

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA POLITÉCNICA E DE ARTES
GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO



**IMPLANTAÇÃO DO PRIVACY BY DESIGN NO SISTEMA DE RECRUTAMENTO
DE PESSOAS: UM ESTUDO SOBRE A ADEQUAÇÃO À LGPD**

LUCAS MELO RODRIGUES

GOIÂNIA
2023

LUCAS MELO RODRIGUES

**IMPLANTAÇÃO DO PRIVACY BY DESIGN NO SISTEMA DE RECRUTAMENTO
DE PESSOAS: UM ESTUDO SOBRE A ADEQUAÇÃO À LGPD**

Monografia apresentada à Escola Politécnica e de Artes da Pontifícia Universidade Católica de Goiás como parte dos requisitos para a obtenção do título de Bacharel em Ciência da Computação.

Orientador(a): Prof^a. Ma. Adriana Silveira de Souza

GOIÂNIA
2023

LUCAS MELO RODRIGUES

**IMPLANTAÇÃO DO PRIVACY BY DESIGN NO SISTEMA DE RECRUTAMENTO
DE PESSOAS: UM ESTUDO SOBRE A ADEQUAÇÃO À LGPD**

Este Trabalho de Conclusão de Curso julgado adequado para obtenção do título de Bacharel em Ciência da Computação, e aprovado em sua forma final pela Escola de Politécnica e de Artes, da Pontifícia Universidade Católica de Goiás em

____/____/____.

Prof^a. Ma. Ludmilla Reis Pinheiro dos Santos
Coordenadora de Trabalho de Conclusão de Curso

Orientadora: Prof^a. Ma. Adriana Silveira de Souza

Prof. Me. Joriver Rodrigues Canedo

Prof. Dr. Juliano Lopes de Oliveira

GOIÂNIA

2023

AGRADECIMENTOS

Aos meus pais, amigos e colegas que me ajudaram e incentivaram ao longo dessa jornada.

RESUMO

Este trabalho tem como objetivo abordar a implantação do Privacy by Design em um sistema de recrutamento de pessoas, com foco na adequação à Lei Geral de Proteção de Dados (LGPD). O objetivo do estudo é analisar as medidas necessárias para incorporar os princípios do PbD no processo de recrutamento, visando garantir a privacidade e a proteção dos dados pessoais dos usuários. O trabalho apresenta uma revisão teórica sobre a LGPD, Privacy by Design e normas que regulamentam o setor, destacando os princípios e requisitos legais relacionados à proteção de dados. Em seguida, é realizada uma análise de um sistema de recrutamento. Espera-se que este estudo contribua para a conscientização sobre a importância da proteção de dados.

Palavras-chave: LGPD, Privacy by Design (PbD), ISO/IEC 29134, ISO/IEC 29184, Avaliação de Impacto na Privacidade (AIP).

ABSTRACT

This work aims to address the implementation of Privacy by Design (PbD) in a recruitment system, with a focus on compliance with the General Data Protection Law (LGPD). The objective of this study is to analyze the necessary measures to incorporate PbD principles into the recruitment process, aiming to ensure privacy and protection of users' personal data. The paper presents a theoretical review of the LGPD, Privacy by Design, and relevant regulations governing the sector, highlighting the principles and legal requirements related to data protection. Subsequently, an analysis of a recruitment system is conducted. It is expected that this study will contribute to raising awareness about the importance of data protection.

Keywords: LGPD, Privacy by Design (PbD), ISO/IEC 29134, ISO/IEC 29184, Privacy Impact Assessment (PIA).

LISTA DE ABREVIATURAS

AIP – Avaliação de Impacto na Privacidade

GDPR – General Data Protection Regulation (Regulamento Geral de Proteção de Dados).

IEC – International Electrotechnical Commission (Comissão Eletrotécnica Internacional)

ISO – International Organization for Standardization (Organização Internacional de Normalização)

LGPD – Lei Geral de Proteção de Dados

LLC - Limited Liability Company

PbD - *Privacy By Design*

SUMÁRIO

1. INTRODUÇÃO.....	8
1.1. OBJETIVOS DA PESQUISA.....	9
1.2. JUSTIFICATIVA.....	9
1.3. ESTRUTURA DO TRABALHO.....	9
2. REVISÃO BIBLIOGRÁFICA.....	9
2.1. LGPD.....	10
2.2. PRIVACY BY DESIGN.....	11
2.3. ISO/IEC 29134:2017 - TECNOLOGIA DA INFORMAÇÃO - TÉCNICAS DE PRIVACIDADE - DIRETRIZES PARA AVALIAÇÃO DE PRIVACIDADE DE INFORMAÇÃO.....	14
2.4. ISO/IEC 29184:2021 - TECNOLOGIA DA INFORMAÇÃO — AVISOS DE PRIVACIDADE ON-LINE.....	16
3. METODOLOGIA.....	16
3.1. DESCRIÇÃO DO APLICATIVO.....	17
4. ANÁLISE E RESULTADOS.....	17
4.1. VISÃO GERAL SOBRE RECRUTAMENTO E SELEÇÃO.....	18
4.2. ENGENHARIA DE REQUISITOS.....	19
4.3. REQUISITOS DO SISTEMA.....	20
4.4. MODELO DE DADOS.....	27
4.5. ARQUITETURA DE SOFTWARE.....	27
4.6. TELAS DO SISTEMA.....	28
4.7. RELATÓRIO DE IMPACTO.....	31
5. CONCLUSÃO E TRABALHOS FUTUROS.....	34
5.1. LIÇÕES APRENDIDAS.....	34
5.2. TRABALHOS FUTUROS.....	34
6. REFERÊNCIAS.....	35

1. INTRODUÇÃO

Nos últimos anos, a digitalização das informações se tornou um fato inegável na sociedade. Com o avanço das tecnologias de informação e comunicação, as informações pessoais dos indivíduos estão cada vez mais expostas na internet e em outros meios digitais como smartphones, tablets, computadores e serviços de armazenamento em nuvem.

Com isso, as preocupações em relação à segurança dos dados se intensificaram, pois, a exposição indevida de informações pessoais pode ter diversas consequências negativas para os indivíduos. Entre as principais consequências se encontram a violação da privacidade, a exposição a riscos de segurança cibernética, o roubo de identidade e a fraude financeira, como por exemplo a exposição de dados pessoais, o que deixa os titulares desses dados vulneráveis a golpes como o *phishing*.

Nesse tipo de golpe, pessoas mal intencionadas se passam por alguma organização e tentam convencer as vítimas a entregarem seus dados. Se essas pessoas já possuírem uma quantidade de informações das vítimas, além de passar mais credibilidade, possibilita os criminosos a pedirem dados mais sensíveis ainda como dados bancários.

Empresas e governos também são afetados pela exposição indevida de informações, podendo enfrentar prejuízos financeiros, perda de confiança dos clientes e impactos na reputação.

A segurança dos dados é, portanto, um tema crucial para garantir a proteção dos direitos fundamentais dos indivíduos, a integridade das organizações e a estabilidade do sistema econômico e político. É necessário implementar medidas adequadas de segurança da informação para garantir a privacidade e a proteção dos dados pessoais em todos os processos que envolvem o tratamento dessas informações.

Com o aumento significativo do uso de tecnologias da informação, tornou-se mais fácil a coleta e o tratamento de dados pessoais em larga escala. Isso faz com que essas informações pessoais estejam armazenadas em diversos bancos de dados, o que faz surgir a necessidade de que a coleta e o tratamento desses dados sejam regulamentados a fim de garantir sua segurança.

No quesito de desenvolvimento de software é importante que se respeite os princípios da LGPD para garantir a conformidade com a legislação evitando multas, sanções ou outras

penalidades. Além disso, deve-se aumentar o nível de confiança dos usuários no software e na empresa que o desenvolve melhorando a reputação e a imagem da organização.

1.1. OBJETIVOS DA PESQUISA

Os objetivos deste trabalho são analisar a legislação brasileira referente à proteção de dados pessoais e a importância do *Privacy by Design* na adequação à LGPD. Identificar os principais requisitos de um sistema de recrutamento de pessoas e os dados pessoais coletados e tratados por ele. Propor um modelo de implantação do *Privacy by Design* no sistema de recrutamento de pessoas, considerando as especificidades do processo de recrutamento e as diretrizes da LGPD. Verificar a efetividade do modelo proposto por meio de testes e validação com usuários e especialistas em privacidade de dados. Discutir os resultados obtidos e as limitações do modelo proposto, bem como apresentar recomendações para futuros estudos e implementações.

1.2. JUSTIFICATIVA

A criação desse site é justificada pela crescente necessidade de fornecer mais transparência aos usuários e total adequação com as legislações vigentes em relação à proteção de dados pessoais. Ao garantir uma abordagem correta no tratamento dos dados, o site pode proporcionar aos usuários maior controle sobre suas informações pessoais e promover a confiança na plataforma.

1.3. ESTRUTURA DO TRABALHO

Este trabalho foi estruturado da seguinte forma: O capítulo 2 apresenta a fundamentação teórica, onde são apresentados os estudos necessários para o desenvolvimento deste trabalho. O capítulo 3 apresenta a metodologia. O capítulo 4 apresenta as análises e resultados. O capítulo 5 apresenta as conclusões obtidas, salientando os pontos mais importantes e sugestões para trabalhos futuros.

2. REVISÃO BIBLIOGRÁFICA

A fundamentação teórica deste trabalho é baseada em três principais assuntos: LGPD (Lei Geral de Proteção de Dados), uma legislação brasileira que estabelece diretrizes e regras para o tratamento de dados pessoais. *Privacy by Design* um conceito que visa incorporar a privacidade e a proteção de dados desde as fases iniciais do desenvolvimento de sistemas e as

normativas ISO 27002 e ISO 29134 padrões relacionados à segurança da informação que estabelece diretrizes para a implementação de controles de segurança da informação e a avaliação de impacto.

2.1. LGPD

A LGPD, ou Lei Geral de Proteção de Dados (Lei nº 13.709/2018), tem como objetivo proteger a privacidade e os dados pessoais dos cidadãos brasileiros (BRASIL, 2018). Esta lei estabelece regras e diretrizes para o tratamento dos dados por empresas e outras organizações.

A LGPD foi inspirada em legislações semelhantes em vigor em outros países, tal como o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia (UNIÃO EUROPEIA, 2016). A lei é importante porque garante que os dados pessoais dos cidadãos brasileiros sejam tratados de forma responsável e ética.

Desta forma, a lei nos protege de abusos e violações como ocorreu em 2018 com usuários da rede social Facebook, na época foram acessados sem autorização os dados de mais de 87 milhões de pessoas pelo mundo e de mais de 443 mil brasileiros pela consultoria Cambridge Analytica. (VEJA, 2018).

A lei estabelece uma série de direitos para os titulares de dados, como o direito de acesso, retificação, exclusão e portabilidade dos seus dados pessoais. Também define as obrigações das empresas e organizações que tratam esses dados, exigindo que elas implementem medidas de segurança e privacidade adequadas para protegê-los. Em relação ao desenvolvimento de software, a LGPD pode impactar essas empresas e organizações a realizar ajustes em suas políticas de privacidade, pedindo autorização dos seus usuários para o armazenamento e utilização dos dados sensíveis.

Também é necessário melhorar a segurança no armazenamento dos dados seja com uso de criptografia, realizando o controle de acesso ou monitorando e detectando ameaças para evitar vazamentos e demais transtornos.

A implementação da LGPD é um processo complexo e desafiador, que envolve a conscientização de toda a equipe de uma organização, incluindo a designação de um Encarregado de Proteção de Dados (DPO). Este papel é responsável por supervisionar o tratamento de dados pessoais e a adoção de novos processos e tecnologias para garantir o cumprimento da lei.

A conscientização e treinamento dos funcionários é fundamental. É necessário que todos entendam suas obrigações legais e sigam a política interna da empresa. Além disso, as empresas precisam estar preparadas para se apresentar aos órgãos reguladores que estão em conformidade com as medidas e que estão protegendo a privacidade dos titulares de dados. Nesse sentido é imprescindível realizar o mapeamento de todos os dados pessoais que a organização coleta, processa e armazena. Isso permite ter uma visão mais clara sobre os tipos de dados envolvidos, a finalidade da coleta, as bases legais e possíveis transferências para terceiros. O uso de um relatório de impacto é importante já que ele é um documento que descreve os possíveis impactos que determinadas mudanças ou decisões têm em um projeto em relação a sua privacidade e proteção de dados.

Para garantir que a privacidade e a proteção de dados pessoais sejam incorporadas em todas as fases do desenvolvimento de produtos e serviços, a LGPD prevê a adoção de princípios que propõem que a privacidade e a proteção de dados pessoais devem ser tratadas desde o início do desenvolvimento de um software, isso é, que as medidas de segurança devem ser adotadas desde a concepção do projeto em vez de ser tratada posteriormente, esse princípio é conhecido como *Privacy by Design*.

Outra abordagem que podemos adotar é a de *Privacy by Default*, que estabelece que as configurações padrão de um sistema devem ser definidas de forma a oferecer maior privacidade e proteção de dados pessoais, sem que os usuários precisem fazer configurações extras para garantir sua privacidade. Isso significa que no processo de desenvolvimento, as predefinições devem minimizar a coleta, o uso e o compartilhamento de dados pessoais, e somente informações necessárias devem ser coletadas, mantidas e processadas.

2.2. PRIVACY BY DESIGN

Privacy by Design (PbD) é uma abordagem de projeto que tem como objetivo incorporar a privacidade e a proteção de dados pessoais em todas as fases do desenvolvimento de produtos, serviços e sistemas. Essa abordagem foi criada por Ann Cavoukian em 1995 (Cavoukian, 1995) e se tornou uma das principais estratégias para garantir a privacidade e a segurança de dados na era digital. Essa abordagem foi incorporada ao Regulamento Geral de Proteção de Dados (GDPR) da União Europeia (UNIÃO EUROPEIA, 2016). O artigo 25 do GDPR estabelece que os controladores de dados devem implementar medidas técnicas e organizacionais apropriadas desde o início do processo de tratamento de dados, para garantir

que os princípios de proteção de dados sejam atendidos. Isso inclui a implementação do PbD, que visa garantir que a proteção de dados seja considerada desde a concepção do sistema.

O desenvolvimento de software com PbD envolve uma série de práticas e processos que visam garantir a privacidade e a segurança dos dados pessoais dos usuários. Algumas das práticas utilizadas são a minimização de dados onde se é coletado apenas os dados necessários para o funcionamento da aplicação, anonimizar os dados, ou seja, remover ou substituir informações que possam identificar diretamente os usuários e exigir o consentimento explícito quando for necessário coletar algum tipo de dado, mostrando para qual finalidade está sendo exigido. Essas práticas nos ajudam além de garantir a conformidade com as legislações e regulamentações de privacidade, também ajuda a proteger a confiança e a fidelidade dos usuários.

Por exemplo uma rede social, ela pode inicialmente coletar apenas os dados essenciais para o funcionamento básico do sistema como nome, email e data de nascimento e por padrão deixar desabilitado a opção de compartilhar esses dados com serviços de terceiros.

A PbD tem como base sete princípios que devem ser seguidos para garantir que a privacidade e a proteção de dados sejam incorporadas em todas as fases do desenvolvimento. Esses princípios são:

- Proatividade - a privacidade e a proteção de dados devem ser incorporadas desde o início do processo de desenvolvimento de software, e não introduzidas posteriormente de forma tardia, ou seja, pensar antecipadamente sobre os requisitos de segurança, confidencialidade, integridade e disponibilidade.
- Privacidade como padrão - as configurações padrões de um software devem ser definidas a fim de maximizar a privacidade do usuário. Isso inclui a coleta mínima de dados pessoais, limitação do acesso a esses dados e a exclusão de dados pessoais desnecessários. Por exemplo, desde o momento em que um usuário utiliza um serviço pela primeira vez, as configurações são definidas de forma a priorizar a privacidade dele
- Privacidade incorporada - garantir que a privacidade esteja incorporada em todos os processos, sistemas e produtos, ou seja, garantir que a privacidade seja considerada de forma automática sem necessidade de

nenhuma ação do usuário. Por exemplo, inicialmente coletar apenas as informações necessárias para o funcionamento do sistema.

- Controle de privacidade - os usuários devem ter total controle sobre como seus dados pessoais são coletados, armazenados, usados e compartilhados. Isso pode incluir a possibilidade de visualizar, editar ou excluir seus dados pessoais sempre que achar necessário.
- Segurança de ponta a ponta - os desenvolvedores de software devem implementar medidas de segurança para proteger os dados pessoais dos usuários contra acesso não autorizado, uso indevido ou divulgação garantindo a segurança dos dados pessoais em todas as fases durante o ciclo de vida do software. Por exemplo, utilizando criptografia de ponta a ponta durante a transmissão dos dados.
- Transparência - os usuários devem ser informados sobre as práticas de privacidade e proteção de dados do software, incluindo como seus dados serão coletados, usados e compartilhados. Isso deve ser feito de forma clara e de fácil entendimento. Por exemplo, toda vez que um sistema solicitar a entrada de algum dado, informar para o usuário qual a finalidade da coleta, por quanto tempo ele ficará retido e a base legal para a coleta.
- Respeito pela privacidade - garantir que a privacidade seja respeitada em todas as fases do desenvolvimento. Isso pode ser feito desde a preocupação com a segurança no início do desenvolvimento até a apresentação de avisos *user-friendly* para o usuário.

A incorporação desses princípios na abordagem de design de produtos e serviços pode ajudar a proteger a privacidade dos usuários e evitar violações de dados.

Além disso, a PbD pode aumentar a confiança dos usuários nos produtos e serviços, o que pode levar a um maior engajamento e fidelidade. No entanto, a implementação da PbD pode ser um desafio, especialmente para empresas que já possuem sistemas e processos em funcionamento. Ainda assim, é importante reconhecer a importância da privacidade e da proteção de dados e trabalhar para incorporar esses princípios em todas as fases do desenvolvimento.

2.3. ISO/IEC 29134:2017 - TECNOLOGIA DA INFORMAÇÃO - TÉCNICAS DE PRIVACIDADE - DIRETRIZES PARA AVALIAÇÃO DE PRIVACIDADE DE INFORMAÇÃO

A norma ISO 29134 é um guia que estabelece diretrizes e princípios para a realização de Avaliações de Impacto à Privacidade (AIP). As AIPs são ferramentas que ajudam as organizações a identificar e avaliar os riscos à privacidade associados às suas atividades de tratamento de dados pessoais.

As AIPs são muito importantes em contextos nos quais os dados pessoais são coletados e tratados em grande escala, ou quando envolvem informações sensíveis ou de alto risco. As AIPs permitem que as organizações identifiquem os riscos à privacidade associados a essas atividades e ajudem a avaliar sua gravidade e implementem medidas para mitigar esses riscos.

As principais etapas das AIPs incluem a identificação de dados pessoais que serão coletados ou processados, a identificação de riscos e ameaças à privacidade, a avaliação da gravidade desses riscos, a identificação de medidas para mitigá-los e a documentação de todo o processo.

Ela fornece diretrizes e orientações que são fundamentais para as empresas que desejam avaliar a conformidade com a privacidade e proteção de dados pessoais em seus sistemas. Para isso, é necessário adotar uma abordagem baseada em riscos, que permita avaliar os potenciais riscos e ameaças à privacidade dos dados coletados pelo software.

Algumas dessas diretrizes são: Realizar uma nova AIP ou atualizar se detectar impactos na privacidade em situações como uma nova funcionalidade ou houver alterações em leis e regulamentações.

Essa abordagem também ajuda a identificar as medidas necessárias para minimizar esses riscos e garantir a proteção dos dados pessoais. A aplicação dessas diretrizes e orientações pode contribuir significativamente para a criação de sistemas de software seguros e confiáveis, que respeitam a privacidade dos usuários e atendem às exigências das regulamentações de proteção de dados. Ela descreve um processo de avaliação em três fases: planejamento, execução e relatório.

O processo envolve a identificação dos processos e sistemas que lidam com dados pessoais, a avaliação dos riscos à privacidade e a identificação das medidas de mitigação apropriadas.

Vamos supor que uma empresa esteja desenvolvendo um novo sistema para gestão de RH que colete, armazene e processe os dados pessoais de seus funcionários como salários, benefícios e empregos anteriores. Se a empresa se preocupa com a privacidade dos dados dos funcionários, ela segue as seguintes etapas:

- Mapear todos os processos e sistemas que lidam com os dados pessoais.
- Avaliar os riscos potenciais à privacidade dos dados em cada um dos processos e sistemas identificados.
- Com base na avaliação de riscos, a empresa identifica as medidas necessárias para minimizar ou eliminar os riscos à privacidade.

Por exemplo, ela pode implementar medidas de segurança adicionais para garantir a proteção dos dados durante a coleta, transmissão e armazenamento dos dados, como criptografia ou autenticação de dois fatores.

Essa norma também fornece orientações para a definição de critérios de avaliação e para a seleção de avaliadores qualificados. Ela incentiva a participação de partes interessadas e o envolvimento de especialistas em privacidade e proteção de dados pessoais para garantir a qualidade da avaliação.

A norma ISO 29134 é importante pois fornece uma estrutura para as organizações avaliarem sua conformidade com as leis e regulamentações de privacidade e proteção de dados pessoais antes do desenvolvimento do produto. Ela também ajuda a garantir que as organizações implementem medidas adequadas de proteção de dados pessoais e ofereçam transparência aos usuários sobre o tratamento de seus dados.

A implementação da norma ISO 29134 pode trazer benefícios significativos para as organizações, incluindo a melhoria da conformidade regulatória, a mitigação de riscos à privacidade e a redução de incidentes de violação de dados pessoais. Além disso, a norma pode ajudar as organizações a demonstrar seu compromisso com a privacidade e proteção de dados pessoais aos usuários.

2.4. ISO/IEC 29184:2021 - TECNOLOGIA DA INFORMAÇÃO — AVISOS DE PRIVACIDADE ON-LINE

A ISO 29184 é uma norma internacional que estabelece diretrizes e recomendações para a criação de avisos de privacidade e mecanismos de consentimento para ajudar os usuários a entender e controlar o uso de suas informações pessoais em sites e aplicativos na internet. Ela também fornece orientações para desenvolvedores, designers de interface e outros profissionais que trabalham em sites e aplicativo para melhorar a transparência e a clareza das práticas de privacidade e de consentimento garantindo que esses recursos sejam projetados com clareza e de forma apropriada para os usuários finais, minimizando confusões ou mal-entendidos que possam afetar negativamente a privacidade.

Com isso, vemos que ela é importante para o desenvolvimento de software por várias razões. A privacidade é um direito fundamental dos usuários, e é essencial garantir que as informações pessoais sejam protegidas durante o uso de nossos sistemas, porém frequentemente os avisos de privacidade e de consentimento são ignorados pelos usuários, pois podem ser difíceis de entender ou serem apresentados de forma confusa ou inapropriada o que pode levar a uma falta de confiança dos usuários nos aplicativos e serviços, bem como a violações de privacidade.

Então essa norma nos ajuda a mitigar esses problemas já que ela nos orienta para a criação de avisos de privacidade e de consentimento mais claros.

Outra vantagem da norma é que ela pode ajudar as empresas a cumprir as leis e regulamentações de privacidade de dados, como o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia ou a Lei Geral de Proteção de Dados (LGPD) no Brasil. Ao seguir as diretrizes estabelecidas na norma, as empresas podem demonstrar seu compromisso com a privacidade do usuário e evitar sanções legais.

3. METODOLOGIA

A proposta deste trabalho é adotar um estudo de caso consistindo no desenvolvimento de uma aplicação de recrutamento de pessoas para um público que deseje uma ferramenta que auxilie o processo de seleção, utilizando como base a LGPD (Lei Geral de Proteção de Dados), a abordagem de Privacy by Design (Privacidade por Design) e as normas ISO 29134 e ISO 29184.

3.1. DESCRIÇÃO DO APLICATIVO

O recrutamento e seleção de talentos é um processo fundamental para o sucesso de uma empresa. Através desse processo, as empresas identificam, atraem, avaliam e selecionam os profissionais mais adequados para ocupar suas devidas vagas. Nessa seção, discutiremos a visão geral do recrutamento e seleção de pessoas, abordando seus principais conceitos, objetivos, etapas e desafios enfrentados pelas empresas nesse processo.

A interface do site foi desenvolvida de forma intuitiva a fim de proporcionar uma experiência agradável aos usuários e uma usabilidade simples para atingir um público amplo, desde os usuários experientes até aqueles com mais familiaridade com a internet.

As funcionalidades implementadas foram:

- Cadastro de usuários
- Cadastro de vagas
- Cadastro de currículos
- Listagem de vagas

Para o desenvolvimento do site foram utilizadas tecnologias amplamente utilizadas no mercado, o que garante sua compatibilidade com um maior número de dispositivos. As tecnologias usadas foram:

- O framework Angular para o desenvolvimento do *frontend* da aplicação.
- O framework Node.js é atrelado ao TypeScript para o desenvolvimento do *backend* da aplicação.
- Banco de dados não relacional MongoDB
- VSCode como ambiente de desenvolvimento integrado (IDE)
- Firebase para a hospedagem do site
- Railway App para a hospedagem da api do site

4. ANÁLISE E RESULTADOS

Neste capítulo apresentamos uma proposta de sistema que demonstra a implementação do PBD visando a implementação da LGPD. O sistema eleito para essa demonstração está relacionado à Gestão de Pessoas, mais especificamente ao subsistema de seleção e

recrutamento. Esse sistema foi eleito, porque ele trata de vários dados pessoais. Para isso, é discutida uma visão geral desse subsistema.

4.1. VISÃO GERAL SOBRE RECRUTAMENTO E SELEÇÃO

O recrutamento e seleção de talentos é um processo fundamental para o sucesso de uma empresa. Através desse processo, as empresas identificam, atraem, avaliam e selecionam os profissionais mais adequados para ocupar suas devidas vagas. Nessa seção, é discutida a visão geral do recrutamento e seleção de pessoas, abordando seus principais conceitos, objetivos, etapas e desafios enfrentados pelas empresas nesse processo.

O recrutamento e seleção consistem em uma série de atividades que visam identificar e escolher os candidatos mais qualificados para preencher as vagas em aberto nas empresas. Esse subsistema visa encontrar os profissionais que possuam Conhecimentos, Habilidades, e Atitudes (CHA) necessárias para atender às demandas das organizações quanto a sua força de trabalho. O recrutamento está relacionado ao processo de divulgação das oportunidades de emprego e ao estímulo para que os candidatos qualificados se candidatem, enquanto a seleção refere-se à avaliação desses candidatos por meio de técnicas e instrumentos específicos. O processo de recrutamento e seleção geralmente é dividido nas seguintes etapas.

- Planejamento, em que são definidas as necessidades e perfil do cargo.
- Análise do mercado de RH e do mercado de trabalho
- Definição das estratégias de recrutamento e seleção
- Divulgação das vagas com a finalidade de anunciar em diferentes canais de comunicação como sites de empregos e redes sociais.
- Triagem dos currículos, onde se é feito a análise dos currículos recebidos com base nos critérios definidos.
- Aplicação de baterias de testes para avaliar habilidades técnicas e comportamentais dos candidatos.
- Entrevistas e/ou dinâmicas, em que se é feito entrevistas com os candidatos pré-selecionados, podendo ser individuais ou em grupo.
- Verificações, onde se pode fazer contato com empregadores antigos ou pessoas de referência para verificar informações sobre o candidato.
- Escolha de candidatos com base em todas as etapas anteriores define-se o selecionado para a vaga.
- Encaminhamento para contratação.

Ao atrair e selecionar os profissionais mais qualificados, as empresas conseguem formar equipes talentosas e alinhadas com os objetivos estratégicos. No entanto, o processo de recrutamento e seleção enfrenta desafios constantes, o que exige adaptação e inovação por parte das empresas a fim de melhorar seus processos de seleção e compreender a visão geral do processo de recrutamento é fundamental para isso.

4.2. ENGENHARIA DE REQUISITOS

A Engenharia de Requisitos desempenha um papel fundamental no desenvolvimento de sistemas de software, garantindo que as necessidades e expectativas dos clientes sejam atendidas. Neste trabalho, a engenharia de requisitos assume uma importância significativa na criação da aplicação de recrutamento e seleção de pessoas.

O processo de engenharia de requisitos começa com o levantamento de requisitos, em que são identificadas as necessidades dos usuários, recrutadores e candidatos. Por meio de entrevistas, questionários e análise de documentação, literatura especializada, buscou-se se obter uma melhor compreensão das funcionalidades e das características que o sistema deveria atender.

A partir dessas informações, são identificados os requisitos funcionais, que descrevem as principais funcionalidades do sistema, como cadastro de candidatos, gerenciamento de vagas. Além disso, também são levantados os requisitos não funcionais, que envolvem aspectos como segurança dos dados, desempenho e usabilidade do sistema.

Após o levantamento dos requisitos, ocorre a análise e a especificação. Nessa etapa, os requisitos são refinados, detalhados e organizados de forma a fornecer uma visão clara e precisa das necessidades do sistema.

Em seguida, ocorre a validação dos requisitos. Na validação dos requisitos, os *stakeholders* têm a oportunidade de revisar e fornecer *feedback* sobre os requisitos levantados. Essa validação é essencial para garantir que os requisitos estejam corretos e atendam às expectativas dos usuários.

Após a validação, os requisitos são documentados em um documento de especificação de requisitos, que serve como referência para o desenvolvimento da aplicação de

recrutamento. Esse documento inclui uma descrição detalhada dos requisitos funcionais e não funcionais, além de possíveis casos de uso e/ ou histórias de usuários e diagramas que auxiliam na compreensão do sistema.

Ao longo do processo de desenvolvimento, é importante realizar o gerenciamento de mudanças nos requisitos. À medida que novas necessidades surgem ou mudanças ocorrem, é necessário avaliar o impacto dessas mudanças nos requisitos existentes e atualizar a documentação.

A Engenharia de Requisitos é um processo contínuo, que ocorre ao longo de todo o ciclo de vida do desenvolvimento do sistema. Ela envolve a comunicação efetiva com os *stakeholders*, a documentação adequada e a validação dos requisitos. Dessa forma, garante-se que a aplicação de recrutamento e seleção atenda às expectativas dos usuários, recrutadores e candidatos, proporcionando uma experiência satisfatória e eficiente para todos os envolvidos.

4.3. REQUISITOS DO SISTEMA

O levantamento de requisitos foi realizado, utilizando entrevista com um profissional da área, análise de processos, avaliação de sistemas de recrutamento e de seleção e análise da literatura especializada. A seguir são descritas as histórias de usuário identificadas para esse sistema.

H1: Eu como analista de RH solicito para o gestor a descrição do cargo para a vaga a ser disponibilizada.

Critério de Aceitação:

- Identificar o analista (nome, e-mail, telefone), identificar o gestor da vaga (nome, e-mail, telefone), data da solicitação.
- Enviar e-mail para o Gestor da vaga solicitando a descrição do cargo, indicando o link para upload do arquivo com a descrição do cargo.
- Um arquivo deve ser disponibilizado com a descrição do cargo pelo gestor
- Comunicação para o analista de RH, quando o gestor efetuar o upload do arquivo com a descrição do cargo.

H2: Eu como analista de RH desejo enviar um novo e-mail para o gestor, caso ele não envie a descrição do cargo em 3 dias.

Critério de aceitação:

- Notificação para o analista de RH do envio do e-mail para o gestor da vaga sobre descrição do cargo.

H3: Eu como analista de RH desejo ver as solicitações de cargo enviadas para os gestores.

Critério de aceitação:

- Deve ser apresentado uma lista de solicitações enviadas com os seguintes dados:
 - tipo de vaga, gestor, data da solicitação, datas dos upload, visualizar as comunicações realizadas .
- Pode-se visualizar os filtros: por data de solicitação, por tempo de envio, abertas, encerradas.

H4: Eu como candidato a usuário da ferramenta de RS (Recrutamento e Seleção) desejo efetuar o meu cadastro.

Critério de aceitação:

- Candidatos a usuários podem ser analista de RH, gestor, candidatos.
- Apresentar a política de privacidade de dados.
- Solicitar o consentimento do usuário para disponibilização dos dados.
- Mostrar em uma janela, para cada entrada de dados pessoais seja apresentado a finalidade do uso dos dados, base legal e o tempo de retenção da informação no sistema.
- Apresentar os direitos do titular de dados:
 - Os usuários têm direito a solicitar, a qualquer momento e mediante requisição expressa:
 - confirmação da existência de tratamento;
 - acesso aos dados;
 - correção de dados incompletos, inexatos ou desatualizados;
 - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;

- portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
 - eliminação dos DPs tratados com seu consentimento, exceto aqueles utilizados no cumprimento de obrigação legal ou regulatória pela EMPRESA;
 - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
 - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
 - revogação do consentimento;
- Para exercer seus direitos de titular ou esclarecer qualquer dúvida que porventura venha a ter, deve entrar em contato com a EMPRESA através do e-mail POC@xxxxx.xxx.xx (Ponto de Contato) que lhe retornará em até 15 dias.
 - De forma a garantir a sua correta identificação como titular dos DPs objeto da solicitação, é possível que sejam solicitados documentos ou demais comprovações que possam validar sua identidade. Nessa hipótese, você será informado previamente.

H5: Eu como usuário desejo saber quais são os dados que tenho armazenado nessa ferramenta.

Critério de Aceitação:

- Disponibilizar todos os dados fornecidos pelo usuário. Caso seja candidato, mostre o currículo.

H6: Eu como usuário desejo alterar os meus dados pessoais.

Critério de Aceitação:

- Disponibilizar todos os dados fornecidos pelo usuário. Caso seja candidato, mostre o currículo.

H7: Eu como usuários desejo remover os meus dados pessoais.

Critério de Aceitação:

- Deve ser informado ao titular dos dados, quais serão as consequências da remoção dos DP da ferramenta.
- Efetuar a remoção lógica do sistema.
- Comunicar ao usuário a remoção dos dados.

H8: Eu como analista de RH desejo preencher a descrição do cargo (Job Description) para disponibilizar vagas para um cargo.

Critério de Aceitação [Camilo et al., 2018]:

- Na descrição da Job Description deve conter:
 - Data da solicitação da vaga
 - Nome da posição: nomenclatura do cargo
 - Informações da posição
 - Departamento: área ou diretoria em que a vaga está sendo disponibilizada
 - Empresa contratante
 - Ramo de atuação
 - Localidade
 - Sites de divulgação: Cato, LinkedIn, grupos whatsapp, grupos telegram, facebook, instagram
 - Gestor responsável do Departamento: pessoa que solicitou a abertura da posição - Gestor do futuro colaborador
 - Modo de divulgação: interna, externa ou mista
 - Principais atividades/ funções a serem desenvolvidas pelo futuro colaborador
 - Principais responsabilidades pertinentes ao futuro colaborador
 - Formação
 - Certificações
 - Experiências prévias
 - Competências técnicas
 - Competências comportamentais
 - Pacote de remuneração: salário, benefícios, bonificações
 - Tipo de vínculo: estagiário, CLT, PJ
 - Condições de trabalho: presencial, remota ou mista. Caso remoto, o candidato poderá receber equipamentos ou mobiliários
 - Horário de trabalho
 - Hierarquias
 - Restrições: situações ou condições que limitam as opções da vaga, por exemplo, para trabalho remoto o candidato deve ter uma sala individual para trabalhar
 - Desafios
 - Requisitos desejáveis
- Enviar confirmação via tela do cadastro da Job Description.
- Caso algum campo não seja informado, comunicar ao analista de RH.

H9: Como um candidato eu quero poder cadastrar meu currículo.

Critério de Aceitação:

- Os formatos dos arquivos aceitos para upload dos currículos são .pdf ou .doc ou .txt.
- Solicitar o consentimento do usuário para disponibilização dos dados em tais situações:
 - envio de vagas disponíveis
 - envio de status da vaga almejada
 - envio de dicas para uma melhor performance profissional
 - envio de propagandas
 - envio de mensagens sobre atualização do currículo
 - solicitar o tempo de retenção do currículo
 - durante o processamento da vaga almejada
 - ou até dois anos do registro do currículo
- Mostrar em uma janela, para cada entrada de dados pessoais seja apresentado a finalidade do uso dos dados, base legal e o tempo de retenção da informação no sistema.

H10: Como um candidato eu quero poder me candidatar a uma vaga.

Critério de Aceitação:

- Somente vagas em aberto podem receber candidaturas
- O sistema informa que a candidatura foi realizada com sucesso
- O candidato deve informar nome completo, e-mail, link para currículo, linkedin, instagram, facebook, whatsapp, etc

H11: Como um candidato, eu quero poder ter a opção de retirar minha candidatura a qualquer momento.

Critério de Aceitação:

- Apresenta a candidatura que tenha sido feita anteriormente
- O sistema informa que a candidatura foi removida com sucesso

H12: Como um candidato, eu quero poder ter acesso a todas as minhas candidaturas.

Critério de Aceitação:

- Apresentar em ordem de data as candidaturas.
- Filtrar por cargo, data, salário, benefícios, dados do Job Description.
- O sistema informa que a candidatura foi removida com sucesso.

H13: Como um gestor eu quero poder visualizar os candidatos das minhas vagas.

Critério de Aceitação:

- Somente os currículos dos candidatos que se candidataram para a vaga são exibidos.

H14: Como um gestor eu quero visualizar o status das minhas vagas disponibilizadas.

Critério de Aceitação:

- Visualizar vagas abertas, fechadas, todas, por data, cargo, por estágio de recrutamento, por estágio de seleção.
- Mostrar lista ordenada por data de registro.
- O status de uma vaga pode ser: em preparação, aprovada, publicada, triagem de currículos, teste escrito, entrevista, entrevista com gestor, congelada, encerrada.

H15: Como assistente de RH, eu desejo visualizar o painel de vagas.

Critério de Aceitação:

- Visualizar vagas abertas, fechadas, todas, por cargo (analista de marketing júnior, desenvolvedor full stack, ...), por data de publicação, por número de vagas, por área, por perfil (analista, especialista desenvolvedor, gerente, estagiário,..), por status de vaga, pelo recrutador responsável, por cidade, por estágio de recrutamento, por estágio de seleção, data de expectativa de fechamento, data de fechamento realizada, farol (em tempo, atrasada, crítica, poucos candidatos) .

H16: Como assistente de RH, eu desejo visualizar dashboard de vagas.

Critério de Aceitação:

- Visualizar vagas publicadas atualmente, posições em aberto atualmente (total de vagas), vagas publicadas por área, vagas publicadas por recrutadores, tempo médio de

preenchimento de vagas, tempo médio de preenchimento de vagas por posição ou por área, vagas por perfil, vagas por status, vagas por recrutadores.

H17: Como assistente de RH, eu desejo cadastrar vagas.

Critério de Aceitação:

- Cadastrar vagas: nome da vaga, área da vaga, data de abertura de vaga, número de posições para a vaga.
- Definir critérios de seleção: critério 1, critério 2, ...,
 - Definir critérios de seleção de vaga e seus respectivos pesos: relevância de currículo, disponibilidade imediata, boa comunicação oral, boa comunicação escrita, conhecimentos básicos em informática, experiência em atendimento, iniciativa, flexibilidade, senso crítico, capacidade de trabalhar sob pressão, saber trabalhar em equipe, etc... Para cada uma definir peso para o critério.
- Atribuir peso para cada critério (valores de 0 a 5 - 0 é não está cadastrado, 1 não possui, 2 razoável, 3 bom, 4 ótimo, 5 excelente).

H18: Como assistente de RH, eu desejo selecionar as etapas da seleção de vagas.

Critério de Aceitação:

- Etapas de vagas: O status de uma vaga pode ser: em preparação, aprovada, publicada, triagem de currículos, teste escrito, entrevista com assistente RH, entrevista com gestor, dinâmica de grupo, congelada, encerrada.

H19: Como assistente de RH, eu desejo cadastrar o desempenho do candidato na etapa.

Critério de Aceitação:

- Etapas de vagas: triagem de currículos, teste escrito, entrevista com assistente RH, entrevista com gestor, dinâmica de grupo.
- Selecionar a etapa.
- Selecionar o candidato.
- Cadastrar nota do candidato em cada etapa.
- Calcular o desempenho do candidato.
- Mostrar o status do candidato: (em avaliação, reprovado).

H20: Como assistente de RH, eu desejo visualizar dashboard de candidatos para uma vaga.

Critério de Aceitação:

- Visualizar vagas publicadas atualmente, número de candidatos por etapa, média de notas dos candidatos por critério de seleção.

4.4. MODELO DE DADOS

O modelo de dados criado para este trabalho foi desenvolvido com o objetivo de fornecer a melhor estrutura para armazenar e manipular as informações relacionadas ao sistema. A figura 4.4.1 mostra o modelo idealizado.

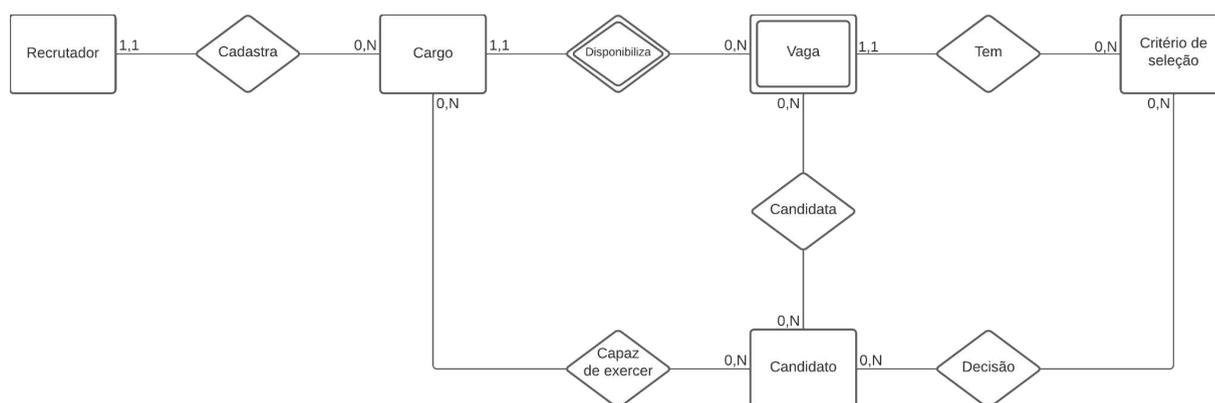


Figura 4.4.1: Modelo de dados

4.5. ARQUITETURA DE SOFTWARE

Uma abordagem amplamente utilizada para o projeto e desenvolvimento de sistemas é a arquitetura de software em 3 camadas. Essa arquitetura divide o sistema em três camadas distintas: a camada de interface do usuário, a camada de negócios e a camada de banco de dados. Cada camada possui responsabilidades específicas e contribui para a funcionalidade do sistema como um todo. A seguir, vamos explorar em detalhes cada uma dessas camadas e como elas interagem para criar uma aplicação robusta e escalável.

A camada de interface do usuário, também conhecida como camada de apresentação, é responsável por toda a interação entre o sistema e o usuário. Essa camada abrange as

interfaces gráficas, páginas da web, APIs ou outros mecanismos utilizados para apresentar informações ao usuário e coletar suas entradas. A principal função da camada de interface do usuário é fornecer uma experiência intuitiva e amigável, garantindo a usabilidade e a satisfação do usuário.

A camada de negócios, também chamada de camada de lógica de negócios, é responsável pela implementação das regras e processos específicos da aplicação. Essa camada processa e manipula os dados recebidos da camada de interface do usuário, aplicando as regras de negócio, validações e cálculos necessários. Aqui, a lógica do sistema é implementada, envolvendo fluxos de trabalho, tomadas de decisão e integração com outros sistemas. A camada de negócios desempenha um papel fundamental na garantia da consistência e integridade dos dados, bem como na execução eficiente das operações.

A camada de banco de dados, também conhecida como camada de persistência, é responsável pelo armazenamento e recuperação dos dados do sistema. Essa camada interage com um sistema de gerenciamento de banco de dados (SGBD) e lida com a persistência dos dados em um formato estruturado. Ela fornece operações de consulta, inserção, atualização e exclusão de dados, permitindo o acesso eficiente às informações armazenadas. A camada de banco de dados desempenha um papel crítico na garantia da integridade dos dados, na segurança e no desempenho do sistema.

A arquitetura de software em três camadas, com a separação da interface do usuário, lógica de negócios e banco de dados, fornece uma estrutura sólida para o desenvolvimento de sistemas escaláveis, modulares e fáceis de manter. A divisão em camadas permite que cada uma delas seja desenvolvida, testada e mantida de forma independente, facilitando a colaboração e a evolução do sistema.

4.6. TELAS DO SISTEMA

O site do Talentos Online foi construído utilizando telas o mais simples possível para facilitar o uso por diferentes tipos de usuários. A seguir algumas telas demonstrativas.

A figura 4.6.1 mostra a tela de login da aplicação, onde o usuário pode realizar o acesso à plataforma.

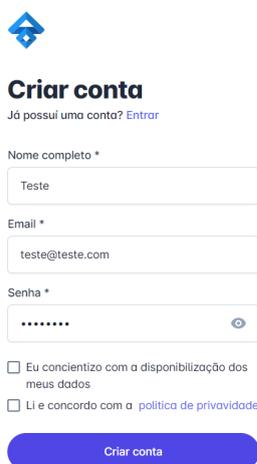


The login form features a blue logo at the top left. Below it, the title "Login" is displayed in bold. A link "Ainda não possui uma conta? Cadastre-se" is positioned below the title. The form includes two input fields: "Email *" with the value "teste@teste.com" and "Senha *" with masked characters. A blue "Entrar" button is located at the bottom.



Figura 4.6.1: Tela de login

A figura 4.6.2 mostra a tela de cadastro da aplicação, onde o usuário pode criar sua conta na plataforma.



The registration form features a blue logo at the top left. Below it, the title "Criar conta" is displayed in bold. A link "Já possui uma conta? Entrar" is positioned below the title. The form includes three input fields: "Nome completo *" with the value "Teste", "Email *" with the value "teste@teste.com", and "Senha *" with masked characters. Below the fields are two checkboxes: "Eu concientizo com a disponibilização dos meus dados" and "Li e concordo com a política de privacidade". A blue "Criar conta" button is located at the bottom.

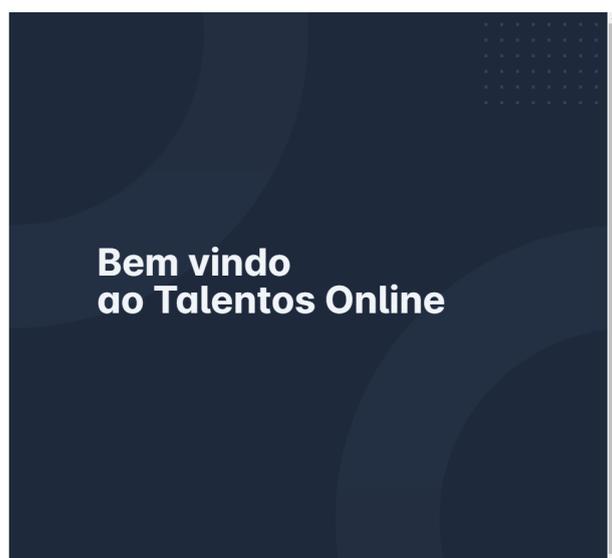


Figura 4.6.2: Tela de cadastro

A figura 4.6.3 mostra a tela de submissão de currículo, onde o usuário pode cadastrar seu currículo na plataforma.

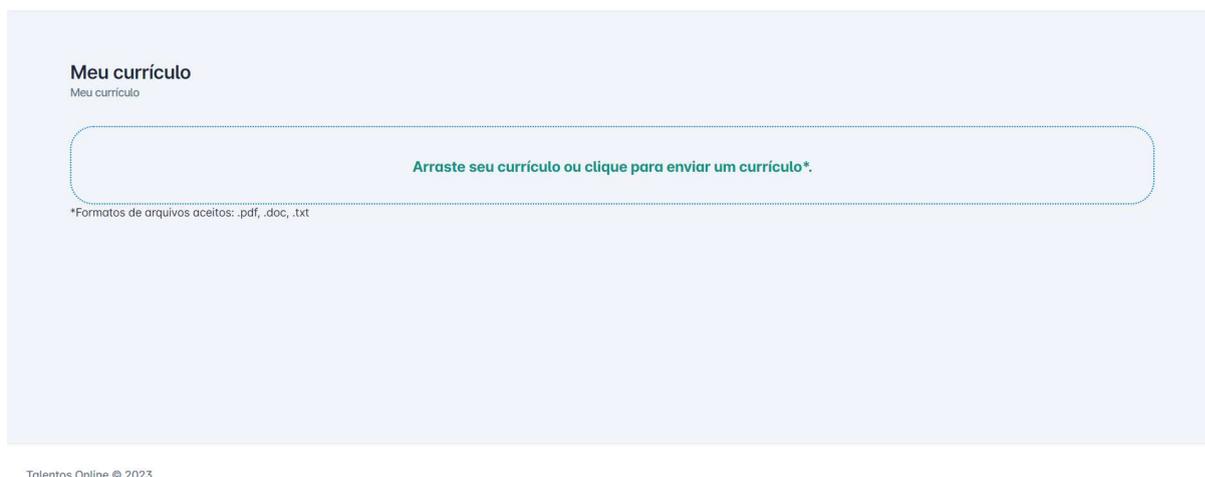


Figura 4.6.3: Tela de submissão do currículo

A figura 4.6.4 mostra a tela de listagem das vagas, onde o usuário pode se candidatar a uma vaga ou visualizar os requisitos exigidos.

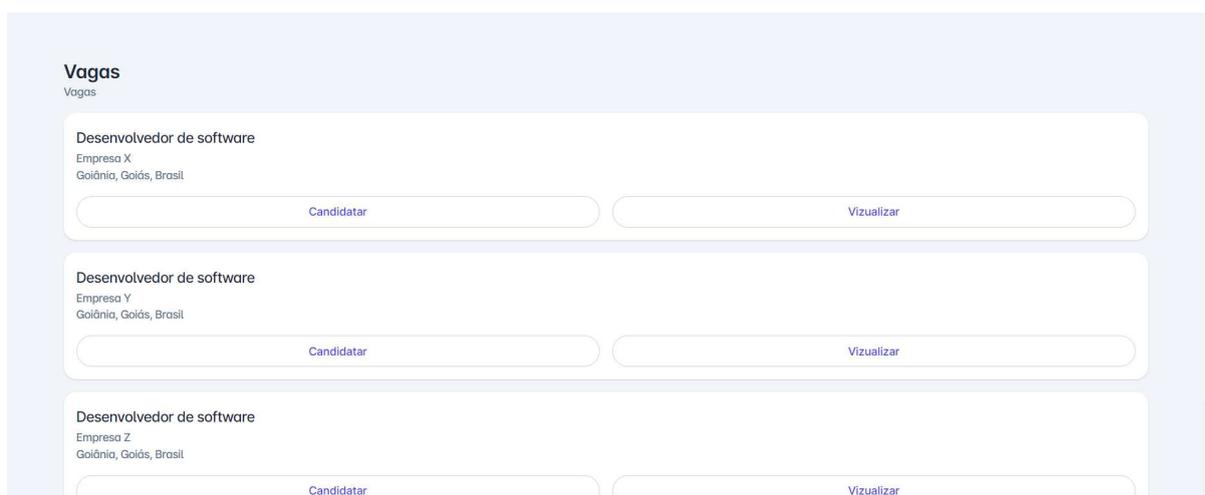


Figura 4.6.4: Tela de listagem de vagas

A figura 4.6.5 mostra a tela de exibição dos dados da, onde o usuário pode visualizar todas as informações fornecidas.

Desenvolvedor de software
Empresa X, Goiânia, Goiás, Brasil

Data da solicitação da vaga 01/06/2023	Posição Desenvolvedor	Informações da posição Desenvolvedor de software
Departamento T.I.	Empresa XYZ	Ramo de atuação Tecnologia
Localidade Goiânia, Goiás, Brasil	Sites de divulgação	Gestor responsável do Departamento
Modo de divulgação	Principais atividades/ funções a serem desenvolvidas	Principais responsabilidades
Formações	Certificações	Experiências prévias
Competências técnicas	Competências comportamentais	Pacote de remuneração Salário de R\$ 1.000,00 + benefícios e bonificações

Figura 4.6.5: Tela de detalhes da vaga

A figura 4.6.6 mostra a tela de exibição dos dados do usuário, onde o usuário pode visualizar todos os dados fornecidos à plataforma, bem como gerenciar eles como adicionar informações, editar ou excluir.

Meus dados
Meus dados

Nome
Lucas Melo

Curriculo
Remover

Vizualizar

Salvar

Talentos Online © 2023

Figura 4.6.6: Tela de listagem dos dados coletados pelo sistema

4.7. RELATÓRIO DE IMPACTO

Uma das exigências que a LGPD estabelece está na elaboração de um relatório de impacto à proteção de dados pessoais (RIPD). Este relatório é um documento que descreve quais processos podem gerar riscos à proteção de dados pessoais previstos na LGPD (ANPD, 2023).

No RIPD, são identificados os dados pessoais envolvidos bem como suas finalidades de tratamento, medidas de segurança que foram adotadas, possíveis riscos e impactos e as medidas utilizadas para mitigar e ficar em conformidade com a legislação. Ou seja, este

relatório visa fornecer uma visão abrangente sobre como os dados pessoais são tratados e como a privacidade e a segurança desses dados são protegidos.

O RIPD também pode abordar outros aspectos relevantes, tais como:

- Requisitos funcionais e não funcionais (RMS)
- Processo de negócios
- Identificar os dados
- Finalidade de processamento
 - identificar a base legal
- Descrição de como os dados são coletados, de quem os dados são coletados (titulares) e o por que?
- Indicação de quais perfis do sistema terão acesso a esses dados
- Com quais sistemas da informação e ou com quais terceiros os DPs serão compartilhados
- Declaração de justificativa para processamento dos DPs
- Visão geral da arquitetura funcional (ou lógica)
- Visão geral da arquitetura física
- Estrutura e lista de bancos de dados (tabelas e campos)
- Diagrama do fluxo de dados por entidades e por interfaces
- Diagrama de fluxo de dados através do ciclo de vida do DP
- Visão geral da arquitetura funcional (ou lógica)
- Visão geral da arquitetura física
- Estrutura e lista de bancos de dados (tabelas e campos)
- Diagrama do fluxo de dados por entidades e por interfaces
- Diagrama de fluxo de dados através do ciclo de vida do DP
- Diagrama de fluxo de dados através do ciclo de vida do DP, exemplo, geração, uso, transferência e descarte de DP
- Diagrama de fluxo de trabalho que descreve quando notificar e obter o consentimento dos titulares do DP
- Mapeamento do processo da interface, definindo as partes conectadas e os campos de dados transferidos
- Detalhes de portas, protocolos, APIs e detalhes de criptografia

É recomendado consultar as melhores práticas fornecidas pelas autoridades de proteção de dados, como a Autoridade Nacional de Proteção de Dados (ANPD) no Brasil, para garantir a conformidade e a eficácia do relatório.

A tabela 4.7.1 mostra para cada história de usuário os potenciais riscos à privacidade dos dados envolvidos considerando as ameaças e vulnerabilidades que podem comprometer a confidencialidade e a integridade das informações.

HISTÓRIAS DE USUÁRIO	RISCOS À PRIVACIDADE
H1	Vazamento de informações sensíveis caso o e-mail seja interceptado ou acessado por terceiros não autorizados
H2	Risco de phishing onde o atacante pode se passar pelo analista de RH para obter informações confidenciais ou induzir o gestor a realizar ações inseguras.
H3	Acesso não autorizado
H4	Consentimento não adequado
H5	Falha na autenticação ou no controle de acesso
H6	Acesso não autorizado Violação na integridade dos dados
H7	Falha na remoção adequada dos dados Acesso não autorizado ao dados
H8	Acesso não autorizado
H9	Vazamentos de dados durante o processo de salvamento do currículo
H10	Divulgação ou acesso de dados não autorizados
H11	Retenção de dados mesmo após o pedido de remoção
H12	Acesso a candidaturas de outros usuários. Violação na integridade dos dados.
H13	Acesso a candidaturas de vagas de outros usuários. Violação na integridade dos dados.
H14	Acesso não autorizado por usuários não gestores. Violação na integridade dos dados.
H15	Acesso não autorizado por usuários não assistentes. Violação na integridade dos dados.

H16	Acesso não autorizado por usuários não assistentes. Violação na integridade dos dados.
H17	Acesso não autorizado por usuários não assistentes. Violação na integridade dos dados.
H18	Acesso não autorizado por usuários não assistentes de RH. Violação na integridade dos dados.
H19	Acesso não autorizado por usuários não assistentes de RH. Violação na integridade dos dados.
H20	Acesso não autorizado por usuários não assistentes de RH. Violação na integridade dos dados.

Tabela 4.7.1: Listagem dos riscos à privacidade para cada história de usuário

5. CONCLUSÃO E TRABALHOS FUTUROS

Este trabalho buscou desenvolver um site que fosse capaz de apoiar empresas e organizações no processo de recrutamento de pessoas, utilizando conceitos que priorizam a privacidade dos dados. Com base nos resultados coletados foi possível identificar o impacto que uma ferramenta que lida de maneira coerente com os dados de seus usuários tem. A confiança aumenta pois o usuário tem total poder sobre seus dados, tendo ciência de quando, onde e por que seus dados podem ser usados. Além de que, pode pedir a remoção deles a qualquer momento mediante solicitação.

Os desafios e dificuldades enfrentadas estão relacionados ao aperfeiçoamento dos conhecimentos nas tecnologias utilizadas para o desenvolvimento do site. Também se tratando da aplicação em si, o grande volume de dados que são necessários coletar e o correto armazenamento deles.

5.1. LIÇÕES APRENDIDAS

Ao final do estudo, podemos destacar algumas lições como a importância de se ter uma abordagem proativa em relação a segurança e privacidade do usuário, buscando mitigar os riscos desde o início do desenvolvimento do software.

5.2. TRABALHOS FUTUROS

Durante o desenvolvimento deste trabalho, foi possível identificar pontos que podem ser abordados para complementa-lo em futuras versões como realizar testes e validação do

sistema de recrutamento com o público geral, desenvolver versões da aplicação que sejam compatíveis nativamente com dispositivos móveis como nas plataformas IOS e Android e adaptação a futuras mudanças nas legislações e regulamentações vigentes.

6. REFERÊNCIAS

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm>. Acesso em: 09 abr. 2023.

UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, de 23 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de Dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).

Mais de 443 mil brasileiros foram vítimas de vazamentos do Facebook, Veja, 2018. Disponível em: <<https://veja.abril.com.br/economia/mais-de-443-mil-brasileiros-foram-afetados-no-escandalo-do-facebook>> Acesso em: 10 jun. 2023

CAVOUKIAN, Ann. Privacy by Design: The 7 Foundational Principles. Disponível em: <<https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf>>

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 29134:2017 - Tecnologia da informação - Técnicas de segurança - Diretrizes para a privacidade no projeto de sistemas. Rio de Janeiro, 2017

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002:2022 - Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão de segurança da informação. Rio de Janeiro, 2022

Autoridade Nacional de Proteção de Dados (ANPD), Relatório de Impacto à Proteção de Dados Pessoais (RIPD). Disponível em: <https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd>. Acesso em: 12 jun. 2023.



PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
GABINETE DO REITOR

Av. Universitária, 1069 • Setor Universitário
Caixa Postal 86 • CEP 74605-010
Goiânia • Goiás • Brasil
Fone: (62) 3946.1000
www.pucgoias.edu.br • reitoria@pucgoias.edu.br

RESOLUÇÃO nº 038/2020 – CEPE

ANEXO I

APÊNDICE ao TCC

Termo de autorização de publicação de produção acadêmica

O estudante LUCAS MELO RODRIGUES do Curso de CIÊNCIA DA COMPUTAÇÃO, matrícula 2019.2.0028.0059-1 na qualidade de titular dos direitos autorais, em consonância com a Lei nº 9.610/98 (Lei dos Direitos do Autor), autoriza a Pontifícia Universidade Católica de Goiás (PUC Goiás) a disponibilizar o Trabalho de Conclusão de Curso intitulado IMPLANTAÇÃO DE PRIVACY BY DESIGN NO SISTEMA DE RECRUTAMENTO DE PESSOAS, gratuitamente, sem ressarcimento dos direitos autorais, por 5 (cinco) anos, conforme permissões do documento, em meio eletrônico, na rede mundial de computadores, no formato especificado (Texto(PDF); Imagem (GIF ou JPEG); Som (WAVE, MPEG, AIFF, SND); Vídeo (MPEG, MWV, AVI, QT); outros, específicos da área; para fins de leitura e/ou impressão pela internet, a título de divulgação da produção científica gerada nos cursos de graduação da PUC Goiás.

Goiânia, 16 de Junho de 2023.

Assinatura do autor: _____

Lucas Melo Rodrigues

Nome completo do autor: Lucas Melo Rodrigues

Documento assinado digitalmente



ADRIANA SILVEIRA DE SOUZA

Data: 30/06/2023 09:41:18-0300

Verifique em <https://validar.itl.gov.br>

Assinatura do professor-orientador: _____

Nome completo do professor-orientador: Adriana Silveira de Souza