



Nome do Projeto: SAFE	Data da Solicitação: 26/10/2020
Responsável: Guilherme Horta Travassos, Patrícia Furtado, Luciana Nascimento, Nicoll Rios	
Solicitante: CAPES TecnoDigital	Clientes:

Versões e Revisões deste documento			
Data	Comentário	Autor	Versão
22/06/2021	Criação do documento	Nicoll Rios	1.0
30/08/2021	Atualização do documento	Nicoll, Cainã e Guilherme	
09/10/2021	Glossário atualizado	Time	
11/10/2021	Glossário atualizado	Kevin	
07/12/2025	Revisão Geral e Relacionamento de Visões	Guilherme	2.0
08/12/2025	Revisão e correção de defeitos	Sabrina, Larissa	

Projeto Sistema SAFE UFRJ



1 Visão

Este documento apresenta uma visão geral do Sistema SAFE. Inicialmente, descreve-se o escopo do projeto, bem como o objetivo e os itens excluídos, a fim de deixar claro o propósito do sistema de software proposto. Além disso, este documento descreve o time de desenvolvimento e seus respectivos papéis no sistema de software. Os requisitos (funcionais e não funcionais) também estão especificados na Seção 2.

1.1 Escopo do Projeto

Em meio à pandemia da COVID-19, a UFRJ ficou impossibilitada de manter suas atividades presenciais em todas as dependências, o que trouxe problemas tanto para os estudantes da universidade quanto para os docentes e terceirizados que nela atuavam.

Como parte do plano de tomada de atividades presenciais na UFRJ, este projeto tem o propósito de apoiar o monitoramento das condições de uso das instalações da UFRJ, considerando os níveis de risco e as condições do ambiente (temperatura, nível de CO₂ e número de pessoas por instalação), conforme definido no Guia de Biossegurança da UFRJ.

Nesse contexto, o projeto COVID SAFE Classrooms tem como objetivos:

- Aplicar regras do Guia de Biossegurança às instalações físicas da UFRJ para ocupação segura contra a COVID-19;
- Garantir monitoramento dos riscos atribuídos às condições de utilização e ocupação das instalações;
- Garantir atuação técnica e gerencial preventiva e de mitigação dos riscos associados às condições monitoradas.

1.2 Escopo Não Incluído no Projeto

Esse sistema apenas fornece as informações sobre os indicadores previstos no Guia de biossegurança para as instalações da UFRJ. Sendo assim, não oferece qualquer funcionalidade para evitar ou reduzir o fluxo de pessoas em cada instalação.

1.3 Envolvidos no Projeto

1.3.1 Equipe Atual

Nome	Papel
Guilherme Horta Travassos	Gerente de Projeto/Engenheiro de Software
André Giron	Desenvolvedor
Kaway Henrique da Rocha Marinho	Desenvolvedor
Leonardo Peres Albertazzi Drumond	Desenvolvedor
Patrícia Furtado	Enfermeira Especialista
Larissa Galeno	Engenheira de Software
Sabrina Rocha	Engenharia de Requisitos
Rodrigo Feitosa	Engenheiro de Software

1.3.2 Histórico da Equipe

Nome	Papel	Período
Alex Teixeira	Integração de sensores	
Bruno Pedraça de Souza	Engenheiro de Software	
Carlos Eduardo Alves	Gerente	2021
Charles Gonçalves	Desenvolvedor Front-End	
Clinton Hudson	Engenheiro de Software	
Gabriel Bastos	Desenvolvedor Back-End	
Gabriel Bulhões	DevOps	
Gabriel Gazola	Integração de sensores	
Gabriel Xará	Front-end	



Juliano Marinho	Desenvolvedor do Servidor/Analista de Testes	
Kevin Vilar	DevOps	
Lucas Santiago	Integração de sensores	
Luciana Nascimento	Engenheira de Software	
Luís Fernando	Front-end	
Luís Pessoa	Front-end	
Nicolli Rios	Engenheira de Software	
Nuno Correia	Desenvolvedor Back-End	
Raul Baptista	Front-end/Analista de Testes	
Victor Rafael	Integração de sensores	
William Lucas	Desenvolvedor Front-End, UX Designer	

1.4 Glossário

Termo	Descrição
AHT21	Sensor de Temperatura e Umidade
AP	Quantidade de pessoas numa instalação específica
Arquitetura dual-core	Arquitetura com dois cores de processamento oferecida pelo ESP32
BioT	Dispositivo IoT composto por sensor de temperatura, sensor de movimento, sensor de CO ₂ . Suas propriedades são: Id, versão do software, porta e data de instalação.
BloT	O BloT é um dispositivo IoT voltado à coleta de dados ambientais internos para biossegurança, integrando sensores de qualidade do ar e de contagem de pessoas para monitorar CO ₂ , temperatura, umidade e ocupação dos ambientes.
Bloco	Espaço físico pertencente a uma ou mais unidades que possui um conjunto de instalações. Pode ter um ou mais andares.
Broker	Agente intermediário que utiliza o protocolo MQTT responsável pela comunicação entre os dados capturados pelo dispositivo IoT e o sistema. Utilizado o Rabbitmq
C++	Linguagem de programação
CJMCU-811	Sensor de CO ₂
CO ₂	Dióxido de carbono. Unidade de medida: ppm.
CT	Centro de Tecnologia
CT-2	Centro de Gestão Tecnológica
DHT11	Sensor de Temperatura e Umidade
Docker	Tecnologia para encapsulamento de aplicações
ENS160	Sensor de CO ₂
ESP32	Processador do BloT
Estados de solicitações de limpeza ou manutenção	“Em andamento”, “Aguardando atendimento”, “Atendida”
Estados de utilização das instalações no SAFE Dashboard	“Aguardando limpeza”, “Aguardando manutenção”, “Aguardando limpeza e manutenção”, “Em uso”, “Disponível para uso”
Estados de utilização das instalações no SAFE Manager	“Liberado”, “Não liberado”
FreeRTOS	Sistema operacional multi-core utilizado no BloT
HC-SR04	Sensor de presença ultrassônico
Instalação	Qualquer ambiente utilizado na UFRJ para o desenvolvimento de atividades presenciais deve possuir as seguintes informações: localização,



	unidade, nível de risco, estado de utilização, dispositivo BloT associado e tipo de instalação.
INTERVALO_ATUALIZACAO_DADOS_BROKER	Corresponde ao intervalo entre acessos sucessivos ao broker, a fim de coletar novos dados transmitidos pelos dispositivos IoT. Seu valor é de 15 segundos.
INTERVALO_ATUALIZAÇÃO_DADOS_CO2	Corresponde ao intervalo de coleta das medidas de CO ₂ e de VOCS. O sensor CJCMU 811 tem restrição temporal. Este intervalo é de 5 segundos.
INTERVALO_ATUALIZACAO_DADOS_TEMPERATURA	Corresponde ao intervalo de coleta das medidas de temperatura e de umidade. O sensor DTH11 tem restrições temporais. Este intervalo deve ser de 7,5 segundos
INTERVALO_ATUALIZACAO_ESTADO	Refere-se ao intervalo de tempo entre as verificações dos estados das instalações. Esse intervalo está definido em 10 minutos.
INTERVALO_ATUALIZACAO_LIMITES	Refere-se ao intervalo de tempo entre os envios dos limites de biossegurança para um dispositivo BloT em uma determinada instalação. Esse intervalo está configurado para 30 minutos.
INTERVALO_ATUALIZACAO_NOTIFICACOES	Corresponde ao intervalo entre as buscas por novas notificações e a manutenção da conexão Wi-Fi do sistema. Seu valor é de 10 segundos.
INTERVALO_ATUALIZAÇÃO_NUMERO_PESSOAS	Corresponde ao intervalo de coleta dos eventos de entrada e de saída de pessoas na instalação. Os sensores HC SR04 devem estar posicionados adequadamente. Este intervalo deve ser de 1 segundo
INTERVALO_ATUALIZAR_DADOS	Corresponde ao intervalo entre acessos sucessivos ao SAFE Manager, para coletar novos dados disponíveis. Seu valor é de 15 segundos.
Localização	Uma localização segue uma estrutura hierárquica que descreve um espaço físico. O nível mais alto da hierarquia é definido pelo centro, seguido pelo bloco e pelo andar. Seu propósito é permitir a identificação do local físico onde uma instalação se encontra.
MQTT	<i>Message Queuing Telemetry Transport (MQTT)</i> é um protocolo leve de mensagens para sensores e pequenos dispositivos móveis, otimizado para redes TCP/IP.
MQTT_TOPICO	Indica o tópico principal a ser usado para organizar os dados dos dispositivos. Neste caso o valor default é "SAFE"
Classificação de Risco	Risco de contaminação por Covid-19, considerando a temperatura, o nível de CO ₂ e o número de pessoas em uma determinada instalação, conforme descrito no Guia de Biossegurança.
Parâmetros de funcionamento	Corresponde aos parâmetros: frequência de leitura dos BloT, período de captura de eventos do sistema, frequência de leitura dos limites de biossegurança das instalações cadastradas.
PERIODO_OBSERVACAO_HISTÓRICO_DADOS	Corresponde ao período em que os dados históricos do sistema serão exibidos. Como padrão, o histórico de dados deve corresponder às últimas QUATRO horas de coleta.
Protocolo MQTT	Protocolo de comunicação utilizado pelo BloT
Temperatura (TEMP)	Temperatura do ambiente fornecida pelo sensor em graus Celsius (°C).
TEMPO_MAXIMO_ANTES_ALERTA_DASHBOARD	Refere-se ao tempo máximo permitido para que o Dashboard receba novos dados. Caso o Dashboard não receba novas informações em 5 minutos, um alerta será exibido.
TEMPO_MAXIMO_INATIVIDADE	Seu valor é de 1 hora.
Tipo de instalação	Podem assumir os seguintes valores: sala de aula, laboratório, sala de reunião, auditório, sala administrativa, refeitório, sala de convivência e biblioteca.
PPM	"partes por milhão" (Parts Per Million) é uma unidade de medida que indica a concentração de dióxido de carbono no ar.
PPB	"partes por bilhão" (parts per billion) é uma unidade de concentração usada para medir quantidades muito baixas de um gás no ar ou em uma solução.



Unidade	Representa a unidade que administra a instalação (por exemplo: COPPE)
VOCs	Refere-se à quantidade de compostos orgânicos voláteis (VOCs) fornecida pelo sensor em pbm. VOCs são substâncias que contêm carbono em sua composição e apresentam ponto de ebulição entre 50 °C e 260 °C. São considerados poluentes perigosos e alguns deles possuem propriedades tóxicas e potencial carcinogênico.

1.5 Definição de papéis

Administrador do Sistema	É o superusuário do sistema. Possui privilégios para realizar as ações de operação inicial do sistema e garantir seu funcionamento, tais como gerenciar as instalações, os gestores das instalações, acompanhar notificações do sistema, como problemas identificados que impedem o correto funcionamento, e gerenciar os dispositivos disponíveis nas instalações.
Gestor das Instalações	Possui privilégios para acompanhar notificações do sistema, gerenciar usuários (Equipe de Manutenção, Equipe de Limpeza, Staff). Além disso, podem gerenciar instalações, limites de biossegurança e solicitações de uso das instalações, incluindo serviços de limpeza e manutenção.
Equipe de Manutenção	Envolve os funcionários de manutenção. Eles têm privilégios que lhes permitem receber e atender solicitações de manutenção de instalações. Representada pelo Gerente da Manutenção
Equipe de Limpeza	Envolve os funcionários de limpeza. Eles têm privilégios que lhes permitem receber e atender solicitações de limpeza das instalações. Representada pelo gerente da limpeza.
Staff	Envolve professores e demais funcionários autenticados no sistema. Estes têm permissão para solicitar o uso de instalações, bem como serviços de limpeza e manutenção.
Usuário não-cadastrado	Envolve todos os demais usuários potenciais do sistema, como alunos e visitantes. A eles é permitido apenas o acesso à interface do Dashboard.

1.6 Regras de Negócio

As regras de negócio, quando pertinentes, são apresentadas em conjunto com seus respectivos requisitos. O Guia de ações de biossegurança para a resposta à pandemia de COVID-19 no âmbito da UFRJ apresenta os princípios motivacionais e comportamentais abordados no projeto.

2 SUBSISTEMAS ASSOCIADOS

Em relação às funcionalidades do sistema disponibilizadas, o Sistema SAFE está representado na Figura 1 abaixo, sendo formado pelos seguintes subsistemas principais:

1. **SAFE BloT - dispositivo IoT** para a coleta e o envio de dados das instalações.
2. **Broker de Mensagem** – subsistema responsável pela comunicação entre os SAE BloT e o SAFE Manager. Este sistema utiliza o protocolo MQTT.
3. **SAFE Dashboard – painel de monitoramento** responsável pela exibição dos dados coletados pelo SAFE Manager das instalações. O subsistema do dashboard tem comunicação direta com o subsistema do SAFE Manager.

4. *SAFE Manager* - subsistema responsável pela configuração e gerenciamento de usuários e dispositivos SAFE BioT em uma determinada instalação (sala, laboratório, auditório, secretaria, entre outras).

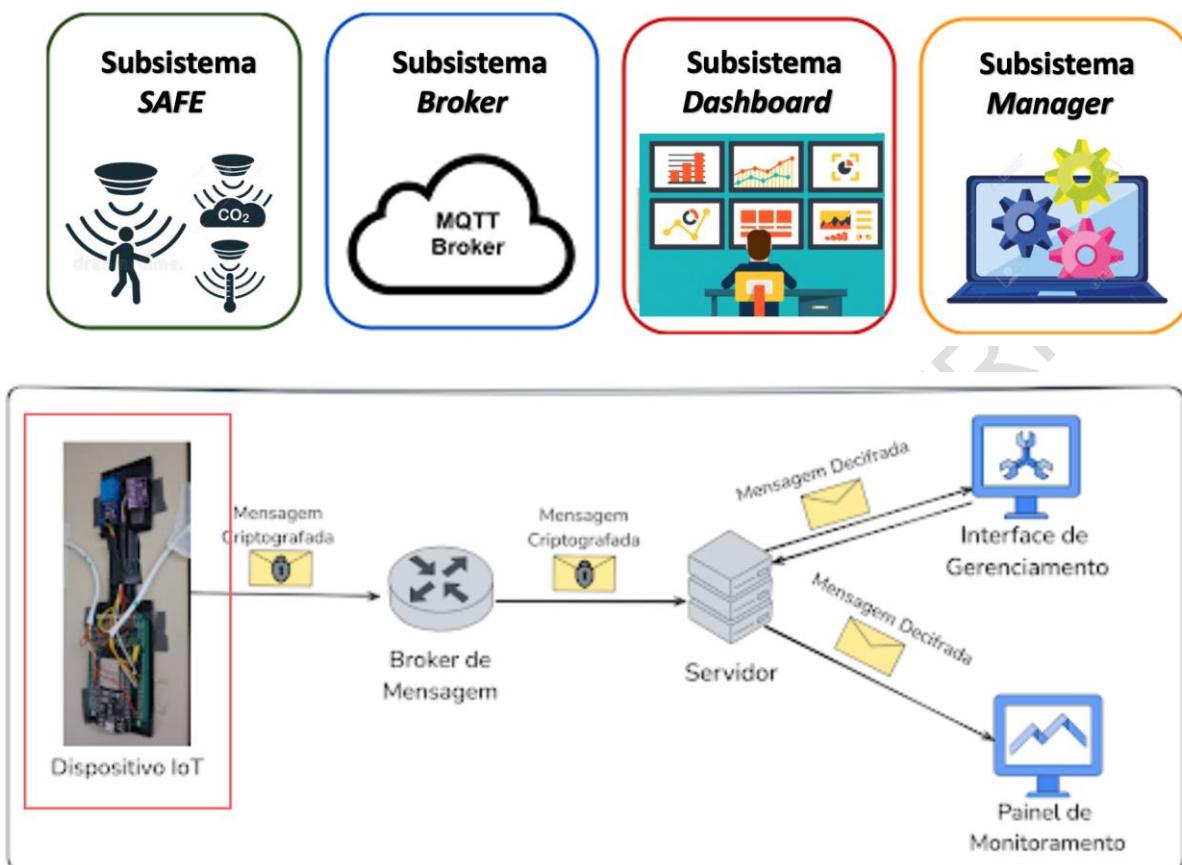


Figura 1. Visão geral do Sistema SAFE

3 SUBSISTEMA MANAGER

O Manager é o componente sistêmico central do SAFE, responsável por orquestrar as ações de monitoramento das instalações. Por meio do Manager, é possível realizar operações de cadastramento e de gestão de instalações e dispositivos BioT. Toda a comunicação com os BioTs é feita pelo Manager, que utiliza o broker MQTT para interagir. O Manager mantém um repositório de dados que garante a preservação do registro de eventos e a correta interação com o SAFE Dashboard.

4 SUBSISTEMA SAFE BIOT

O BioT é um dispositivo IoT projetado para coletar dados ambientais em instalações internas, com foco em parâmetros de biossegurança, conforme mostrado na Figura 1. Ele é composto por dois módulos principais de sensoriamento: o módulo de qualidade do ar, que utiliza sensores CJMCU-811 (ou ENS160) e DHT11 (ou AHT21) para medir níveis de CO₂, temperatura e umidade; e o módulo de contagem de pessoas, baseado em sensores ultrassônicos HC-SR04, que permite monitorar a entrada e a saída de pessoas nos ambientes.



Para lidar com a periodicidade de funcionamento distinta entre os módulos, o dispositivo utiliza um microcontrolador ESP32 com suporte ao FreeRTOS, devido à sua arquitetura dual-core, que permite que cada núcleo fique responsável por um dos módulos.

As rotinas do dispositivo foram desenvolvidas em C++, incluindo um componente próprio de criptografia responsável por proteger os dados antes de sua transmissão. Os dados coletados são enviados pela rede Wi-Fi, por meio do protocolo MQTT, para um broker de mensagens, garantindo a comunicação com os demais subsistemas da arquitetura.

5 SUBSISTEMA SAFE DASHBOARD

O Dashboard é o **Painel de Monitoramento** do sistema SAFE, visando viabilizar o acompanhamento contínuo dos indicadores de biossegurança dos ambientes monitorados pelo sistema, conforme mostra a Figura 1. Esse painel foi desenvolvido com tecnologias front-end, como React, e oferece uma interface visual para a visualização contínua dos dados, a emissão de alertas em situações críticas e apoio à mitigação de riscos nos espaços.

Além disso, o Dashboard serve também como **Interface de Gerenciamento**, que permite aos usuários solicitarem remotamente serviços de limpeza ou manutenção, além de informar o estado atual do ambiente, especificando se ele está bloqueado ou liberado para uso. Com base nessas informações, o SAFE IoT gerencia e comunica dois estados possíveis para cada instalação: disponível e indisponível. Quando o ambiente estiver disponível, o sistema notifica os usuários interessados sobre sua liberação. Quando está indisponível, além da notificação, o sistema informa o motivo, que pode estar relacionado à necessidade de limpeza, à manutenção em andamento ou ao bloqueio operacional.

6 CONSIDERAÇÕES

Escopo Não Incluído no Projeto

Esse sistema apenas fornece as informações sobre os indicadores previstos no Guia de Biossegurança para as instalações da UFRJ. Sendo assim, não oferece qualquer funcionalidade para evitar ou reduzir o fluxo de pessoas em cada instalação.

Impactos:

- Monitoramento contínuo de biossegurança em ambientes fechados: mesmo após a pandemia, o monitoramento de temperatura, umidade, CO₂ e número de pessoas permanece necessário para garantir condições saudáveis e confortáveis em ambientes com circulação de pessoas, como salas de aula, laboratórios e ambientes hospitalares.
- Automatização de processos operacionais: o sistema permite não só a solicitação de serviços (como limpeza ou manutenção), mas também o bloqueio ou liberação de ambientes com base em critérios objetivos de biossegurança, reduzindo decisões manuais e aumentando a eficiência.

Expectativas:

- Fornecer dados de monitoramento em tempo real do ambiente: espera-se que o painel exiba, de forma clara, as informações de temperatura, umidade, nível de CO₂ e número de pessoas no ambiente.
- Emitir um alerta inteligente para condições críticas: o sistema deve notificar automaticamente quando os níveis definidos pelo usuário ultrapassarem o limite seguro.

Público alvo:

- Profissionais da área de saúde, segurança do trabalho e biossegurança;
- Equipes de manutenção, limpeza;



- Usuários dos espaços monitorados (colaboradores, estudantes, pacientes, visitantes).

7 REQUISITOS GERAIS DO SISTEMA

Os requisitos representam as necessidades que o sistema deve atender para alcançar seus objetivos. Eles são classificados em:

- Requisitos Funcionais (**RF**): especificam o que o sistema deve fazer, ou seja, suas funcionalidades e comportamentos esperados.
- Requisitos Não Funcionais (**RNF**): definem como o sistema deve se comportar, abordando atributos como desempenho, segurança, usabilidade e confiabilidade.
 - Requisitos de Comunicação de Dados, Interface e Interoperabilidade (**COM**): descrevem como será a comunicação de dados no software, com outros softwares e até com hardware. É importante definir as interfaces de comunicação que o aplicativo deve suportar. Todas as interfaces de hardware que devem ser suportadas pelo software, incluindo a estrutura lógica, os endereços físicos, o comportamento esperado, dentre outros, devem ser identificadas, bem como as interfaces de software com outros componentes do software.
 - Requisitos de Confiabilidade (**CONF**): envolvem tolerância a falhas, previsibilidade, recuperação e precisão das informações.
 - Requisitos de Desempenho e Robustez (**DR**): especificam a velocidade de processamento e de recuperação de informações, o tempo de resposta, a taxa de utilização dos recursos computacionais, entre outros.
 - Requisitos de Disponibilidade (**DISP**): envolvem o tempo de ociosidade e a disponibilidade do software.
 - Requisitos de Manutenibilidade (**MAN**): aprimoram a manutenibilidade do software, incluindo padrões de codificação, convenções de nomeação, bibliotecas de classes, acesso à manutenção e utilitários de manutenção. Esses requisitos estão relacionados com a habilidade do software em ser modificado de forma rápida e com baixo custo, geralmente esses requisitos não são impostos ao software, mas ao seu processo de desenvolvimento.
 - Requisitos de Portabilidade (**PORT**): relacionados com a habilidade do software em rodar em diferentes configurações de ambiente, como de hardware, software, browsers, etc.
 - Requisitos de Usabilidade (**US**): incluem requisitos baseados em fatores humanos e em questões de interface de usuário, tais como acessibilidade, estética e consistência da interface.
 - Restrições de Projeto e Tecnológicas (**PROT**): indicam restrições de projeto e de utilização de tecnologias que foram impostas e devem ser respeitadas.
 - Requisitos de Escalabilidade (**RNFE**): definem a capacidade do sistema de crescer ou se adaptar ao aumento no número de dispositivos conectados, de dados gerados, de usuários simultâneos e de instalações monitoradas, sem comprometer o desempenho, a disponibilidade ou a confiabilidade do sistema.

Manager

Requisitos Funcionais

RF01	O Manager deve permitir que os administradores gerenciem os gestores das instalações.
------	---



RF02	O Manager deve permitir que administradores gerenciem dispositivos BloT, caracterizados pelas seguintes informações: id, versão do software, porta, data de instalação.
RF03	O Manager deve permitir que administradores e gestores das instalações gerenciem as instalações, caracterizadas pelas seguintes informações: localização do espaço e de suas sublocalizações (salas, laboratórios, auditório). Regra de negócio: Um gestor de instalação só pode gerenciar instalações incluídas na sua hierarquia de localização.
RF04	O Manager deve permitir que gestores, staff, equipe de manutenção, equipe de limpeza informem que uma instalação cadastrada necessita de manutenção.
RF05	O Manager deve notificar por e-mail a equipe de manutenção quando alguma manutenção para uma instalação for cadastrada.
RF06	O Manager deve permitir que a equipe de manutenção informe o aceite de uma solicitação de serviço de manutenção para uma instalação cadastrada.
RF07	O Manager deve permitir que o gerente da instalação informe que uma solicitação de serviço de manutenção foi concluída.
RF08	O Manager deve permitir que gestores das instalações, staff, equipe de manutenção, equipe de limpeza informem que uma instalação cadastrada necessita de serviço de limpeza.
RF09	O Manager deve notificar a equipe de limpeza quando algum serviço de limpeza for solicitado para uma instalação cadastrada.
RF10	O Manager deve permitir que a equipe de limpeza informe o aceite de uma solicitação de serviço de limpeza para uma instalação cadastrada.
RF11	O Manager deve permitir que o gerente de instalação informe que uma solicitação de serviço de limpeza foi concluída.
RF12	O Manager deve permitir que o Staff solicite o uso de uma instalação cadastrada em determinada data e horário.
RF13	O Manager deve armazenar em banco de dados todos os dados recebidos dos dispositivos BloT, incluindo número de pessoas na instalação, temperatura, CO ₂ , umidade, VOCs, data, hora, identificador da instalação e do dispositivo.
RF14	O Manager deve guardar o histórico de eventos (nome do solicitante, data/hora da solicitação, nome do funcionário que atendeu à solicitação, data/hora do atendimento, data/hora da conclusão e a instalação para a qual o pedido foi realizado).
RF15	O Manager deve exibir o estado de utilização de cada instalação monitorada, atualizando-o conforme os eventos percebidos pelo sistema. Sendo estes: <ul style="list-style-type: none">● “Não Liberada”; e um dos motivos:<ul style="list-style-type: none">○ Aguardando limpeza;○ Aguardando manutenção;○ Aguardando limpeza e manutenção;○ Em uso;● “Liberado”: disponível para uso.
RF16	O Manager deve notificar os gestores das instalações em caso de uso não autorizado de instalações cadastradas (por exemplo, alguém acessa uma sala com alto risco de contaminação sem autorização).



RF17	O Manager deve permitir o login no SAFE com os dados de e-mail e de senha do usuário.
RF18	O Manager deve permitir que o usuário modifique a senha após o primeiro acesso. As senhas devem seguir os critérios: <ul style="list-style-type: none">● Maior que 6 caracteres;● Possuir números;● Possuir letras maiúsculas e minúsculas;● Possuir caracteres especiais;

Requisitos não funcionais

RNF01	O Manager deve se comunicar com o broker pelo protocolo MQTT.
RNF02	O Manager deve enviar os limites de biossegurança das instalações cadastradas aos dispositivos BloT por meio do broker e ao subsistema Dashboard, por meio da API.
RNF03	O Manager deve obter os dados enviados pelos dispositivos BloT por meio do broker.
RNF04	O Manager deve enviar o estado de uma instalação ao subsistema Dashboard a cada mudança de estado, por meio do Broker.
RNF05	O Manager deve exibir, na tela, aos administradores e gestores das instalações o alerta “FALTA DE DADOS DA INSTALAÇÃO <ID>” quando detectar a falta de dados de um dispositivo IoT associado a uma instalação cadastrada.
RNF06	O Manager deve exibir aos administradores do sistema e gestores das instalações o alerta “DADOS DO DISPOSITIVO <ID> EM FORMATO ERRADO” na tela em caso de recebimento de dados (do Broker) em um formato inválido.
RNF07	O Manager deve buscar novos dados transmitidos pelos dispositivos BloT no broker a cada INTERVALO_ATUALIZAR_DADOS (ver glossário).
RNF08	O Manager deve buscar novas notificações no broker a cada INTERVALO_ATUALIZACAO_NOTIFICACOES (ver glossário).
RNF09	O Manager deve garantir disponibilidade mínima de 99,9% ao mês, exceto durante as janelas de manutenção previamente comunicadas.
RNF10	O Manager deve permitir atualizações de versão por meio de Docker.
RNF11	O Manager deve oferecer aos Administradores do Sistema um meio direto de acesso ao servidor do Manager em caso de falha sistêmica.
RNF12	O Manager deve realizar atualizações mensais dos componentes de software (dependências, bibliotecas).
RNF13	O Manager deve garantir compatibilidade com, no mínimo, as versões: Chrome 118, Firefox 115, Edge 118 e Safari 16.
RNF14	O Manager deve realizar o controle de acesso baseado em papéis (administrador do sistema e gestor da instalação), garantindo que apenas o pessoal autorizado acesse elementos da rede, informações armazenadas, serviços e aplicações.



RNF15	O Manager deve encerrar automaticamente a sessão do usuário após atingir o tempo máximo de inatividade configurado (TEMPO_MAXIMO_INATIVIDADE), contado a partir da última ação do usuário.																								
RNF16	O Manager deve utilizar o CryptoComponent, com o protocolo Speck, para o tratamento dos dados recebidos dos dispositivos BloT.																								
RNF17	O Manager deve utilizar algoritmos de criptografia, com o CryptoComponent, usando o protocolo Speck, para o tratamento dos dados enviados aos dispositivos BloT.																								
RNF18	O Manager deve oferecer uma interface responsiva ao usuário considerando os seguintes critérios: <table border="1"><thead><tr><th>Classe Size</th><th>Pontos de interrupção</th><th>Tamanho da tela típico (diagonal)</th><th>Dispositivos</th><th>Tamanhos de janela</th></tr></thead><tbody><tr><td>Pequeno</td><td>640px ou menos</td><td>4" a 6"; 20" a 65"</td><td>Telefones e TVs</td><td>320x569, 360x640, 480x854</td></tr><tr><td>Médio</td><td>641px a 1007px</td><td>7" a 12"</td><td>Phablets, tablets</td><td>960 x 540</td></tr><tr><td>Grande</td><td>1008px ou mais</td><td>13" e maior</td><td>Computadores, laptops, Surface Hubs</td><td>1.024 x 640, 1.366 x 768, 1.920 x 1.080</td></tr></tbody></table>					Classe Size	Pontos de interrupção	Tamanho da tela típico (diagonal)	Dispositivos	Tamanhos de janela	Pequeno	640px ou menos	4" a 6"; 20" a 65"	Telefones e TVs	320x569, 360x640, 480x854	Médio	641px a 1007px	7" a 12"	Phablets, tablets	960 x 540	Grande	1008px ou mais	13" e maior	Computadores, laptops, Surface Hubs	1.024 x 640, 1.366 x 768, 1.920 x 1.080
Classe Size	Pontos de interrupção	Tamanho da tela típico (diagonal)	Dispositivos	Tamanhos de janela																					
Pequeno	640px ou menos	4" a 6"; 20" a 65"	Telefones e TVs	320x569, 360x640, 480x854																					
Médio	641px a 1007px	7" a 12"	Phablets, tablets	960 x 540																					
Grande	1008px ou mais	13" e maior	Computadores, laptops, Surface Hubs	1.024 x 640, 1.366 x 768, 1.920 x 1.080																					
RNF19	O Manager deve consumir o que o BloT publicou via broker nos tópicos (escritos em JSON) "SAFE_IAQ" e "SAFE_ENTRY_FLOW".																								

BloT

Requisitos Funcionais

RF01	O dispositivo BloT deve, no momento de sua inicialização, obter do broker, por meio do tópico MQTT definido para os parâmetros de biossegurança, os limites de temperatura (em °C), de CO ₂ e de ocupação da instalação, publicados pelo SAFE Manager.
RF02	O dispositivo BloT deve contabilizar cada movimento de entrada e saída de pessoas na instalação por meio dos sensores HC-SR04.
RF03	O dispositivo BloT deve coletar a temperatura (em °C) da instalação utilizando o sensor DHT11 ou AHT21.
RF04	O dispositivo BloT deve coletar a medida da concentração de eCO ₂ (CO ₂ equivalente, em ppm) da instalação, usando o sensor CJMCU-811 ou o ENS160.
RF05	O dispositivo BloT deve apresentar o estado da instalação em relação aos parâmetros monitorados (temperatura, CO ₂ , número de pessoas presentes) e emitir um sinal de risco em um painel sinalizador localizado na instalação.
RF06	O dispositivo BloT deve coletar a medida de umidade da instalação utilizando o sensor DHT11 ou AHT21.
RF07	O dispositivo BloT deve coletar a medida de VOCs (Compostos orgânicos voláteis) (ppm) da instalação.



Requisitos não funcionais

RNF1	O dispositivo BloT deve se comunicar com o broker por meio do protocolo MQTT.
RNF2	<p>O dispositivo BloT deve enviar as informações dos sensores para o broker utilizando o formato JSON através dos respectivos tópicos:</p> <pre>SAFE_IAQ: { "idBloT": <MAC number>, "timestamp": <dd/mm/yyyy HH:mm: ss>, "temperatura": <valor>, "umidade": <valor>, "co2": <valor>, "vocs": <valor>, "erro": <valor> }</pre> <p>Onde o campo "temperatura" deverá estar em °C, "umidade" em percentual, "CO₂" em ppm e "VOCs" em ppb; o "erro" corresponde a uma lista com as flags de erro.</p> <pre>SAFE_ENTRY_FLOW: { "idBloT": <MAC number>, "timestamp": <dd/mm/yyyy HH:mm: ss>, "entry_flow": <valor>, "erro": <valor> }</pre> <p>Onde o campo "entry_flow" corresponde a uma entrada ou saída de indivíduo, e o campo "erro" corresponde a uma lista de flags de erro.</p>
RNF3	O dispositivo BloT deve obter os valores atualizados dos parâmetros de biossegurança da instalação a cada INTERVALO_ATUALIZACAO_LIMITES.
RNF4	<p>O dispositivo BloT deve consultar as informações dos parâmetros no broker com o tópico MQTT_TOPICO no formato JSON com a seguinte estrutura:</p> <pre>{ "idBloT": <MAC number>, "temperaturaMin": <valor>, "temperaturaMax": <valor>, "umidadeMin": <valor>, "umidadeMax": <valor>, "numeroPessoasMin": <valor>, "numeroPessoasMax": <valor>, }</pre> <p>Os campos "temperaturaMin" e "temperaturaMax" deverão estar em °C; "numeroPessoasMin" e "numeroPessoasMax" deverão ser números inteiros; "umidadeMin" e "umidadeMax" deverão estar em percentual.</p>
RNF5	Os dados (Número de pessoas na instalação, Temp, CO ₂ , umidade) devem ser informados com precisão de pelo menos 90%.



RNF6	O dispositivo BloT, em caso de falta de energia, deve ser capaz de retomar automaticamente suas atividades ao restabelecimento do fornecimento de energia.
RNF7	O dispositivo BloT, em caso de falta de internet, deve ser capaz de se reconectar à internet quando ela voltar a estar disponível.
RNF8	O dispositivo BloT deve sincronizar seu relógio com o horário da Internet sempre que publicar um tópico no broker.
RNF9	O dispositivo BloT deve armazenar os dados mais recentes (CO ₂ , VOCs, umidade relativa e temperatura) em memória local, caso haja falha de conexão. Esses dados devem ser enviados ao broker assim que a conexão for restabelecida.
RNF10	O dispositivo BloT deve publicar no Broker os dados referentes ao módulo de qualidade de ar (DHT11/AHT-21) e (CJMCU811/ENS160) em um intervalo de 15 segundos (INTERVALO_ATUALIZACAO_DADOS_QUALIDADE_AR)
RNF11	O dispositivo BloT deve publicar no Broker os dados referentes ao módulo de contagem de pessoas (HC-SR04) quando detectar um evento de entrada/saída
RNF12	O dispositivo BloT deverá atualizar os limites dos parâmetros de biossegurança (no formato especificado em COM04) assim que se ligar e a cada INTERVALO_ATUALIZACAO_LIMITES.
RNF13	O dispositivo BloT deve coletar e enviar as informações dos sensores de uma instalação de maneira ininterrupta na semana, seguindo os intervalos de medição colocados nos RNF10 e RNF11.
RNF14	O dispositivo BloT deve ser compatível com a plataforma NodeMCU.
RNF15	O dispositivo BloT deve estabelecer comunicação autenticada com o Broker por meio de chaves.
RNF16	O dispositivo BloT não deve permitir acesso ou login via Wi-Fi.
RNF17	O dispositivo BloT deve criptografar os dados transmitidos com o CryptoComponent, com o protocolo Speck.
RNF18	Os dispositivos devem ser encapsulados em uma estrutura protetora para evitar a exposição dos fios.
RNF19	O dispositivo BloT deve possuir um broker privado.
RNF20	O dispositivo BloT deve se comunicar a partir de uma rede local e sem fio.
RNF21	O dispositivo BloT deve ser alimentado por meio de uma fonte 5V, utilizando a porta micro USB
RNF22	<p>O dispositivo BloT deve reportar falhas reconhecidas durante o processo de coleta de medidas através da inclusão de etiquetas de erro na mensagem que será enviada ao broker. Os erros são incrementados na mensagem de forma binária, permitindo que o backend identifique todas as falhas por meio de operações bit a bit. A definição para cada erro segue a seguinte estrutura:</p> <ol style="list-style-type: none">1. Falha na obtenção de data e hora pelo servidor (1);2. Falha na coleta da medida de temperatura (2);3. Falha na coleta da medida de umidade (4);4. Falha na coleta da medida de CO₂ (8).



```
#define ERROR_TIME (1 << 0) // 1
#define ERROR_TEMP (1 << 1) // 2
#define ERROR_HUMID (1 << 2) // 4
#define ERROR_CO2 (1 << 3) // 8
#define ERROR_TVOC (1 << 4) // 16
```

Dashboard

Requisitos Funcionais

RF01	O Dashboard deve exibir a temperatura, em graus Celsius (°C), de cada instalação cadastrada que possua algum dispositivo vinculado, sem necessidade de autenticação.
RF02	O Dashboard deve mostrar a concentração de CO ₂ em partes por milhão (ppm) de cada instalação cadastrada que possua algum dispositivo vinculado, sem a necessidade de autenticação.
RF03	O Dashboard deve mostrar o número de pessoas presentes em cada instalação cadastrada que possua algum dispositivo vinculado, sem necessidade de autenticação.
RF04	O Dashboard deve mostrar a classificação de risco de cada instalação cadastrada, tendo como base os limites dos parâmetros de biossegurança informados, conforme o Guia de Biossegurança [1], sem a necessidade de autenticação.
RF05	O Dashboard deve mostrar o estado de utilização ("bloqueado (em manutenção)", "bloqueado (em limpeza)" e "liberado") de cada instalação cadastrada, sem necessidade de autenticação.
RF06	O Dashboard deve apresentar a localização da instalação cadastrada, juntamente com as informações da unidade.
RF07	O Dashboard deve apresentar, para cada instalação cadastrada, a evolução dos marcadores (temperatura, concentração de CO ₂ , umidade, VOCs, número de pessoas) na última hora, em gráficos lineares temporais, com intervalo de 2 minutos.
RF08	O Dashboard deve exibir os valores máximos de cada medida na última hora.
RF09	O Dashboard deve exibir o percentual de umidade de cada instalação cadastrada que possua algum dispositivo vinculado, sem necessidade de autenticação.
RF10	O Dashboard deve mostrar a unidade de VOCs de cada instalação que possua algum dispositivo vinculado, sem a necessidade de autenticação.
RF11	O Dashboard deve alertar o usuário quando o limite máximo de qualquer medição (número de pessoas, VOCs, CO ₂ , umidade e temperatura) definido no SAFE Manager pelo gerente da instalação for atingido.
RF12	O Dashboard deve exibir uma legenda no rodapé da página indicando o que as cores e ícones significam, → Bloqueado;



- | | |
|--|---|
| | ● → Liberado;
△ → Limite máximo atingido |
|--|---|

Requisitos Não Funcionais

RNF01	O Dashboard deve se comunicar com o subsistema SAFE Manager (servidor) por meio das rotas de API do SAFE Manager.
RNF02	O Dashboard deve obter os limites dos parâmetros de segurança das instalações cadastradas, utilizando um dispositivo vinculado ao subsistema SAFE Manager. Deve consultar as informações dos parâmetros no SAFE Manager a partir da rota de API com a seguinte estrutura JSON: <pre>{ "id": <valor>, "name": <valor>, "installation_requests": [<valor>], "installation_threshold": [{ "temperature": <valor>, "humidity": <valor>, "ppmco2": <valor>, "number_people": <valor> }] }</pre>
RNF03	O Dashboard deve obter os dados enviados pelos dispositivos IoT do subsistema SAFE Manager (servidor).
RNF04	O Dashboard deve manter um alerta “OS DADOS NÃO ESTÃO SENDO ATUALIZADOS”, caso não consiga atualizar as informações no TEMPO_MAXIMO_ANTES_ALERTA_DASHBOARD (ver glossário).
RNF05	O Dashboard deve obter novos dados enviados pelos dispositivos a cada INTERVALO_ATUALIZAR_DADOS (ver glossário).
RNF06	O Dashboard deve atualizar os limites dos parâmetros de biossegurança a cada INTERVALO_ATUALIZACAO_LIMITES (ver glossário).
RNF07	O Dashboard deve atualizar os estados de utilização das instalações cadastradas a cada INTERVALO_ATUALIZACAO_ESTADO (ver glossário).
RNF08	O Dashboard deve informar caso haja indisponibilidade no subsistema SAFE Manager (servidor).
RNF09	O Dashboard deve permitir atualizações por meio de Docker.
RNF10	O Dashboard deve oferecer aos Administradores do Sistema um meio direto de acesso ao servidor do Manager em caso de falha sistêmica.
RNF11	O Dashboard deve realizar atualizações mensais dos componentes de software.



RNF12	O Dashboard deve garantir compatibilidade com, no mínimo, as versões: Chrome 118, Firefox 115, Edge 118 e Safari 16.																				
RNF13	O Dashboard deve oferecer uma interface responsiva ao usuário considerando os seguintes critérios: <table border="1"><thead><tr><th>Classe Size</th><th>Pontos de interrupção</th><th>Tamanho da tela típico (diagonal)</th><th>Dispositivos</th><th>Tamanhos de janela</th></tr></thead><tbody><tr><td>Pequeno</td><td>640px ou menos</td><td>4" a 6"; 20" a 65"</td><td>Telefones e TVs</td><td>320x569, 360x640, 480x854</td></tr><tr><td>Médio</td><td>641px a 1007px</td><td>7" a 12"</td><td>Phablets, tablets</td><td>960 x 540</td></tr><tr><td>Grande</td><td>1008px ou mais</td><td>13" e maior</td><td>Computadores, laptops, Surface Hubs</td><td>1\,024 x 640, 1.366 x 768, 1.920 x 1.080</td></tr></tbody></table>	Classe Size	Pontos de interrupção	Tamanho da tela típico (diagonal)	Dispositivos	Tamanhos de janela	Pequeno	640px ou menos	4" a 6"; 20" a 65"	Telefones e TVs	320x569, 360x640, 480x854	Médio	641px a 1007px	7" a 12"	Phablets, tablets	960 x 540	Grande	1008px ou mais	13" e maior	Computadores, laptops, Surface Hubs	1\,024 x 640, 1.366 x 768, 1.920 x 1.080
Classe Size	Pontos de interrupção	Tamanho da tela típico (diagonal)	Dispositivos	Tamanhos de janela																	
Pequeno	640px ou menos	4" a 6"; 20" a 65"	Telefones e TVs	320x569, 360x640, 480x854																	
Médio	641px a 1007px	7" a 12"	Phablets, tablets	960 x 540																	
Grande	1008px ou mais	13" e maior	Computadores, laptops, Surface Hubs	1\,024 x 640, 1.366 x 768, 1.920 x 1.080																	
RNF14	O Dashboard deve apresentar as instalações cadastradas em espaços individuais na interface (cards)																				
RNF15	O Dashboard deve se comunicar com o subsistema SAFE Manager por meio de internet																				

8 REFERÊNCIAS

Título do Documento	Versão	Onde pode ser obtido
Guia de ações de biossegurança para a resposta à pandemia de COVID-19 no âmbito da UFRJ.	1.0	Link

9 CONCORDÂNCIA DO CLIENTE/REPRESENTANTE DO CLIENTE

Concordo com os requisitos listados neste documento. Estou ciente de que o planejamento do projeto será realizado com base nesses requisitos aprovados.

Nome:

Cargo:

Assinatura (ou cópia de e-mail enviado):