UNIVERSIDADE EVANGÉLICA DE GOIÁS - UNIEVANGÉLICA
ENGENHARIA DE SOFTWARE

GOODYER SOUSA DE ARAUJO
VICTOR HUGO PIGNATA DOS SANTOS

DESENVOLVIMENTO DE SOFTWARE GERENCIAL PARA PROVEDORES DE INTERNET CONSIDERANDO ASPECTOS DA SEGURANÇA DA INFORMAÇÃO E LEI GERAL DE PROTEÇÃO DE DADOS

ANÁPOLIS – GO
2022

GOODYER SOUSA DE ARAUJO
VICTOR HUGO PIGNATA DOS SANTOS

DESENVOLVIMENTO DE SOFTWARE GERENCIAL PARA PROVEDORES DE INTERNET CONSIDERANDO ASPECTOS DA SEGURANÇA DA INFORMAÇÃO E LEI GERAL DE PROTEÇÃO DE DADOS

Trabalho apresentado ao Curso de Engenharia de Software da Universidade Evangélica de Goiás – UniEVANGÉLICA, da cidade de Anápolis-GO como requisito parcial para obtenção do Grau de Bacharel em Engenharia de Software.

Orientador (a): Prof. Eduardo Ferreira de Souza

ANÁPOLIS - GO
2022

FICHA CATALOGRÁFICA

ARAUJO, Goodyer Sousa. PIGNATA, Victor Hugo; SANTOS**. Desenvolvimento de Software Gerencial para Provedores de Internet Considerando Aspectos da Segurança da Informação e Lei Geral de Proteção de Dados. Anápolis**, 2022. (Universidade Evangélica de Goiás – UniEVANGÉLICA, Engenheiro(a) de Software, 2022).

Monografia. Universidade Evangélica de Goiás, Curso de Engenharia de Software, da cidade de Anápolis-GO.

1. LGPD. Segurança. Software. Dados.

REFERÊNCIA BIBLIOGRÁFICA

ARAUJO, Goodyer Sousa. PIGNATA, Victor Hugo; SANTOS. **Desenvolvimento de Software Gerencial para Provedores de Internet Considerando Aspectos da Segurança da Informação e Lei Geral de Proteção de Dados.** Anápolis, 2022. 30 páginas. Monografia - Curso de Engenharia de Software, Universidade Evangélica de Goiás - UniEVANGÉLICA.

CESSÃO DE DIREITOS

NOMES DOS AUTORES: VICTOR HUGO PIGNATA DOS SANTOS
GOODYER SOUSA DE ARAUJO
TÍTULO DO TRABALHO: DESENVOLVIMENTO DE SOFTWARE GERENCIAL PARA PROVEDORES DE INTERNET CONSIDERANDO ASPECTOS DA SEGURANÇA DA INFORMAÇÃO E LEI GERAL DE PROTEÇÃO DE DADOS.
GRAU/ANO: 10 Período / 2022

É concedida à Universidade Evangélica de Goiás - UniEVANGÉLICA, permissão para reproduzir cópias deste trabalho, emprestar ou vender tais cópias para propósitos acadêmicos e científicos. O autor reserva outros direitos de publicação e nenhuma parte deste trabalho pode ser reproduzida sem a autorização por escrito do autor.

_____

Goodyer Sousa de Araujo
Victor Hugo Pignata dos Santos
Anápolis – GO.

GOODYER SOUSA DE ARAUJO
VICTOR HUGO PIGNATA DOS SANTOS

DESENVOLVIMENTO DE SOFTWARE GERENCIAL PARA PROVEDORES DE INTERNET CONSIDERANDO ASPECTOS DA SEGURANÇA DA INFORMAÇÃO E LEI GERAL DE PROTEÇÃO DE DADOS

Trabalho de Conclusão de Curso de Engenharia de Software da Universidade Evangélica de Goiás - UniEVANGÉLICA, da cidade de Anápolis-GO apresentado como requisito parcial para obtenção do grau de Engenheiro(a) de Software.

Aprovado por:

_____

Prof. Eduardo Ferreira de Souza

_____

Prof. Ms.
(AVALIADOR)

Anápolis 2022

RESUMO

A LGPD (Lei Geral de Proteção de Dados) tem como objetivo proteger os direitos fundamentais de liberdade e privacidade às empresas brasileiras que trabalham com dados, a mesma se aplica ao tratamento de dados de clientes e potenciais clientes classificados como pessoas jurídicas ou físicas. O objetivo da lei é estabelecer regras sobre coleta, armazenamento, tratamento e compartilhamento de dados pessoais, incluindo informações coletadas por instituições jurídicas. Empresas responsáveis pelo fornecimento de internet já estão diretamente ligadas à nova lei,. Para que os provedores de internet correspondam com a LGPD, algumas medidas devem ser adotadas, entre elas a criação da política de proteção de dados e a documentação das ferramentas utilizadas para a coleta e armazenamento de dados. Diante deste contexto, este trabalho, apresentará o desenvolvimento de um software gerencial para controle de atendimento destinado a provedores de internet. Voltado para empresas que atendem às normas da LGPD e em conjunto ao desenvolvimento será criado um modelo de política de proteção de dados.

Palavras-Chave: provedor de internet, dados, privacidade, aplicativo, lei geral de proteção de dados.

ABSTRACT

The General Data Protection Law brings new guidelines for Brazilian companies that work with data, which does not only apply to the treatment of customer data or potential customers classified as legal entities. The purpose of the law is to properly handle the personal data of individuals, including information collected by legal institutions. As a result of the provisions of the law for the treatment of this data, the companies responsible for providing the internet are directly linked to the new law, the internet providers that are the main internet service providers must comply with the terms of the law. Thus, for internet providers to comply with the LGPD, some measures must be adopted, including the creation of a data protection policy and documentation of the tools used for data collection and storage. Given this context, in this work, the development of management software to control service for internet providers that meets the LGPD standards will be presented and, in parallel with the development, a model of data protection policy will be created.

Keywords: internet provider, data, privacy, application, general data protection law.

LISTA DE ABREVIATURAS E SIGLAS

LGPD	Lei Geral de Proteção de Dados
RG	Carteira de Identidade ou Registro Geral
CPF	Cadastro de Pessoa Física
IP	Endereço do Protocolo de Internet
ANPD	Autoridade Nacional de Proteção de Dados
MCTIC	Ministério da Ciência, Tecnologia e Inovações
IBGE	Instituto Brasileiro de Geografia e Estatística
UML	*Unified Modeling Language*
TI	Tecnologia da Informação
CMS	Content Management System Sistema de Gerenciamento de Conteúdo
DPIA	Relatório de Impacto à Proteção de Dados
GRPD	Regulamento Geral de Proteção de Dados
TCP	Protocolo de controle de transmissão
SCM	Serviço de Comunicação Multimídia
ANATEL	Agência Nacional de Telecomunicações
SICI	Sistema Integrado de Coleta de Informações
SQG	Sistema de Gestão da Qualidade
CHAT	Conversa na Internet cujos participantes trocam mensagens
MVP	*Minimum Viable Product*
WEB	*World Wide Web*
RF	Requisito Funcional
RNF	Requisito não Funcional
RN	Regra de negócio

SUMÁRIO

1 INTRODUÇÃO

Atualmente, a Lei n.º 13.709/2018, chamada de Lei Geral de Proteção de Dados (LGPD), trouxe diversas garantias e segurança para a população brasileira referente às suas informações pessoais, bem como a responsabilidade dos provedores de internet no tratamento de dados pessoais e sensíveis de seus clientes, visando regulamentar os atos irregulares no tratamento de informações pessoais (MORELLATO, 2021).

A LGPD foi promulgada para proteger os direitos fundamentais à liberdade e privacidade, bem como o livre desenvolvimento da personalidade de cada indivíduo. A lei regulamenta o tratamento de dados pessoais armazenados em meio físico ou eletrônico, seja por pessoa física ou pessoa jurídica de direito público ou privado, e abrange um amplo leque de operações de dados que podem ocorrer em meio manual ou eletrônico (ABRINT, 2020).

Com isso, no presente trabalho será explorado a responsabilidade dos provedores perante a LGPD e as principais características da Lei e dos provedores de internet, onde será tratado quais medidas os provedores de acesso devem acolher para se precaver partindo desde a contratação do serviço até o atendimento aos clientes.

Ainda nesse sentido, será desenvolvido um aplicativo de serviços de chamados (help desk), onde a principal função de um sistema de *help desk* é receber consultas e fornecer soluções, as perguntas são dúvidas em necessidades ou problemas relatados pelos usuários por meio de mensagens eletrônicas cadastradas no sistema. A área de Help Desk oferece soluções em que a empresa possa agilizar o serviço de atendimento ao cliente, o aplicativo realizará a coleta e tratamento de dados pessoais dos usuários, atendendo os princípios da LGPD.

1.1. Problema

A LGPD aborda diversos tipos de informações que devem ser tratados como dados pessoais de uma pessoa física, sendo os principais Nome, sobrenome, data de nascimento, documentos pessoais (como RG, CPF, CNH, Carteira de Trabalho, passaporte, título de eleitor e outros), endereço residencial ou comercial, telefones, endereços de e-mail, geolocalização coordenadas, cookies e endereços IP.

Tudo o que é feito com dados pessoais é considerado tratamento de dados, incluindo coleta, classificação, armazenamento, transferência, consulta, transmissão a terceiros, exclusão e qualquer outro tipo de uso (MORELLATO, 2021).

Empresas responsáveis pelo fornecimento de serviços de internet devem se adequar à nova lei geral de proteção de dados, para que essa adaptação o uso de aplicativos/softwares de gerenciamento de serviços e coleta de dados é essencial para facilitar o atendimento ao cliente e o controle dos dados coletados, dessa maneira, os aplicativos utilizados também devem estar dentro dos temos da lei, principalmente aqueles onde os dados são disponibilizados para mais de uma pessoa sendo ela colaboradores ou prestadores de serviços, nisso o cliente também deve estar ciente sobre como serão tratados seus dados pessoais. Nesse sentido, como o uso de software de gerenciamento de dados deve atender a LGPD e quais as principais adequações que o provedor de internet deve aderir nos processos envolvendo os dados pessoais dos clientes?

1.2. Objetivos Gerais

Apresentar as etapas de adequação para provedores de internet segundo a LGPD e desenvolver um aplicativo de chamados para tratamento de dados que esteja dentro das normas da lei de proteção de dados.

1.3. Objetivos Específicos

- Criação do processo de adequação à LGPD.
- Criação da política de privacidade para provedores atendendo os requisitos da LGPD.
- Identificar dados sensíveis que serão processados pelo aplicativo.
- Desenvolver aplicativo de abertura de chamados.

1.4. Justificativa

A LGPD - Lei n.º 13.709/2018 — foi aprovada em 14 de agosto de 2018 e entrou em atividade a partir de 15/08/2020, influenciada pela lei europeia de proteção de dados (MURELLATO, 2021), além da própria LGPD, também foi criada a Lei n.º 13.853/2019, que criou a Autoridade Nacional de Proteção de Dados (ANPD) e estabelece sanções para os casos de descumprimento da LGPD, a regulamentação da ANPD foi aprovada em 28 de outubro de 2021 (BRASIL, 2018).

Para Abrint (2020) entender o propósito e os princípios básicos da LGPD é o primeiro passo para iniciar qualquer trabalho. Isso porque o objetivo do provedor de Internet na coleta e processamento de dados deve ser coerente com esses princípios, influenciando a tomada de decisão no desenvolvimento e/ou implementação de novas tecnologias e serviços para seus clientes. Segundo Morellato (2021), um provedor de Internet que realiza coleta de dados é chamado de controlador de dados, sendo ele responsável pela manutenção e proteção dos dados. A proteção de dados deve ser observada em todas as fases de implantação de um serviço, e sempre da forma mais protetora para o titular dos dados ou seja, desde o momento da contratação de um serviço e/ou produto, medidas técnicas e administrativas devem ser implementadas para evitar o acesso não autorizado aos dados de qualquer pessoa que esteja envolvida no processo prestação e contratação de serviços, sendo eles funcionários ou clientes.

No decorrer desse trabalho, será apresentado como é feita a obtenção de dados e que medidas devem ser tomadas pelos provedores para atender a lei de proteção de dados.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Segurança da Informação e a LGPD

Para Fontes (2012) a segurança da informação é fundamental para a sobrevivência de qualquer organização que faça parte da sociedade da informação. Observa-se que as atividades de uma organização são vulneráveis a ameaças internas e externas, que podem variar desde vulnerabilidades tecnológicas em software e hardware até vulnerabilidades humanas, oriundas de funcionários despreparados para trabalhar nesse ambiente. As organizações devem implementar um processo de segurança da informação, que, como muitos outros, deve ser considerado uma atividade organizacional.

A segurança da informação é alcançada por meio da implementação de um conjunto apropriado de controles, que inclui políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware. Estes controles devem ser estabelecidos, implementados, monitorados, analisados criticamente e aprimorados, conforme necessário, para garantir que os objetivos de negócios e a segurança da informação da organização sejam atendidos (BAARS, 2018).

Sêmola (2014) define a segurança da informação como uma área do conhecimento dedicada à proteção das atividades relacionadas à informação contra acesso não autorizado, alterações não autorizadas ou inacessibilidade, ou como uma prática de gerenciamento de risco que envolve o compromisso com os três principais princípios de segurança: confidencialidade, integridade e disponibilidade da informação.

- **Confidencialidade:** Todas as informações devem ser protegidas de acordo com o nível de sigilo a elas atribuído, com o objetivo de restringir o acesso e uso apenas aos indivíduos a quem se destinam;
- **Integridade:** Para proteção contra alterações não autorizadas, intencionais ou acidentais, todas as informações devem ser mantidas nas mesmas condições em que foram fornecidas pelo seu titular;
- **Disponibilidade:** Toda a informação gerada ou adquirida por um indivíduo, ou organização deve estar à disposição dos seus utilizadores sempre que dela necessitem por qualquer motivo.

Como resultado, é necessário que organizações públicas e privadas busquem proteção contra possíveis eventos de segurança da informação, sendo definidos como um estado identificado de um sistema, serviço ou rede que indica uma possível violação da política de segurança da informação ou uma falta de proteção, ou uma situação previamente desconhecida que pode ser relevante, o que pode ocasionar uma violação direta a Lei Geral de Proteção de Dados (LGPD).

A Lei Geral de Proteção de Dados (LGPD) foi criada com o objetivo de regulamentar a coleta, tratamento, armazenamento e compartilhamento de dados pessoais por empresas e organizações (BRASIL,2020). A nova lei, que visa proteger os direitos fundamentais de todos os cidadãos à liberdade e à privacidade, adotou uma abordagem didática ao apresentar definições e conceitos que podem ser compreendidos por todos. Ela possui dez capítulos e 65 artigos, que estão organizados da seguinte forma: Capítulo primeiro introduz as disposições gerais e inclui no art. 2.º os princípios que sustentam a proteção de dados pessoais, no art. 3.º a territorialidade de aplicação da lei, no art. 4.º a inaplicabilidade da lei, e no art. 5.º os conceitos gerais (BRASIL, 2018).

Maldonado (2019) afirma que a LGPD pode ser vista como um freio e um transformador das atuais técnicas do capitalismo de vigilância, com o objetivo de impedir a mineração de dados e as diversas aplicações e usos a que possam ser submetidos sem o conhecimento ou consentimento informado dos usuários. A lei regulamenta o tratamento de dados pessoais, incluindo dados digitais, por pessoas físicas ou jurídicas com direitos públicos, ou privados, com o objetivo de salvaguardar os direitos fundamentais à liberdade e à privacidade, bem como o livre desenvolvimento da personalidade da pessoa. A LGPD estabelece alguns conceitos básicos são estabelecidos pela Lei, em que deve ser de conhecimento de toda empresa que trabalha com dados pessoais:

- **Dados Pessoais:** Informações relativas à pessoa física identificada;
- **Tratamento de Dados:** Toda edição, coleta, arquivamento, transferência, armazenamento, uso, remoção, e/ou classificação de dados pessoais;
- **Controlador:** Determina quais são os dados sobre a atividade de tratamento, devem estudar, elaborar relatórios de impacto, manter as operações de tratamento, determinar as operações de tratamento e adotar medidas responsáveis pela segurança;
- **Operador:** Administra os dados em nome do controlador e é responsável por fazer o processamento dos dados de acordo com as instruções do controlador — interesses e objetivos podem ser uma pessoa física ou jurídica;

- **Autoridade Nacional de Proteção de Dados – ANPD:** órgão da administração pública que faz parte da Presidência da República e tem como finalidade a proteção de dados pessoais e de privacidade.

A LGPD, marcará o início de um processo de adaptação tanto para as empresas quanto para o setor público em termos de práticas de privacidade, terá um impacto significativo na coleta de dados e nos modelos de negócios das empresas. Para os usuários, será uma grande vitória, porque a privacidade é crucial em um mundo onde tudo está conectado.

Como resultado, toda organização deve buscar a conformidade legal e, neste caso, manter-se atualizada sobre as leis, regulamentos e padrões de segurança que se aplicam à privacidade e proteção de dados. Em caso de descumprimento, existe a possibilidade de responsabilização por uma ampla gama de violações, não apenas aquelas relacionadas à Lei Geral de Proteção de Dados (COTS e OLIVEIRA, 2019, p.141). Portanto, organizações públicas e privadas, servidores públicos e funcionários devem entender suas responsabilidades e obrigações legais neste ambiente de alto risco.

A LGPD é fortemente influenciada pelo GRPD (Regulamento Geral de Proteção de Dados), um padrão da União Europeia que rege o tratamento de dados pessoais. Como resultado dessa inspiração, muitos dos conceitos, princípios e interpretações da LGPD são derivados de entendimentos baseados em GDPR (SANTOS, 2021). No que se refere ao Relatório de Impacto à Proteção de Dados – DPIA, porém, diferentemente do GDPR, que possui uma seção específica para esse fim, a LGPD possui disposições para a realização de avaliações de impacto.

O Relatório de Impacto à Proteção de Dados da LGPD é citado pela primeira vez no parágrafo 3º do artigo 4º, inciso III, que estabelece que a ANPD (Autoridade Nacional de Proteção de Dados) deve emitir pareceres técnicos ou recomendações relacionadas às exceções estabelecidas no inciso III e deve solicitar relatórios de impacto aos responsáveis.

A DPIA também é citada no parágrafo 3.º do artigo 10 da LGPD, que trata das situações em que o processamento de dados é permitido com base em interesses legítimos do controlador. No entanto, deve — se notar que o conceito de Relatório de Impacto na Proteção de Dados está definido no artigo 5º, inciso XVII da LGPD, que o define como “documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco” (BRASIL,2020).

De fato, não há orientação sobre o formato do documento na definição da Lei,

cabendo à ANPD tratar da situação e dar a necessária segurança jurídica. Além do conceito esboçado no Artigo 5º, inciso XVII, também é necessário observar o que exige o Artigo 38 da Lei:

> Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial (BRASIL, 2020).

Quando se trata de obrigações, enquanto o GDPR específica alguns tipos de tratamento que precisam da criação de um Relatório, a LGPD não faz, com isso, ainda existe a possibilidade de solicitação da ANPD, sobre a DPIA, com descrição geral do conteúdo do documento no parágrafo único do citado artigo 38 (SANTOS, 2021). Ainda que esta indefinição seja apenas temporária e venha a ser substituída por posterior regulamentação da LGPD pela ANPD ou por atividade legislativa, recomenda — se a elaboração de um Relatório de Proteção de Dados para fins de garantia do comprimento da lei.

Nos tópicos seguintes serão abordados um modelo de negócio e como ele deve se adequar a Lei geral de proteção de dados.

2.2 Provedores de Internet

Os provedores de Internet são ferramentas usadas para navegar na Internet. Como o principal meio de acesso à Internet no Brasil e no mundo o provedor de acesso é uma empresa prestadora de serviço, FARIAS et al (2015) afirma que,

> Em princípio, os provedores de acesso oferecem conexão à internet. Alguns vão além. Muitos deles têm feição híbrida: (a) oferecem conexão à internet e (b) oferecem conteúdo (reportagens, serviços etc.). Ostentam, desse modo, muitos deles, uma função dúplice. Atuam: (a) abrindo as portas da internet aos usuários e (b) produzindo conteúdo. O ideal é que os provedores, ao hospedarem páginas, definem quem é o responsável editorial pela publicação.

Muitas pessoas usam um provedor de Internet, mas poucos entendem como ele funciona. Esse termo foi amplamente utilizado nos primórdios da Internet no Brasil, na década de 1990. Na época, o acesso à rede era fornecido por meio de uma linha telefônica conhecida como "conexão desconectada" (dial-up) (PREVISA, 2020).

Na década de 90, uma série de empresas surgiu com o objetivo de tornar a Internet

uma realidade nos lares brasileiros, entre eles, IG, UOL e TERRA se destacaram e continuam a fazê-lo, reformulando- se e conquistando um nicho único no mercado. Porém, hoje já existem outras maneiras de se conectar, inclusive por meio de redes sem fio, fibra óptica, internet via satélite ou rádio, graças aos provedores de serviços de Internet (LARA, 2019).

Para ter acesso à Internet, o provedor se conecta a redes locais usando TCP/IP, um protocolo de transmissão e recepção de dados baseado no endereçamento de cada um dos pontos ou computadores da rede. Os dados de um provedor de acesso são recebidos por um provedor de serviços de Internet, que os distribui aos usuários por meio de vários métodos, incluindo telefone, fibra óptica, wireless e rádio. Com isso, as empresas que contratam o sinal fornecem acesso à Internet para seus clientes por meio de planos personalizados. Um provedor operacional deve ser responsável por gerenciar e executar processos relacionados, administrativos e gerenciamento de dados de seus clientes e colaboradores, cuidando da rede interna e externa e pela infraestrutura, garantindo uma conexão de qualidade (BESWEB, 2021).

Para se tornar um provedor, a empresa deve primeiro obter uma licença SCM (Serviço de Comunicação Multimídia) da Anatel (Agência Nacional de Telecomunicações). Este certificado evita que a empresa esteja em uma situação anormal, ao mesmo tempo, em que confirma ao cliente que ele receberá um serviço regular, em caso de adversidade, o usuário está legalmente protegido (RESENDE, 2022).

Sempre que um provedor oferece ou fornece produtos, ou serviços a uma pessoa física no Brasil, está sujeito às regras da LGPD para o tratamento de dados pessoais. A proteção de dados deve ser observada em todas as fases de desenvolvimento de produtos e/ou serviços, e sempre da forma mais protetora para o titular dos dados — ou seja, desde o momento da concepção do serviço ao encerramento do mesmo, segurança, medidas técnicas e administrativas devem ser implementados para evitar o acesso não autorizado e destruição de dados (MURELLATO, 2021). Qualquer informação que corresponda a pessoa identificada e que permite descobrir a sua identidade a partir de análise de seu perfil, essa informação está sujeita às regras da LGPD.

Para Maldonado (2019) antes de disponibilizarem um serviço, os provedores devem declarar um objetivo claro, simples e explícito, bem como adequar o tratamento a esse objetivo, limitando-se ao que foi proposto ou ao que o cliente desejava. É importante destacar que o cliente ou potencial cliente tem o direito de acesso fácil, claro e gratuito a todas essas informações e dados pessoais e o acesso gratuito também é uma forma de o titular garantir

que seus dados permaneçam seguros e não adulterados, auxiliando na aplicação de outro princípio da Lei: não haver discriminação ilegal ou abusiva contra pessoas em decorrência do processamento de dados (BRASIL, 2018).

Para evitar o tratamento discriminatório, é necessário aderir a outro princípio legal, o da qualidade dos dados. Os dados devem ser precisos, claros, relevantes e atualizados, reduzindo a possibilidade de erros e abusos. Como resultado, é fundamental que os dados sejam devidamente protegidos, sendo os seguintes três princípios da lei particularmente importantes: segurança de dados, prevenção de acidentes ou atividades ilegais e prestação de contas.

Para situações onde ocorre a irregularidade da Lei, a LGPD estabelece uma série de sanções administrativas que podem ser aplicadas pela Autoridade Nacional aos agentes de tratamento (controladores e / ou operadores), que vão desde uma carta de advertência com prazo para implementação de medidas corretivas a multa simples de até 2% (dois por cento) do faturamento bruto da empresa. Estabelece ainda multa diária, obrigação de divulgação de infrações, bloqueio ou remoção de dados pessoais relacionados a infrações (BRASIL, 2020).

Existem situações em que os provedores terceirizam a responsabilidade do tratamento de dados, porém segundo a LGPD as responsabilidades foram divididas, pois, como dito o provedor é responsável pela posse dos dados dos clientes e funcionários, sendo caracterizado como controlador, e a empresa terceirizada também estará sujeita a nova lei na qualidade de operador de dados, essas que em muitos casos são responsáveis pelo gerenciamento de aplicativos help desk ou servidores de dados (MORELLATO, 2021).

Para Pinheiro (2020) o controlador e o operador devem pensar em regras e meios técnicos para proteger os dados pessoais e verificar sua eficiência nas empresas, seja via uso de recursos de anonimidade, controle de acesso, procedimentos, políticas de gestão e treinamentos para equipes.

Os artigos 37 a 40 da LGPD apresenta as responsabilidades do controlador e operador:

- Manter os registros das operações de tratamento de dados;
- Elaborar o relatório à proteção de dados pessoais;
- Atribuir instruções ao operador;
- Disponibilização aos dados e segurança.

Por outro lado, a LGPD não especifica como será a relação entre o controlador e a

operadora ou se serão agentes internos da empresa, no entanto, é uma circunstância em que pelo menos um contrato de prestação de serviços entre eles serão exigidos, sendo diferenciadas as obrigações de cada um (RIBEIRO, 2019,). Para abrint (2020), a Lei geral de proteção de dados também permite que em algumas situações ocorram exceções no tratamento de dado onde não necessita do consentimento prévio do titular, sendo eles:

- Fornecer esses dados ao governo;
- Armazenamento dos registros de acesso a aplicações;
- Inserir a previsão expressa de tratamento dos dados pessoais no contrato de adesão de serviço;
- Tratamento para processo judicial, administrativo ou arbitral;
- Compartilhamento com empresas terceiras para fins de prevenção à fraude;
- Tratamento para proteção de crédito.

A LGPD estipula que qualquer ação sobre os dados do cliente que não sejam os direitos acima descritos devem ser exercidos mediante solicitação expressa do titular ou representante legal, iniciando - se o prazo para recebimento de resposta do controlador de dados. Diante disso , o provedor deve estabelecer um formulário padrão que inclua o número de identificação do documento, o nome do cliente, sua solicitação e a data. A resposta do provedor deve ser acompanhada do número de protocolos abertos com esse objetivo de tratamento.

2.3 **Processo e Tecnologias de desenvolvimento**

O Processo de software caracteriza-se como um conjunto de tarefas para a criação de um software, essas tarefas podem incluir o desenvolvimento de software desde o início de um produto, porém para aplicações de negócios não são obrigatoriamente desenvolvidas dessa forma, grande parte dos softwares de negócios são criados por meios de extensão e atualização de sistemas existentes (SOMMERVILLE, 2013).

Existem diversos modelos de processos de software, mas independente do modelo todos devem inserir quatro atividades essenciais para a engenharia de software (SOMMERVILLE, 2013) sendo elas.

- Engenharia de requisitos: Requisitos funcionais e não funcionais.
- Planejamento e implementação de software: O produto deve ser criado para

atender às especificações.

- Validação de software: O software deve ser aprovado para atender às requisições do cliente.
- Evolução de software: O software deve atualizar-se para atender às necessidades de mudança do cliente.

Embora não haja um processo de "software" ideal, o escopo e requisitos do sistema definirá qual o processo mais indicado para a construção do projeto (SOMMERVILLE, 2013).

Modelagem UML

A linguagem UML visa fornecer ferramentas para levantamento de requisitos para o desenvolvimento de sistemas, bem como recursos para modelagem das estruturas que farão parte deles. Devido à sua forte relação com os conceitos de Orientação a Objetos (OO), UML tornou-se um padrão amplamente aceito no mercado. A construção de documentos que modelam os componentes esperados atualmente é feita usando diagramas UML, pois muitos sistemas são criados usando métodos e metodologias OO (DEVMEDIA).

Aplicativos Help Desk

Tornou - se essencial a utilização de um sistema de Help Desk para melhorar o nível de atendimento ao cliente e manter sua qualidade e eficiência. Os sistemas de atendimento ao cliente estão cada vez mais tomando o mercado de TI. Se tornando hoje o primeiro contato para resolver problemas com seus clientes, ele está sendo usado em muitas empresas para lidar com questões comerciais, solicitações de clientes, gerenciar produtos e liberar serviços.

A principal característica de um aplicativo de help desk é que ele facilita a comunicação com o cliente sobre um determinado problema, atuando como um ponto único de contato para usuários e equipe de suporte em relação a uma ou mais questões em aberto. Este ponto pode ser uma linha telefônica que distribui tarefas para a equipe técnica, ou um formulário web, ou chat online (COHEN, 2008).

Segundo Coêlho (2003, p.2), os sistemas de Help Desk competem cada vez mais com o crescente mercado de tecnologias computacionais. Para Silva (2004, P.12), "uma ferramenta de Help Desk, sem dúvida, oferece uma vantagem diferenciada, pois além de documentação e sistematização, oferece a capacidade de análise de processos e fluxo de dados".

Com a alta demanda para o desenvolvimento de software as empresas têm a necessidade de obter uma forma de realizar todas as atividades de formas mais rápidas e eficientes, para se adaptar à concorrência do mercado. Na forma convencional de desenvolvimento os códigos complexos dificultam a produção e aumentam a demanda por

profissionais super capacitados que por sua vez geram custos maiores (KARMALI, 2019).

Pensando nisso, em 2014 Forrester Research criou o termo “low-code” que é uma metodologia direcionada para a criação de programas e aplicativos em que a constituição dessas soluções recorre a poucos códigos. As plataformas low-code tem facilidade de programar em blocos e em poucas ou nenhuma linha de código. Usuários sem conhecimento avançado de programação podem usar técnicas intuitivas para criar software para diversos fins, incluindo a criação de aplicativos móveis e aplicativos de negócios. (KOVACS, 2021).

A seguir algumas das principais plataformas de Low Code;

- **Strapi**: O Strapi é um Framework de Gerenciamento de Conteúdo, que nos oferece facilidades no desenvolvimento de um CMS e/ou no desenvolvimento de software no geral. Traz o acesso a diversas features como painel administrativo, performance, plugins, segurança, front-end agnóstico, open source e comunidade, que ajudam no desenvolvimento, gerando uma interface de fácil aprendizagem. Suporta diferentes bancos de dados como PostgreSQL, MySQL, SQLite e MongoDB.
- **Zeev:** Zeev é a plataforma low-code pioneira no Brasil. Ele permite que você transforme seu fluxograma em um aplicativo. Assim você converte seus fluxogramas em fluxos de trabalho automatizados, tendo a capacidade de desenvolver soluções rapidamente e agregar valor significativo ao seu negócio.
- **Mendix:** Quando falamos de plataformas low-code, a Mendix é líder de mercado, é uma empresa sediada em Rotterdam, Holanda, ganhado notoriedade quando apareceram nos relatórios da Forrester e Gartner sobre low code.

Apesar de compartilharem alguns recursos, não existem duas plataformas low — code idênticas. O resultado final é determinado pelos objetivos estabelecidos, bem como pelo esforço do usuário para alcançá- los (KATAGUIRE, 2022).

O desenvolvimento de aplicativos sem o uso de nenhum código é possível usando ferramentas sem código. Como resultado, a lacuna de conhecimento que existia entre desenvolvedores e usuários deixou de ser um impedimento. Por causa disso, qualquer pessoa que esteja disposta a criar seu próprio aplicativo pode ser capaz de produzi-lo rápido e sem a necessidade de codificar (TOTVS, 2020).

Como dito anteriormente, o desenvolvimento ocorre mais rapidamente usando esse método. Isso se traduz em uma quantidade menor de trabalho de codificação e na capacidade de executar testes automatizados. Além disso, vários elementos (como relatórios, fórmulas e

estruturas de dados) podem ser atualizados em tempo real, isso aumenta ainda mais a agilidade dos negócios, característica que lhes confere vantagem competitiva (SOUZA, 2021).

3 METODOLOGIA

Os métodos utilizados incluem a coleta e análise de informações e o desenvolvimento de uma aplicação que demonstra a ligação da LGPD e o problema apresentando, assim, do ponto de vista da natureza pode ser classificado como uma pesquisa explicativa.

Para investigar aspectos relacionados ao tratamento de dados da LGPD, com base nas informações levantadas foi criado uma política de proteção de dados que corresponderá com os serviços prestados por um provedor de internet. Também foi elaborada a criação da DPIA (Data Protection Impact Assessment) referente aos setores comercial e suporte do modelo de empresa apresentado.

Para o modelo de política de proteção foi utilizado o padrão criado pelo site JURISTA 2022, modelo que foi adequado e preenchido de acordo com o modelo de empresa desse trabalho.

A implementação do (app) foi realizada em 2 Minimum Viable Product (MVP). O MVP 1 foi implementado o cadastro de chamados, juntamente com a listagem de chamados. No MVP 2 foi implementado o cadastro de usuário e a visualização dos chamados em uma tela de gerenciamento, onde foi utilizado a metodologia Kanban como modelo de interface.

A análise de requisitos começou com um estudo e observação das principais necessidades do cliente alvo do sistema, esses dados geraram uma base de conhecimento necessária para a proposta e desenvolvimento do sistema, a partir da qual foi definido o escopo do aplicativo, bem como os requisitos que devem estar presentes no aplicativo, os requisitos foram divididos em duas categorias funcionais e não funcionais.

A análise do projeto foi definido os principais autores e ações executadas por ele, sendo apresentado no diagrama de casos de uso do sistema, bem como a criação de um diagrama de sequência, diagrama entidade, diagrama de relacionamento para o banco de dados.

Para a implementação do sistema foi utilizado a ferramenta de desenvolvimento low-code strap.io, ferramenta que agilizará a criação da aplicação através de um painel administrativo totalmente funcional, facilitando a implementação do sistema. Este método apresentado foi utilizado para encontrar uma aplicação prática de conceitos para a solução proposta, que resultou no desenvolvimento de um sistema de gestão de dados, que será apresentado ao final deste projeto.

4 DESENVOLVIMENTO

4.1 Criação da política de proteção de dados

De acordo com o APÊNDICE I, para formalizar a política de proteção de dados foi implementado um conjunto de medidas. Lembrando que, como em qualquer política interna, as particularidades e interesses do provedor devem ser avaliados. É necessário que o provedor identifique alguém para coordenar esse processo, alguém que seja capaz de interagir com outros departamentos e tenha responsabilidades claras pela implementação de uma política de privacidade de dados. A pessoa indicada deve trabalhar com uma equipe multidisciplinar composta pelos setores de TI, comercial, financeiro e recursos humanos.

Após a indicação do responsável, será necessário a criação do DPIA (Data Protection Impact Assessment) ou como foi incorporado na LGPD "Relatório de impacto à proteção de dados pessoais". O documento descreve os processos de coleta e tratamento de dados pessoais, que podem gerar algum risco, bem como as medidas e mecanismos implementados para mitigar esses riscos, o modelo que será apresentado foi criado por uma planilha do Excel.

A construção do relatório inclui a descrição detalhada de todos os processos de recolha e tratamento de dados pelos quais os dados pessoais passam ao longo do seu ciclo de vida no seu fornecedor, desde o primeiro contato com os dados pessoais até à sua remoção das bases de dados. Apesar de a LGPD não especificar passo a passo o processo de desenvolvimento da RIPDP, os requisitos da lei são compatíveis com as práticas de trabalho existentes e comprovadamente eficazes.

Com base no modelo europeu o PIA (paradigma de Avaliação de Impacto de Privacidade) segue na imagem abaixo as etapas para a criação da RIPDP.

Figura 1 – Etapas para criação da RIPDP

Fonte: Próprio autor

Embora a criação do relatório não seja obrigatório por parte da LGPD, o relatório preserva a empresa para em caso de uma eventual auditoria ou processo administrativo

perante a Autoridade Nacional – ANPD, esta documentação pode ser utilizada para demonstrar boa-fé, diligência e compromisso do provedor com a governança da empresa, o comprimento da lei e a preocupação com a segurança e confidencialidade dos dados pessoais dos titulares e, consequentemente, evitar sanções administrativas.

Para o processo de atendimento ao cliente a figura abaixo apresenta como será a descrição do DPIA utilizando o excel de acordo com o processo de abertura de um chamado.

Figura 2 – Painel de cadastro individual de chamados.

DPIA – Suporte		
Setor:	*Suporte*	***Base Legal***
Pessoas:	*Técnicos de Suporte*	Levantamento de informação para suporte ao cliente
Terceiros:	*Atendimento, Departamento Ti*	***Armazenamento***
Processo:		Banco de Dados
Coleta de informação do cliente por telefone ou meios digitais		***Prazo de Armazenamento***
Instalação do serviço;		1 anos pós fim de contrato
Suporte técnico		***Medidas de Segurança***
Consentimento :	*SIM*	Restrito a usuários, criptografia, etc.

Fonte: Próprio autor

Outra situação seria quando o setor de vendas recebe uma ligação de um cliente, solicitando a contratação de um serviço, nesse relatório deve constar, minimamente:

- Setor envolvido: Comercial.
- Pessoas envolvidas: Vendedores, setor financeiro.
- Terceiros envolvidos: Departamento de TI, suporte.
- Processos envolvidos;
    - Coleta de informação do cliente por telefone ou meios digitais;
    - Consulta de créditos;
    - Processo de contratação;
    - Instalação do serviço;
- Base legal / finalidade: contratação e levantamento de informações para cadastro do cliente.
- Local de armazenamento dos dados: Servidor de banco de dados, Local físico (contratos impressos).
- Prazo de armazenamento dos dados: 1 ano após cancelamento do contrato de serviço;
- Há contrato/documento envolvido? Sim: formulário de aceitação de disponibilidade de dados.
- Medidas de segurança: acesso restrito de categoria de usuário, criptografia, etc.

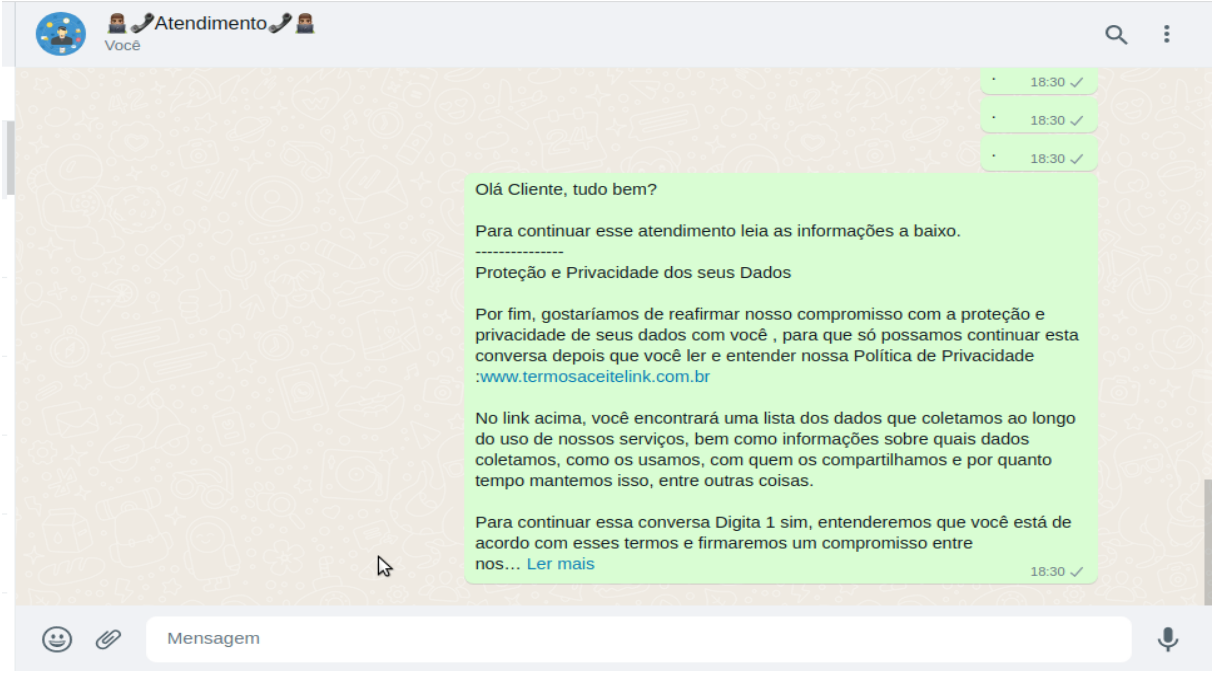
- Consentimento prévio: sim - Inserção de cláusula em contrato da ativação de serviço.

Esclarecendo: aqui temos um processo básico para a contratação de um serviço, sendo identificado e mapeado estabelecendo as medidas de segurança e a necessidade de consentimento prévio.

Apesar de o uso de redes sociais ser uma ferramenta útil para as empresas, ele deve ser usado com cautela. A equipe responsável pela sua utilização como ferramenta de trabalho deve estar sempre atenta às regras de proteção de dados e às obrigações inerentes ao tratamento de dados. Além disso, caso este seja o primeiro contato com um cliente e ele ainda não tenha lido ou entendido a política, ou o aviso de privacidade da empresa, a empresa deverá cumpri-lo, assim atendendo a LGPD.

Para isso, será apresentado algumas boas práticas às empresas que desejam promover o contato com seus clientes, via redes sociais, e reduzir os riscos associados ao seu uso, para o modelo apresentado foi utilizado a rede social WhatsApp, na figura abaixo temos a representação de uma solicitação de aceite.

Figura 3 – Modelo termo de solicitação de aceite.



Fonte: Próprio autor

Outra situação seria na solicitação de um chamado técnicos para determinado problema, nesse exemplo será utilizado o protótipo de aplicativo para chamados que foi desenvolvido para este trabalho e servirá para o gerenciamento dos chamados e tratamento dos dados solicitados.

4.2 Descrição do Sistema

O sistema de atendimento de chamados será um software que recebe e organiza os tickets de atendimento ao cliente, todos os chamados, sendo eles realizados por ligação ou digitalmente, será centralizado em um único local nesse caso no aplicativo, onde o técnico de suporte que será responsável pelo atendimento terá acesso às informações do chamado.

Os requisitos funcionais e não funcionais foram desenvolvidos como primeira etapa do processo de análise e modelagem do sistema, com o objetivo de delinear as características e operações que o sistema deve e não deve ter. Os seguintes requisitos serão apresentados nos quadros a seguir.

	Requisitos	**Descrição**	**Prioridade**
RF01	Manter usuário	O sistema contará com cadastro de usuário (CPF, SENHA, ENDEREÇO, CONTATO, EMAIL). Login (Usuário “cpf” e Senha “cpf”).	1-Alta
RF02	Manter Técnico	Contará com cadastro e login, Respostas de chamados, para atualização de status do chamado (Em aberto, Resolvido).	1-Alta
RF03	Manter Chamado	Disponibilizando a opção para iniciar um chamado onde deverá ter as opções de tipo (Sem rede, Lenta, instável) / prioridade (Baixa, Alta, Urgente).	1-Alta

Quadro 1 – Requisitos funcionais

No Quadro 2 estão os requisitos não funcionais identificados para o aplicativo.

	Requisitos	**Descrição**	**Prioridade**
RNF01	Manter Cliente	O cadastro só poderá ser concluído se todos os campos obrigatórios forem preenchidos.	1-Alta
RNF02	Manter Chamado	Para abertura do chamado todos os campos obrigatórios devem ser preenchidos sendo eles CPF do titular, endereço e telefone de contato devem ser preenchidos.	1-Alta
RNF02	Manter Usuário	Somente o gerente poderá criar, editar e excluir usuários de acesso ao sistema.	1-Alta

Quadro 2 – Requisitos não funcionais

No Quadro 3 estão sendo apresentadas as regras de negócio.

	Requisitos	**Descrição**	**Prioridade**
RN01	Manter Cliente	● O cadastro do usuário só poderá ser realizado para CPFs sem restrições. ● O cadastro só poderá ser iniciado após a autorização do titular. ● Em caso de desistência de cadastro todos os	1-Alta

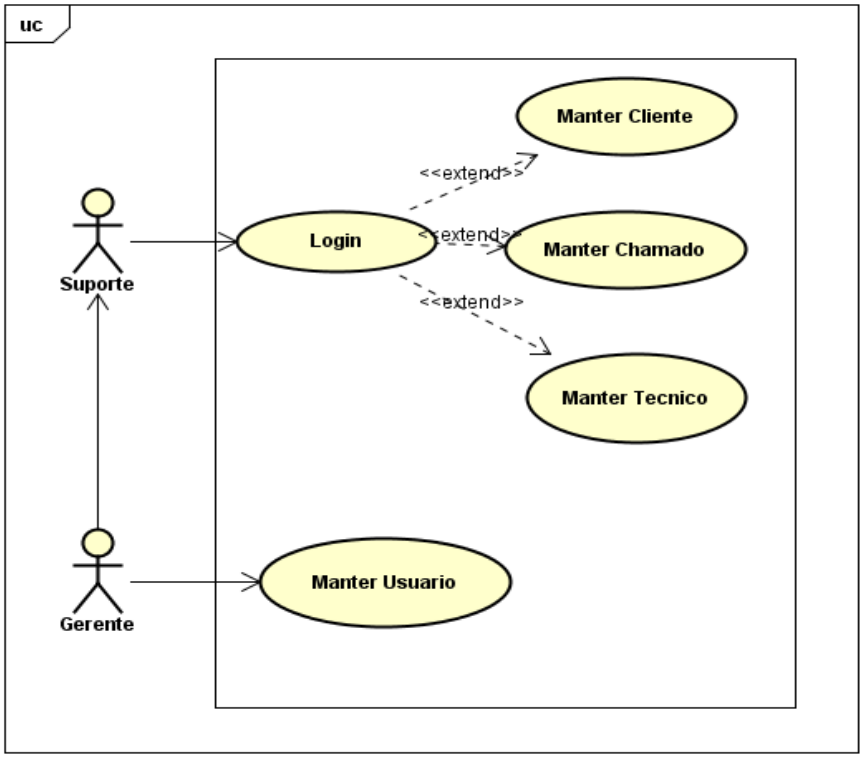
		dados devem ser deletados.	
RN02	Manter Chamado	• Para abertura do chamado todos os campos obrigatórios devem ser preenchidos sendo eles CPF do titular, endereço e telefone de contato devem ser preenchidos. • Para que o atendimento seja realizado a solicitação deve ser solicitada por um pessoa maior de 18 anos. • Somente clientes ativos podem solicitar uma abertura de chamada.	1-Alta

Quadro 3 – Regras de negócios

Os requisitos foram organizados em casos de uso. A Figura 1 apresenta o diagrama de casos de uso. Dessa forma foi identificado um ator para interação com as funcionalidades do sistema:

- Suporte – Terá acesso a todas as funcionalidades do sistema exceto a criação de novo usuário.
- Gerente - O autor gerente terá acesso a toda funcionalidade do sistema, também sendo o único a poder editar ou criar novos usuários.

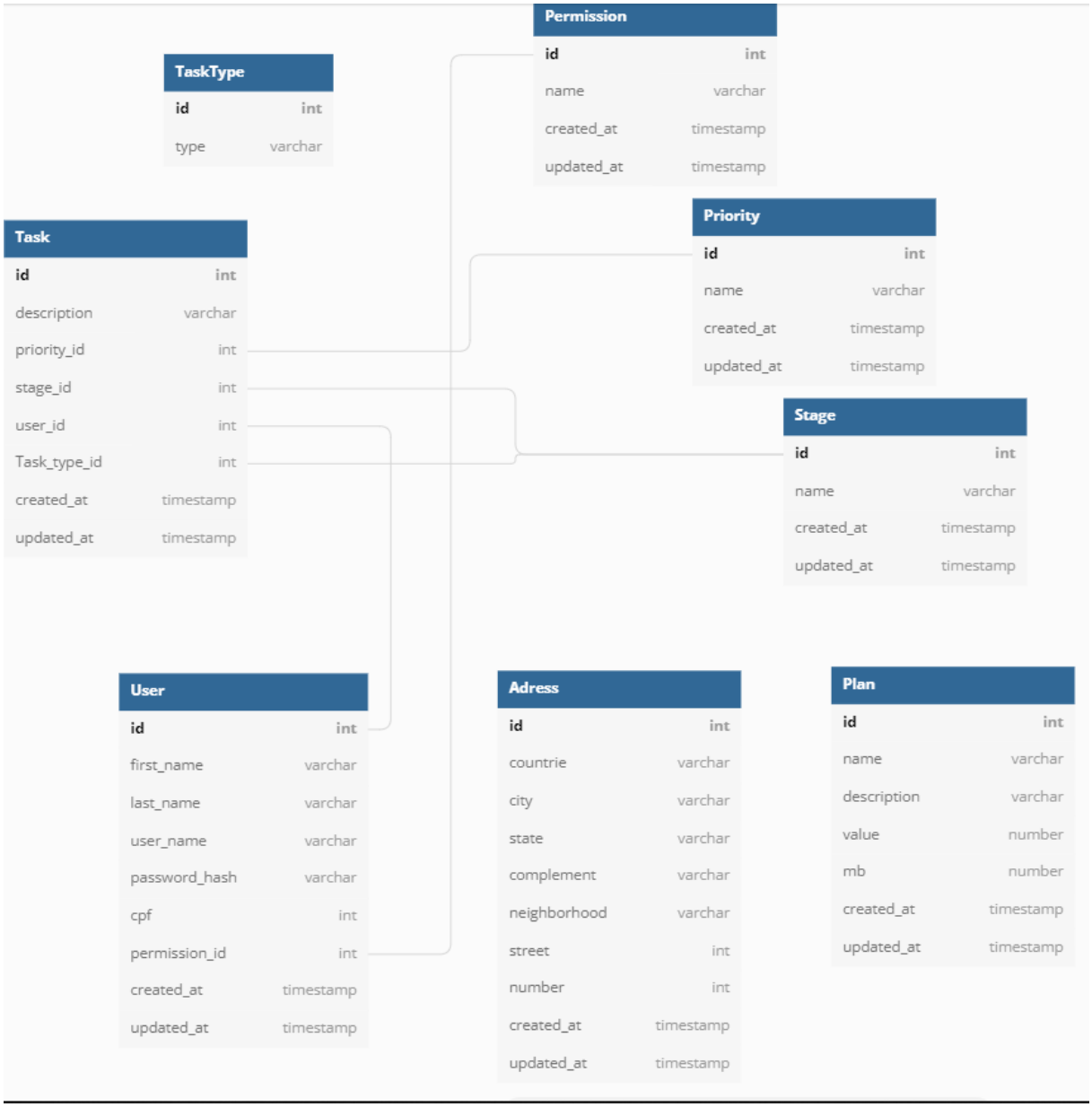
Figura 4 - Diagrama de caso de uso.



Fonte: Próprio autor

Na Figura 5 o diagrama representa o banco de dados da versão web da aplicação.

Figura 5 - Diagrama de classe principal da aplicação web.



Fonte: Próprio autor

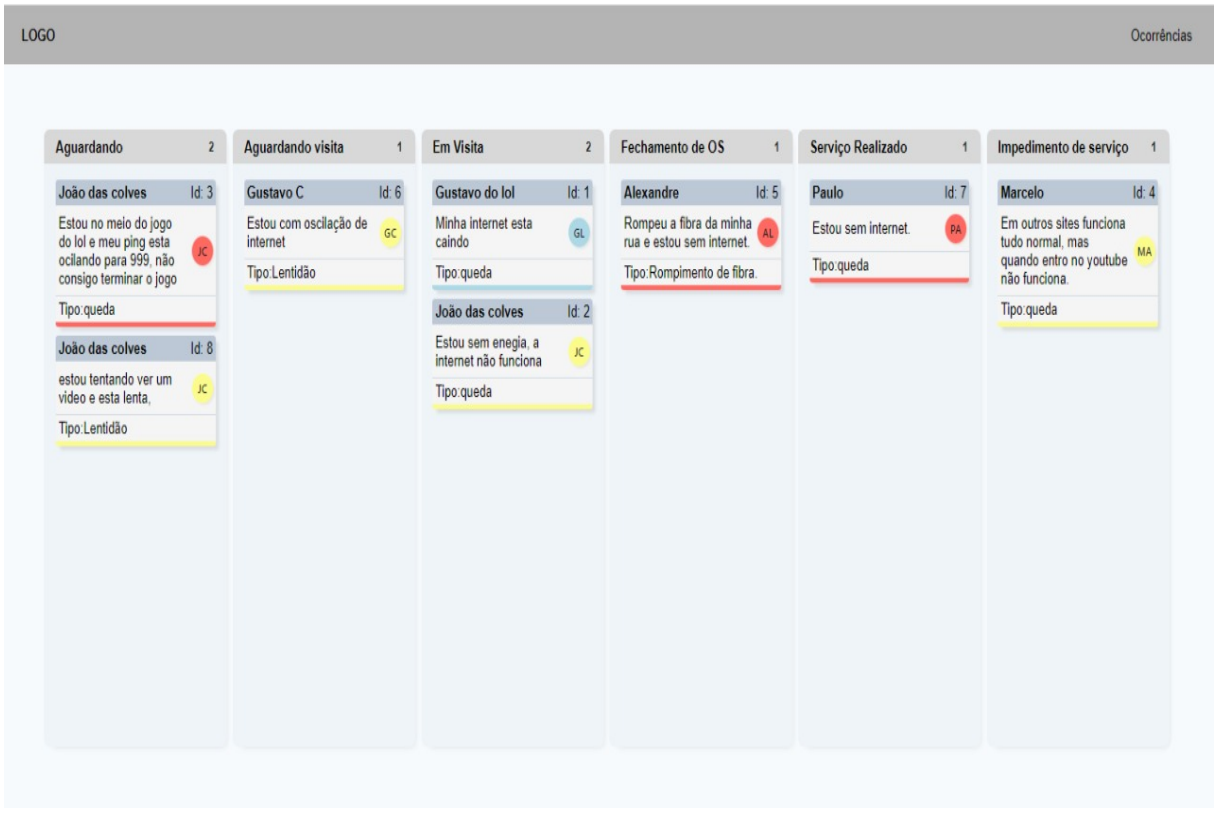
A figura 5 mostra o modelo relacional de banco de dados onde demonstra as tabelas do banco e como serão implementadas, onde a tabela Task tem como objetivo salvar os dados de um “Chamado” com a sua descrição, prioridade, estado (feita, em andamento, finalizada) e id do cliente. Trata-se da tabela responsável por gerir e armazenar os dados sensíveis coletados para a abertura de um chamado.

A tabela User contém os dados sensíveis do usuário (ID, nome, endereço, CPF, senha e permissão).

A tabela Stage guarda informação de qual é o estado da Task” Chamado". A tabela Priority define a prioridade dos chamados, sendo eles baixa, média ou alta.

O leiaute da página de gerenciamento de chamados composto quadros de trabalho, inspirados no modelo Kanban, conforme apresentado na Figura 5. Em cada quadro é apresentado o status do chamado, cada chamado será gerado um ticket, nele estão os dados do cliente, sendo ele nome e endereço, vale ressaltar que somente clientes ativos podem abrir chamados, pois somente aqueles que aceitaram os termos de política de privacidade podem abrir chamados.

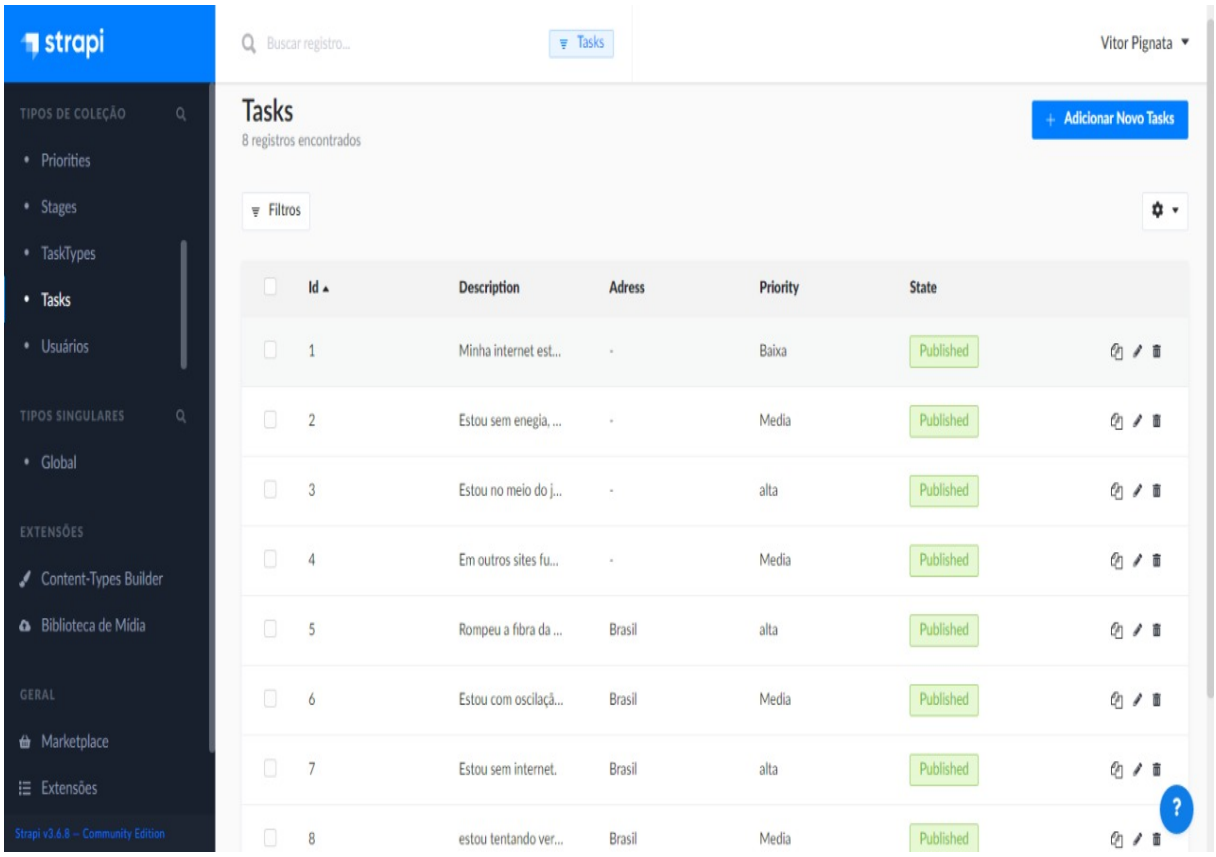
Figura 6 – Painel de gerenciamento de chamados



Fonte: Próprio autor

Cada ticket funciona como um bilhete onde o usuário pode arrastar com um clique e direcionando cada quadro de acordo com o andamento do chamado.

Figura 7 – Painel de cadastro de chamados

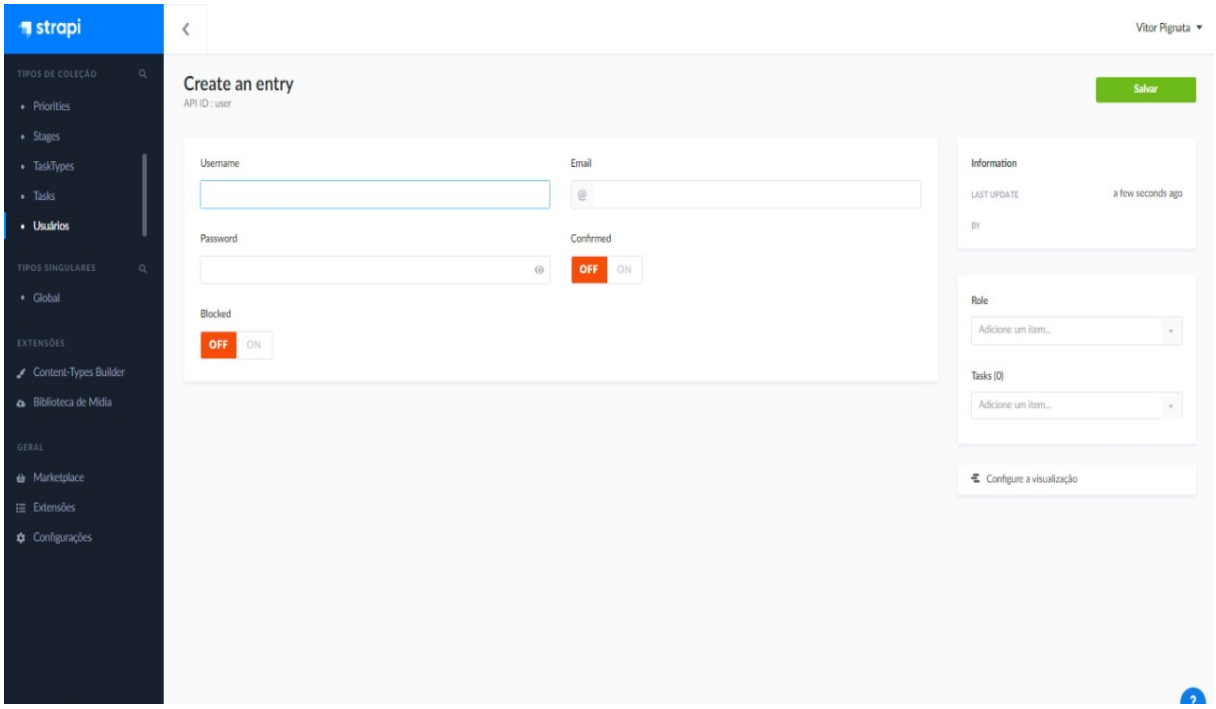


Fonte: Próprio autor

Para a implementação do protótipo foi utilizado a plataforma low code strap.io, plataforma que possibilitou a criação da API sem a necessidade de codificação assim facilitando a implementação do protótipo, as telas apresentadas foram criadas diretamente na plataforma, para a implementação da figura 6 foi necessária a utilização da linguagem de consulta GraphQL, ambiente para implementação de interfaces com API's.

A Figura 7 apresenta a interface de cadastro de chamados, nela estão disponíveis as opções para adicionar novos chamados exibindo uma lista dos chamados já em aberto, também está disponível as opções de visualizar, editar e excluir.

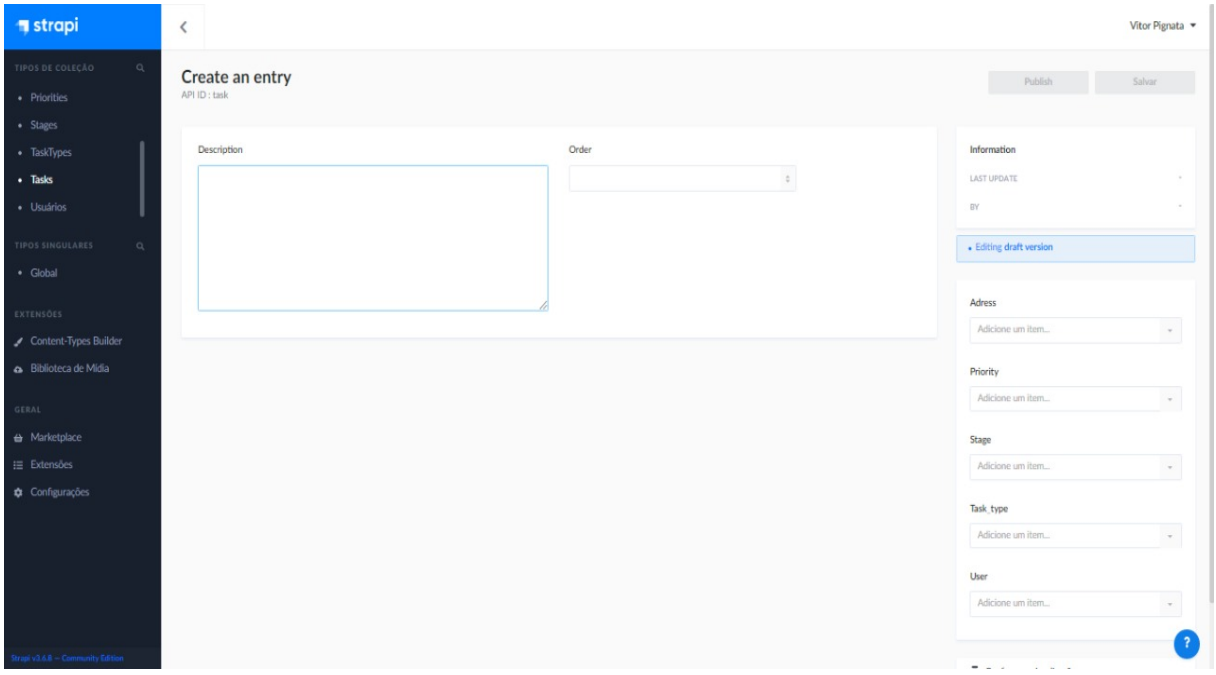
Figura 8 – Painel de cadastro de usuários.



Fonte: Próprio autor

Na figura 8 apresenta a tela de cadastro de usuários, esses serão responsáveis pelo atendimento do cliente e terão acesso ao sistema e os dados dos que serão cadastrados no sistema.

Figura 9 – Painel de cadastro individual de chamados.



Fonte: Próprio autor

Na figura 9 está a apresentação da interface de abertura de chamados, nela estão disponíveis as opções para inserir a descrição do chamado, sua prioridade e dados do cliente, a interface é disponibilizada no próprio sistema, criada na plataforma strap.io.

Como apresentado nas figuras acima, percebe-se que algumas informações pessoais sempre estarão expostas no processo de abertura do chamado, é importante destacar que para atender a Lei de proteção de dados, há uma regra de negócio que foi destacada no quadro 3 RN02, que para qualquer abertura de chamado somente clientes ativos podem fazer a solicitação, ou seja, clientes que já estão cientes da política de proteção de dados da empresa, com isso a exposição dos dados no aplicativo quanto para os funcionários não acarretarão em uma infração da lei.

CONSIDERAÇÕES FINAIS

Para a realização deste trabalho foi necessário primeiramente entender a relação entre a LGPD e Provedores de Internet e quais pontos vulneráveis e de riscos para o não cumprimento das normas e regras. Com isso, a próxima etapa foi compreender quais são os tipos de dados e como esses dados são coletados. A partir disso foram levantados os requisitos de acordo com as técnicas da Engenharia de Software para o início da construção do MVP.

Com base nos estudos realizados para conclusão deste trabalho, entende - se a importância da segurança dos dados e do comprimento das regras e adequações à lei LGPD. A identificação dos dados pessoais e de como tratá-los foi fundamental para a criação do documento de política de proteção de dados e o desenvolvimento do protótipo MVP.

Se após a implementação for aprovado pelo cliente a viabilidade do produto, pretende-se adicionar novas funcionalidades expandindo para o uso não só de funcionários mas também de usuários clientes, adicionando área para cadastro onde os próprios clientes irão efetuar seus chamados.

5 REFERÊNCIAS BIBLIOGRÁFICAS

ABRINT. A LGPD e os Provedores de acesso à internet. Brasília, 2020. Disponível em: <https://www.pontoisp.com.br/wp-content/uploads/2020/08/LGPD-Provedores-cartilha.pdf>. Acesso em: 23/04/2022.

ADITYA, S. K.; MOHANTA, P.; KARN, V. K. Android SQLite Essentials. Packt Publishing, 2014. isbn: 9781783282951.

BAARS, Hans – HINTZBERGEN, Kees - HINTZBERGEN, Juli – SMULDERS, André. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002. BRASPORT; Edição: 1. 2018.

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/L13709.htm. Acesso em: 01/04/2022.

BRASIL, LEI No 13.853 DE 10 DE JULHO DE 2020. Lei Geral de Proteção de Dados (LGPD). BrasíliaDF, Ago 2020. Disponivel em: <http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art1>.Acesso em: 01/04/2022.

COMO funciona um provedor de internet? BessWeb, 13 de Jun de 2021. Disponível em: <https://beesweb.com.br/blog/como-funciona-um-provedor-de-internet//>. Acesso em: 6 de abr. de 2022.

COÊLHO, A. V. S. ; FERNEDA, E. ; MARTINS, A. de S. ; BARROS, M. A. ; GORGÔNIO, F. L. E. . Help Desk inteligente em gestão do conhecimento: Um tratamento integrador de paradigmas. Inesc Em Revista, Unaí, v. 1, p. 46-51, 2003. Disponível em:<http://www.exercito.gov.br/06OMs/gabcmtex/PEG-EB/artigopdf/help.PDF>. Acesso em 15 abr. 2007.

COHEN, Roberto. Implantação de Help Desk e Service Desk. Novatec, 2008

FARIAS, C.C.de; ROSENVALD, N.; NETTO, F.P.B. Responsabilidade Civil. 2º ed. São Paulo: Atlas S.A., 2015.

FONTES, Edison. Políticas e Normas para a Segurança da Informação. BRASPORT; Edição: 1. 2012.

KATAGUIRE, Tayelli. 5 plataformas Low-Code que vão revolucionar sua empresa. Zeev, 02 de jan. de 2022. Disponível em: <https://blog.zeev.it/5-plataformas-low-code-para-criacao-de-aplicativos/>. Acesso em: 11 de abr. de 2022.

KOVACS, Leandro. O que são plataformas low code?. Tecnoblog, 11 de dez. de 2021. Disponível em: <https://tecnoblog.net/responde/o-que-sao-plataformas-low-code/>. Acesso em: 11 de abr. de 2022.

LARA, Rodrigo. O que é provedor de internet? Folha de S.Paulo, UOL, 11 de jun. de 2019. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2019/06/11/o-que-e-provedor-de-internet.htm>.

Acesso em: 06 de abr. de 2022.
Modelo – Política de Privacidade – LGPD – Dados Pessoais. JURISTA. 2022. Disponível em:

<https://juristas.com.br/2022/02/01/politica-de-privacidade/>. Acesso em: 02 jun 2022.

MORELLATO, Fernando César. LGPD – O que significa, e como se aplica no meu provedor?. Blog IPV7. Brasília, 18 de fevereiro de 2021. Disponível em: <.https://www.blog.ipv7.com.br/cliente/lgpd-o-que-significa-e-se-aplica-no-meu-provedor/.> Acesso em: 23/03/2022.

MOZILLA e colaboradores individuais. MDN web docs. Mozilla, 2020. Disponível em: https://developer.mozilla.org/. Acesso em: 10 ago. 2020.

PINHEIRO, Patrícia Peck. Contratos digitais ou eletrônicos: apenas um meio ou uma nova modalidade contratual? Revista dos Tribunais. Brasil. vol. 966, abril.2016. Disponível em: http://www.tjpa.jus.br/CMSPortal/VisualizarArquivo?idArquivo=340926. Acesso em: 15 abr. 2022.

Modelagem de sistemas através de UML: uma visão geral. Devmedia. [s/i], [s/d], Disponível em:
<.https://www.devmedia.com.br/modelagem-de-sistemas-atraves-de-uml-uma-visao-geral/27913.>. Acesso em: 15/04/2022.

SANTOS, Fernanda Cristina. Relatório de Impacto à Proteção de Dados – DPIA. Lage e Portilho Jardim. Belo Horizonte, Minas Gerais, 06 de julho de 2021. Disponível em: <.https://lageportilhojardim.com.br/blog/dpia-lgpd/.> Acesso em: 15 mai 2022.

SQLITE. What Is SQLite? SQLite Open Source, 2020. Disponível em: https://www.sqlite.org/. Acesso em: 20 abr. 2022.

RESENDE, Juliana. O que é provedor de internet e para que ele serve?. Portal de Planos. 31 de Jan de 2022. Disponível em: <.https://portaldeplanos.com.br/artigos/provedor-de-internet//.> Acesso em: 06/04/2022.

RIBEIRO, Cinthya Imano Vicente. Privacidade digital das instituições bancárias. 2019. 123 f. Dissertação (Mestrado em Direito) - Programa de Estudos Pós-Graduados em Direito, Pontifícia Universidade Católica de São Paulo, São Paulo, 2019. Disponível em: https://tede2.pucsp.br/handle/handle/22990. Acesso em: 15 abr. 2022.

SOMMERVILLE, Ian. Engenharia de Software. 9ed. São Paulo:Pearson Prentice Hall, 2011.
SCHMIDEK, A.; DURÁN. H.; COSTA, M.J.R.P. Boas Práticas de Manejo. Jaboticabal: Funep, 2009.

SÊMOLA, Marcos. Gestão da Segurança da Informação: Uma Visão Executiva. Rio de Janeiro: Elsevier; 2ª Edição, 2014.

SILVA, Jaime J. Help Desk com sistema RBC para as gerências de aplicativos do Banco do Brasil. 2004. 45 f. Trabalho de Conclusão de Curso (Curso de Especialização e Desenvolvimento, segurança e Qualidade na Internet) – Instituto de Informática, Universidade Federal do Rio Grande do Sul, Porto Alegre.

SOUZA, Kymberli. No-code: o que é?. Zeev, 02 de dez. de 2021. Disponível em: <https://blog.zeev.it/o-que-e-no-code//>. Acesso em: 12 de abr. de 2022.

TELECOM: O que é um provedor de internet e quanto custa montar um?. Previsa, 6 de out de 2020. Disponível em: <https://www.previsa.com.br/telecom-o-que-e-um-provedor-de-internet-e-quanto-custa-montar-um/>. Acesso em: 6 de abr. de 2022.

VERMAAT, Misty E. et al. Discovering Computers, Essentials ©2018: Digital Technology, Data, and Devices. 1ª. ed. Cengage Learning, f. 168, 2018. 336 p.

6 APÊNDICE I

POLÍTICA DE PROTEÇÃO DE DADOS

INTRODUÇÃO

A privacidade e a segurança de nossos usuários/clientes são nossas principais prioridades e nos comprometemos a ser transparentes sobre como lidamos com seus dados pessoais. Como resultado, esta Política de Privacidade estabelece como coletamos, usamos e transmitimos informações de clientes e outros indivíduos que usam ou usam nosso site.

Ao utilizar nossos serviços, você concorda que coletamos e usamos suas informações pessoais nas formas descritas nesta política, de acordo com as leis da Lei Geral de Proteção de Dados Pessoais (LGPD, Lei Federal 13.709 / 2018), o consumidor disposições de proteção da Lei Federal 8078/1990, e quaisquer outras leis aplicáveis do ordenamento jurídico brasileiro.

Quais dados coletamos sobre você e para qual finalidade?

A empresa irá coletar e usar alguns de seus dados pessoais para garantir a entrega do serviço e melhorar a experiência do usuário.

Dados pessoais fornecidos pelo titular

- Nome completo; Cadastro e consulta em órgãos de proteção ao crédito (SPC).
- CPF; Cadastro e consulta em órgãos de proteção ao crédito (SPC).
- RG; Cadastro e documentação de contrato.
- Endereço; Cadastro de sistema e contrato de serviço.
- Telefone; Cadastro e contrato de serviço, atendimento e suporte.

Dados pessoais coletados automaticamente

- Telefone; Atendimento e suporte.
- Nome completo; Cadastro e consulta de banco de dados.

Como coletamos os seus dados?

Dessa forma, a coleta dos seus dados pessoais ocorre da seguinte forma:

- Atendimento telefônico.
- Atendimento por redes sociais.
- Presencialmente (físico).

Consentimento

Só usamos suas informações pessoais com sua permissão, constatação e a declaração livre, registrada por você e autorizada a tratar seus dados.

Como resultado, de acordo com a Lei Geral de Proteção de Dados Pessoais (LGPD), seus dados só serão coletados, processados e armazenados com sua prévia e expressa concordância.

O seu compromisso será obtido de forma específica para cada finalidade descrita acima, evidenciando o provedor de transparência e fidelidade com seus usuários /clientes, seguindo as regulamentações relevantes.

Ao utilizar nossos serviços e fornecer dados pessoais, você reconhece e concorda com o disposto nesta Política de Privacidade, bem como conhece seus direitos e como exercê - los.

Você pode revogar sua permissão a qualquer momento e sem incorrer em custos.

Quais são os seus direitos?

Nossa empresa garantirá aos seus usuários/clientes os direitos de titularidade previstos na Lei Geral de Proteção de Dados Pessoais – LGPD. Usando este método, você pode fazer gratuitamente e a qualquer momento:

- **Confirme a existência de tratamento de dados**, seja de forma simples ou em formato claro e abrangente.
- **Acesso aos seus dados**, que poderá solicitar sob a forma de cópia legível ou cópia eletrônica segura e idônea.
- **Ao solicitar a edição, correção, ou atualização de seus dados**, você deve corrigir seus dados.
- **Limitar seus dados quando desnecessários**, excessivos ou usados de forma contrária à lei, tornando- os anônimos, bloqueando ou apagando-os.

- **Solicite a portabilidade dos seus dados**, através de um relatório de dados cadastrais elaborado a seu pedido por (nome da empresa).
- **Eliminar os seus dados tratados com base no seu consentimento**, exceto nos casos em que a lei o exija.
- **Revogação da sua aceitação**, para o tratamento dos seus dados pessoais.
- **Informar-se sobre a possibilidade de não dar seu consentimento** e as consequências de fazê -lo negativa.

Como você pode exercer seus direitos?

Para exercer seus direitos legais, entre em contato com nossa empresa usando um dos seguintes métodos:

- Pessoalmente, telefones e redes de mídia social (Whatsapp, Facebook, Instagram).

Para garantir a sua correta identificação como titular dos dados pessoais solicitados, podemos solicitar documentos ou outros comprovativos da sua identidade. Se este for o caso, você será avisado com antecedência.

Como e por quanto tempo seus dados serão armazenados?

Seus dados coletados serão usados e armazenados pelo tempo necessário para a prestação do serviço ou para o comprimento das metas estabelecidas nesta política de privacidade, respeitando os direitos dos titulares e controladores dos dados.

Em geral, seus dados serão mantidos enquanto você e nossa empresa tiverem uma relação contratual. Após a determinação do período de retenção de dados, os dados serão removidos ou anonimizados das nossas bases de dados, reiterando as hipóteses legais previstas no artigo 16.º do Regulamento Geral de Proteção de Dados, a saber:

I – Realização da obrigação legal ou regulatória pelo controlador;
II – Estudo por órgão de pesquisa assegurado, sempre que possível, anonimidade de dados pessoais;
III – Transferência a terceiro, sempre que os requisitos de tratamento de dados estipulados na

Lei for satisfeitos;
IV – uso exclusivo do controlador, bloqueado o acesso por terceiro, e anonimidade dos dados.

Isto é, os dados pessoais sobre você que sejam necessários para o cumprimento de obrigações legais, judiciais e administrativas, e/ou para o exercício do direito de defesa em processos judiciais e administrativos, serão mantidos, apesar da exclusão de outros dados.

O armazenamento dos dados coletados reflete nosso compromisso com a segurança e privacidade de suas informações pessoais. Implementamos medidas e técnicas de segurança para garantir a confidencialidade, integridade e inviolabilidade dos seus dados. Além disso, temos em vigor medidas de segurança adequadas ao risco, bem como controle de acesso aos dados armazenados.

Como mantemos seus dados seguros?

O armazenamento dos dados coletados reflete nosso compromisso com a segurança e privacidade de suas informações pessoais. Implementamos medidas e técnicas de segurança para garantir a confidencialidade, integridade e inviolabilidade dos seus dados.

Além disso, temos em vigor medidas de segurança adequadas ao risco, bem como controle de acesso aos dados armazenados.

Entre as medidas que utilizamos, destacam — se:

- Somente indivíduos autorizados têm acesso às suas informações pessoais.
- Só após aceitar este documento teremos acesso aos seus dados pessoais.
- Suas informações pessoais são mantidas em um ambiente seguro e protegido.

Nossa empresa está comprometida em adotar as melhores práticas para evitar incidentes de segurança. No entanto, é preciso ressaltar que nenhuma página virtual é totalmente segura e isenta de riscos. É possível que, apesar de todos os nossos protocolos de segurança, ocorram problemas causados apenas por terceiros, como ataques cibernéticos de hackers, ou como resultado de negligência ou imprudência do usuário ou cliente.

No caso de um problema de segurança que possa representar um risco ou causar danos a você, ou a qualquer um de nossos usuários/clientes, notificaremos os afetados, bem como a Autoridade Nacional de Proteção de Dados sobre o incidente, de acordo com as disposições da Lei Geral de Proteção de Dados.

Com quem seus dados podem ser compartilhados?

Com a preservação de sua privacidade em mente, não compartilharemos suas informações pessoais com terceiros que não estejam autorizados.

Suas informações podem ser compartilhadas com nossos parceiros comerciais: (nome completo ou e-mail do parceiro de negócios), cadastrados no CPF/CNPJ sob o número (CNPJ ou CPF do parceiro de negócios).

Estes só recebem seus dados se for necessário para a execução dos serviços que você contratou, e nossos contratos são orientados pelas leis brasileiras de proteção de dados.

No entanto, nossos parceiros têm suas próprias políticas de privacidade, que podem diferir das nossas. Recomendamos a leitura destes documentos, que podem ser encontrados aqui: **(link para a política de privacidade do parceiro comercial).**

Além disso, existem outros cenários em que seus dados podem ser compartilhados, como:

I - Determinação legal, pedido, requisição ou ordem judicial, junto às autoridades judiciais, administrativas ou governamentais competentes.

II – No caso de movimentos societários automáticos, como fusões, aquisições e incorporações.

III - Proteção dos direitos do (nome da empresa) em qualquer tipo de conflito, inclusive disputas judiciais.

Isenção de responsabilidade

Conforme mencionado anteriormente, apesar de empregarmos rigorosas medidas de segurança para evitar incidentes, não existe uma página virtual totalmente livre de riscos. Neste sentido, a empresa não é responsável por:

I – As consequências decorrentes do descuido, imprudência ou impertinência do usuário em relação aos seus dados pessoais. Apenas garantimos e somos responsáveis pela segurança dos processos de tratamento de dados e pelo cumprimento dos objetivos estabelecidos neste documento.

Queremos enfatizar que o usuário é responsável pela confidencialidade dos dados de acesso.

II - Ações maliciosas de terceiros, como ataques de hackers, exceto quando nossa conduta for

comprovadamente culposa ou deliberada.

Gostaríamos de enfatizar que no caso de um problema de segurança que possa representar um risco ou causar danos a você, ou a qualquer um de nossos usuários / clientes, notificaremos os afetados, bem como a Autoridade Nacional de Proteção de Dados sobre a ocorrência e tomar as devidas precauções.

III – Na utilização de informações incorporadas por usuários / clientes nos registros para a utilização dos serviços da empresa (nome empresarial); quaisquer consequências de informações falsas ou incorporadas de má-fé de forma totalmente

Encarregado de Proteção de Dados

Disponibilizaremos os seguintes métodos para você entrar em contato conosco a fim de exercer seus direitos legais: (telefone para contato)

Caso tenha alguma questão sobre a nossa Política de Privacidade ou sobre os dados pessoais que tratamos, poderá contatar o nosso Encarregado de Proteção de Dados Pessoais através dos seguintes canais:

Provedor de internet - CNPj

empresa@empresa.com.br