Universidade Federal de Ouro Preto
Instituto de Ciências Exatas e Aplicadas
Departamento de Computação e Sistemas

Adaptação do SisGera à Lei Geral de Proteção de Dados

Matheus Nunes Martins de Barros

TRABALHO DE CONCLUSÃO DE CURSO

ORIENTAÇÃO:

Prof. Me. Euler Horta Marinho

COORIENTAÇÃO:

Silvandro Sergio Martins Oliveira

Março, 2023
João Monlevade–MG

Matheus Nunes Martins de Barros

Adaptação do SisGera à Lei Geral de Proteção de Dados

Orientador: Prof. Me. Euler Horta Marinho

Coorientador: Silvandro Sergio Martins Oliveira

Monografia apresentada ao curso de Sistemas de Informação do Instituto de Ciências Exatas e Aplicadas, da Universidade Federal de Ouro Preto, como requisito parcial para aprovação na Disciplina "Trabalho de Conclusão de Curso II".

Universidade Federal de Ouro Preto

João Monlevade

Março de 2023

SISBIN - SISTEMA DE BIBLIOTECAS E INFORMAÇÃO

B277a Barros, Matheus Nunes Martins de.
Adaptação do SisGera à Lei Geral de Proteção de Dados. [manuscrito] / Matheus Nunes Martins de Barros. - 2023.
55 f.: il.: color..

Orientador: Prof. Me. Euler Horta Marinho.
Coorientador: Silvandro Sergio Martins Oliveira.
Monografia (Bacharelado). Universidade Federal de Ouro Preto. Instituto de Ciências Exatas e Aplicadas. Graduação em Sistemas de Informação .

1. Banco de dados - Gerência. 2. Lei Geral de Proteção de Dados (LGPD). 3. Proteção de dados. 4. Sistemas de recuperação da informação. 5. Software - Desenvolvimento. I. Marinho, Euler Horta. II. Oliveira, Silvandro Sergio Martins. III. Universidade Federal de Ouro Preto. IV. Título.

CDU 004.6-049.65

Bibliotecário(a) Responsável: Flavia Reis - CRB6-2431

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE OURO PRETO
REITORIA
INSTITUTO DE CIENCIAS EXATAS E APLICADAS
DEPARTAMENTO DE COMPUTACAO E SISTEMAS

FOLHA DE APROVAÇÃO

Matheus Nunes Martins de Barros

Adaptação do SisGera à Lei Geral de Proteção de Dados

Monografia apresentada ao Curso de Sistemas de Informação da Universidade Federal de Ouro Preto como requisito parcial para obtenção do título de Bacharel em Sistemas de Informação

Aprovada em 29 de março de 2023

Membros da banca

Mestre - Euler Horta Marinho - Orientador (Universidade Federal de Ouro Preto)
Silvandro Sergio Martins Oliveira - Coorientador (Clube FII)
Mestre - Igor Muzetti Pereira - (Universidade Federal de Ouro Preto)
Mestra - Daniela Rodrigues Dias - (Doutoranda em Educação - Universidade Federal de Ouro Preto)

Euler Horta Marinho, orientador do trabalho, aprovou a versão final e autorizou seu depósito na Biblioteca Digital de Trabalhos de Conclusão de Curso da UFOP em 24/04/2023

Documento assinado eletronicamente por **Euler Horta Marinho**, **PROFESSOR DE MAGISTERIO SUPERIOR**, em 24/04/2023, às 18:19, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.ufop.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0514238** e o código CRC **743B1C6A**.

R. Diogo de Vasconcelos, 122, - Bairro Pilar Ouro Preto/MG, CEP 35402-163
Telefone: (31)3808-0819 - www.ufop.br

Este trabalho é dedicado especialmente ao meu pai, que sempre teve o desejo de ver um de seus filhos formar, e para a minha família, amigos e a todos que ajudaram com o meu desenvolvimento pessoal e acadêmico.

Agradecimentos

Agradeço ao meu pai, que sempre me apoiou em tudo, e imagino que estaria muito feliz nesse momento. A minha mãe Cláudia por sempre apoiar-me e ajudar-me todos os dias, ao meu irmão João Américo que além de ser meu irmão é meu melhor amigo também e sempre ajuda-me em todos os momentos, e a toda minha família, por sempre confiar em mim.

Aos meus amigos, por todo apoio e companheirismo em todos os momentos, tristes e alegres.

Aos meus orientadores, Euler e Silvandro, por todos os conselhos e ensinamentos que me foram passados no decorrer deste trabalho.

Ao Bráulio da corporação de São Domingos do Prata, por acreditar e contribuir com esse projeto.

Aos professores e professoras que tive durante toda a minha vivência na graduação, pelo ensino de qualidade que me proporcionaram.

"Learning never exhausts the mind."

— Leonardo da Vinci (1452 – 1519).

Resumo

O SisGera é um sistema de informação *Web* de registro de ocorrências e atividades administrativas das corporações de bombeiros voluntários, e apesar de estar em funcionamento, não está seguindo totalmente os padrões da Lei Geral de Proteção de Dados (LGPD). Sendo assim, o objetivo principal deste trabalho é fazer com que o SisGera siga os padrões desta lei, para que assim melhore o tratamento de dados atual do sistema, enquanto aumenta as funcionalidades do sistema, acrescentando opções de anonimização e exclusão de dados, termos de uso e política de privacidade para detalhar as descrições das atividades realizadas no sistema. A LGPD, por sua vez, tem como um dos seus objetivos principais, aumentar a segurança dos sistemas em relação ao tratamento de dados. Portanto, o tema principal trabalhado nesta lei é o tratamento de dados, o qual consiste em qualquer atividade que utiliza um dado pessoal na execução da sua operação. Após feita a adaptação do sistema, o mesmo não estará passível às infrações que estão sujeitas, caso este não siga os padrões da LGPD. Além disso, o sistema estará mais seguro e transparente em relação ao uso dos dados coletados.

Palavras-chave: SisGera. Lei Geral de Proteção de Dados. Tratamento de Dados.

Abstract

SisGera is a Web information system used for recording occurrences and administrative activities of voluntary fire brigades, and despite being in operation, it is not following the standards of *General Data Protection Law* (GDPL),thus, the main objective of this work is to make SisGera follow the standards of this law, doing so will improve the current data processing of the system, while increasing the system's functionalities, adding options for anonymization and data deletion , terms of use and privacy policy to detail the descriptions of the activities carried out on the system. GDPL, in turn, has as one of its main objectives to increase the security of systems in relation to data processing. Therefore, the main theme worked on in this law is data processing, which consists of any activity that uses personal data in the execution of its operation. After adapting the system, it will not be liable to the infractions that are subject in case it isn't following the standards of the GDPL, in addition the system will be safer and more transparent in relation to the use of its collected data.

Key-words: SisGera. General Data Protection Law. Data Processing.

Lista de ilustrações

Lista de abreviaturas e siglas

LGPD Lei Geral de Proteção de Dados

GDPL *General Data Protection Law*

SisGera Sistema de Gerenciamento e Registro de Atividades

GDPR *General Data Processing Regulation*

SGBD Sistema de gerenciamento de banco de dados

WSL2 *Windows subsystem for Linux 2*

ANPD Autoridade Nacional de Proteção de Dados

URL *Uniform Resource Locator*

WWW *World Wide Web*

ANPD Autoridade Nacional de Proteção de Dados

Sumário

1 Introdução

O projeto Sistema de Gerenciamento e Registro de Atividades (SisGera) teve início em 2018, a partir do trabalho de conclusão de curso de Arantes (2018), sobre "Um Sistema de Informação para apoio ao registro de ocorrências atendidas por grupos de bombeiros voluntários". Nesse trabalho, foi criado um sistema para controle de ocorrências das corporações de bombeiros voluntários de São Domingos do Prata e Barão de Cocais. Houveram depois novos incrementos no sistema a partir do trabalho de Oliveira (2018), sobre "Sistema de Informação para controle de materiais e doações aos bombeiros voluntários". Esse trabalho teve como objetivo principal adicionar novas funcionalidades ao SisGera, assim como melhorar os processos internos com um foco na gestão de atividades administrativas e auxiliando nas tomadas de decisões das corporações envolvidas. Após o trabalho de Oliveira (2018), houve o trabalho de Silva (2021), sobre "Desenvolvimento de uma aplicação web progressiva para o registro de ocorrências de um grupo de bombeiros voluntários.". O objetivo principal desse trabalho foi desenvolver uma versão *Web* progressiva para apoio ao registro de ocorrências do SisGera. Por fim, após o projeto de Silva (2021), teve o trabalho de Castro (2022), sobre "Desenvolvimento de um módulo de *help desk* para o sistema SisGera.", cujo objetivo principal era de criar um módulo de *help desk*, que seria um canal de comunicação entre os usuários do SisGera com os desenvolvedores do sistema.

Atualmente, o sistema SisGera está em operação, apoiando as atividades de bombeiros voluntários em diversas cidades do estado de Minas Gerais, como São Domingos do Prata, Barão de Cocais, dentre outras, facilitando as tarefas administrativas e operacionais, o que acaba tornando as rotinas diárias dos bombeiros mais eficientes.

Entretanto, devido ao fato de o sistema não estar seguindo por completo os padrões da Lei Geral de Proteção de Dados (LGPD), surgiu a necessidade de realizar essa adaptação. Portanto, esse é o objetivo principal deste trabalho.

1.1 Problema

A LGPD entrou em vigor no Brasil, oficialmente em 18 de setembro de 2020. A LGPD é fruto da junção do Projeto de Lei 4.060/2012, de iniciativa parlamentar, com o Projeto de Lei 5.276/2016. A ideia da adoção desta lei foi influenciada principalmente pelo modelo de proteção de dados adotado na Europa, como diz Selma e Lívia (Filho, E. T, 2021, p.243): "(...) a legislação da União Europeia, a *General Data Processing Regulation* (GDPR), na qual a LGPD se inspirou(...)". Outro ponto que influenciou na criação da LGPD foi que a existência de uma legislação e uma autoridade administrativa de proteção de dados, era algo tido como uma condição para que o país pudesse participar

de acordos internacionais de comércio baseados na livre circulação de dados, e cooperações internacionais para o combate do crime organizado, ou a investigação de crimes cibernéticos, assim como a própria entrada na Organização para a Cooperação e o Desenvolvimento Econômico (OCDE).

O objetivo principal da LGPD é aumentar a segurança dos sistemas em relação ao tratamento de dados. Portanto, o tema principal trabalhado nessa lei é o tratamento de dados, o qual consiste em qualquer atividade que utiliza um dado pessoal na execução da sua operação. Antes de iniciar qualquer tipo de tratamento de dados pessoais, o agente deve se certificar que a finalidade da operação está registrada e os propósitos especificados ao titular dos dados. Portanto, é de suma importância estar em conformidade com a LGPD, pois também ajuda a evitar ataques cibernéticos e melhorar a reputação do sistema em questão.

1.2 Objetivos

A seguir são apresentados o objetivo geral e os específicos deste trabalho.

1.2.1 Objetivo Geral

O objetivo principal deste trabalho envolve fazer com que o SisGera, o qual não está seguindo totalmente os padrões da LGPD, por ter sido criado antes desta lei ter entrado em vigor, seja atualizado para se adequar totalmente às normas desta lei.

1.2.2 Objetivo Específicos

Este trabalho possui os seguintes objetivos específicos:

- Realizar um estudo sobre a LGPD.
- Desenvolver o ambiente virtual no Docker a fim de facilitar futuras manutenções no sistema.
- Criar um documento contendo boas práticas de segurança da informação, com o intuito de se repassado à equipe da corporação de bombeiros;
- Elaborar os termos de uso e a política de privacidade;
- Adicionar a ferramenta Fale Conosco para a página inicial;
- Criar a opção de anonimização de dados das vítimas;
- Criar a opção de exclusão de dados dos usuários;

1.3 Organização do trabalho

O restante deste trabalho é organizado como se segue. O Capítulo 2 apresenta a revisão bibliográfica do trabalho, introduzindo os principais conceitos presentes. O Capítulo 3 demonstra as adaptações que serão realizadas para o SisGera e os resultados obtidos ao decorrer do desenvolvimento do trabalho. Por fim no Capítulo 4 apresenta as principais observações, bem como sugere abordagens para trabalhos futuros.

2 Revisão bibliográfica

Apresenta-se a seguir a revisão bibliográfica, com base nos autores e trabalhos correlatos. Destacam-se os conceitos já levantados nos trabalhos anteriores, de Arantes (2018), Oliveira (2018), Silva (2021) e Castro (2022), assim como também conceitos de Sistemas de Informação, Engenharia de Software, Aplicações *Web* e Segurança da Informação.

2.1 Sistemas de Informação

Segundo Audy, Andrade e Cidral (2005), sistemas de informação podem ser definidos como uma combinação de recursos humanos e computacionais, os quais inter-relacionam a coleta, o armazenamento, a recuperação, a distribuição e o uso de dados, isso com o objetivo de eficiência gerencial (planejamento, controle, comunicação e tomada de decisão) nas organizações. Completando a descrição sobre sistemas de informação de O'Brien (2004) que afirma que sistemas de informação abrangem um conjunto organizado de pessoas, hardware, software, redes de comunicações e recursos de dados que coleta, transforma e dissemina informações em uma organização. Para Laudon e Laudon (2010), os sistemas de informação são formados pelas dimensões organizacional, humana e tecnológica, conforme apresentado na figura 1.

Figura 1 – Dimensões dos sistemas de informação

Fonte: Adaptado de Laudon e Laudon (2010)

Além do mais, segundo Rezende (2005), a classificação dos sistemas de informação pode ser definida em: operacional, gerencial e estratégico. Os sistemas de informação ope-

racionais atuam no processamento das operações ou transações do cotidiano da empresa e auxiliam na execução das tarefas operacionais. Os sistemas de informação gerenciais atuam no processamento de um grupo de dados gerados pelas operações da empresa, transformando em informações agrupadas para gestão da empresa. Os sistemas de informação estratégicos atuam no suporte a decisão, onde processam as informações do nível operacional e as transações do nível gerencial transformando em informações estratégicas, auxiliando no processo de tomada de decisão.

2.2 Segurança da Informação

Segurança da informação é a prática de proteger as informações confidenciais de indivíduos, organizações e governos contra ameaças internas e externas, garantindo a integridade, confidencialidade e disponibilidade das informações. A segurança da informação envolve a utilização de medidas técnicas, administrativas e físicas para proteger as informações.

De acordo com Barreto et al. (2018), a segurança da informação tem como base os seguintes aspectos, denominados pilares da segurança da informação, assim como é possível notar com a figura 2:

Figura 2 – Pilares da Segurança da Informação.

Fonte: Retirado de Barreto et al. (2018)

- Confidencialidade: Se trata da capacidade de um sistema de impedir que usuários não autorizados "vejam" determinada informação a qual foi delegada somente a usuários autorizados a vê-la.

- Integridade: É um atributo de segurança o qual garante que a informação seja alterada somente de forma autorizada, sendo assim, mantida correta e completa.
- Disponibilidade: Indica a quantidade de vezes em que o sistema cumpriu uma tarefa solicitada sem falhas internas, para um número de vezes em que foi solicitado a fazer a tarefa.

As possíveis ameaças à segurança da informação podem incluir ataques de *hackers*, *malware*, *phishing*, roubo de dados e até mesmo espionagem industrial. Portanto é muito importante que indivíduos e organizações tomem medidas para proteger suas informações, a fim de evitar possíveis danos financeiros, perda de reputação e violações de privacidade.

2.3 Lei Geral de Proteção de Dados LGPD

A Lei Geral de Proteção de Dados Pessoais LGPD, Lei n° 13.709/2018, Brasília DF (2020), foi promulgada para proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo. Essa Lei fala sobre o tratamento de dados pessoais, dispostos em meio físico ou digital, feito por pessoa física ou jurídica de direito público ou privado, englobando um amplo conjunto de operações que podem ocorrer em meios manuais ou digitais. Um dos aspectos mais importantes ressaltados desta lei está no objetivo de aumentar a segurança para o consumidor, conforme afirma Lima (2021) "...a Lei Geral de Proteção de Dados Pessoais (LGPD), sua entrada em vigor, em 18 de setembro de 2020, trouxe uma maior segurança para o consumidor, impactando as organizações que realizam tratamento de dados pessoais, inclusive nos meios digitais."

No âmbito da LGPD, o tratamento dos dados pessoais pode ser realizado por dois agentes de tratamento, o Controlador e o Operador. Além deles, há a figura do Encarregado, que é a pessoa indicada pelo Controlador para atuar como canal de comunicação entre o Controlador, o Operador, os(as) titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

O tema fundamental trabalhado pela Lei é o tratamento de dado, o qual se diz a respeito sobre qualquer atividade que utiliza um dado pessoal na execução da sua operação, como, por exemplo: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Antes de iniciar qualquer tipo de tratamento de dados pessoais, o agente deve se certificar que a finalidade da operação está registrada de forma clara e explícita e os propósitos especificados e informados ao(à) titular dos dados. No caso do setor público, a principal finalidade do tratamento está relacionada à execução de políticas públicas,

devidamente previstas em lei, regulamentos ou respaldadas em contratos, convênios ou instrumentos semelhantes.

O compartilhamento dentro da administração pública, no âmbito da execução de políticas públicas, é previsto na Lei e dispensa o consentimento específico. Contudo, o órgão que coleta deve informar com transparência qual dado será compartilhado e com quem. Do outro lado, o órgão que solicita receber o compartilhamento precisa justificar esse acesso com base na execução de uma política pública específica e claramente determinada, descrevendo o motivo da solicitação de acesso e o uso que será feito com os dados. Informações protegidas por sigilo seguem protegidas e sujeitas a normativas e regras específicas. Essas e outras questões fundamentais devem ser observadas pelos órgãos e entidades da administração federal no sentido de assegurar a conformidade do tratamento de dados pessoais de acordo com as hipóteses legais e princípios da LGPD.

A Lei estabelece uma estrutura legal de direitos dos(as) titulares de dados pessoais. Esses direitos devem ser garantidos durante toda a existência do tratamento dos dados pessoais realizado pelo órgão ou entidade. Para o exercício dos direitos dos(as) titulares, a LGPD prevê um conjunto de ferramentas que aprofundam obrigações de transparência ativa e passiva, e criam meios processuais para mobilizar a Administração Pública.

2.3.1 Dados Pessoais e Dados Sensíveis

Os dados pessoais, são informações que identificam ou tornam identificável uma pessoa física, direta ou indiretamente. Essas informações podem incluir nome, endereço, número de telefone, data de nascimento, número de identificação, informações de conta bancária, informações médicas, histórico de compras, hábitos de navegação na Internet e outros dados que permitem que uma pessoa seja identificada.

Já os dados sensíveis, são informações pessoais que, se divulgadas ou usadas de maneira inadequada, podem causar danos significativos, discriminação, prejuízos emocionais, financeiros ou até mesmo físicos à pessoa. Esses dados podem incluir informações sobre a saúde, origem racial ou étnica, orientação sexual, convicções religiosas, opiniões políticas, filiação sindical, dados genéticos e biométricos, entre outros. Esses tipos de dados possuem uma proteção mais rigorosa, conforme afirma Lima (2021), “Nesse caso, é importante relembrar que dados de saúde são considerados dados pessoais sensíveis na LGPD e, portanto, devem ter atenção e cuidado redobrados.”

A proteção de ambos os dados pessoais e sensíveis estão contidos na LGPD, onde caso algum usuário solicite a exclusão ou anonimização dos mesmos, a organização que está com a posse desses dados deve por lei acatar ao pedido. Entretanto, existem algumas exceções, por exemplo, quando o usuário que esteja solicitando esse pedido tenha alguma pendência com a empresa. Nesse caso, a pendência tem que ser finalizada antes da exclusão

ou anonimização puderem ser realizadas.

2.3.2 Metodologia BEST

Inicialmente, os passos para a implantação da LGPD, foram seguidos do livro de Garcia (2020), em seu guia de implantação. Nesse livro, é sugerida a utilização da metodologia BEST, a qual oferece uma abordagem sustentável e adaptável para a implementação do sistema de gestão de atendimento à LGPD, independente do porte das operações ou área de atuação. Essa metodologia foi concebida pela Fundação Vanzolini para o desenvolvimento de sistemas de gestão visando à acreditação em cibersegurança e à privacidade de dados. Seu principal diferencial é a promoção da conscientização e do engajamento dos colaboradores para a autotransformação de seus negócios, processos e sistemas, em atendimento aos requisitos de garantia da integridade, disponibilidade, sigilo e privacidade das informações transmitidas, processadas e armazenadas pela empresa.

Na figura 3, estão os passos retirados das sugestões apresentadas no livro: "Lei geral de proteção de dados (LGPD): Guia de implantação" de Garcia (2020).

Figura 3 – Sugestão de ordem de implantação

Fonte: Adaptado de Garcia (2020)

A ordem lógica de implantação impõe o início pelos controles relativos ao PG00 – Programa de Gestão de Cibersegurança e Segurança da Informação. Esses controles, a rigor, não se referem diretamente à LGPD, entretanto, a implantação desse passo é necessário para que possua consistência e acompanhamento dos princípios da lei. O próximo passo sugerido é a implantação do programa PG06 – Programa de Informações Protegidas, o qual inclui a maior parte das exigências relativas à lei. Os programas PG03 e PG08, são sugeridos para serem implantados parcialmente, completando o conjunto identificado diretamente com a LGPD.

2.3.3 Passos para implantação da LGPD

Para realizar a implantação da LGPD, primeiramente, foi feito um mapeamento dos dados analisando o caminho que o dado pessoal percorre desde o momento em que é coletado pela organização até o seu descarte.

O próximo passo foi fazer o mapeamento dos riscos do tratamento, cujo objetivo é identificar possíveis riscos de vazamento de dados, pois é responsabilidade da empresa garantir a proteção dessas informações e a privacidade de seus usuários e clientes.

O passo em seguida foi elaborar o relatório de impacto, isso se refere a um documento a ser elaborado pelo controlador dos dados, sempre que for identificado algum risco possível decorrente do processo de tratamento de dados.

Logo após, o próximo passo então foi a criação da política de privacidade e os termos de uso, para realizar a implementação da LGPD, é necessário contar com a definição de regras a serem seguidas pela organização e os usuários, e para isso é utilizada a política de privacidade e os termos de uso.

Por fim, o último passo seguido foi criar um documento contendo boas práticas de segurança da informação a fim de alertar os usuários do SisGera sobre as importâncias e os riscos que envolvem os dados pessoais que serão trabalhados. Foi necessário fazer esse documento, visto que não seria possível realizar um treinamento mais especializado com a equipe em questão.

2.3.4 Mapeamento de dados

O mapeamento de dados geralmente é o primeiro passo a ser tomado, durante as implementações das empresas à LGPD. Conforme Lima (2021), "Talvez o ponto-chave no processo de adequação de empresas de tecnologia da informação seja exatamente o mapeamento de dados ou *data mapping*. Esse processo, comum a qualquer outro ramo de atividade, consiste em identificar sempre que, na execução do negócio, dados pessoais são coletados e tratados.". Portanto, esse passo é muito importante para esse processo de implantação, para justamente ganhar o conhecimento de como é feito o tratamento de dados atualmente na empresa em questão e como isso deve ser alterado.

2.3.5 Termos de Uso e Política de Privacidade

Os termos de uso são um conjunto de regras que estabelecem os direitos e obrigações dos usuários ao utilizar um determinado serviço ou site, aplicativo ou rede social. Os termos de uso especificam as condições de acesso, as limitações de uso, as responsabilidades do usuário, as condições de pagamento, entre outras informações relevantes.

Já a política de privacidade se trata de um documento que estabelece como as informações coletadas de usuários serão utilizadas, compartilhadas e protegidas por uma empresa ou organização. A política de privacidade especifica quais tipos de informações serão coletados, como nome, endereço de e-mail, número de telefone, endereço de IP, entre outros, e como essas informações serão utilizadas, como para fins de marketing, pesquisa de mercado ou melhoria de produtos e serviços. A política de privacidade também pode

especificar quais terceiros terão acesso às informações coletadas e como a empresa se responsabiliza pela proteção e segurança dos dados dos usuários.

De acordo com a LGPD, é necessário que a empresa possua tanto os termos de uso quanto a política de privacidade para estar dentro dos padrões exigidos pela lei.

2.3.6 Boas Práticas de Segurança da Informação

Um dos passos descritos pela metodologia BEST, está em reforçar em manter as boas práticas de segurança da informação aos colaboradores da organização, pois caso o mesmo não seja cumprido, a empresa com o tempo não manterá os padrões de segurança exigidos pela LGPD. Essas práticas podem variar entre coisas simples, como, manter uma boa gestão de senhas, se atentar ao navegar por sites de terceiros, entre outras práticas. Apesar de serem ações simples, ajudam a manter a segurança de informações.

2.3.7 Anonimização de dados

A LGPD cita que o dado anonimizado, é caracterizado como um dado que corresponde aquele que, originariamente, era relativo a uma pessoa, mas que passou por etapas que vieram a garantir a desvinculação dele a essa pessoa, ou seja, analisando os dados que foram anonimizados, é impossível descobrir à quem especificamente esse dado se refere. Segundo Cots e Oliveira (2019), sobre os dados anonimizados, "não define apenas como pessoais os dados que, imediatamente, identifiquem uma pessoa natural (viés do critério reducionista), como poderia ser informações como o nome, número do CPF, imagem etc., mas abarcou também os dados que tornam a pessoa identificável de forma não imediata ou direta".

Caso um dado seja anonimizado, então a LGPD não se aplicará a ele. Vale frisar que um dado só é considerado efetivamente anonimizado caso o mesmo não permitir que, via meios técnicos e outros, se reconstrua o caminho para vincular quem era a pessoa titular do dado, se de alguma forma a identificação ocorrer. Isso implica que o dado não é, de fato, um dado anonimizado e sim, apenas, um dado pseudoanonimizado, o qual estará, portanto, sujeito à LGPD.

A necessidade de se anonimizar um dado pode ser variada. Geralmente, ela ocorre quando é necessária a exclusão do dado específico. Porém, ao invés de excluir, pode ser feita a anonimização. O motivo é que a organização em questão deseja manter o dado anonimizado para fins de pesquisas, ou estudos com aquele dado anonimizado. Assim, para essas pesquisas, os dados pessoais dos usuários ou clientes não serão utilizados. Portanto, é possível utilizar os dados anonimizados para a mesma.

2.4 Engenharia de Software

A Engenharia de Software se concentra na aplicação de princípios científicos e técnicas de engenharia para o desenvolvimento de softwares. Ela envolve a aplicação sistemática de métodos e ferramentas para especificar, projetar, implementar, testar e manter o software de uma maneira eficiente e eficaz. Segundo Pressman e Maxim (2016), "A base da Engenharia de Software é a camada de processos. O processo de Engenharia de Software é a liga que mantém as camadas de tecnologia coesas e possibilita o desenvolvimento de software de forma racional e dentro do prazo.". Essa camada de processos se refere figura 4.

Figura 4 – Camadas de Engenharia de Software

Fonte: Adaptado de Pressman e Maxim (2016)

De acordo com Pressman e Maxim (2016), as ferramentas da Engenharia de Software são responsáveis por fornecer suporte automatizado ou semi automatizado para o processo e para os métodos. Quando as ferramentas são integradas, de modo que as informações criadas por uma ferramenta possam ser utilizadas por outra, é estabelecido um sistema para o suporte ao desenvolvimento de software, denominado Engenharia de Software com o auxílio do computador.

Já o processo, segundo Pressman e Maxim (2016), é responsável por definir uma metodologia (*framework* / paradigma) e constituir a base para o controle do gerenciamento de projetos de software. O processo também busca estabelecer o contexto no qual são aplicados métodos técnicos, são produzidos artefatos (modelos, documentos, dados, relatórios, formulários etc.), são estabelecidos marcos, a qualidade é garantida e mudanças são geridas de forma apropriada.

E, por fim, foco na qualidade. Conforme Pressman e Maxim (2016), qualquer abordagem de engenharia (inclusive Engenharia de Software) deve estar fundamentada em um comprometimento organizacional com a qualidade.

2.5 Aplicações *Web*

Aplicações *Web* podem ser definidas como programas de software projetados para serem acessados e executados através de um navegador da *Web*. Essas aplicações são executadas em servidores remotos e são acessadas pelos usuários por meio de uma *Uniform Resource Locator* (URL). Além disso, esse modelo de sistema, tem como uma de suas principais características a sua acessibilidade e mobilidade, isso porque não requer nenhum tipo de instalação no dispositivo do usuário, sendo então possível obter acesso quando e onde quiser, isso é, desde que esteja conectado a Internet.

Tudo isso teve início por volta dos anos 90, com a criação da *World Wide Web* (WWW), que foi o começo da construção da Internet que conhecemos nos dias atuais. Desde então, as aplicações *Web* evoluem cada vez mais, ampliando assim seu acesso, portabilidade e utilidade. Pressman (2011) afirma que essas aplicações têm evoluindo“ para sofisticadas ferramentas computacionais que não apenas oferecem funções especializadas ao usuário, como também foram integradas aos bancos de dados corporativos e as aplicações de negócio.”. Isso torna possível a percepção da constante evolução dessa tecnologia.

3 Desenvolvimento e Resultados

Nessa seção serão apresentados aspectos do desenvolvimento da adaptação do SisGera à LGPD, será apresentado também o levantamento de requisitos, a elaboração das histórias do usuário, as escolhas tecnológicas e os resultados contendo os visuais finais das ferramentas que foram adicionadas ao sistema. A seção 3.1 introduz o SisGera. Na sequência, a seção 3.2 aborda as escolhas tecnológicas para o trabalho. Durante a seção 3.3, é apresentado o processo de desenvolvimento das funcionalidades adicionadas. Finalmente, na seção 3.4, são exibidos os resultados obtidos.

3.1 SisGera

Conforme o conteúdo abordado durante a introdução, o SisGera é uma aplicação *Web* desenvolvida durante os trabalhos de Arantes (2018), Oliveira (2018), Silva (2021) e Castro (2022) para atender as necessidades observadas das organizações de Bombeiros Voluntários de São Domingos do Prata e Bombeiros Voluntários de Barão de Cocais. Atualmente, esse sistema se encontra em uso pelos bombeiros, atendendo suas principais necessidades, conseguindo assim, facilitar suas tarefas administrativas e operacionais, tornando as rotinas diárias mais eficientes.

3.2 Escolhas Tecnológicas

Esta seção apresenta as principais tecnologias e ferramentas que foram utilizadas no decorrer do desenvolvimento deste trabalho.

3.2.1 WSL2

O *Windows subsystem for Linux 2* (WSL2) é um módulo do sistema operacional Windows que visa disponibilizar um ambiente Linux compatível para o Windows, de forma assim que se possam executar programas (baseados em texto) nativos dos sistemas GNU/Linux dentro do próprio Windows, ou seja, sem a necessidade de emuladores ou do uso de máquinas virtuais.

3.2.2 Ubuntu

Ubuntu é um sistema operacional ou sistema operacional de código aberto, construído a partir do núcleo Linux que foi utilizado juntamente com o WSL2 para utilizar sistema operacional Linux dentro do Windows.

3.2.3 Docker

O Docker é um *software* de código aberto usado para implantar aplicativos dentro de contêineres virtuais. A conteinerização permite que vários aplicativos funcionem em diferentes ambientes complexos. O Docker foi utilizado para gerar um ambiente virtual contendo as versões de MySQL e de PHP que são utilizadas no SisGera. Foi decidido fazer esse ambiente virtual para facilitar e melhorar futuras interações com o SisGera. O Docker *engine* faz virtualização a nível de sistema operacional, ou seja, usa chamadas de sistema específicas do kernel Linux e, como o Docker *engine*, foi feito para realizar chamadas de sistema do Linux, foi necessário utilizar o WSL2 e o Ubuntu para implementar essas chamadas no Windows.

3.2.4 NGINX

NGINX é um servidor *Web* que também funciona como *proxy* de *email*, *proxy* reverso, e balanceador de carga. A sua estrutura é assíncrona e orientada a eventos, o que acaba por permitir o processamento de muitas solicitações ao mesmo tempo.

3.2.5 MySQL

O MySQL é um Sistema de gerenciamento de banco de dados (SGBD) relacional de código aberto que permite criar e gerenciar bases dados. Essa ferramenta possui características como alta performance, implementa mecanismos de segurança, conta com meios para realizar *backups* de dados, dentre outras vantagens

3.2.6 PHP

PHP é uma linguagem de código aberto muito utilizada para desenvolvimento *Web*, a qual pode ser incluída junto a códigos HTML. É uma linguagem que é executada no *back-end* da aplicação (no lado servidor), e envia resultados de processamentos para o navegador das máquinas clientes sem ter o código-fonte exposto, oferecendo portanto uma maior segurança.

3.3 Processo de desenvolvimento

Nesta seção, será apresentado o processo de desenvolvimento das funcionalidades que foram adicionadas no SisGera para corresponder a LGPD, assim como outras alterações que foram feitas tanto na parte *back-end*, como na parte *front-end* da aplicação durante o desenvolvimento do trabalho.

3.3.1 Levantamento de requisitos

Para realizar o levantamento de requisitos do SisGera, inicialmente foram realizadas reuniões com os orientadores deste trabalho, para discutirmos quais problemas deveriam ser levantados. Depois, foram feitas reuniões com o coordenador geral da equipe de Bombeiros Voluntários de São Domingos do Prata, ao qual foram trazidos os problemas discutidos anteriormente e foram sugeridas etapas que foram seguidas para o desenvolvimento deste projeto.

Os principais pontos destacados nas reuniões foram:

- A criação de um ambiente de desenvolvimento utilizando o Docker, para facilitar futuros projetos envolvendo o SisGera;
- A necessidade de ter uma opção para anonimizar ou excluir dados de usuários e vítimas;
- Permitir o uso da ferramenta do Fale Conosco para usuários externos;
- Realizar todas as adaptações necessárias do sistema para estar nos padrões da LGPD, garantindo assim a legalização dos usos dos dados adquiridos pelo sistema e prevenindo quaisquer punições que acarretam não seguir com os termos da LGPD.

Portanto, as reuniões e discussões realizadas no início deste projeto foram fundamentais para o entendimento do problema, e serviram de ponto de partida para o desenvolvimento das etapas posteriores.

3.3.2 Histórias de Usuário

As Histórias de usuário consistem em uma técnica utilizada em métodos ágeis de desenvolvimento de *software* para descrever uma funcionalidade ou recurso de um produto ou sistema sob a perspectiva do usuário final. O modelo que será utilizado neste projeto será o que foi apresentado por Longo e Silva (2014), o qual possui a estrutura seguinte:

- **Como um...** (Quem?) (Papel, ator);
- **eu quero...** (O que?) (Funcionalidade desejada);
- **de modo que...** (Por que?) (Trará algum benefício ou valor).

As histórias de usuário para as novas funcionalidades do SisGera, desenvolvidas neste trabalho estão apresentadas abaixo:

- **Ambiente Docker**

  Como um... Desenvolvedor

  eu quero... desenvolver o projeto SisGera utilizando um ambiente virtual

  de modo que... Facilite o acesso ao projeto

- **Fale Conosco**

  Como um... Usuário externo

  eu quero... comunicar com os responsáveis do SisGera

  de modo que... informe sobre, erros, sugestões, dúvidas sobre o sistema

- **Anonimização e exclusão de dados**

  Como um... Usuário interno

  eu quero... anonimizar ou excluir meus dados que o SisGera coletou

  de modo que... Mantenha em sigilo meus dados pessoais

- **Termos de Uso e Política de Privacidade**

  Como um... Usuário interno

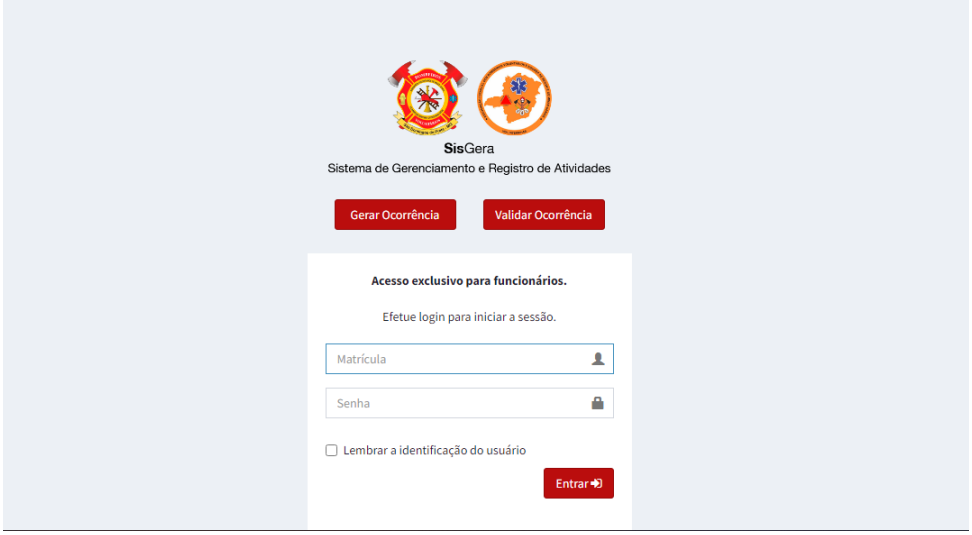
  eu quero... ter conhecimento sobre como é feito o tratamento de dados do SisGera

  de modo que... eu entenda como os dados coletados são utilizados no sistema

3.3.3 Alterações realizadas

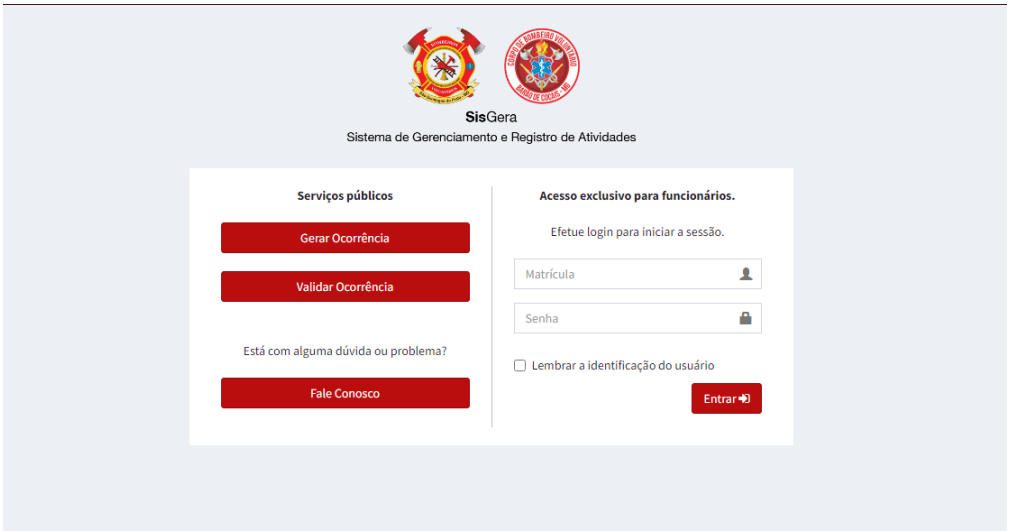
Ao longo do projeto, foram feitas algumas alterações em cima de algumas funcionalidades e visuais no SisGera. As figuras 5 e 6 representam, respectivamente, a tela inicial antiga, antes da adição da ferramenta Fale Conosco para a página de usuários externos, e a tela depois de uma alteração mais detalhada, a fim de ressaltar de uma forma mais clara que o objetivo dessa nova ferramenta é para o uso de usuário externos especificamente. Por outro lado, já existe uma outra ferramenta para usuários internos com propósitos semelhantes, o *Help Desk*. Portanto, para evitar que usuários internos precisem utilizar o SisGera, neste caso, foi necessário realizar uma adaptação geral na tela inicial.

Figura 5 – Tela inicial antiga



Fonte: Elaborado pelo autor. (2023)

Figura 6 – Tela inicial nova



Fonte: Elaborado pelo autor. (2023)

Além das mudanças feitas na tela inicial, houveram outras pequenas alterações em relação à algumas cores e tamanhos dos botões já existentes. Isso foi feito a fim de deixar o ambiente mais apropriado e menos confuso em relação as novas funções de exclusão e anonimização que foram adicionadas. Além disso, era utilizado anteriormente o servidor *web* Apache. Entretanto, com a criação do ambiente Docker, foi alterado para o servidor web NGINX, devido ao fato de consumir menos memória que o Apache, por lidar com requisições Web do tipo *"event-based web server"*.

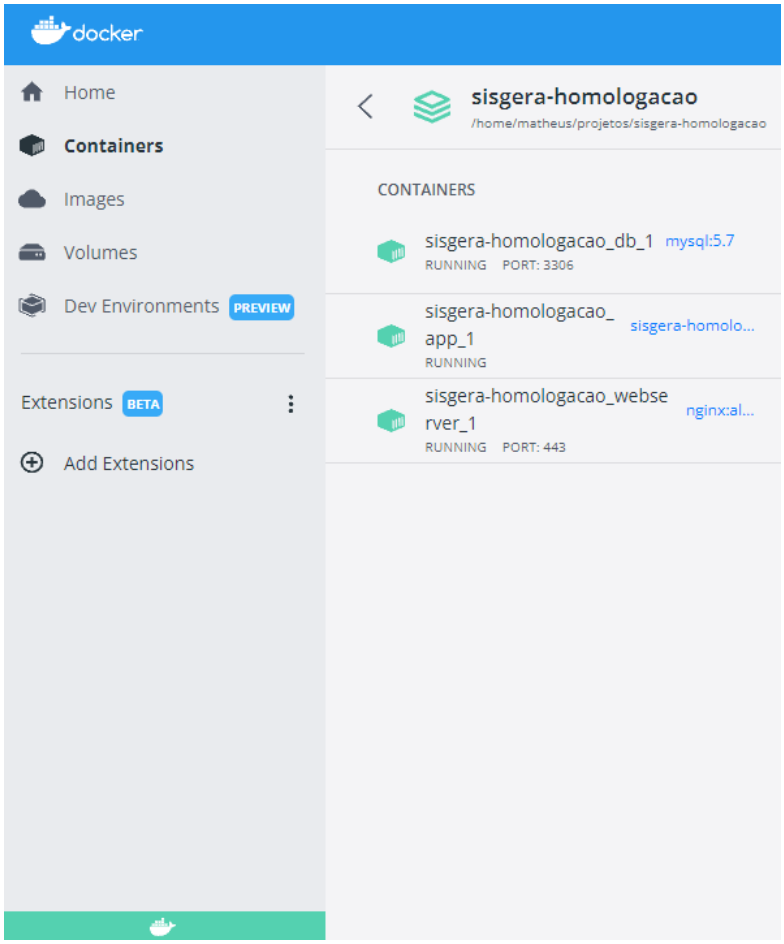
3.4 Apresentação das Funcionalidades

Esta seção tem o objetivo de apresentar as novas aplicações desenvolvidas para o projeto SisGera, irá conter uma breve descrição de cada uma dessas funcionalidades, assim como um exemplo visual das telas principais de cada uma das aplicações adicionadas.

3.4.1 Ambiente Docker

Um dos pontos levantados no começo do projeto foi a criação de um ambiente no Docker com o objetivo de facilitar futuros projetos envolvendo o SisGera. Isso porque, para começar a desenvolver o projeto utilizando o ambiente Docker, será necessário somente a instalação do Docker e o WSL2 caso o desenvolvedor não possua uma máquina com Linux instalado. Esse ambiente contém contêineres com PHP na versão 7.2, MySQL na versão 5.7 e um servidor web NGINX. A figura 7 mostra os contêineres do ambiente Docker criado.

Figura 7 – Ambiente Docker



Fonte: Elaborado pelo autor. (2023)

Devido ao ambiente Docker, para ativar os servidores e acessar o projeto no

"localhost" da máquina, basta seguir as instruções no *Readme.md* que se encontra no projeto. A figura 8 apresenta este arquivo de instrução.

Figura 8 – Arquivo *Readme.md*

README.md > # Instruções para Instalação e Execução > ## Configuração do Projeto:

You, 3 months ago | 1 author (You)

```
1  # Instruções para Instalação e Execução
2
```

You, 3 months ago | 1 author (You)

```
3  ## Pré-requisitos:
4
5  - Ambiente linux
6  - Instalar o Docker: https://docs.docker.com/get-docker/
7
```

You, 3 months ago | 1 author (You)

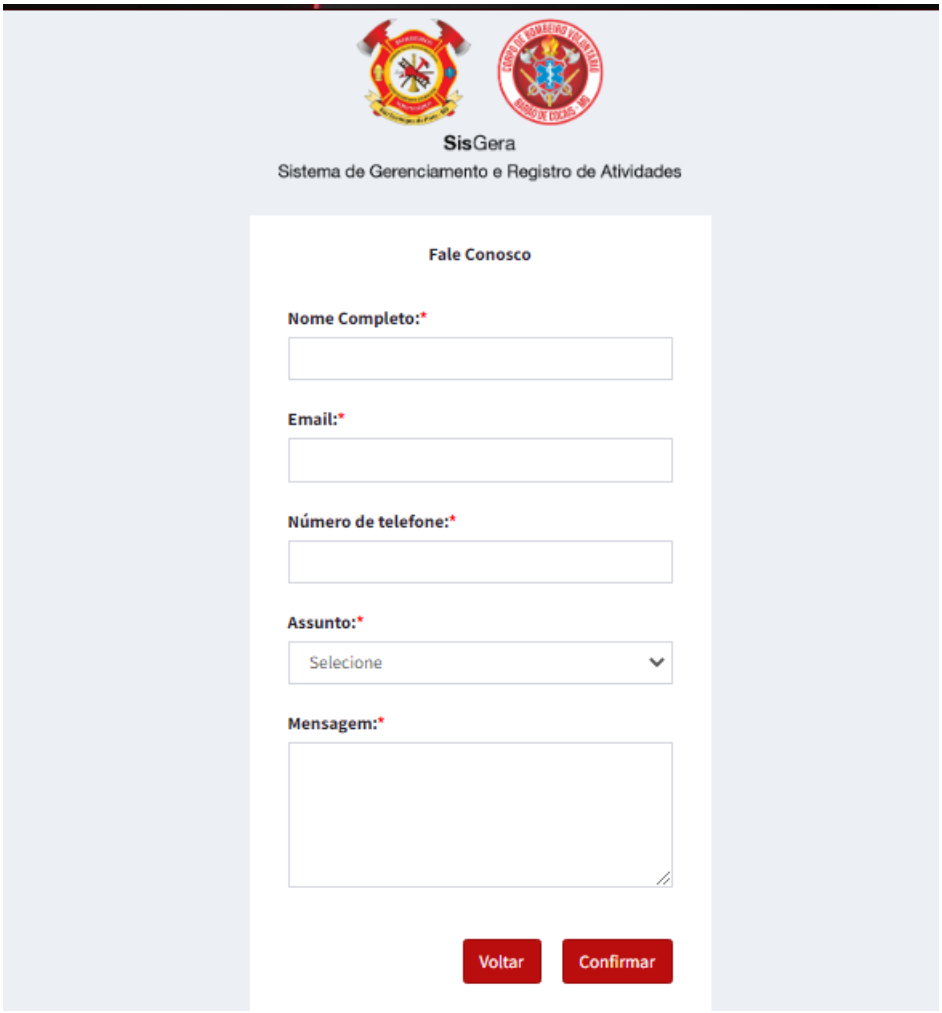
```
8  ## Configuração do Projeto:
9
10 Na raiz do projeto, execute o comando:
11 `docker-compose up -d`
12
13 Para popular o banco, execute:
14 `docker-compose exec -T db mysql -proot "sisgera_db_test" < "sisgera_db_test.sql"`
15
```

Fonte: Elaborado pelo autor. (2023)

3.4.2 Fale Conosco

A funcionalidade do Fale Conosco, foi inicialmente criada por Oliveira (2018), com o objetivo de se ter um canal de comunicação mais formal entre os voluntários das corporações e a equipe de desenvolvimento do SisGera, na qual os usuários do SisGera poderiam enviar mensagens de assuntos pertinentes ao sistema, sendo que tais mensagens eram visualizadas pela equipe de desenvolvimento do SisGera. Entretanto, com a criação do *Help Desk* do trabalho de Castro (2022), a funcionalidade do Fale Conosco já estaria sendo executada pelo *Help Desk*. Portanto, foi proposta a ideia de utilizar o Fale Conosco para usuários externos, e acrescentar a opção de anonimização, já que esta funcionalidade também foi adicionada com este trabalho. A figura 9 exibe a tela do Fale Conosco após a mudança para usuários externos.

Figura 9 – Tela do Fale Conosco



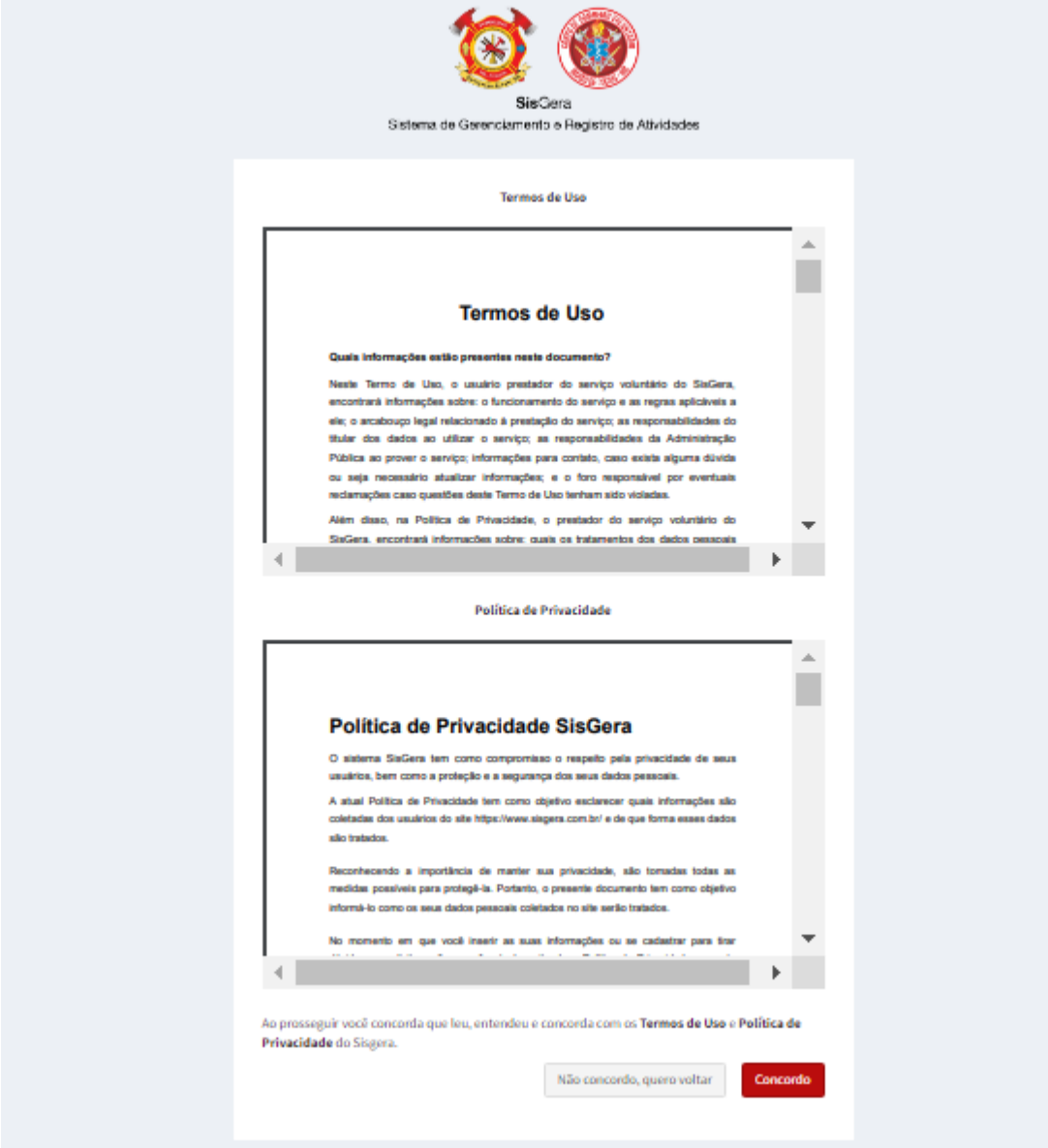
Fonte: Elaborado pelo autor. (2023)

A funcionalidade atual do Fale Conosco que está disponível para usuários externos é de permitir que esses usuários possam comunicar à equipe de desenvolvimento do SisGera possíveis erros, sugestões, dúvidas, reclamações ou exigir a anonimização dos dados e, se for o caso, será analisado se o usuário externo em questão condiz com alguma vítima que teve os dados armazenados pelo SisGera.

3.4.3 Termos de Uso e Política de Privacidade

A funcionalidade dessa tela é de informar os usuários do SisGera dos termos de uso e política de privacidade do sistema, bem como garantir que os mesmos concordem que, ao utilizarem o SisGera, estarão de acordo com tais termos. Caso o usuário em questão recuse, o mesmo retornará para a página inicial. Portanto, será apenas possível o usuário entrar no sistema, caso o mesmo concorde com os termos de uso e política de privacidade do SisGera. A figura 10 se refere a tela em questão.

Figura 10 – Tela dos Termos de Uso e Política de Privacidade



Fonte: Elaborado pelo autor. (2023)

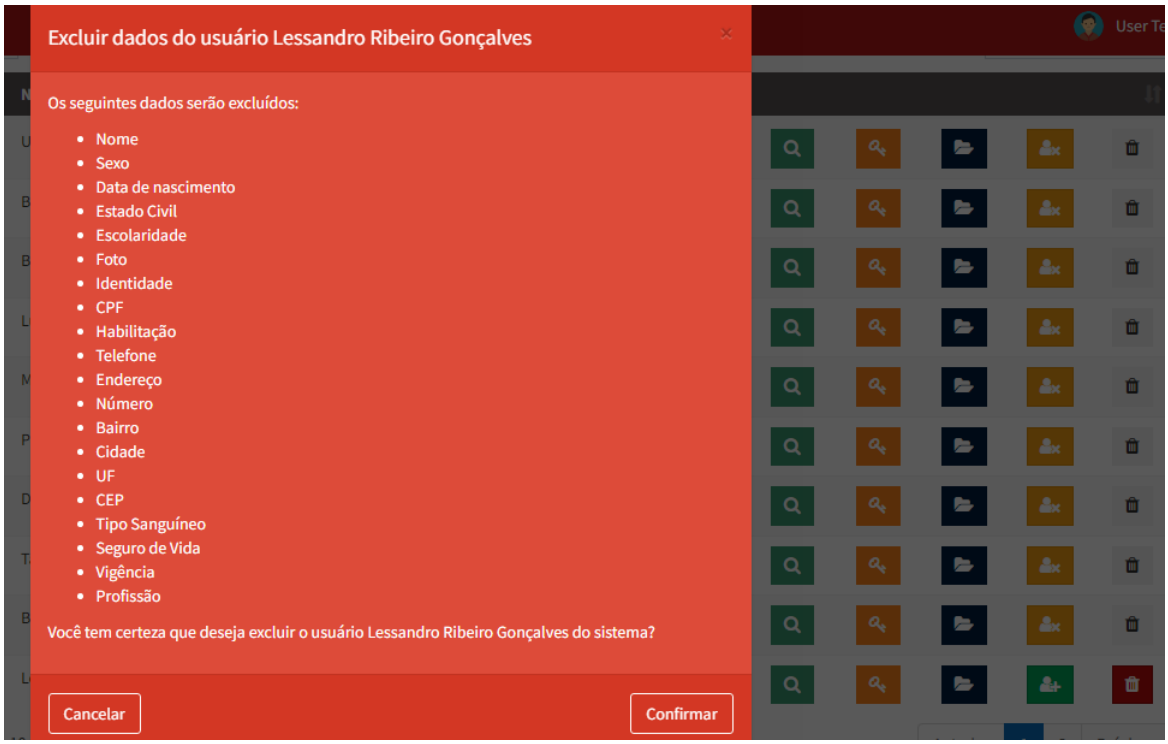
Os termos de uso e a política de privacidade criados, foram baseados nos termos de outras corporações de bombeiros, e hospitais. Isso por causa que tais organizações estão envolvidas com o uso de dados pessoais e sensíveis de forma semelhante ao nosso contexto. Um exemplo foi o Corpo de Bombeiros Voluntários de Joinville, em que a política de privacidade do mesmo pode ser encontrada no seguinte *link*: "https://www.cbvj.org.br/politica-de-privacidade/". Outro ponto importante na criação dos nossos termos de uso e política de privacidade, foi o estudo do atual termo de compromisso utilizado quando um usuário entra na Corporação de Bombeiros Voluntários de São Domingos do Prata. Tal termo foi disponibilizado para nós pelo coordenador geral, com intuito de possíveis alterações

no termo, assim como para ampliar nosso entendimento no contexto da corporação em questão.

3.4.4 Exclusão de Usuários

Essa nova funcionalidade tem como objetivo excluir os dados de um usuário do banco de dados do sistema. Ao tentar efetuar essa ação, aparecerá um *"prompt"* avisando quais dados serão excluídos e que tal ação é irreversível. A figura 11 mostra o aviso ao tentar excluir um usuário.

Figura 11 – Tela de exclusão do usuário



Fonte: Elaborado pelo autor. (2023)

Após a exclusão dos dados de um usuário, o nome do usuário desaparece da lista de usuários e quaisquer Boletins de ocorrência que o mesmo tenha criado continuará existindo. Entretanto, onde constar o nome do usuário em questão estará descrito como "Usuário excluído". Portanto, a exclusão de um usuário não estará afetando negativamente nenhuma parte do sistema. A figura 12 se refere as informações que ficam de um usuário após o mesmo estar excluído.

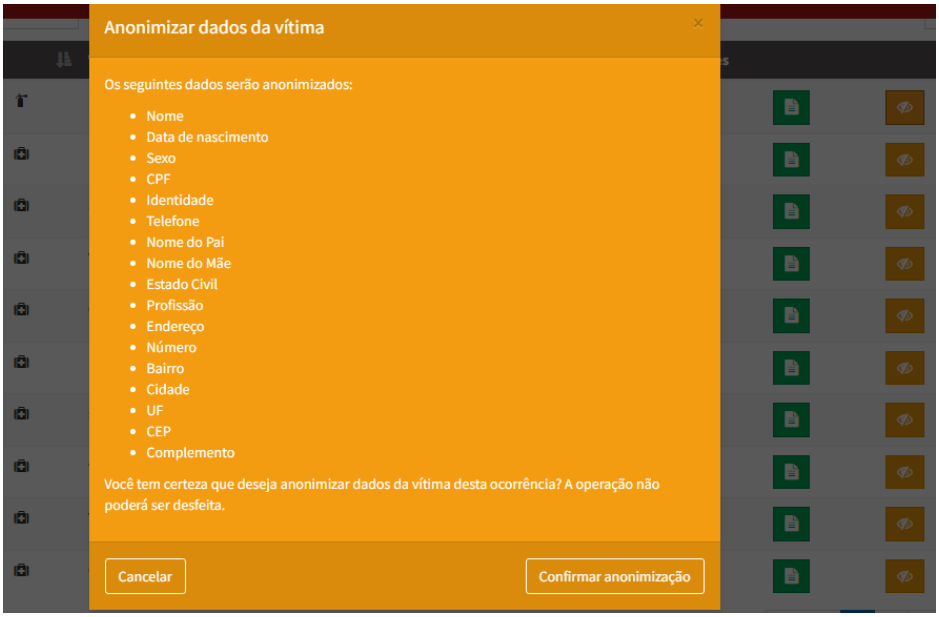
Figura 12 – B.O. feito por um usuário excluído

Fonte: Elaborado pelo autor. (2023)

3.4.5 Anonimização das Vítimas

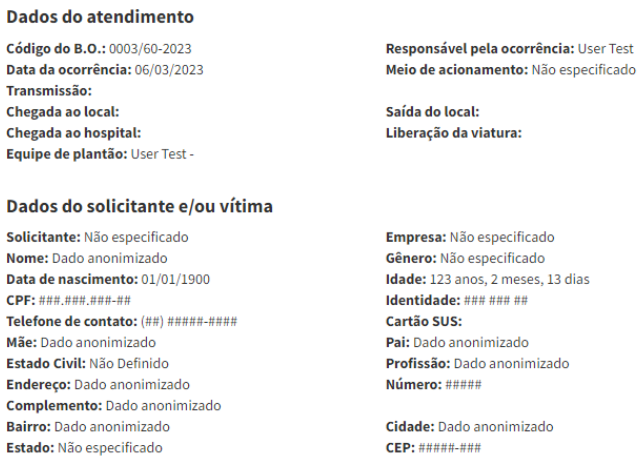
A funcionalidade da anonimização das vítimas é um dos pontos principais deste trabalho, pois a LGPD ressalta a importância de permitir que os dados de usuários e clientes possam ter a opção de serem anonimizados ou excluídos. No caso do SisGera, foi decidido fazer a anonimização desses dados, pois a corporação de bombeiros voluntários realiza algumas pesquisas utilizando dados adquiridos dos boletins de ocorrência registrados no sistema. Entretanto, nessas pesquisas não são utilizados os dados pessoais das vítimas. Portanto, mesmo com os dados anonimizados, será possível realizar essas pesquisas. As figuras 13 e 14 representam, respectivamente, o *"prompt"*, ao tentar anonimizar os dados de uma vítima, e os dados de uma vítima no boletim de ocorrência, após terem sido anonimizados.

Figura 13 – *"Prompt"* ao tentar anonimizar uma vítima



Fonte: Elaborado pelo autor. (2023)

Figura 14 – B.O. contendo informações de uma vítima anonimizada



Dados do atendimento

Código do B.O.: 0003/60-2023
Data da ocorrência: 06/03/2023
Transmissão:
Chegada ao local:
Chegada ao hospital:
Equipe de plantão: User Test -

Responsável pela ocorrência: User Test
Meio de acionamento: Não especificado

Saída do local:
Liberação da viatura:

Dados do solicitante e/ou vítima

Solicitante: Não especificado
Nome: Dado anonimizado
Data de nascimento: 01/01/1900
CPF: ###.###.###-##
Telefone de contato: (##) #####-####
Mãe: Dado anonimizado
Estado Civil: Não Definido
Endereço: Dado anonimizado
Complemento: Dado anonimizado
Bairro: Dado anonimizado
Estado: Não especificado

Empresa: Não especificado
Gênero: Não especificado
Idade: 123 anos, 2 meses, 13 dias
Identidade: ### ### ##
Cartão SUS:
Pai: Dado anonimizado
Profissão: Dado anonimizado
Número: #####

Cidade: Dado anonimizado
CEP: #####-###

Fonte: Elaborado pelo autor. (2023)

4 Considerações Finais

Este trabalho apresentou o desenvolvimento de novas funcionalidades no projeto SisGera, sendo que essas funcionalidades adicionadas têm como objetivo tornar o sistema padronizado de acordo com as exigências da LGPD, garantindo assim uma maior segurança para os usuários que acessam o sistema, e para as vítimas que tem seus dados coletados nos boletins de ocorrência, além disso impossibilita o sistema de receber as penalidades sujeitas por não estar nos padrões da LGPD.

Primeiramente, foi realizada uma revisão da literatura envolvida neste trabalho. Foram levantadas informações sobre sistemas de informação, LGPD, Engenharia de Software e aplicações *Web*. Na etapa seguinte, foi apresentado o SisGera, a escolha das ferramentas utilizadas para o desenvolvimento da aplicação e, logo na sequência, foi demonstrado o levantamento de requisitos, os quais foram retratados também por meio de um modelo de história de usuário. Foi descrito todo o processo de desenvolvimento da aplicação, incluindo o pensamento por trás das funcionalidades da aplicação observadas nos requisitos, e por fim, os testes funcionais realizados. Foram apresentados os resultados obtidos neste trabalho, por meio das telas e descrições das funcionalidades produzidas.

As mudanças ainda não foram oficialmente implementadas, estando disponível apenas na versão de teste do sistema, entretanto futuros trabalhos envolvendo SisGera, já irão trabalhar utilizando o ambiente Docker feito neste trabalho, assim como as novas funcionalidades projetadas.

Durante o desenvolvimento deste trabalho, foi possível perceber a importância em manter um sistema aos padrões da LGPD, pois manter esses padrões melhora na segurança da informação do sistema em questão, e portanto, espera-se que com a adaptação e adição das funcionalidades do sistema que foram realizadas, ajude os grupos de bombeiros que utilizam o SisGera, e com isso, impacte positivamente as comunidades apoiadas pelo trabalho voluntário das corporações.

4.1 Trabalhos Futuros

Durante o desenvolvimento deste trabalho e após uma análise de possíveis cenários que podem acontecer, foram identificadas algumas propostas de trabalhos futuros, apresentados na lista abaixo.

- Adicionar uma funcionalidade para armazenamento de imagens em boletins de ocorrência, seguindo os padrões da LGPD;

- Alterações em algumas páginas e funcionalidades do sistema, com o objetivo de melhorar a usabilidade para o usuário;
- Acrescentar mais segurança nas funcionalidades do sistema;
- Avaliar a resposta dos usuários em relação às novas funcionalidades e visuais adicionadas.

Referências

ARANTES, V. M. Um sistema de informação para apoio ao registro de ocorrências atendidas por grupos de bombeiros voluntários. 11 2018. Disponível em: <https://www.monografias.ufop.br/handle/35400000/1188>. Citado 3 vezes nas páginas 13, 16 e 25.

AUDY, J. L. N.; ANDRADE, G. K.; CIDRAL, A. Fundamentos de sistemas de informação. 2005. Citado na página 16.

BARRETO, J. S. et al. Fundamentos de segurança da informação. *Grupo A*, 2018. Citado na página 17.

BRASíLIA DF, P. d. R. Lei geral de proteção de dados pessoais (lgpd). 2020. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Citado na página 18.

CASTRO, L. H. M. d. Desenvolvimento de um módulo de help desk para o sistema sisgera. 2022. Disponível em: <https://monografias.ufop.br/handle/35400000/4515>. Citado 4 vezes nas páginas 13, 16, 25 e 31.

COTS, M.; OLIVEIRA, R. Lei geral de proteção de dados pessoais comentada. *São Paulo: Revista dos Tribunais*, v. 2, 2019. Citado na página 22.

GARCIA, L. R. Lei geral de proteção de dados (lgpd): Guia de implantação. 2020. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555060164/.> Citado na página 20.

LAUDON, K.; LAUDON, J. Sistemas de informações gerenciais. *São Paulo: Pearson Prentice Hall*, v. 9, 2010. Citado na página 16.

LIMA, A. P. M. C. d. Lgpd aplicada. *Grupo GEN*, 2021. Citado 3 vezes nas páginas 18, 19 e 21.

LONGO, H. E. R.; SILVA, M. P. d. A utilização de histórias de usuários no levantamento de requisitos Ágeis. *International Journal of Knowledge Engineering and Management*, 2014. Citado na página 27.

O'BRIEN, J. A. Sistemas de informação e as decisões gerenciais na era da internet. *São Paulo: Saraiva*, v. 2, 2004. Citado na página 16.

OLIVEIRA, S. S. M. Sistema de informação para controle de materiais e doações aos bombeiros voluntários. 2018. Disponível em: <https://www.monografias.ufop.br/handle/35400000/1621>. Citado 4 vezes nas páginas 13, 16, 25 e 31.

PRESSMAN, R. S. Engenharia de software: Uma abordagem profissional. *McGraw Hill*, v. 7, 2011. Citado na página 24.

PRESSMAN, R. S.; MAXIM, B. Engenharia de software. *McGraw Hill*, v. 8, 2016. Citado na página 23.

REZENDE, D. A. Sistemas de informações organizacionais. *Atlas*, 2005. Citado na página 16.

SILVA, G. O. Desenvolvimento de uma aplicação web progressiva para o registro de ocorrências de um grupo de bombeiros voluntários. 2021. Disponível em: <https://monografias.ufop.br/handle/35400000/3503>. Citado 3 vezes nas páginas 13, 16 e 25.

APÊNDICE A – Termos de uso

A seguir apresentamos os Termos de Uso utilizados no sistema SisGera.

Quais informações estão presentes neste documento?

Neste Termo de Uso, o usuário prestador do serviço voluntário do SisGera, encontrará informações sobre: o funcionamento do serviço e as regras aplicáveis a ele; o arcabouço legal relacionado à prestação do serviço; as responsabilidades do titular dos dados ao utilizar o serviço; as responsabilidades da Administração Pública ao prover o serviço; informações para contato, caso exista alguma dúvida ou seja necessário atualizar informações; e o foro responsável por eventuais reclamações caso questões deste Termo de Uso tenham sido violadas. Além disso, na Política de Privacidade, o prestador do serviço voluntário do SisGera, encontrará informações sobre: quais os tratamentos dos dados pessoais realizados, de forma automatizada ou não, e a sua finalidade; os dados pessoais dos voluntários necessários para a prestação do serviço; a forma como eles são coletados; se há o compartilhamento de dados com terceiros; e quais as medidas de segurança implementadas para proteger os dados.

Aceitação do Termo de Uso e Política de Privacidade

Ao se inscrever para o serviço voluntário do CBMSC, denominado Bombeiro Comunitário, o voluntário confirma que leu e compreendeu os Termos e Políticas aplicáveis ao serviço voluntário e concorda em ficar vinculado a eles.

Definições

Para melhor compreensão deste documento, neste Termo de Uso e Política de Privacidade, consideram-se:

Agente público: Todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública, direta ou indireta.

Agentes de tratamento: o controlador e o operador.

Anonimização: Utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

Apoio ao SisGera: atividades típicas de bombeiro, não privativas de agente público, desempenhadas por voluntários.

Autoridade nacional: órgão da Administração Pública responsável por zelar, imple-

mentar e fiscalizar o cumprimento desta Lei em todo o território nacional.

Banco de dados: Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico

Bloqueio: Suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.

Códigos maliciosos: é qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores.

Consentimento: Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

Dado anonimizado: Dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Dado pessoal: informação relacionada a pessoa natural identificada ou identificável.

Dado pessoal sensível: Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Eliminação: Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes.

Lei Geral de Proteção de Dados: Lei Federal n. 13.709, de 14 de agosto de 2018, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador

Órgão de pesquisa: Órgão ou entidade da Administração Pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.

Serviço voluntário: atividade não remunerada, prestada por pessoa física, com objetivos cívicos, culturais, educacionais, científicos ou de assistência social, espontaneamente, sem vínculo empregatício e sem encargos trabalhistas, por pessoa física com idade superior a 18 (dezoito) anos, conforme preconizado na Lei federal nº 9.608, de 1998.

Sites e aplicativos: sites e aplicativos por meio dos quais o usuário acessa os serviços e conteúdos disponibilizados.

Terceiro: Pessoa ou entidade que não participa diretamente em um contrato, em um ato jurídico ou em um negócio, ou que, para além das partes envolvidas, pode ter interesse num processo jurídico.

Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entes privados.

Usuários (ou "Usuário", quando individualmente considerado): todas as pessoas naturais que prestam o serviço voluntário do SisGera.

Validação biográfica: Conforme a Decreto nº 10.543, de 13 de novembro de 2014, a validação biográfica é definida como a confirmação da identidade da pessoa natural mediante comparação de fatos da sua vida, tais como nome civil ou social, data de nascimento, filiação, naturalidade, nacionalidade, sexo, estado civil, grupo familiar, endereço e vínculos profissionais, com o objetivo de identificá-la unicamente com médio grau de segurança.

Validação biométrica: Conforme a Decreto nº 10.543, de 13 de novembro de 2014, a validação biométrica é definida como a confirmação da identidade da pessoa natural mediante aplicação de método de comparação estatístico de medição biológica das características físicas de um indivíduo com objetivo de identificá-lo unicamente com alto

grau de segurança.

Violação de dados pessoais: É uma violação de segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso não autorizado a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

Voluntários (ou "voluntários", quando individualmente considerado): prestador do serviço voluntário.

Quais são as leis e normativos aplicáveis a esse serviço?

- Lei nº 12.965, de 23 de abril de 2014: Marco Civil da Internet – Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;
- Lei nº 12.527, de 18 de novembro de 2011: Lei de Acesso à Informação – Regula o acesso a informações previsto na Constituição Federal;
- Lei nº 13.460, de 26 de junho de 2017: Dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública;
- Lei nº 13.709, de 14 de agosto de 2018: Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Quais são os direitos do titular dos dados?

O titular dos dados possui os seguintes direitos, conferidos pela Lei de Proteção de Dados Pessoais:

Direito de confirmação e acesso (Art. 18, I e II): é o direito do usuário de obter do serviço a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de acessar os seus dados pessoais.

Direito de retificação (Art. 18, III): é o direito de solicitar a correção de dados incompletos, inexatos ou desatualizados.

Direito à limitação do tratamento dos dados (Art. 18, IV): é o direito do usuário de limitar o tratamento de seus dados pessoais, podendo exigir a eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei Geral de Proteção de Dados.

Direito de oposição (Art. 18, § 2º): é o direito do usuário de, a qualquer momento, se opor ao tratamento de dados por motivos relacionados com a sua situação particular, com fundamento em uma das hipóteses de dispensa de consentimento ou em caso de descumprimento ao disposto na Lei Geral de Proteção de Dados.

Direito de portabilidade dos dados (Art. 18, V): é o direito do usuário de realizar a 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.

Direito de não ser submetido a decisões automatizadas (Art. 20, LGPD): o titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

Quais são as obrigações dos titulares dos dados?

O titular dos dados se responsabiliza pela precisão e veracidade dos dados informados e reconhece que a inconsistência destes poderá implicar a impossibilidade de se prestar o serviço voluntário, denominado Bombeiro Comunitário.

Durante a prestação do serviço, a fim de resguardar e proteger os direitos de terceiros, o titular dos dados se compromete a fornecer somente seus dados pessoais, e não os de terceiros.

O login e senha só poderão ser utilizados pelo titular dos dados cadastrais. Ele se compromete em manter o sigilo da senha, que é pessoal e intransferível, não sendo possível, em qualquer hipótese, a alegação de uso indevido, após o ato de compartilhamento.

O titular dos dados é responsável pela atualização das suas informações pessoais e consequências na omissão ou erros nas informações pessoais cadastradas.

O titular dos dados é responsável pela reparação de todos e quaisquer danos, diretos ou indiretos (inclusive decorrentes de violação de quaisquer direitos de terceiros, inclusive direitos de propriedade intelectual, de sigilo e de personalidade), que sejam causados à Administração Pública, a qualquer terceiro, inclusive em virtude do descumprimento do disposto nestes Termos de Uso e Política de Privacidade ou de qualquer ato praticado a partir de seu acesso ao serviço.

O Órgão não poderá ser responsabilizado pelos seguintes fatos:

- Equipamento infectado ou invadido por atacantes;
- Proteção do computador;
- Proteção das informações baseadas nos computadores dos usuários;
- Abuso de uso dos computadores dos usuários;
- Monitoração clandestina do computador dos usuários;
- Vulnerabilidades ou instabilidades existentes nos sistemas dos usuários;

- Perímetro inseguro.

O uso comercial das expressões utilizadas de propriedade do SisGera como marca e nome de domínio, além dos conteúdos do serviço, assim como os programas, bancos de dados, redes, arquivos que permitem que o usuário acesse sua conta estão protegidos pelas leis de direito autoral, marcas, patentes, modelos e desenhos industriais.

Ao acessar aplicativos e sistemas internos, os usuários declaram que irão respeitar todos os direitos de propriedade intelectual e os decorrentes da proteção de marcas, patentes, depositados ou registrados em, bem como todos os direitos referentes a terceiros que porventura estejam, ou estiveram de alguma forma, disponíveis no serviço. O simples acesso ao serviço não confere aos usuários qualquer direito ao uso dos nomes, títulos, palavras, frases, marcas, patentes, imagens, dados e informações, dentre outras, que nele estejam ou estiverem disponíveis.

A reprodução de conteúdo descritos anteriormente está proibida, salvo com prévia autorização por escrito ou caso se destinem ao uso exclusivamente pessoal e sem que em nenhuma circunstância os usuários adquiram qualquer direito sobre esses conteúdos.

É vedada a utilização do serviço para finalidades comerciais, publicitárias ou qualquer outra que contrarie a finalidade para a qual foi concebido, conforme definido neste documento, sob pena de sujeição às sanções cabíveis na Lei nº 9.610/1998, que protege os direitos autorais no Brasil.

Os visitantes e usuários assumem toda e qualquer responsabilidade, de caráter civil e/ou criminal, pela utilização indevida das informações, textos, gráficos, marcas, imagens, enfim, todo e qualquer direito de propriedade intelectual ou industrial do serviço.

Em nenhuma hipótese, a Administração Pública Estadual será responsável pela instalação no equipamento do usuário ou de terceiros, de códigos maliciosos (vírus, trojans, *malware, worm, bot, backdoor, spyware, rootkit,* ou de quaisquer outros que venham a ser criados), em decorrência da navegação na Internet pelo usuário.

Quais são as responsabilidades da Administração Pública com os meus dados?

A Administração Pública, no papel de custodiante das informações pessoais dos titulares dos dados, deve cumprir todas as legislações inerentes ao uso correto dos dados pessoais do cidadão de forma a preservar a privacidade dos dados utilizados pelo SisGera

Publicar as futuras alterações a estes Termos de Uso e Política de Privacidade por meio do site (https://www.sisgera.com.br), conforme o princípio da publicidade estabelecido no artigo 37, caput, da Constituição Federal.

Em hipótese alguma, o SisGera se responsabiliza por eventuais danos diretos, indiretos, emergentes, especiais, imprevistos ou multas causadas, em qualquer matéria

de responsabilidade, seja contratual, objetiva ou civis (inclusive negligência ou outras), decorrentes de qualquer forma de uso do serviço, mesmo que advertida a possibilidade de tais danos.

Tendo em vista que o serviço lida com informações pessoais, o usuário concorda que não usará robôs, sistemas de varredura e armazenamento de dados (como "spiders" ou "scrapers"), links escondidos ou qualquer outro recurso escuso, ferramenta, programa, algoritmo ou método coletor/extrator de dados automático para acessar, adquirir, copiar ou monitorar o serviço, sem permissão expressa por escrito do órgão.

Caso o titular dos dados descumpra o Termo de Uso ou a Política de Privacidade, ou seja investigado em razão de má conduta, o órgão poderá restringir seu acesso, além das medidas previstas na legislação em vigor. O titular dos dados também deverá responder legalmente por essa conduta.

A Administração Pública poderá, quanto às ordens judiciais de pedido de informações, compartilhar informações necessárias para investigações ou tomar medidas relacionadas a atividades ilegais, suspeitas de fraude ou ameaças potenciais contra pessoas, bens ou sistemas que sustentam o serviço ou de outra forma necessária para cumprir com as obrigações legais. Caso ocorra, a Administração Pública notificará os titulares dos dados, salvo quando o processo estiver em segredo de justiça.

As informações relativas aos dados pessoais dos titulares, coletadas pelo SisGera, são de uso para fins de segurança pública.

APÊNDICE B – Política de Privacidade

A seguir apresentamos a Política de Privacidade utilizada no sistema SisGera.

O sistema SisGera tem como compromisso o respeito pela privacidade de seus usuários, bem como a proteção e a segurança dos seus dados pessoais.

A atual Política de Privacidade tem como objetivo esclarecer quais informações são coletadas dos usuários do site https://www.SisGera.com.br/ e de que forma esses dados são tratados.

Reconhecendo a importância de manter sua privacidade, são tomadas todas as medidas possíveis para protegê-la. Portanto, o presente documento tem como objetivo informá-lo como os seus dados pessoais coletados no site serão tratados.

No momento em que você inserir as suas informações ou se cadastrar para tirar dúvidas ou solicitar ações, você estará aceitando a Política de Privacidade presente neste documento

Isso indicará que você está ciente e em total acordo com a forma que utilizaremos as suas informações e seus dados. Caso não concorde com esta política, por favor, não continue o seu procedimento de cadastro.

INFORMAÇÕES COLETADAS

- Informações fornecidas por você – Das informações fornecidas por você com o preenchimento dos formulários disponíveis em nosso site, o SisGera coletará aquelas de identificação pessoal, como por exemplo nome, *email*, telefone, empresa, CNPJ, cidade, Estado. É possível que eventualmente a solicitação de outras informações possa ser feita por meio de contato direto, presencialmente ou via *email* ou telefone, dependendo da ação que esteja querendo executar.

  Informações coletadas por socorristas - Das informações coletadas por socorristas em meio de algum acidente ou ocorrência de natureza similar, podem ser coletadas informações pessoais e sensíveis, dentro da permissão da pessoa em questão, a não ser que a mesma não esteja em condições para a coleta de informações, caso esse seja a situação, o socorrista pode coletar as informações que são necessárias para a proteção da vida.

  Informações de navegação no site – Quando você acessa nosso site, poderá ser instalado um "*cookie*" no seu navegador para identificar quantas vezes você retorna ao nosso endereço. Nesta hipótese, poderão ser coletadas informações como endereço

IP, localização geográfica, fonte de referência, tipo de navegador, duração da visita e páginas visitadas.

Dados gerados pela utilização de atendimentos de acidentes, incêndios e outros, além de cadastro solicitando informações e ações – O SisGera poderá coletar outras informações necessárias para contato posterior, seja esse contato com fins de avaliação do atendimento prestado ou mesmo sugerindo doação para a entidade. Nesse caso, poderão ser coletados dados de contato como seu nome completo, *email* e telefone, RG e CPF, cidade e Estado, logradouro, número do logradouro e complemento.

PARA QUE USAMOS SUAS INFORMAÇÕES

Todos os dados coletados são utilizados para comunicação de nossas ações e sugestão de contribuição para manutenção de nossas atividades, assim como o possível compartilhamento de dados, estritamente necessários, para entidades de saúde por possíveis motivos de proteção à vida. Por isso, todos os dados e informações sobre você serão tratados como confidenciais e somente utilizados para os fins aqui descritos e autorizados por você, visando sempre melhorar a sua experiência como usuário e o retorno para a comunidade de nossas atividades

Eventualmente, poderemos utilizar dados para finalidades não previstas nesta Política, mas que estejam dentro das suas legítimas expectativas. O eventual uso dos seus dados para finalidades que não cumpram com essa prerrogativa será feito mediante autorização que solicitaremos previamente.

Além das hipóteses citadas nesta Política, seus dados poderão ser utilizados para as seguintes finalidades:

- Seu *email* poderá ser utilizado para a operação de envio de informações por você requisitada no preenchimento dos formulários disponíveis em nosso site. Também poderá ser utilizado para o envio de notícias e outras informações, sempre relacionadas ao SisGera;
- Funcionários do SisGera poderão eventualmente entrar em contato via *email* ou telefone para fazer pesquisas;
- Poderão ser enviadas, pelo SisGera a você, mensagens a respeito de suporte ou serviço, como alertas, notificações e atualizações;
- O SisGera poderá informá-lo sobre serviços, notícias, atualizações e outros assuntos que você possa ter interesse;
- O SisGera poderá utilizar seus dados para qualquer fim que você autorize no momento da coleta;

- O SisGera poderá utilizar seus dados para cumprir obrigações legais e regulatórias.

SOBRE O ACESSO AOS SEUS DADOS PESSOAIS

O acesso às suas informações pessoais estará restrito apenas aos colaboradores do SisGera, e dentre estes, somente as pessoas com autorização interna específica para tanto. Eventualmente, caso a inserção de suas informações se dê em ações criadas em parcerias, os parceiros explicitamente identificados também terão acesso à informação. Exceto se de outra forma for previsto em Lei, nenhum dado pessoal poderá ser divulgado publicamente sem a sua prévia e expressa autorização.

Todos os seus dados são confidenciais e qualquer uso de tais dados estará de acordo com a Lei e com a presente Política. O SisGera empreenderá todos os esforços razoáveis de mercado para garantir a segurança dos nossos sistemas e, consequentemente, dos seus dados pessoais.

Todas as suas informações serão, sempre que possível, anonimizadas, caso não inviabilizem o seu uso pelo SisGera.

Dentre outros direitos previstos em Lei, mediante requisição e a qualquer momento, você poderá ter acesso aos seus dados pessoais armazenados em nossos sistemas.

O SisGera manterá os seus dados pessoais e informações somente até quando estas forem necessárias ou relevantes para as finalidades descritas nesta Política, ou em caso de períodos pré-determinados por lei, ou até quando estas forem necessárias para a manutenção de interesses legítimos do SisGera, nos termos da lei.

SOBRE O COMPARTILHAMENTO DE DADOS

O SisGera poderá compartilhar os seus dados pessoais com parceiros, terceiros, conforme for razoavelmente necessário para os propósitos estabelecidos na presente Política e para a devida prestação de nossos serviços.

O SisGera se reserva no direito de fornecer dados e informações sobre você, incluindo suas interações, caso seja requisitado judicialmente, ato necessário para que o SisGera esteja em conformidade com as leis nacionais, ou caso você autorize expressamente.

SOBRE O CANCELAMENTO DO CADASTRO E ALTERAÇÃO/EXCLUSÃO DE DADOS PESSOAIS

Você pode optar por não receber mais *email*s do SisGera, exceto em relação aos *email*s essenciais para a continuidade da prestação de nossos serviços ou mesmo aqueles que, por obrigação legal ou regulatória, o SisGera necessita enviar a seus usuários.

É importante mencionar que, ao preencher qualquer formulário ou realizar qualquer tipo de cadastro novamente, ficará caracterizada a reinserção do seu *email* à lista de contatos do SisGera. Portanto, a requisição de cancelamento deverá ser feita novamente

caso seja de seu interesse.

Todos os dados coletados serão excluídos de nossos servidores quando você assim requisitar ou quando estes não forem mais necessários ou, salvo se houver qualquer outra razão para a sua manutenção, como eventual obrigação legal de retenção de dados ou necessidade de preservação destes para resguardo de direitos do SisGera. Para alterar suas informações pessoais ou excluí-las do nosso banco de dados, entre em contato via *email* ou presencialmente ou por telefone com um dos responsáveis do SisGera

ALTERAÇÕES NA POLÍTICA DE PRIVACIDADE

Essa Política pode passar por atualizações. Portanto, recomendamos visitar periodicamente esta página para que você tenha conhecimento sobre as modificações. Caso sejam feitas alterações relevantes que ensejem novas autorizações suas, tornamos pública a nova política de privacidade.

Esta Política foi modificada pela última vez em outubro de 2022.

LEI APLICÁVEL

Este documento é regido e deve ser interpretado de acordo com as leis da República Federativa do Brasil.

POLÍTICA DE *COOKIES*

- **O que são**

  Um *cookie* é uma informação armazenada em seu computador ou dispositivo, por um site que você visita. Costumam armazenar informações de configuração da sua visita a um site, como seu local ou idioma preferido. Quando você retorna ao site, permite melhor interação, pela apresentação de informações personalizadas de acordo com suas necessidades. No caso específico, pretende-se melhorar sua experiência quando o site do SisGera é visitado. Quanto aos dados coletados, o objetivo é a obtenção de informações que ajudem a navegação do site, tornando a experiência da visita mais personalizada. Dados pessoais podem ser coletados, mas desde que sejam fornecidos. Importante ressaltar que os sites não conseguem obter dados não informados e nem obter dados existentes em seu computador.

- **Para que servem**

  O SisGera utiliza *cookies* para facilitar o uso e melhor adaptar o site aos seus interesses e necessidades, bem como para compilar informações sobre as utilizações, auxiliando a melhorar suas estruturas e seus conteúdos. Da mesma forma, os *cookies* ajudam e melhoram as atividades e experiências daqueles que visitam nosso site.

- **Como utilizamos *cookies***

Se habilitados / autorizados, esses *cookies* têm por único objetivo aprimorar a personalização, melhorando cada vez mais a experiência de quem visita o site do SisGera. Os *cookies* que utilizamos no momento em que foi atualizado este documento são os *cookies* de login e *cookies* de seguranças, padrões do Google.

- **Como habilitar *cookies***

  Grande parte dos navegadores de internet aceita *cookies* automaticamente, ainda que muitos deem a opção de recusar os *cookies* ou avisá-los quando um site estiver tentando inserir um cookie em seu dispositivo. Após você autorizar a utilização de *cookies*, o SisGera armazenará esses registros (*cookies*) em seu dispositivo, melhorando sua utilização para a próxima visita ao nosso site.

- **Não fornecimento de *cookies***

  Você poderá desabilitar, por meio das configurações de seu navegador de internet, a coleta automática de informações por meio de algumas tecnologias, como *cookies* e caches, bem como em nosso Site, especificamente quanto aos *cookies*. Nestes casos, certos serviços poderão não funcionar de maneira ideal, sem que isso possa ser responsabilidade do SisGera.

APÊNDICE C – Boas Práticas de Segurança da Informação

Apresentamos a seguir o documento de Boas práticas de Segurança da Informação.

Gestão de senhas para acesso seguro:

- Criar senhas diferentes para as diversas contas e aplicações, o que evita danos "em cadeia" caso uma senha corporativa seja vazada;
- Incluir letras, números e caracteres especiais, totalizando ao mínimo 8 dígitos;
- Evitar usar geradores automáticos de senhas;
- Trocar senhas que são utilizadas por muito tempo;
- Caso o usuário sentir a necessidade de guardar sua senha, o melhor a se fazer é utilizar ferramentas de gestão de senhas, são programas utilizados para armazenar todas as suas senhas em segurança, em um cofre criptografado, evitando ter que se lembrar de cada uma delas toda vez que for feito login em sites e serviços protegidos por códigos, exigindo apenas que o usuário memorize apenas a senha mestra para acessá-lo.

Navegação segura pela web:

- Identificação de domínios falsos e ilegais, isso pode ser feito até mesmo através de métodos simples como perceber possíveis erros de ortografia e gramática na URL ou no próprio site em questão, apesar de não garantir a veracidade do site, esse método é rápido e simples de se executar; F
- Distinção entre redes seguras e redes inseguras de navegação, um exemplo simples para esse caso é que sites com HTTP na URL, são considerados inseguros e HTTPS seguros;
- Conscientização acerca da não divulgação de informações pessoais e corporativas em sites ou *emails* suspeitos;
- Conscientização do perigo do *download* de programas sem o devido licenciamento;
- Tomar cuidado com ataques comuns na navegação online, tais como o *phishing*, que é uma técnica usada para enganar usuários de internet através da fraude eletrônica

para obter informações confidenciais, como nome de usuário, senhas entre outras informações.

Uso seguro de dispositivos removíveis e USB

- Não use mídias removíveis que você considera inseguras;
- Evite executar mídias removíveis automaticamente em todos os seus dispositivos.

Comportamento adequado dentro e fora do ambiente de Trabalho

- Aconselhe a equipe a se atentar a quem possa estar prestando atenção no momento de acesso às aplicações corporativas, especialmente novos membros e desconhecidos em ambientes públicos;
- Deve-se suspeitar qualquer remetente online que se apresente como inspetor, policial, autoridade ou profissional de TI;
- Oriente a equipe a não escrever suas senhas e credenciais em papéis ou dispositivos que permaneçam visualmente disponíveis;
- Alertar o time a não deixar papéis e impressões contendo informações sensíveis, pessoais ou confidenciais na mesa de trabalho.

Dispositivo Pessoais:

Caso algum membro da equipe utilize os dispositivos pessoais, tenha atenção para essas práticas:

- Fazer o *download* de aplicações nos dispositivos pessoais somente de sites aprovados e licenciados;
- Para prevenir o roubo de dados, aposte em senhas fortes de acesso nos dispositivos;
- Utilizar aplicações de antivírus licenciados e de boa qualidade nos dispositivos pessoais;
- Em caso em que tenha ocorrido um furto de dispositivo de algum membro da equipe, tentar alertar os membros da equipe e os responsáveis pela TI, a fim de minimizar ou impedir possíveis danos que possam ocorrer por algum vazamento de informação.

Boas práticas de cibersegurança contra *phishing*

Devem ser considerados suspeitos os *emails* que:

- Tenham remetentes desconhecidos;
- Incluem solicitações de dinheiro ou pagamento do destinatário;
- Vão parar na caixa de *SPAM*;
- Contêm um *link* desconhecido;
- Contém um anexo suspeito ou claramente malicioso.

Vale lembrar que o *phishing* também pode ocorrer via chamadas ligações, SMS, plataformas corporativas e outros canais.

Software malicioso (*malware*)

- Não baixar softwares que não sejam legítimos ou oficiais;
- Manter a cautela acerca dos *emails* recebidos e dos arquivos encontrados em sites suspeitos;
- Verificar se o programa de antivírus está funcionando corretamente, assim como a frequência de atualizações;
- Notificar a TI rapidamente caso haja suspeita de infecção por *malware* no computador.