otimizar a busca, triagem e comunicação com os candidatos, tornando o processo totalmente digital e mais acessível.

Às vezes as empresas procuram esse tipo de ferramenta para compartilharem a responsabilidade de estarem

usando essa abordagem com IA, pois a empresa pode contratar a plataforma, descrevendo os dados da vaga, o perfil da empresa, dentre outros aspectos, e todas as outras medidas que envolvam o tratamento de dados (seja a guarda, armazenamento, exclusão, o tratamento *per si*) ficam sob responsabilidade da plataforma.

Cabe lembrar que se a própria empresa criar situações ilegais ou discriminatórias, é de sua inteira responsabilidade.

HR Techs: mais de 125 no mundo

As HR Techs são empresas que desenvolvem tecnologias específicas para recursos humanos, como ferramentas de recrutamento baseadas em IA. No mundo, existem mais de 125 dessas empresas, que ajudam as organizações a melhorar seus processos de contratação, oferecendo soluções inovadoras, desde a

triagem de currículos até a análise de desempenho dos colaboradores.

O surgimento desse tipo de empresa nada mais é que a consequência dessa digitalização que estamos passando, que foi acelerada pela pandemia de covid.

Aumento da assertividade e redução do *turnover*

A IA pode aumentar a assertividade nas contratações, ajudando a identificar os candidatos mais alinhados com a cultura organizacional e as necessidades da vaga. Isso contribui para a redução do *turnover* (taxa de rotatividade de funcionários), já que a probabilidade de contratar um profissional que se encaixa bem no time aumenta.

Redução do custo de contratação

Ao diminuir o tempo que a vaga fica aberta e a necessidade de processos manuais demorados, a IA contribui para reduzir o custo de contratação. Além disso, ao otimizar a seleção, a IA ajuda a garantir que a empresa contrate o candidato certo da primeira vez, evitando contratações erradas – através de parâmetros que auxiliem o responsável pela contratação a tomar a decisão apoiada por dados.

Uso de redes sociais no recrutamento

As redes sociais, como LinkedIn, Facebook e até plataformas especializadas, desempenham um papel crucial no recrutamento. A IA pode ser utilizada para monitorar essas redes e identificar talentos que podem não ser encontrados por meio

de métodos tradicionais, ampliando o alcance das empresas a grupos diversos de candidatos.

Feedback para os candidatos

A IA também pode fornecer feedback para os candidatos, ajudando-os a entender seus pontos fortes e áreas de melhoria. Isso não só melhora a experiência do candidato, mas também os motiva a aperfeiçoar suas habilidades, o que é positivo para sua jornada profissional.

Inclusão digital

É importante que o uso de IA não restrinja o atendimento a pessoas que não possuem facilidade com tecnologias ou acesso à internet. Por isso, as empresas devem garantir que seus

processos de recrutamento incluam alternativas para candidatos que não têm familiaridade com plataformas digitais.

Cyber Vetting: Avaliação de Candidatos na Internet

A IA também pode ser utilizada no processo de *cyber vetting*, que envolve a análise da presença online de um candidato. Isso ajuda a obter informações adicionais que podem ser úteis para avaliar a adequação do candidato à cultura da empresa. Mas, claro, esse tipo de abordagem deve ser utilizado com o devido cuidado, não ferindo a privacidade do candidato, evitando excessos. Por exemplo, ao analisar o Linkedin de um candidato, você pode observar alguma habilidade: se ele gosta de estar sempre atualizado, pois está

sempre adicionando certificados de cursos, se gosta de escrever sobre determinado assunto e este é importante para empresa, se se porta com um perfil de liderança ou se prefere ser liderado. Por outro lado, se for utilizada para excluí-lo por conta de alguma manifestação pessoal (desde que não seja algo que fira direitos humanos ou seja criminosa), já é um mal-uso do recurso.

Centralização de informações e gestão de dados

A IA permite centralizar informações em um único sistema, facilitando a gestão e o cruzamento de dados de candidatos. Com isso, fica mais fácil para os recrutadores acessarem todas as informações relevantes em um único lugar e tomarem decisões mais informadas.

Automação de processos e tomada de decisões

A IA é capaz de automatizar tarefas repetitivas e específicas, como agendamento de entrevistas e envio de notificações. Além disso, ela pode ajudar na tomada de decisões, oferecendo insights baseados em dados para ajudar os recrutadores a escolherem o candidato mais adequado.

A Inteligência Artificial (IA) é uma ferramenta poderosa que está remodelando vários setores, mas seu uso traz também uma série de desafios, especialmente no que se refere à responsabilidade civil e à gestão de dados. A seguir, abordaremos como a IA se relaciona com a centralização de informações, a automação de processos, a responsabilidade por danos causados e os princípios éticos necessários para sua governança.

Centralização de Informações (Gestão de Dados) e Cruzamento

A centralização de informações é um dos principais benefícios do uso de IA em processos organizacionais. Por meio de sistemas integrados, a IA permite que as empresas centralizem dados em um único ponto, facilitando o acesso e a análise dessas informações. Isso é fundamental para realizar o cruzamento de dados, que ajuda a identificar padrões, fazer previsões e tomar decisões informadas. No contexto do recrutamento, por exemplo, isso pode significar a análise de currículos e o histórico de candidatos, todos centralizados em uma plataforma de fácil acesso para os recrutadores.

Utilização para Tarefas Repetitivas, Automação de Processos e Tomada de Decisões

A IA é altamente eficaz para automatizar tarefas repetitivas e específicas, como triagem de currículos, agendamento de entrevistas ou a gestão de dados de candidatos. Isso economiza tempo e recursos humanos, permitindo que as equipes de RH se concentrem em tarefas mais estratégicas. Além disso, a IA pode auxiliar na tomada de decisões, oferecendo *insights* valiosos sobre quais candidatos têm o maior potencial ou quais ações devem ser tomadas para otimizar processos de recrutamento.

Responsabilidade Civil e a IA

A responsabilidade civil envolve a obrigação de reparar os danos causados a terceiros devido a ações ou

omissões de um indivíduo ou entidade. Quando se trata de IA, surge uma questão importante: quem é o responsável por danos causados por falhas ou erros de sistemas de IA?

Ausência de Regulamentação Específica

Atualmente, a responsabilidade civil relacionada ao uso de IA ainda carece de uma regulamentação clara e específica. Isso gera incertezas sobre quem deve ser responsabilizado em casos de danos causados por IA, seja no contexto de erro de decisão, falha de sistema ou violação de privacidade.

Artigo 186 do Código Civil

O Artigo 186 do Código Civil brasileiro estabelece que a responsabilidade civil decorre da ação ou omissão

voluntária, negligente ou imperita que cause dano a outrem. No caso da IA, a aplicação deste artigo pode ser complexa, uma vez que nem sempre é claro quem é o responsável pela falha do sistema.

IA Baseada em Machine Learning (ML): Dificuldades na Identificação de Responsabilidade

As IA baseadas em Machine Learning (ML) são projetadas para aprender e tomar decisões de forma autônoma, sem a intervenção humana direta. Isso complica a identificação de quem é o responsável por erros ou danos causados por essas tecnologias. Será o desenvolvedor do algoritmo, a empresa que fornece os dados ou a empresa que detém a tecnologia a responsável pelo erro? Essa falta de clareza é um dos principais desafios legais que precisam ser abordados

para garantir que as vítimas de danos tenham uma forma de obter reparação.

Regulação do Uso de IA: Portaria 4.617/21 e PL 21/20

O Ministério da Ciência, Tecnologia e Inovação (MCTI) publicou a **Portaria 4.617/21**, que trata da política nacional de Inteligência Artificial e de como o governo planeja regulamentar o uso dessa tecnologia. Além disso, o **Projeto de Lei 21/20** propõe a criação de um regime jurídico específico para a responsabilidade civil decorrente do uso da IA. Esses movimentos buscam estabelecer normas claras sobre quem deve ser responsabilizado em casos de danos causados por sistemas de IA.

Chatbots e o Impacto da IA no Atendimento ao Cliente

Os chatbots, sistemas de IA que simulam uma conversa humana, são amplamente utilizados em empresas para automatizar o atendimento ao cliente. Embora eles aumentem a eficiência, é fundamental que os *chatbots* sejam projetados com ética e responsabilidade, garantindo que sua utilização não prejudique a experiência do usuário ou cause danos.

Princípios Éticos e Governança da IA

A implementação de IA deve ser acompanhada de uma governança responsável para evitar abusos e garantir que as tecnologias sejam utilizadas de forma ética. Alguns dos **principais princípios éticos** que devem ser seguidos no uso de IA são:

- **Responsabilidade**: As empresas e desenvolvedores devem ser responsáveis pelas decisões tomadas pelos sistemas de IA.

- **Autonomia Humana**: A IA deve ser projetada para complementar, não substituir, o julgamento humano.

- **Explicabilidade**: Deve ser possível entender como a IA chegou a determinada decisão.

- **Prevenção**: A IA deve ser projetada para minimizar riscos e danos, prevenindo situações de erro.

Requisitos a Serem Implementados

A governança da IA deve incluir uma série de requisitos, como:

- · **Ação Humana e Supervisão**: Mesmo que a IA seja autônoma, deve haver supervisão humana para garantir que as decisões sejam justas e apropriadas.
- **Robustez Técnica e Segurança**: A IA deve ser segura, garantindo a proteção de dados e evitando falhas técnicas.
- **Privacidade e Governança de Dados**: A privacidade dos dados pessoais dos usuários deve ser respeitada, com medidas adequadas para proteger essas informações.
- **Transparência**: As decisões da IA devem ser claras e explicáveis para os usuários e partes interessadas.
- **Diversidade e Não Discriminação**: A IA deve ser inclusiva, evitando discriminação contra qualquer grupo de pessoas.

- **Justiça**: As decisões tomadas pela IA devem ser justas e imparciais, sem prejudicar grupos específicos.
- **Bem-Estar Social e Ambiental**: A IA deve ser usada de maneira a promover o bem-estar das pessoas e a sustentabilidade ambiental.
- ***Accountability***: A responsabilidade por falhas ou danos causados pela IA deve ser claramente definida.

O uso de IA apresenta desafios significativos, especialmente no que diz respeito à responsabilidade civil e à governança ética. À medida que a tecnologia avança, é fundamental que as empresas e legisladores trabalhem juntos para criar regulamentações claras que garantam o uso responsável e seguro da IA, protegendo os direitos dos indivíduos e promovendo a transparência e a justiça.

Cuidados e Responsabilidades ao Usar Inteligência Artificial (IA) em Processos Seletivos

A utilização de Inteligência Artificial (IA) em processos seletivos oferece uma série de benefícios, como a agilidade e a eficiência na triagem de currículos e na escolha de candidatos. No entanto, também traz responsabilidades importantes, principalmente no que diz respeito ao tratamento de dados, à prevenção de preconceitos e discriminação, e ao cumprimento de normas éticas e legais, como a Lei Geral de Proteção de Dados (LGPD). A seguir, explicamos como garantir que o uso da IA seja responsável e livre de viés.

Cuidados no Tratamento de Dados

Ao utilizar IA em processos seletivos, é fundamental garantir que os **dados dos candidatos sejam inseridos e**

analisados de forma correta. Isso significa que a coleta, armazenamento e análise dos dados devem ser feitas de maneira transparente e segura, respeitando a privacidade dos candidatos. O tratamento inadequado de dados pode resultar em decisões erradas e prejudiciais, além de violar as normas de proteção de dados, como a **LGPD**.

Preconceito nas Descrições de Cargos e Análise de Currículos

Um dos principais desafios ao usar IA em recrutamento e seleção é o risco de **preconceito nas descrições de cargos e na análise de currículos**. A linguagem usada nas descrições de vagas ou nos currículos pode refletir estereótipos de gênero, raça, idade ou outros preconceitos. Esses vieses podem ser reforçados pelos algoritmos de IA, que aprendem com os dados históricos e, muitas vezes, replicam as desigualdades existentes.

Por exemplo, se os dados históricos de uma empresa mostram que apenas homens foram contratados para cargos de liderança, a IA pode aprender a priorizar candidatos do sexo masculino, perpetuando essa desigualdade. A mesma lógica pode se aplicar a questões raciais, étnicas ou relacionadas à idade.

O Desafio dos Dados Históricos que Refletem Desigualdades

Os **dados históricos de contratação** muitas vezes refletem desigualdades sociais e econômicas, como o preconceito racial ou de gênero, que estão presentes na sociedade. Quando esses dados são usados para treinar sistemas de IA, há o risco de esses vieses serem incorporados nos algoritmos. Por isso, é importante realizar uma **análise crítica e cuidadosa** dos dados utilizados, para garantir que não se perpetue a discriminação.

A Diversidade e a Inclusão

A IA deve ser usada de forma a **promover a diversidade** e não reforçar estereótipos ou discriminação. Isso significa que os sistemas de IA devem ser programados para identificar e selecionar candidatos com base em habilidades, experiência e competências, e não em características pessoais que não são relevantes para o cargo. Além disso, é necessário garantir que a IA seja capaz de identificar e valorizar a diversidade **de perspectivas**, permitindo a inclusão de candidatos de diferentes origens, gêneros, etnias e idades.

LGPD e Proteção de Dados Pessoais

No contexto da **Lei Geral de Proteção de Dados (LGPD)**, as empresas têm a responsabilidade de proteger os **dados pessoais dos candidatos**, garantindo que esses dados sejam tratados de forma transparente e segura. Isso envolve a obtenção de **consentimento adequado**

dos candidatos para o uso de seus dados no processo seletivo e a implementação de medidas de segurança para evitar vazamentos ou acessos não autorizados.

Além disso, as empresas devem assegurar que os dados sejam utilizados **somente para as finalidades específicas do processo seletivo**, e não para outros fins. Qualquer uso inadequado ou fora do escopo pode gerar **riscos legais** significativos para a organização.

Riscos de Segurança e Vazamentos de Dados

Os **riscos de segurança** também são uma preocupação importante. O uso de IA em processos seletivos envolve o armazenamento e processamento de grandes volumes de dados sensíveis. Se esses dados não forem adequadamente protegidos, a organização pode se expor a **vazamentos de informações** e a **ataques cibernéticos**, com graves consequências tanto legais quanto reputacionais.

Estruturas Claras de Responsabilidade para Erros Algorítmicos

É fundamental que as empresas estabeleçam **estruturas claras de responsabilidade** para lidar com erros algorítmicos ou violações éticas. Se a IA cometer um erro, como a seleção de candidatos com base em critérios discriminatórios, é preciso ter um **processo transparente** para corrigir esses erros e lidar com as consequências. Além disso, as empresas devem ter um **comitê ético** ou responsável pelo monitoramento contínuo do uso da IA, garantindo que ela seja utilizada de forma justa e responsável.

Avaliação de Desempenho e Feedback

A **avaliação de desempenho** dos candidatos também deve ser realizada de maneira justa e sem viés. A IA pode ser útil para avaliar habilidades e competências de

maneira objetiva, mas é necessário garantir que os **critérios de avaliação** não sejam baseados em preconceitos ou estereótipos. Além disso, a IA pode fornecer **feedback construtivo** para os candidatos, ajudando-os a entender seus pontos fortes e áreas de melhoria, o que contribui para uma **experiência positiva** no processo seletivo.

Como Prevenir Vieses e Discriminação

Existem várias medidas que podem ser tomadas para **prevenir vieses e discriminação** ao usar IA em processos seletivos:

1. **Treinamento de IA com dados diversos**: Utilize dados que representem uma ampla variedade de candidatos e não reforcem estereótipos ou discriminação.

2. **Auditoria regular dos algoritmos**: Realize auditorias periódicas nos sistemas de IA para

identificar e corrigir qualquer viés que possa ter sido incorporado.

3. **Transparência no processo seletivo**: Informe aos candidatos como seus dados estão sendo utilizados e ofereça a possibilidade de revisar as decisões feitas pela IA.

4. **Integração de supervisão humana**: Apesar da automação, é importante que um recrutador humano esteja envolvido no processo, especialmente na fase de decisão final, para garantir que a IA não esteja sendo utilizada de forma discriminatória.

5. **A participação de um time diverso** no momento de levantamento de requisitos para a vaga, treinamento dessa inteligência, e até na hora da contratação.

O uso de Inteligência Artificial em processos seletivos pode ser extremamente benéfico para agilizar e otimizar as contratações, mas é fundamental que as empresas tomem medidas para evitar preconceitos, discriminação e violação de direitos dos candidatos. Isso envolve garantir a transparência no tratamento de dados, implementar estruturas claras de responsabilidade e seguir princípios éticos para promover a diversidade e inclusão. Além disso, o cumprimento da LGPD e a proteção dos dados pessoais são essenciais para garantir que o uso da IA seja seguro e responsável.

Cuidados com a Privacidade e Proteção de Dados no RH

O setor de **Recursos Humanos (RH)** é, sem dúvida, um dos que mais concentra **dados e informações sensíveis** dentro de uma organização. Esses dados incluem desde informações pessoais e profissionais dos candidatos até registros sobre seu desempenho, histórico de

empregabilidade e até aspectos de suas características comportamentais. Quando o RH adota tecnologias, como a **Inteligência Artificial (IA)**, para otimizar seus processos seletivos, torna-se ainda mais importante garantir que os dados dos candidatos sejam tratados com transparência, segurança e respeito aos direitos previstos pela **Lei Geral de Proteção de Dados Pessoais (LGPD)**.

A LGPD e os Princípios que Regem o RH

A **LGPD** estabelece princípios fundamentais para o tratamento de dados pessoais, e o setor de RH deve atentar-se a eles de maneira cuidadosa para assegurar que seus processos sejam **transparentes**, **seguros** e **éticos**. Entre os principais princípios da LGPD que se aplicam diretamente ao RH, destacam-se:

1. **Finalidade**: O RH deve garantir que os dados coletados durante o recrutamento e seleção sejam utilizados apenas para as finalidades específicas, como a análise de candidatos para determinada vaga, e não para outros fins sem o consentimento do candidato.

2. **Adequação**: Os dados coletados devem ser **adequados, pertinentes e limitados** ao necessário para os processos seletivos. O RH não deve coletar informações excessivas ou irrelevantes para o cargo.

3. **Transparência**: É imprescindível que o RH forneça informações claras e acessíveis aos candidatos sobre quais dados estão sendo coletados, com quais finalidades e como esses dados serão tratados. **Comunicados, avisos e políticas de privacidade** devem ser disponibilizados na plataforma da empresa **antes**

do início do processo seletivo, garantindo que os candidatos possam dar seu consentimento informado.

4. **Segurança**: A empresa deve adotar **medidas de segurança adequadas** para proteger os dados pessoais dos candidatos contra acessos não autorizados, vazamentos ou incidentes de segurança.

5. **Não Discriminação**: A LGPD proíbe a utilização dos dados pessoais para fins discriminatórios, ilícitos ou abusivos, sendo essencial que o RH tenha práticas de coleta e processamento de dados que respeitem esses princípios.

6. **Responsabilidade**: O RH deve **assumir a responsabilidade** sobre o tratamento dos dados dos candidatos, garantindo que todos os

processos estejam em conformidade com a LGPD.

Importância dos Comunicados e Políticas na Plataforma

É de suma importância que a empresa publique, de forma clara e acessível, **comunicados e políticas de privacidade** na plataforma onde o processo seletivo acontece. Esses documentos devem detalhar:

- **Quais informações** serão coletadas durante o recrutamento e seleção.
- **Qual a finalidade** de cada dado coletado e como ele será utilizado.
- **O tempo de retenção** desses dados, ou seja, quanto tempo as informações serão armazenadas.

- **A política de descarte** de dados pessoais, que deve ocorrer de forma segura e conforme a legislação.

Além disso, o RH deve oferecer um **canal de comunicação** para que os candidatos possam acessar seus dados, solicitar **correções** ou, se desejado, **pedir a exclusão** das suas informações. Esse processo assegura a **transparência** e o **controle** por parte do candidato sobre seus dados pessoais, conforme estabelecido pela LGPD.

Artigo 20 da LGPD: Revisão de Decisões Automatizadas

O **Artigo 20 da LGPD** trata de um ponto crucial para o contexto de recrutamento e seleção: a **possibilidade de revisão das decisões automatizadas**. Isso é particularmente importante para os candidatos que estão sendo avaliados por **algoritmos de IA**, os quais podem influenciar diretamente sua seleção ou rejeição.

Este artigo garante que os candidatos têm o direito de **solicitar a revisão de decisões automatizadas** que afetem seus interesses, especialmente quando essas decisões se baseiam em aspectos da **personalidade** ou traçam um perfil sobre o candidato, como seu **perfil profissional** ou **psicológico**. Se uma decisão automatizada for tomada e impactar negativamente o candidato, ele tem o direito de contestá-la e exigir uma revisão humana do processo.

Decisões Discriminatórias e Violação de Direitos

As **decisões discriminatórias**, especialmente as feitas por sistemas automatizados sem supervisão humana, podem configurar uma **violação dos direitos humanos** e da boa-fé, além de infringirem os **princípios da LGPD**. O uso de IA no recrutamento pode, se não for bem monitorado, resultar em escolhas baseadas em **viés** ou **discriminação** contra candidatos de determinados

grupos, como mulheres, negros, pessoas com deficiência, entre outros.

Essas decisões podem também infringir os direitos previstos no **Artigo 6º da LGPD**, que proíbe o uso de dados pessoais para fins discriminatórios. A empresa deve garantir que os dados utilizados no processo seletivo não sejam usados para excluir, de forma injusta, candidatos por características pessoais irrelevantes para a vaga.

Consequências de Não Cumprir a LGPD

Empresas que não cumprirem a **LGPD** podem enfrentar **consequências jurídicas e financeiras**. As sanções previstas pela LGPD começam desde a advertência, indicando prazo para adoção de medidas corretivas, até multa simples ou diária, publicização da infração, bloqueio dos dados pessoais a que se refere a infração

até sua regularização ou até mesmo a eliminação dos dados pessoais a que se refere a infração.

Bem como a responsabilização judicial no caso de vieses discriminatórios, antiética ou vexatórios, por essa infração.

Além disso, a empresa pode sofrer uma **auditoria da ANPD** (Autoridade Nacional de Proteção de Dados), o que pode resultar em sanções adicionais caso sejam identificadas falhas na conformidade com a LGPD.

A Revisão Humana das Decisões Automatizadas

Embora a LGPD não exija explicitamente a revisão humana das decisões automatizadas, **é altamente recomendada**. A revisão humana pode ajudar a evitar **erros algorítmicos** e garantir que o processo seletivo seja conduzido de maneira justa e imparcial. A

intervenção humana também é essencial para garantir que as decisões respeitem os direitos dos candidatos e estejam de acordo com os princípios da **não discriminação** e **justiça**.

A **LGPD** desempenha um papel crucial na proteção dos dados dos candidatos durante o recrutamento e seleção. O RH deve adotar práticas transparentes, seguras e éticas, respeitando os princípios da LGPD, evitando discriminação e garantindo que as decisões sejam tomadas de forma justa. Isso inclui a revisão das decisões automatizadas, o respeito aos direitos dos candidatos e a implementação de medidas de segurança adequadas. Com essas precauções, as empresas podem garantir um processo seletivo mais **ético**, **inclusivo** e **responsável**.

Responsabilidade Judicial no Contexto do Uso da IA

Responsabilidade Judicial por IA Antiética no RH

O uso de IA no RH pode ser considerado antiético quando não respeita os princípios fundamentais da boa-fé, transparência e não discriminação. Se os sistemas de IA forem programados ou treinados de forma inadequada, sem supervisão humana, ou com base em dados enviesados, a decisão automatizada pode ser prejudicial ao candidato, afetando sua trajetória profissional de maneira injusta e antiética.

Por exemplo, se um algoritmo de IA for utilizado para desclassificar candidatos com base em características pessoais irrelevantes para a vaga, como idade, gênero, etnia, ou deficiência, essa prática pode ser considerada discriminatória e violar os direitos fundamentais do candidato. Nesses casos, a empresa pode ser

responsabilizada judicialmente por ferir princípios constitucionais e da LGPD relacionados à não discriminação e à proteção de dados pessoais.

A responsabilidade civil da empresa pode ser acionada por danos morais e materiais causados aos candidatos que se sentirem prejudicados pela utilização inadequada da IA. Se a IA discrimina um candidato de maneira injustificada, o impacto pode ser tanto no processo seletivo quanto na sua dignidade e autonomia.

Responsabilidade Judicial por IA Discriminatória

O uso de IA de maneira discriminatória no RH ocorre quando a tecnologia favorece ou desfavorece grupos específicos de candidatos com base em características protegidas pela legislação, como raça, gênero, orientação sexual, idade ou deficiência. A discriminação algorítmica pode acontecer quando o algoritmo é treinado com dados históricos que refletem preconceitos e desigualdades, ou quando ele é mal projetado para

segmentar e classificar os candidatos de forma inadequada.

Exemplo disso seria o uso de um sistema de IA que classifica negativamente mulheres ou pessoas com deficiência em processos seletivos, com base em dados históricos que indicam uma predominância de homens sem deficiência em cargos semelhantes. Isso violaria os princípios da LGPD (como o de não discriminação e igualdade de tratamento) e direitos fundamentais relacionados à igualdade e não discriminação presentes na Constituição Federal.

Se um candidato for discriminado dessa maneira, ele pode acionar a justiça para pedir reparação por danos morais e materiais. Além disso, a empresa pode ser multada pela ANPD (Autoridade Nacional de Proteção de Dados) caso se comprove que os dados pessoais dos candidatos foram tratados de maneira ilegítima ou discriminatória.

Responsabilidade Judicial por IA Vexatória

A utilização de IA no RH pode ser considerada vexatória quando a tecnologia submete o candidato a situações humilhantes ou constrangedoras no processo seletivo. Isso pode ocorrer, por exemplo, quando sistemas de IA impõem perguntas invasivas, exigem avaliações subjetivas ou fazem julgamentos baseados em informações não relevantes, com o potencial de prejudicar a autoestima e a dignidade do candidato.

Em um exemplo prático, se um algoritmo é usado para classificar candidatos com base em perguntas pessoais ou intrometidas (como aspectos íntimos da vida pessoal, saúde ou opinião política), isso pode ser considerado um tratamento vexatório. O candidato pode alegar que foi submetido a uma situação humilhante e prejudicial para sua imagem, além de violar direitos fundamentais de privacidade e dignidade.

Nesses casos, a responsabilidade judicial da empresa pode envolver danos morais, sendo a empresa obrigada a reparar os prejuízos causados ao candidato, bem como a corrigir seus processos internos de coleta e análise de dados para evitar futuros abusos.

Responsabilidade por Erros e Violações da LGPD

A LGPD impõe responsabilidades claras sobre o tratamento de dados pessoais e a proteção da privacidade dos candidatos. Empresas que utilizam IA no RH devem seguir a lei à risca, garantindo que o tratamento dos dados seja transparente, legítimo e com o consentimento do candidato. Caso a IA use dados de maneira discriminatória, vexatória ou antiética, a empresa poderá ser responsabilizada por violação da LGPD.

O artigo 6º da LGPD proíbe o tratamento discriminatório, e o artigo 20 garante o direito dos candidatos à revisão de decisões automatizadas que afetem seus interesses. A empresa deve ser capaz de justificar qualquer decisão automatizada, com base em dados objetivos e critérios transparentes.

Em caso de erro algorítmico, a empresa deve ser responsabilizada por eventuais danos causados e tomar medidas corretivas para mitigar os efeitos. Isso pode incluir a remodulação dos algoritmos, a supervisão humana das decisões e o treinamento ético da IA.

A responsabilidade judicial em casos de uso de IA no RH de maneira antiética, discriminatória ou vexatória é um tema fundamental que envolve questões jurídicas, éticas e de conformidade com a LGPD. As empresas devem garantir que a IA seja utilizada de forma transparente, justa e respeitosa, levando em consideração os direitos e a dignidade dos candidatos. Caso contrário, as

organizações podem enfrentar consequências jurídicas graves, incluindo danos morais, multas da ANPD e a responsabilidade civil por violação dos direitos dos candidatos.

Por fim, é fundamental que as empresas se comprometam com a governança ética no uso da IA, garantindo que suas decisões sejam sempre baseadas em princípios de igualdade, não discriminação, transparência e justiça, promovendo um ambiente de trabalho mais inclusivo e responsável.

Devemos pensar na utilização de inteligência artificial no nosso dia a dia como uma ferramenta de integração humano-máquina, sendo a IA uma ferramenta colaboradora, não decisiva, que nos ajude a ampliar nossas capacidades de inteligência e analíticas.

Referências

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Diário Oficial da União, Brasília, DF, 11 jan. 2002.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018.

BRASIL. Ministério da Ciência, Tecnologia e Inovações. Portaria nº 4.617, de 6 de abril de 2021. Institui a Estratégia Brasileira de Inteligência Artificial - EBIA. Diário Oficial da União, Brasília, DF, 09 abr. 2021.

CÂMARA DOS DEPUTADOS. Projeto de Lei nº 21, de 2020. Estabelece fundamentos, princípios e diretrizes para o desenvolvimento e a aplicação da inteligência artificial no Brasil. Brasília, DF: Câmara dos Deputados.

DONEDA, Danilo; MACHADO, Caio. Desafios à implementação do direito à explicação de decisões automatizadas. In: BIONI, Bruno (Coord.). Proteção de Dados Pessoais: A Função e os Limites do Consentimento. São Paulo: Forense, 2019.

RUSSELL, Stuart J.; NORVIG, Peter. Inteligência Artificial. 4. ed. Rio de Janeiro: GEN LTC, 2021.