



**Unidade Acadêmica de Engenharia Elétrica
Centro de Engenharia Elétrica e Informática (CEEI)
Universidade Federal de Campina Grande (UFCG)**

Disciplina: Informática Industrial

Especificação do Projeto

Equipe:

**Julia Ramalho Costa Souza
Samara Lima Cardoso**

21 de março de 2024

SUMÁRIO

1. Introdução.....	3
1.1. Objetivos.....	3
2. Cenários de Uso.....	4
3. Glossário.....	6
4. Requisitos do Usuário.....	7
4.1. Requisitos Funcionais.....	7
4.2. Requisitos Não Funcionais.....	8
5. Requisitos do Sistema.....	9
5.1. Requisitos Funcionais.....	9
5.2. Requisitos Não Funcionais.....	16
6. Arquitetura.....	18
6.1. Visão Lógica.....	18
6.1.1. Diagrama de Blocos.....	18
6.2. Visão de Desenvolvimento.....	18
6.2.1. Diagrama de Classes.....	18
6.3. Visão de Processo.....	20
6.3.1. Diagrama de Atividades.....	20
6.3.2. Diagrama de Sequência.....	22
6.3.3. Máquina de Estados.....	23
6.3.4. Diagrama de Fluxo de Dados.....	23
6.4. Visão Física.....	24

1. Introdução

Com a crescente incidência de desastres naturais, eventos climáticos extremos e emergências de segurança pública, a necessidade de um sistema eficaz de comunicação e alerta se torna cada vez mais notória. Nesse sentido, a implementação de um sistema de alerta de emergência abrangente e confiável visa garantir a segurança e o bem-estar das comunidades em situações críticas, proporcionando uma maneira rápida e confiável de disseminar informações vitais para os cidadãos, ao passo que atende às necessidades do mercado. Essas informações permitem a minimização de danos e o potencial ato de salvar vidas.

Assim, considerando que o mercado busca por soluções que ofereçam uma resposta ágil e coordenada diante de adversidades imprevistas, o **RescueWave** abrange uma ampla gama de situações de emergência, desde desastres naturais até incidentes de segurança pública.

1.1. Objetivos

O objetivo principal do sistema é aprimorar substancialmente a segurança pública, oferecendo um meio de comunicação confiável para reduzir o impacto de desastres, bem como proteger a vida e o bem-estar dos cidadãos em situações de desaparecimento e desastres naturais. A tabela a seguir apresentará os objetivos a serem alcançados e os requisitos correspondentes para atingir esses objetivos.

Definição dos Macro Objetivos		
Código	Descrição	Requisitos
#OBJ01	Desenvolver um Sistema de Alerta de Emergência que permita que instituições como delegacias de polícia, corpo de bombeiros e agências meteorológicas enviem solicitações de mensagem para o sistema, garantindo uma resposta rápida a emergências.	RFU02 RFU04 RFS01 RFS07 RFS10 RFS11 RFS13 RFS16 RFS22 RNFS01
#OBJ02	Implementar o uso do Wireless Emergency Alerts (WEA) para enviar mensagens de emergência para os smartphones dos cidadãos de acordo com sua localização geográfica, garantindo que os alertas sejam direcionados especificamente para áreas afetadas.	RFU02 RFS07 RFS20 RFS21 RFS23

		RNFS02
#OBJ03	Integrar um sistema de georreferenciamento preciso que permita direcionar alertas específicos para áreas afetadas, garantindo que apenas as pessoas que estão em áreas de risco recebam os alertas relevantes.	RFU02 RFS07 RFS09 RFS11 RFS12 RFS21 RFS23
#OBJ04	Desenvolver uma integração eficaz com o Wireless Emergency Alerts (WEA), seguindo os protocolos estabelecidos para garantir a confiabilidade e eficácia na entrega de mensagens de emergência.	RFU02 RFS07 RFS20 RFS23 RNFS01 RNFS04

2. Cenários de Uso

No contexto do projeto do **RescueWave**, diversos atores desempenham papéis fundamentais, cada um contribuindo para garantir a segurança e o bem-estar das comunidades em situações críticas. Esses *stakeholders* são:

- Funcionário/Servidor de órgão de autoridade : usuário do sistema;
- Receptor/Cidadão: usuário final;
- Administrador/Desenvolvedor: gerente do sistema ;
- Operadoras de telefone: agentes externos.

Para uma visualização clara das interações do sistema com seus diferentes *stakeholders*, foi elaborado um diagrama de casos de uso. Este diagrama descreve os atores envolvidos, como autoridades de segurança pública, operadoras de telefonia móvel e cidadãos, juntamente com os casos de uso que representam as principais funcionalidades do sistema.

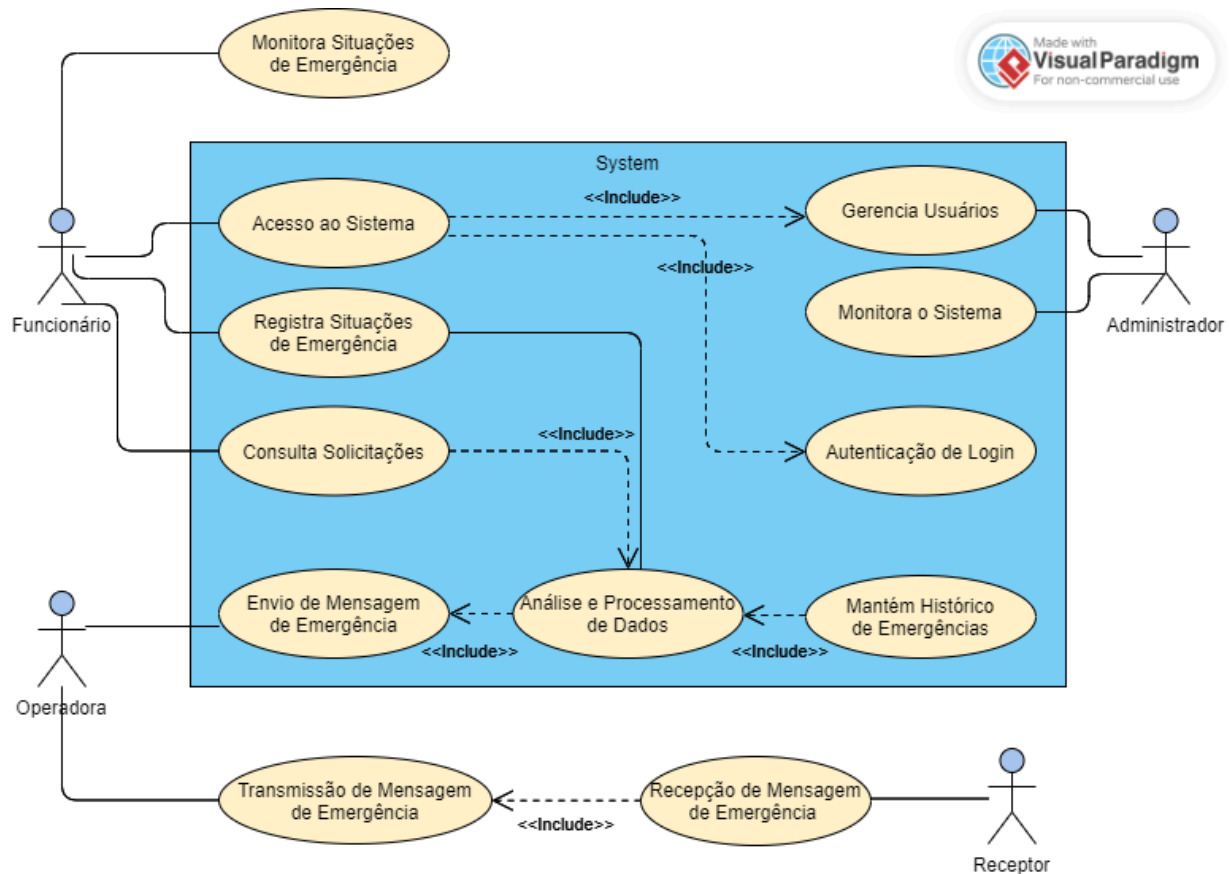


Figura 1. Diagrama de Caso de Uso

Os cenários de uso de cada ator são definidos e detalhados a seguir.

- Funcionário/Servidor de Órgão de Autoridade
 - Monitorar Situações de Emergência: O funcionário deve identificar e acompanhar situações de emergência, tais como desaparecimentos ou desastres naturais.
 - Acesso ao Sistema: O funcionário deve ter a capacidade de acessar o sistema para poder registrar e consultar informações sobre situações de emergência.
 - Registrar Situações de Emergência: Quando necessário, o funcionário deve registrar detalhes sobre situações de emergência no sistema, fornecendo informações cruciais para uma resposta eficaz.
 - Consultar Solicitações: O funcionário tem a opção de consultar e revisar solicitações de emergência registradas no sistema, garantindo uma compreensão abrangente do panorama emergencial.
- Administrador/Desenvolvedor

- Gerenciar Usuários: O administrador é quem gerencia os usuários do sistema (funcionários), incluindo novas contas (cadastros), atribuindo permissões e monitorando a atividade dos usuários.
- Monitorar o Sistema: O administrador gerencia o funcionamento do sistema, identificando e resolvendo problemas técnicos e garantindo o seu bom funcionamento.
- Operadora de Telefone
 - Transmissão de Mensagens de Emergência: A operadora de telefone deve transmitir as mensagens de emergência recebidas do sistema para os dispositivos móveis dos cidadãos, garantindo uma entrega oportuna e eficaz.
- Receptor/Cidadão
 - Recebimento de Mensagens de Emergência: O receptor deve receber as mensagens de emergência enviadas pelo sistema e transmitidas pelas operadoras em seus dispositivos móveis (WEAs), permitindo que tomem medidas apropriadas em resposta às situações de emergência.

Em relação aos casos dentro do próprio sistema, consideram-se as seguintes funcionalidades:

- Sistema
 - Autenticar Login: O sistema é responsável por autenticar o login dos usuários, garantindo que apenas usuários autorizados tenham acesso às funcionalidades do sistema.
 - Análise e Processamento de Dados: Após os funcionários/servidores registrarem as informações sobre situações de emergência, o sistema é responsável por analisar e processar esses dados para fornecer alertas precisos e relevantes.
 - Manter Histórico de Emergências: O sistema deve manter um histórico detalhado de todas as situações de emergência registradas, permitindo uma análise retrospectiva e aprimoramento contínuo do sistema.
 - Envio de Mensagens de Emergência: O sistema deve ser capaz de enviar mensagens de emergência para as operadoras de telefone, garantindo que os alertas sejam transmitidos para os cidadãos de acordo com sua localização geográfica.

3. Glossário

Na tabela 1 é apresentada a lista de siglas utilizadas ao longo do documento. Já na tabela 2, são mostradas algumas definições relevantes.

Sigla	Descrição
WEA	Wireless Emergency Alerts

Tabela 1. Siglas Utilizadas

Definição	Descrição
Prioridade	Define a prioridade do requisito, onde a prioridade do requisito é classificada como "Alta" para requisitos essenciais e "Baixa" para opcionais.
Status	Ele define o fluxo de trabalho do requisito. O status do requisito pode ser "Proposto" quando inicialmente sugerido, "Aprovado" após revisão interna formal, "Excluído" quando não mais necessário e "N/A" quando não aplicável à conclusão final.
Estabilidade	Define a probabilidade de mudanças na definição do requisito. A estabilidade do requisito pode ser classificada como "Alta" quando é improvável que sofra alterações, "Média" quando mudanças podem ocorrer, mas não são iminentes, e "Baixa" quando é mais propenso a revisões ou modificações.
Versão	Esta é a versão do requisito. Ela identifica a versão do documento de requisitos onde o requisito foi criado ou atualizado pela última vez. Em uma nova versão do documento de requisitos, os requisitos que não foram alterados manterão o número da versão. Cada requisito terá sua própria versão, permitindo assim a rastreabilidade das mudanças nos requisitos ao longo de diferentes versões do documento. As versões são numeradas a partir de 0 e incrementadas sequencialmente por 1 unidade.
Rastreabilidade	Este campo consiste em um ou mais requisitos de usuário de alto nível a partir dos quais cada requisito de sistema consolidado particular foi derivado.

Tabela 2. Definições Relevantes

4. Requisitos do Usuário

4.1. Requisitos Funcionais

RFU01- Login de Usuário			
Status:	Proposto	Estabilidade:	Alta
Prioridade:	Alta	Versão:	0
O usuário deve fazer login a partir de um ID e senha específicos para conectar-se à plataforma do sistema.			
Notas:	—		

RFU01- Login de Usuário	
Rastreabilidade:	RFS03

RFU02- Cadastro de Alerta			
Status:	Proposto	Estabilidade:	Alta
Prioridade:	Alta	Versão:	0
O usuário deve realizar o cadastro do alerta para viabilizar sua emissão, fornecendo os dados solicitados pelo sistema.			
Notas:	—		
Rastreabilidade:	RFS04, RFS05		

RFU03- Acesso às Informações de Alertas			
Status:	Proposto	Estabilidade:	Alta
Prioridade:	Baixa	Versão:	0
O usuário deve ter acesso ao histórico e <i>status</i> de solicitações de emissões de alertas realizadas pela entidade à qual faz parte.			
Notas:	—		
Rastreabilidade:	RFS17		

RFU04- Permissão de Acesso			
Status:	Proposto	Estabilidade:	Alta
Prioridade:	Alta	Versão:	0
O sistema deve garantir segurança e controle de acesso, permitindo apenas que servidores de órgãos de autoridade devidamente autenticados e autorizados acessem o sistema.			
Notas:	—		
Rastreabilidade:	RFS01		

RFU05- Solicitação de Ajuda			
Status:	Proposto	Estabilidade:	Média
Prioridade:	Baixa	Versão:	0

RFU05- Solicitação de Ajuda	
O usuário deve ter a capacidade de solicitar assistência através da interface do sistema.	
Notas:	—
Rastreabilidade:	—

4.2. Requisitos Não Funcionais

RNFU01- Habilitação de Usuário			
Status:	Proposto	Estabilidade:	Alta
Prioridade:	Alta	Versão:	0
O usuário deve ser habilitado para interpretar e cadastrar alertas.			
Notas:	—		
Rastreabilidade:	RFS01		

RNFU02- Proteção de dados			
Status:	Proposto	Estabilidade:	Alta
Prioridade:	Alta	Versão:	0
O sistema deve implementar mecanismos robustos de autenticação, autorização e proteção de dados para proteger as informações sensíveis e garantir a conformidade com regulamentos de segurança e privacidade.			
Notas:	—		
Rastreabilidade:	RFS18		

5. Requisitos do Sistema

5.1. Requisitos Funcionais

RFS01- Cadastro de Usuários			
Status:	Proposto	Estabilidade:	Alta
Prioridade:	Alta	Versão:	0
O sistema deve permitir a solicitação de cadastro de usuários qualificados.			

RFS01- Cadastro de Usuários	
Notas:	Usuários qualificados são aqueles pertencentes às autoridades conveniadas/competentes, como: institutos meteorológicos, corpo de bombeiros, delegacias de polícia.
Rastreabilidade:	RFU05, RFS02 e RFS03

RFS02- Análise de Solicitação de Cadastro			
Status:	Proposto	Estabilidade:	Alta
Prioridade:	Alta	Versão:	0
O sistema deve analisar a solicitação de cadastro com base na autenticação dos dados fornecidos pelo usuário com o intuito de permitir ou não a efetivação da solicitação.			
Notas:	—		
Rastreabilidade:	RFS01		

RFS03- Autenticação de Usuário			
Status:	Proposto	Estabilidade:	Alta
Prioridade:	Alta	Versão:	0
O sistema deve permitir o <i>login</i> do usuário qualificado a partir de ID e senha cadastrados.			
Notas:	Cada ID relaciona-se com o respectivo órgão competente.		
Rastreabilidade:	RFU01 e RFS01		

RFS04- Preenchimento de Formulário			
Status:	Proposto	Estabilidade:	Alta
Prioridade:	Alta	Versão:	0
O sistema deve permitir que o usuário preencha um formulário para solicitar a emissão de alerta.			
Notas:	—		
Rastreabilidade:	RFU02		

RFS05- Autenticação de Dados do Alerta			
Status:	Proposto	Estabilidade:	Alta
Prioridade:	Alta	Versão:	0
O sistema deve verificar se o tipo de alerta está de acordo com a função da entidade e se os dados submetidos no formulário estão corretamente preenchidos.			
Notas:	—		
Rastreabilidade:	RFU02		

RFS06- Registro de Auditoria			
Status:	Proposto	Estabilidade:	Alta
Prioridade:	Alta	Versão:	0
O sistema deve registrar todas as interações relacionadas à emissão de alertas em um <i>log</i> de auditoria.			
Notas:	Isso inclui detalhes sobre o solicitante, o tipo de alerta emitido e verificações realizadas durante o processo de autenticação		
Rastreabilidade:	—		

RFS07- Transmissão de Mensagens de Emergência			
Status:	Proposto	Estabilidade:	Alta
Prioridade:	Alta	Versão:	0
Com base nos alertas, o sistema deve transmitir mensagens de emergência por torres de celular via WEA.			
Notas:	—		
Rastreabilidade:	—		

RFS08- Visualização de Mensagens de Emergência			
Status:	Proposto	Estabilidade:	Alta
Prioridade:	Alta	Versão:	0
As mensagens enviadas pelo sistema devem ser exibidas na tela inicial dos dispositivos dos receptores.			

RFS08- Visualização de Mensagens de Emergência	
Notas:	—
Rastreabilidade:	—

RFS09- Recepção de Mensagens de Emergência			
Status:	Proposto	Estabilidade:	Alta
Prioridade:	Alta	Versão:	0
O sistema deve ser capaz de transmitir mensagens de emergência para dispositivos <i>smartphones</i> .			
Notas:	—		
Rastreabilidade:	—		

RFS10- Concorrência de Mensagens de Emergência			
Status:	Proposto	Estabilidade:	Alta
Prioridade:	Alta	Versão:	0
O sistema deve ser capaz de receber mais de uma solicitação e emitir mais um alerta simultaneamente.			
Notas:	—		
Rastreabilidade:	—		

RFS11- Classificação de Mensagens de Emergência			
Status:	Proposto	Estabilidade:	Alta
Prioridade:	Alta	Versão:	0
O sistema deve ser capaz de diferenciar os diferentes tipos de alertas com base na solicitação dos usuários em classes.			
Notas:	—		
Rastreabilidade:	—		

RFS12- Anonimato de Receptores			
Status:	Proposto	Estabilidade:	Alta

RFS12- Anonimato de Receptores			
Prioridade:	Alta	Versão:	0
O sistema deve manter os receptores de mensagens em anonimato, sem ter acesso a números de celular e sem necessitar de cadastro/ <i>login</i> .			
Notas:	—		
Rastreabilidade:	—		

RFS13- Customização de Formulários			
Status:	Proposto	Estabilidade:	Alta
Prioridade:	Alta	Versão:	0
O sistema deve fornecer um formulário específico para cada tipo de ocorrência de acordo com o ID do usuário.			
Notas:	—		
Rastreabilidade:	—		

RFS14- Feedbacks			
Status:	Proposto	Estabilidade:	Alta
Prioridade:	Alta	Versão:	0
O sistema deve fornecer um parecer sobre o <i>status</i> das ocorrências registradas para os usuários.			
Notas:	—		
Rastreabilidade:	—		

RFS15- Classificação por Prioridade			
Status:	Proposto	Estabilidade:	Alta
Prioridade:	Alta	Versão:	0
O sistema deve classificar as ocorrências em níveis de prioridade.			
Notas:	—		
Rastreabilidade:	—		

RFS16- Identificação de Ocorrências			
Status:	Proposto	Estabilidade:	Alta
Prioridade:	Alta	Versão:	0
O sistema deve gerar um número de protocolo para cada ocorrência registrada.			
Notas:	—		
Rastreabilidade:	—		

RFS17- Histórico de Ocorrências			
Status:	Proposto	Estabilidade:	Alta
Prioridade:	Alta	Versão:	0
O sistema deve exibir um histórico de solicitações para os usuários dos respectivos órgãos competentes.			
Notas:	—		
Rastreabilidade:	RFU03		

RFS18- Comunicação Segura			
Status:	Proposto	Estabilidade:	Alta
Prioridade:	Alta	Versão:	0
O sistema deve garantir a comunicação segura dos dados submetidos nos formulários para o servidor em nuvem.			
Notas:	—		
Rastreabilidade:	RNFU02		

RFS19- Banco de Dados			
Status:	Proposto	Estabilidade:	Alta
Prioridade:	Alta	Versão:	0
O sistema deve armazenar em nuvem o conteúdo submetido nas solicitações de mensagens de emergências.			
Notas:	—		
Rastreabilidade:	—		

RFS20- Controle de Transmissão WEA			
Status:	Proposto	Estabilidade:	Alta
Prioridade:	Alta	Versão:	0
Ao autenticar uma solicitação de usuário, o sistema deve realizar um comando de controle para realizar a transmissão da mensagem de emergência.			
Notas:	—		
Rastreabilidade:	—		

RFS21- Tipos de Emergências			
Status:	Proposto	Estabilidade:	Alta
Prioridade:	Alta	Versão:	0
O sistema deve emitir mensagens de emergência sobre desaparecimentos e desastres naturais.			
Notas:	—		
Rastreabilidade:	—		

RFS22- Convênio com Operadoras			
Status:	Proposto	Estabilidade:	Alta
Prioridade:	Alta	Versão:	0
O sistema deve estabelecer convênios com operadoras de telefone para permitir a transmissão de WEAs.			
Notas:			
Rastreabilidade:	—		

RFS23- Processamento de Dados de Emergência			
Status:	Proposto	Estabilidade:	Alta
Prioridade:	Alta	Versão:	0

O sistema deve ser capaz de receber e analisar os dados na nuvem, garantindo uma análise eficiente e em tempo real das informações fornecidas pelas entidades competentes.

Notas:	—
Rastreabilidade:	—

RFS24- Interface Intuitiva

Status:	Proposto	Estabilidade:	Alta
Prioridade:	Alta	Versão:	0

O sistema deve oferecer um formulário com uma interface intuitiva e de fácil utilização, garantindo a coleta eficiente de informações essenciais.

Notas:	—
Rastreabilidade:	—

5.2. Requisitos Não Funcionais

RNFS01- Interoperabilidade

Status:	Proposto	Estabilidade:	Alta
Prioridade:	Alta	Versão:	0

O sistema deve garantir interoperabilidade e capacidade de lidar com volumes significativos de alertas ao estabelecer convênios com operadoras de telefones para a transmissão de WEAs.

Notas:	
Rastreabilidade:	RFS22

RNFS02- Transmissão Instantânea

Status:	Proposto	Estabilidade:	Alta
Prioridade:	Alta	Versão:	0

O sistema deve assegurar a transmissão em tempo real de WEAs considerando uma latência máxima de 5s na entrega das mensagens.

Notas:	—
Rastreabilidade:	RFS20

RNFS03- Limitação de Caracteres			
Status:	Proposto	Estabilidade:	Alta
Prioridade:	Alta	Versão:	0
O sistema deve enviar mensagens de, no máximo, 130 caracteres.			
Notas:	—		
Rastreabilidade:	—		

RNFS04- Segurança de Comunicação			
Status:	Proposto	Estabilidade:	Alta
Prioridade:	Alta	Versão:	0
O sistema deve garantir que a comunicação entre as entidades, o sistema e as torres operadoras sejam criptografadas.			
Notas:	—		
Rastreabilidade:	RFS18		

6. Arquitetura

Para o sistema de alerta de emergência **RescueWave**, foi selecionada a arquitetura de *Microservices* devido à sua capacidade de fornecer uma solução altamente escalável e flexível. Com essa abordagem, o sistema é dividido em serviços independentes, cada um responsável por uma função específica. Isso permite uma maior modularidade e facilita a manutenção, além de garantir maior resiliência e tolerância a falhas, uma vez que cada serviço pode ser escalado separadamente e substituído sem impactar outros componentes.

Além disso, a arquitetura de microservices facilita uma evolução gradual do sistema, permitindo que novos recursos sejam adicionados com facilidade e que atualizações sejam implementadas de forma incremental. Isso é importante para um sistema de alerta de emergência, onde a capacidade de adaptação rápida a novos requisitos e situações críticas é relevante. A partir dos microservices, o **RescueWave** pode oferecer uma solução eficiente, garantindo a rápida disseminação de informações vitais durante emergências, contribuindo assim para a segurança e o bem-estar das comunidades afetadas.

Além disso, na engenharia de software, são definidos quatro tipos principais de visões: visão lógica, visão de desenvolvimento, visão de projeto e visão física. No contexto da implementação deste projeto, as considerações para cada um dos tipos de visão estão detalhadas a seguir.

6.1. Visão Lógica

6.1.1. Diagrama de Blocos

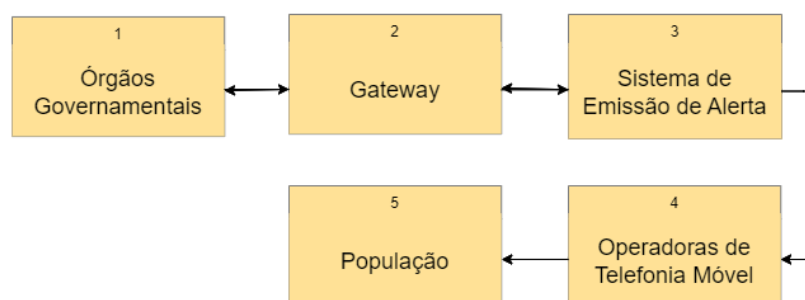


Figura 2. Diagrama de Blocos

O diagrama de blocos acima representa a visão lógica do sistema. Ele inicia com uma situação de emergência, na qual os órgãos governamentais responsáveis monitoram a ocorrência. Quando confirmada a situação de emergência, os órgãos governamentais enviam uma mensagem para um gateway no passo 2. Esse gateway, integrado ao software **RescueWave** no passo 3, recebe e encaminha a solicitação de alerta.

No passo 4, o software **RescueWave** analisa os dados recebidos e envia o alerta para as operadoras de telefonia. Por fim, as operadoras emitem o alerta para toda a população que se encontra na área afetada, utilizando tecnologia WEA (Wireless Emergency Alerts). Além disso, o software também armazena tanto os alertas emitidos quanto os não emitidos, para a criação de um histórico.

6.2. Visão de Desenvolvimento

6.2.1. Diagrama de Classes

O diagrama da Figura 3 representa as classes necessárias para o desenvolvimento da interface do **RescueWave**. A classe **Funcionario** é criada pela classe **Administrador**. Além disso, a classe **Funcionario** possui uma relação múltipla com o **Histórico Alerta**, o que significa que vários funcionários podem visualizar o estado de um histórico de alerta de acordo com o órgão.

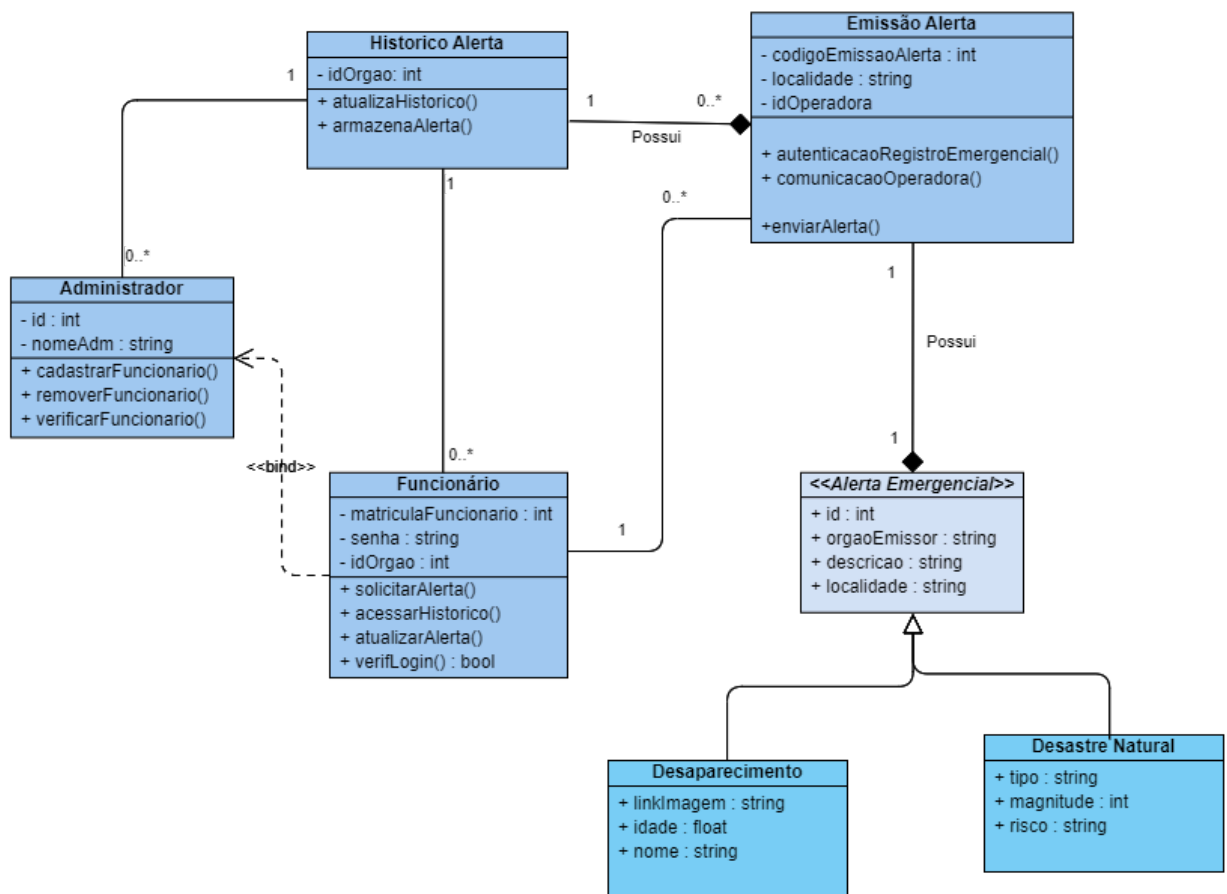


Figura 3. Diagrama de Classes

A classe Funcionario também possui uma relação se um para muitos com a classe Emissão Alerta, pois somente um funcionário pode emitir um alerta com um determinado ID. Embora um funcionário possa emitir vários alertas, o mesmo alerta não pode ser emitido por vários funcionários.

A classe Histórico Alerta possui uma relação de um para muitos com a classe Emissão Alerta, pois um histórico de alerta pode conter várias emissões de alertas. Esta relação é de composição, indicando que as emissões de alerta são partes integrantes do histórico de alerta.

Por sua vez, a classe Emissão Alerta tem um relacionamento de composição com a classe abstrata Alerta Emergencial, em um relacionamento de um para um. Isso significa que cada emissão de alerta está associada a um único tipo de alerta.

A classe abstrata Alerta Emergencial possui as seguintes subclasses: Desaparecimento e Desastre Natural, que representam os diferentes tipos de alertas emitidos.

6.3. Visão de Processo

6.3.1. Diagrama de Atividades

- Diagrama de Atividades para o Funcionário:

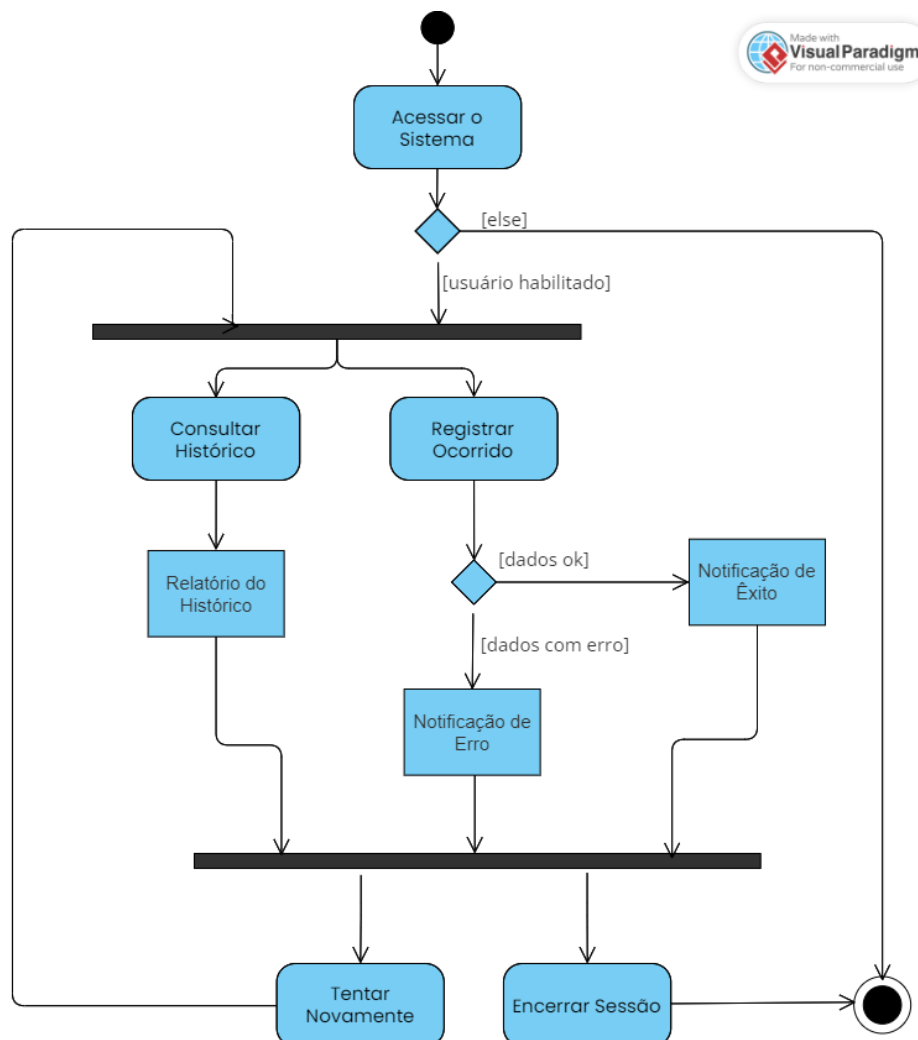


Figura 4. Diagrama de Atividades para o Funcionário

O diagrama de atividades do nosso projeto de sistema de alerta de emergência ilustra o processo de interação entre os funcionários (usuários) e o sistema do **RescueWave**. Ao acessar o sistema, o funcionário tem tanto a opção de registrar uma emergência, quanto a de consultar o histórico de emergências anteriores.

Após o registro, o sistema processa os dados e, se necessário, verifica o funcionamento das máquinas. Se um erro for detectado, ou caso a emergência seja registrada, o sistema notifica o usuário por meio de uma notificação de erro ou de êxito, respectivamente, fornecendo informações sobre a situação e possíveis ações a serem tomadas.

O diagrama de atividades mostra claramente as etapas do processo e os diferentes caminhos que o usuário pode seguir, dependendo de suas interações com o sistema. Isso ajuda a compreender a lógica do fluxo de trabalho e como as atividades estão relacionadas entre si.

- Diagrama de Atividades para o Administrador:

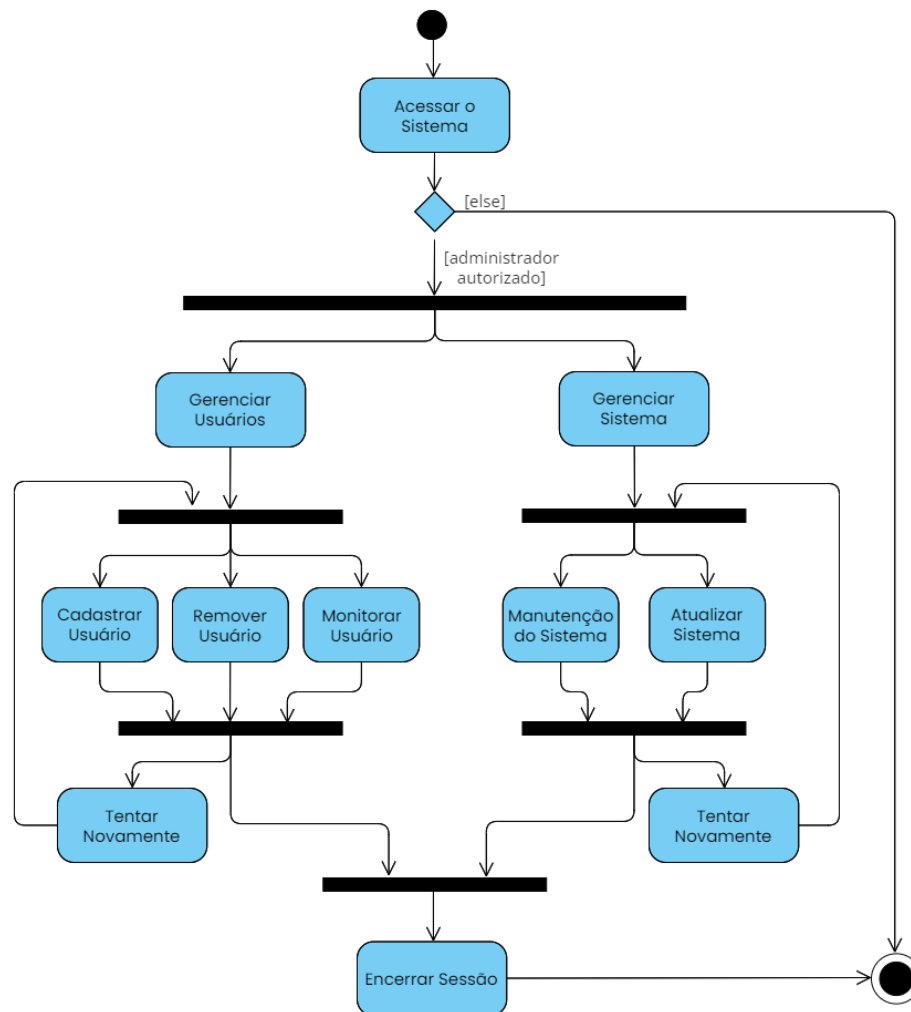


Figura 5. Diagrama de Atividades para o Administrador

O diagrama acima tem uma proposta similar ao anterior, porém voltada para as atividades do administrador, o qual, inicialmente, acessa o sistema, onde é verificada sua autorização. Caso seja autorizado, ele tem duas opções principais: gerenciar usuários ou realizar a manutenção do sistema.

Optando por gerenciar usuários, ele pode realizar várias ações, incluindo cadastrar novos usuários, remover usuários existentes e monitorar a atividade dos usuários ativos. Essas atividades buscam garantir a segurança e o bom funcionamento do sistema, permitindo ao administrador controlar quem tem acesso e como o sistema é utilizado.

Por outro lado, se o administrador optar pelo sistema, ele pode executar tarefas como atualizar o software, corrigir falhas ou realizar ajustes na configuração. Essas ações visam manter o sistema em pleno funcionamento para que ele atenda às necessidades dos usuários de forma eficaz. Após concluir suas atividades, o administrador pode tentar novamente ou encerrar a sessão, finalizando sua interação com o sistema.

6.3.2. Diagrama de Sequência

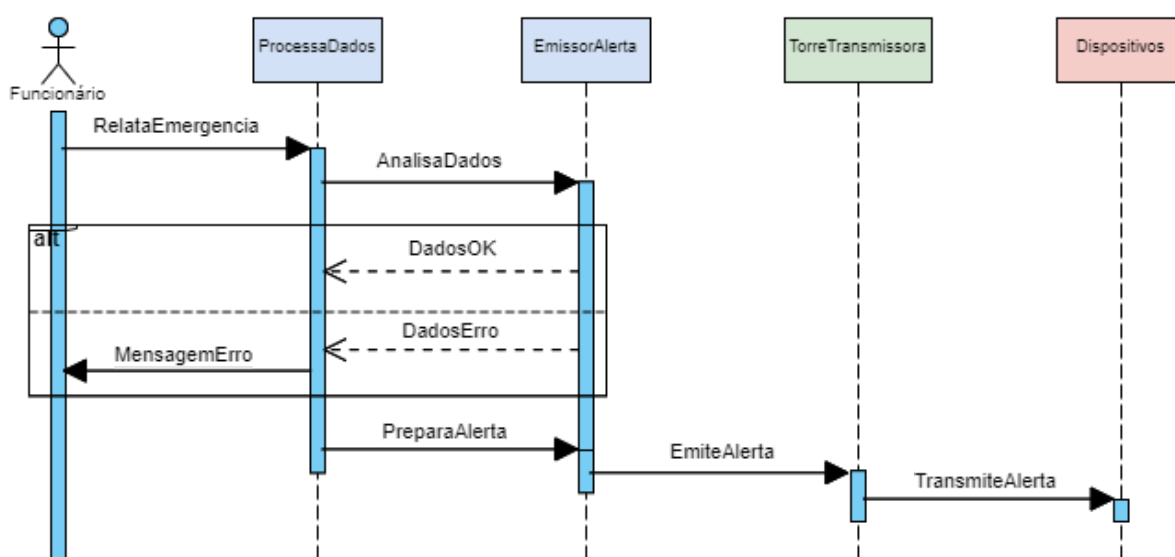


Figura 6. Diagrama de Sequência

O diagrama de sequência ilustra o caso de uso em que um funcionário (ator) solicita o envio de uma mensagem de emergência. Inicialmente, ele registra o incidente, permitindo que o sistema processe os dados para verificar sua autenticidade.

Caso o registro atenda aos critérios do sistema, a emissão do alerta é confirmada como válida pelo objeto responsável por processar os dados. Em seguida, a mensagem de emergência é preparada e enviada para as torres de telefonia, que realizam a transmissão do WEA para os dispositivos dos receptores.

Em caso de registro inadequado, o sistema retorna uma mensagem de erro ao usuário, informando sobre a inconsistência dos dados registrados.

6.3.3. Máquina de Estados

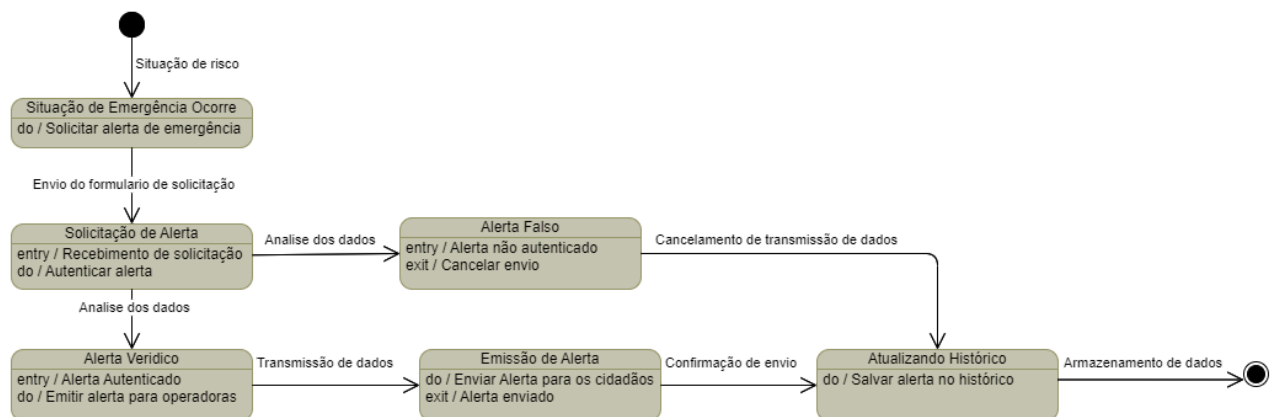


Figura 7. Máquina de Estados

O diagrama acima descreve o comportamento geral do sistema em um caso de uso em que ocorre uma situação de emergência. O processo é iniciado quando o sistema detecta uma situação de risco, que está sendo monitorada pelos órgãos competentes. Em seguida, é solicitado um alerta de emergência e o formulário para solicitação de alerta é enviado. Após o recebimento desta solicitação, o sistema autentica o alerta.

Se os dados do alerta estiverem conforme o formulário e forem verdadeiros, o alerta é autenticado. Nesse caso, ocorre a transmissão do alerta para os cidadãos. Após a confirmação do envio pelas operadoras, o alerta é salvo no histórico. No entanto, se o alerta for falso ou não estiver conforme o formulário, a transmissão desse alerta é cancelada. O alerta também é salvo no histórico, indicando que não foi autenticado.

6.3.4. Diagrama de Fluxo de Dados

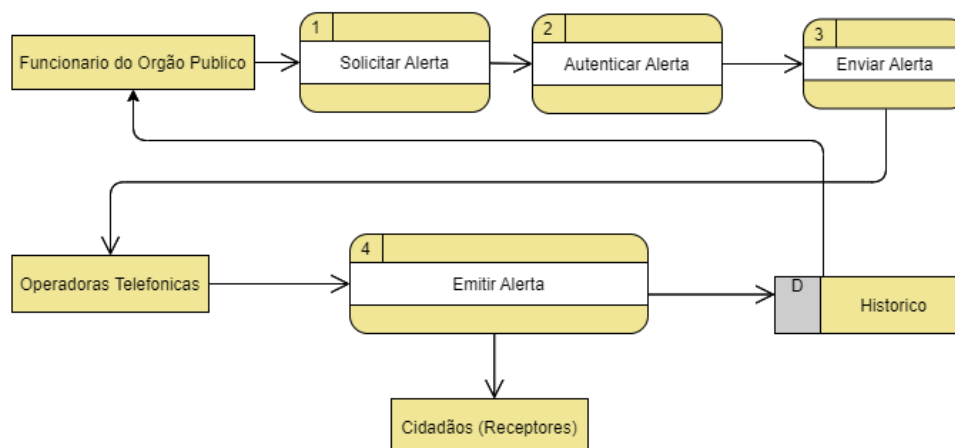


Figura 8. Diagrama de Fluxo de Dados

O diagrama de fluxo de dados ilustra a trajetória dos dados dentro do sistema, detalhando as entradas, processos e saídas. A principal entrada de dados é o alerta de emergência, enviado pelos órgãos competentes ao detectarem uma situação de risco. Assim que o sistema recebe o alerta de emergência, dá-se início ao processamento dos dados, que inclui a verificação da autenticidade do alerta e a validação dos dados.

Após o processamento, o sistema encaminha o alerta para as operadoras telefônicas, as quais emitem o alerta para a população afetada. Esse procedimento é realizado por meio de tecnologia wireless, como os Wireless Emergency Alerts (WEA), garantindo a entrega do alerta aos dispositivos móveis das pessoas na área afetada.

Além da transmissão do alerta, o sistema registra todos os alertas emitidos, incluindo aqueles que foram autenticados e transmitidos com sucesso, assim como os alertas que foram cancelados devido a serem falsos ou não estarem em conformidade com os requisitos. Esse histórico de dados pode ser usado para análises futuras, elaboração de relatórios e condução de investigações.

6.4. Visão Física

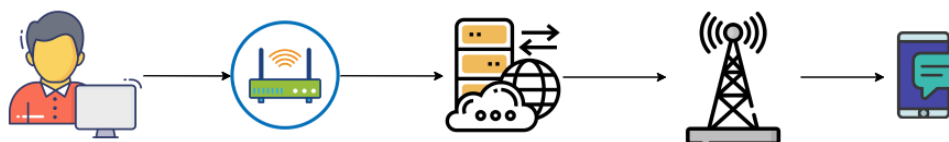


Figura 9. Visão Física do Sistema

A visão física engloba a interação dos usuários com os diversos componentes e camadas do sistema. O servidor de órgão de autoridade inicialmente interage com a interface por meio de um computador, acessando o sistema para registrar emergências e consultar status de alertas..

Os dados registrados pelo usuário no computador são então enviados para o servidor, sendo essa comunicação representada pelo gateway entre a aplicação e o sistema de software, permitindo uma troca de informações eficiente e segura. No servidor, os dados são processados e analisados para identificar emergências, gerar alertas relevantes e armazenar informações.

Após o processamento, os alertas são transmitidos para os dispositivos finais por meio de uma torre de telefone. Essa torre atua como um ponto de acesso à rede celular, permitindo que os alertas sejam entregues aos dispositivos móveis dos usuários, como celulares e smartphones.