RP-0001

SISTEMA DE CONTROLE DE ACESSO SATC

Relatório de projeto

Revisão 1.0 – 18/06/2022

Índice

1. Introdução 4
   1.1. Objetivos do documento 4
   1.2. Escopo do produto 4
   1.3. Definições e siglas 4
   1.4. Referências 4
   1.5. Visão geral deste documento 5
2. Análise de Requisitos 5
   2.1. Perspectiva do produto 5
      2.1.1. Diagrama de contexto 5
      2.1.2. Interfaces de usuário 6
      2.1.3. Interfaces de hardware e software 6
      2.1.4. Restrições de memória 7
   2.2. Funções do produto 7
   2.3. Descrição do cenário 7
      2.3.1. Requisitos de adaptação ao ambiente 7
   2.4. Características dos usuários 8
   2.5. Restrições 8
   2.6. Hipóteses de trabalho 9
   2.7. Requisitos adiados 9
   2.8. Requisitos específicos - Interfaces externas 9
      2.8.1. Visão geral 9
      2.8.2. Requisitos para interfaces gráficas de usuário 10
   2.9. Requisitos funcionais 11
      2.9.1. Lista de Requisitos funcionais 11
   2.10. Requisitos não-funcionais 11
      2.10.1. Requisitos de desempenho 11
      2.10.2. Requisitos de dados persistentes 12
      2.10.3. Restrições ao desenho 12
      2.10.4. Atributos de Qualidade 12
      2.10.5. Lista de Requisitos não-funcionais 12
   2.11. Análise de riscos 13
3. Modelagem UML 14
   3.1. Diagramas de casos de uso 14
      3.1.1. Fluxos dos casos de uso 15
   3.2. Diagrama de sequência 15
      3.2.1. Operação 15
      3.2.2. Sincronização de dados com servidor externo 16
4. Modelo de arquitetura do sistema 17
   4.1. Arquitetura Catracas 17
   4.2. Arquitetura Servidor WEB 17

4.3. Arquitetura Servidor de dados 17
4.4. Diagrama de blocos da arquitetura 17
5. Testes 18
5.1. Teste Unitário 18
5.2. Teste de Componente 18
5.3. Teste de Sistema 19
6. Apêndices 19
7. Controle de revisão 20

1. Introdução

1.1. Objetivos do documento

Desenvolvimento de um sistema de controle de acessos (catracas) de alunos, professores e demais colaboradores da SATC sem haver o contato físico dos usuários com qualquer equipamento de uso coletivo.

1.2. Escopo do produto

O produto que será desenvolvido tem por principal tecnologias o uso de Sensor Biométrico sem contato, identificando até 4 digitais do indivíduo. Com tempo de resposta de até 1 segundo, é a opção ideal para evitar contatos físicos e garantir a autenticidade do indivíduo. Como tecnologia secundária será utilizado câmeras para leitura de QR Code e leitor de Cartão RFID para visitantes; os dados dos indivíduos serão atualizados via servidor em rede LAN (TCP/IP) para consulta ao banco de dados centralizado, sincronizado periodicamente com o servidor geral da instituição.

1.3. Definições e siglas

- QR Code: *Quick Response Code,* código de resposta rápida;
- Cartão RFID: Cartão com identificador por rádio frequência;
- LAN: *Local Área Network*, rede de área local;
- TCP/IP: Conjunto de protocolos de comunicação entre computadores em rede. TCP sendo Protocolo de controle de transmissão, e IP o Protocolo de Internet, contendo um identificador do dispositivo na rede.
- API Rest: Transferência Representacional de Estado, é uma arquitetura de software que define um conjunto de restrições a serem usadas para a criação de serviços web;
- USB: *Universal Serial Bus*, ou porta universal, tecnologia que permite a conexão de periféricos sem a necessidade de desligar o computador

1.4. Referências

[1] ROCKEN. **BIOMETRIA (IMPRESSÃO DIGITAL).** Disponível em: <https://www.rocken.com.br/cartao-de-aproximacao/>. Acesso em: 21 abril 2022.

[2] Bianca. **Conheça os tipos de rede e entenda qual o melhor para sua empresa.** Disponível em: <https://blog.algartelecom.com.br/mge/tipos-de-rede/>. Acesso em: 21 abril 2022.

[3] ALECRIM, Emerson. **O que é USB? (Velocidades, conectores e versões).** Disponível em: <https://blog.algartelecom.com.br/mge/tipos-de-rede/>. Acesso em: 21 abril 2022.

[4] **O modelo de referência TCP/IP.** Disponível em: <https://sites.google.com/site/estudandoredes/capitulo-01---introducao/1-4-modelos-de-referencia/1-4-2-o-modelo-de-referencia-tcp-ip/>. Acesso em: 22 abril 2022.

[5] IBM. **Referência da API REST.** Disponível em: <https://www.ibm.com/docs/pt-br/psww2500/2.3.2.0?topic=rest-api-reference/>. Acesso em: 22 abril 2022.

[6] PUHLMANN, Henrique. **Introdução à tecnologia de identificação RFID**. Disponível em: <https://www.embarcados.com.br/introducao-a-rfid//>. Acesso em: 22 abril 2022.

[7] SECUGEN. **U-AIR Touchless USB Fingerprint Sensor.** Disponível em: <https://secugen.com/products/u-air/>. Acesso em: 22 abril 2022.

1.5. Visão geral deste documento

Este documento tem por objetivo documentar o processo de análise de requisitos do projeto. Estruturado de modo a abranger as definições do produto, usuários, ambiente, interface, hardware e riscos ao sistema.

2. Análise de Requisitos

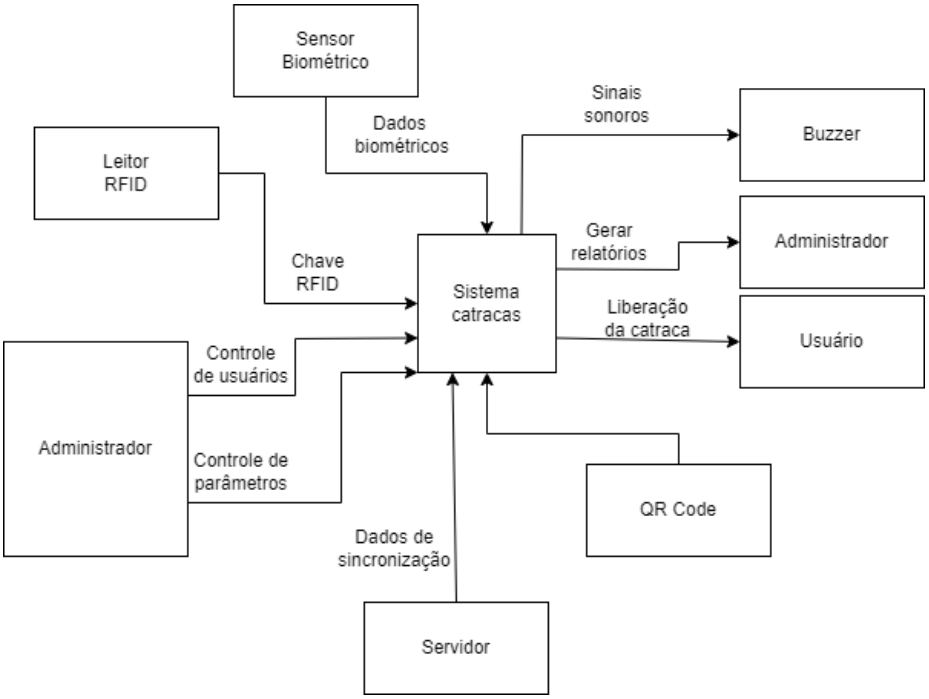
2.1. Perspectiva do produto

O produto é independente, sendo necessário a configuração através do servidor local.

Podendo se tornar parte de um sistema maior, com a utilização de sincronização de base de dados.

2.1.1. Diagrama de contexto

Figura 1 – Diagrama de contexto.



Fonte: O autor (2022)

2.1.2. Interfaces de usuário

A interface com os usuários será através de catracas mecânicas, saída sonora e luz indicadora, para identificar a liberação ou bloqueio do indivíduo.

Para o administrador da rede, a interface também será o servidor da aplicação.

2.1.3. Interfaces de hardware e software

É necessário possuir uma rede LAN para a comunicação entre as catracas e o servidor.

O sistema possuirá alimentação de 110 até 240 VCA e nobreak com duração de 10 horas para até 10 catracas;

O sistema possuirá um servidor contendo teclado e mouse USB, e monitor para visualização do software.

Servidor deverá contar com Windows server 2019 ou superior, compatível com a aplicação. O banco de dados será do tipo SQL Server ou PostGreSQL. Portas de rede Ethernet para comunicação com os dispositivos. Já processador, memória e HD/SSD dependerão da quantidade de usuários do sistema.

No modo de sincronização de banco de dados com o servidor da instituição, é necessário possuir uma API Rest.

2.1.4. Restrições de memória

O limite de cadastros é de 50 mil usuários, sendo possível o aumento da memória do servidor local para até 150 mil cadastros.

2.2. Funções do produto

A principal função do desenvolvimento deste produto é para auxiliar no controle de entrada e saída de alunos, funcionários e visitantes que circulam com frequência na instituição de ensino, impedindo o acesso dos demais que não estejam cadastrados no sistema.

Modo de Cadastro de biometria: o indivíduo aproxima sua mão do leitor biométrico, e o sistema grava o novo identificador caso já não exista;

Modo de Cadastro de Cartão RFID: o indivíduo aproxima o cartão RFID no leitor e o sistema grava o novo identificador caso já não exista;

Modo de Configuração: O administrador do sistema pode parametrizar as funcionalidades do sistema através do servidor, habilitando o modo de sincronia de banco de dados, bloqueando ou liberando usuários, configurando períodos de atividade ou inatividade do sistema.

Modo de Relatório: O administrador acessa via servidor local os registros dos últimos 1 milhão de registros, com opção de exportação do relatório de eventos.

Modo de Operação: o indivíduo se aproxima do leitor biométrico ou utiliza o QR Code ou cartão RFID, a catraca consultará o banco de dados local e verificará se o mesmo está apto para realizar o acesso, em caso positivo a catraca será liberada para passagem.

2.3. Descrição do cenário

O sistema será instalado para realizar o controle de acesso das pessoas dentro da instituição, sendo assim, o fluxo de pessoas nas catracas será extremamente alto. Além disso, o sistema deverá ser adaptado ao ambiente da instituição. Sendo necessário atentar aos requisitos do produto para adaptação ao ambiente.

2.3.1. Requisitos de adaptação ao ambiente

Seguem requisitos de adaptação do produto ao ambiente onde será implantado.

- O ambiente deve possuir uma rede LAN para comunicação entre as catracas e servidor. A rede não poderá ter acesso direto à internet, sendo necessário um dispositivo de segurança, como um Firewall.
- O sistema não deve estar exposto diretamente ao tempo. O grau de proteção é IP64 de acordo com a norma IEC 60529. A prova de poeira é protegida contra jorro de água.

2.4. Características dos usuários

Dentre os usuários estão inclusos os alunos, professores e os demais colaboradores da instituição de ensino, considerando que todos participarão do cadastro biométrico para serem controladas suas entradas e saídas. Os alunos vão desde o Ensino Fundamental I, II, Ensino Médio 1º, 2º e 3º ano, Ensino Técnico, Graduação e Pós-graduação.

Quanto aos alunos do Ensino Fundamental I, eles terão que ter uma atenção maior por parte da instituição, pois podem apresentar alguma dificuldade inicial com a utilização do sistema, considerando que ainda estão em fase de desenvolvimento intelectual, já os demais alunos possuirão uma facilidade para utilização do sistema. Os alunos que vão do Ensino Fundamental até o Ensino Médio, utilizarão diariamente, apenas podendo variar na frequência de uso para alunos do Ensino Técnico, Graduação e Pós-graduação.

Professores e colaboradores acabam por se incluir na mesma categoria e também não terão dificuldade para utilizar o sistema, dependendo da instituição de ensino, os alunos do Ensino Fundamental I necessitarão de um auxílio, que pode vir do professor ou de algum colaborador que ficaria responsável por um possível auxílio na utilização do sistema. Professores podem ter uma frequência de uso alternada, pois não necessariamente terão aulas diariamente. Já os colaboradores, dependendo da função, utilizarão diariamente.

2.5. Restrições

Uma restrição relacionada ao desenvolvimento do projeto é a capacidade de controles que podem ser feitos simultaneamente que estão relacionados à quantidade de estações de controle de entrada disponíveis em cada ponto onde elas estão instaladas. Além do número máximo de requisições que o banco de dados consegue suprir simultaneamente para a aplicação desenvolvida. Pessoas portadores de deficiências especiais que necessitam de utilização de cadeira de rodas ou outros meios de locomoção semelhantes não poderão usar as estações normais para acesso da instituição.

2.6. Hipóteses de trabalho

O uso do sensor biométrico embora muito prático tem restrições referente a limitações físicas do usuário como, por exemplo, em casos de síndrome de Nagali, os usuários deverão utilizar o cartão RFID ou QR Code. Assim como doenças, deficiências físicas, incapacitação das mãos devido à utilização de gesso ou talas para recuperação que possam impedir a utilização da biometria ou até mesmo do cartão RFID ou QR Code, deverão receber o auxílio do colaborador responsável pelo auxílio nessas situações adversas.

2.7. Requisitos adiados

Reconhecimento facial, pode em alguns casos gerar uma inclusão maior do sistema em casos de deficiências por parte dos usuários, porém isso foi deixado de lado para primeiramente fazer uma avaliação da demanda, se realmente é necessária tamanha inclusão, além de requisitar um esforço muito maior para entrega do produto.

2.8. Requisitos específicos - Interfaces externas

2.8.1. Visão geral

As entradas do sistema são:

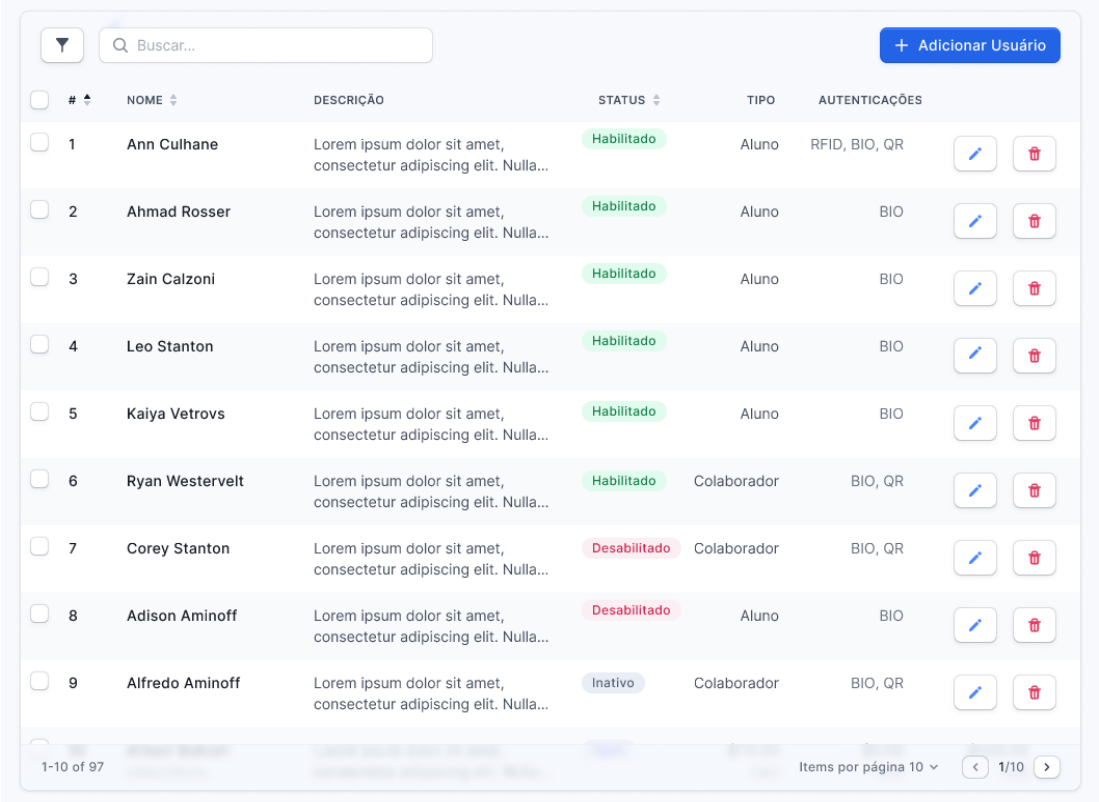
- **Sensor biométrico sem contato**: um módulo de sensor de impressão digital sem contato que captura imagens de impressão digital altamente precisas e de alta qualidade sem exigir que os usuários entrem em contato ou toque no dispositivo. Com tecnologia óptica compacta e sem toque que pode escanear uma única impressão digital do dedo de um usuário posicionado no ar acima do dispositivo. A imagem obtida é CMOS com resolução de 500 DPI no tamanho de 500 x 700 pixels.
- **Leitor Sensor RFID**: Utiliza-se de cartões de proximidade RFID, que consiste em um chip eletrônico no qual é armazenado um código numérico. Ao ser aproximado de uma leitora RFID este cartão é identificado e fará a abertura do bloqueio (catraca, portão, torniquete) ou somente para identificação, conforme a necessidade do cliente. A grande vantagem desta tecnologia é a segurança, uma vez que não pode ser copiado ou clonado.
- **Câmera para leitura de QR Code**: módulo para escanear o código de um QR Code impresso ou digitalizado em telas de dispositivos móveis. Possui luz infravermelha para não precisar de luzes externas.
- **Interface de cadastro de usuários**: A interface deverá conter campos para cadastro das informações de identificação do usuário.

As saídas do sistema:

- **Catracas**: para controle de acesso dos indivíduos.
- **Sinal luminoso**: para interface com o usuário, contendo duas cores: verde para indicar a liberação e vermelho para indicar sistema bloqueado.
- **Sinal sonoro**: para interface com o usuário. Um bip longo para indicar liberação e 2 bips rápidos para indicar bloqueio.
- **Relatório gerencial**: contém o log de eventos do sistema dos últimos 7.200.000 eventos, considerando 10000 indivíduos passando 4 vezes por dia durante 6 meses.

2.8.2. Requisitos para interfaces gráficas de usuário

Figura 2 – Tela de cadastro.



Fonte: O autor (2022)

A lista de cadastro como pode ser vista na Figura 2, segue o padrão de estilos que serão utilizados no sistema todo. Ao clicar em “Adicionar Usuário” um formulário aparecerá e os campos de Nome, Descrição, Status e Tipo do usuário deverão ser preenchidos, serão adicionados também os modos de autenticação do usuário, e apenas ao selecionar o modo Biometria o usuário deve estar no local de cadastro para que sua biometria seja lida pelo sistema para cadastro, os outros modos, RFID e QR Code, poderão ser cadastrados sem que o usuário esteja presente no local, já que serão gerados automaticamente e entregues ao usuário.

Ainda na lista de cadastro do sistema, usuários poderão ser excluídos ou editados por um administrador, sendo que na edição um administrador do sistema poderá alterar todos os campos do cadastro e ainda inativar, habilitar ou desabilitar o usuário selecionado, impedindo-o ou possibilitando-o de usar o sistema. Além disso, através dessa tabela poderá ser gerado um relatório com os filtros selecionados na barra de pesquisa.

Haverá uma tela de parametrização das funcionalidades do sistema, onde terá a opção para escolha da sincronização do banco de dados e a configuração dos períodos de atividade e inatividade do sistema. Além da possibilidade de alterar o status de vários alunos.

2.9. Requisitos funcionais

2.9.1. Lista de Requisitos funcionais

N°	Descrição Requisitos Funcionais
RF1	O Software deverá permitir cadastrar usuários.
RF2	O Software deverá permitir a emissão de relatórios de acesso.
RF3	O Software deverá permitir realizar uma autenticação via hardware.
RF4	O Software deverá realizar a sincronização com o banco de dados centralizado.
RF5	O software deverá permitir uma autenticação via login.
RF6	O Software deverá permitir a edição dos usuários.
RF7	O hardware deverá identificar a digital do indivíduo.
RF8	O hardware deverá ler um QR Code através de um leitor.
RF9	O software deverá permitir a ativação e desativação dos usuários.
RF10	O hardware deverá ter um leitor de Cartão RFID.
RF11	O hardware deverá ter uma saída sonora para interface com usuário.
RF12	O hardware deverá ter uma saída luminosa para interface com usuário.
RF13	A catraca deverá identificar para que lado a mesma girou para saber se o indivíduo está entrando ou saindo.
RF14	O protocolo de comunicação entre as catracas e servidores devem ser no protocolo TCP/IP e API Rest no HTTP/1.1.
RF15	A entrada de alimentação do sistema deverá ser de 110 até 240 VCA.

2.10. Requisitos não-funcionais

2.10.1. Requisitos de desempenho

O sistema deve ser capaz de oferecer suporte simultâneo a todas as 10 catracas, devendo responder cada utilização por usuário em até 1 segundo.

2.10.2. Requisitos de dados persistentes

Como estrutura lógica de dados, temos o banco de dados relacional principal da aplicação, o qual armazenará os dados biométricos e identificadores de cada usuário, bem como o histórico de utilização dos equipamentos.

2.10.3. Restrições ao desenho

O software deverá seguir a norma IEC 9126 para padronização do desenvolvimento.

2.10.4. Atributos de Qualidade

Acurácia para a assertividade da permissão de acesso, tolerância a falhas para casos de falta de energia, conformidade em relação a confiabilidade, comportamento em relação ao tempo para tempos de resposta e estabilidade para capacidade do software de evitar efeitos colaterais decorrentes de modificações introduzidas.

2.10.5. Lista de Requisitos não-funcionais

N°	Descrição Requisitos Não-Funcionais
RNF1	A sincronização do banco de dados não deverá ocorrer em horários de pico.
RNF2	O sistema deverá funcionar sem energia por um período de 10 horas para 10 catracas.
RNF3	O sistema terá limite de cadastros 50 mil usuários.
RNF4	O sistema deverá possibilitar o aumento da memória do servidor local para até 150 mil cadastros.
RNF5	Os relatórios deverão ser emitidos com bases diárias/semanais/mensais com períodos manhã/tarde/noite
RNF6	A sincronização deverá ser realizada a cada 30 minutos
RNF7	A área de login deverá ser restrita a outros usuários.
RNF8	O desbloqueio da catraca acontecerá automaticamente ao detectar queda de energia
RNF9	Edição será restrita à usuários Administradores
RNF10	O tempo de detecção não poderá ultrapassar um segundo.
RNF11	O bloqueio do indivíduo deverá ser temporário ou permanente.

RNF12	O sinal sonoro deverá emitir um bip longo para liberação e dois bips curtos para bloqueio.
RNF13	O sinal luminoso deverá ser verde para liberação e vermelho para bloqueio.
RNF14	A catraca deverá permitir a saída ao existir uma falta de energia
RNF15	O sistema deverá possibilitar o aumento da memória do servidor local para até 150 mil cadastros.
RNF16	O grau de proteção é IP64 de acordo com a norma IEC 60529. A prova de poeira é protegida contra jorro de água.
RNF17	A rede não poderá ter acesso direto à internet, sendo necessário um dispositivo de segurança, como um Firewall.
RNF18	O log de eventos do sistema deverá ser dos últimos 7.200.000 eventos, considerando 10000 indivíduos passando 4 vezes por dia durante 6 meses
RNF19	O framework no frontend deverá ser Angular 2+
RNF20	O framework no backend deverá ser Quarkus
RNF21	O banco de dados deverá ser PostgreSQL

2.11. Análise de riscos

De acordo com os requisitos funcionais e não funcionais, segue tabela de análise das consequências potenciais de falhas devido à natureza de produtos e serviços. Foram consideradas as tolerâncias a falhas e as medidas preventivas no sistema.

Tabela 1 - Análise de riscos

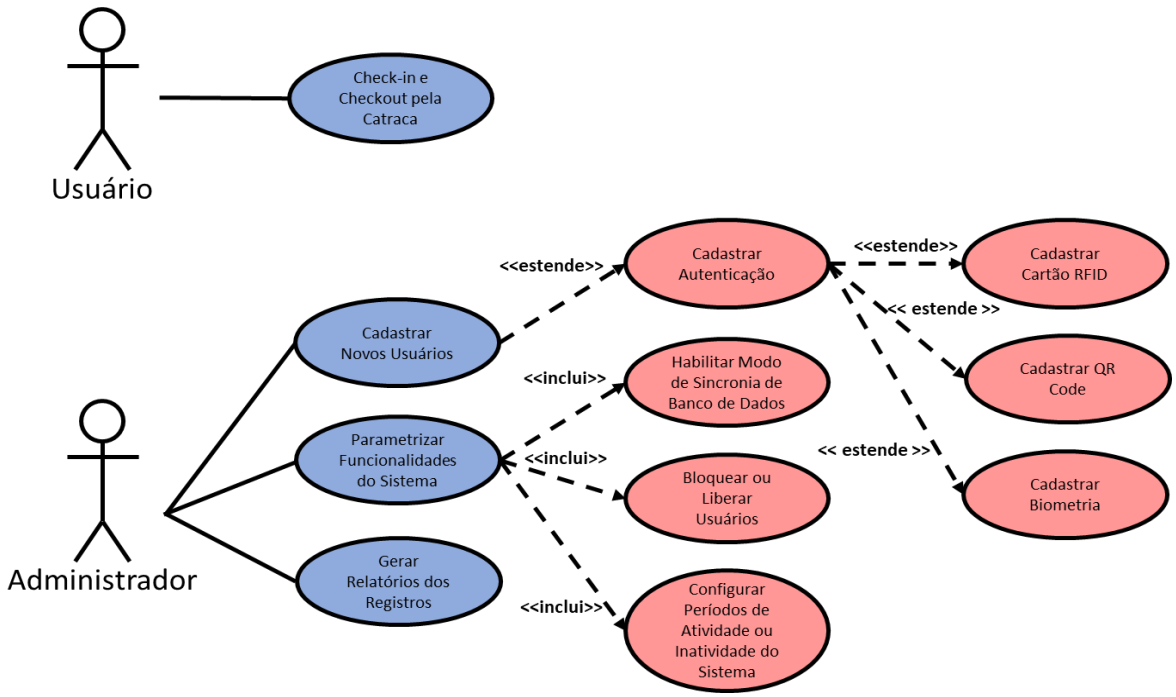
Falha	Consequência	Medida preventiva
Falta de energia	Produto irá desligar.	O sistema possuirá alimentação de 110 até 240 VCA e nobreak com duração de 10 horas para até 10 catracas;
Sem comunicação com o servidor de dados externo	Sistema não irá atualizar o banco.	Utilizar o banco de dados dos usuários do servidor local até que a comunicação retorne e seja possível atualizar o banco de dados. Sinal de erro será exibido no LED.
Sem comunicação com o servidor local	Falha no controle de acesso.	Utilizar cabos e conectores de boa qualidade, cliente realizar

		verificação preventiva periódica. Sinal de erro será exibido no LED.
Grau de proteção violado. Infiltração de água.	Falha no sistema.	Cliente deverá seguir o grau de proteção estabelecido. Em caso de falhas por infiltração, a catraca deverá ser encaminhada para a assistência técnica.
Pessoa recém cadastrada no banco de dados tenta passar na catraca.	A pessoa não será liberada.	Deverá esperar o tempo de configurado de sincronização do sistema. Modo de sincronização manual via dashboard no servidor local.
Deficientes visuais utilizando a catraca.	Não saberá se foi liberado ou bloqueado.	Sistema deverá ter um sinal sonoro para aviso de liberação ou bloqueio.
Deficientes auditivos utilizando a catraca.	Não saberá se foi liberado ou bloqueado.	Sistema deverá ter um sinal visual para aviso de liberação ou bloqueio.
Cadeirantes utilizando o controle de acesso.	Não será possível passar pela catraca comum.	O cliente deverá adquirir uma catraca para cadeirantes.
Comunicação local está lenta.	O usuário precisará esperar mais do que o normal.	Instalar switch com portas gigabit, e o cliente deve garantir que a rede LAN do sistema está isolada.
Usuário nunca é autorizado.	Não poderá passar pela catraca.	Neste caso: utilizar outra catraca. Se o problema persistir deverá ser realizado o treinamento do usuário novamente. Caso a troca resolva o problema, verificar se é indicado algum erro no sistema.

3. Modelagem UML

3.1. Diagramas de casos de uso

Figura 3 – Diagrama de casos de uso.



Fonte: O autor (2022)

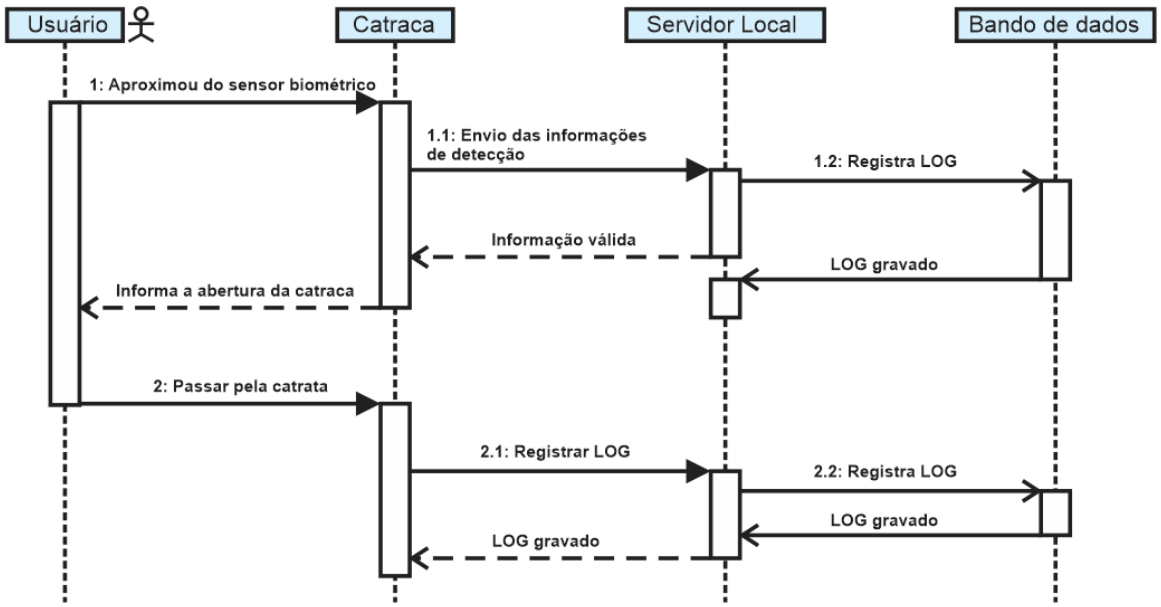
3.1.1. Fluxos dos casos de uso

1. O caso de uso inicia quando o Administrador seleciona **“Cadastrar Novos Usuários”**;
   1.1. O novo usuário deve ter alguma relação com a instituição de ensino, como colaborador ou aluno;
   1.2. O usuário após ser cadastrado pode ter autenticação por Cartão RFID, QR Code ou Biometria, sendo que por padrão o sugerido é Biometria;
2. O sistema pode ter funcionalidades parametrizadas;
   2.1. O modo de sincronia de banco de dados pode ser habilitado;
   2.2. Usuários podem ser bloqueados ou liberados pelo sistema;
3. Relatórios dos registros podem ser gerados;
4. Como usuário ele pode realizar o check-in ou check out pela forma de autenticação escolhida.

3.2. Diagrama de sequência

3.2.1. Operação

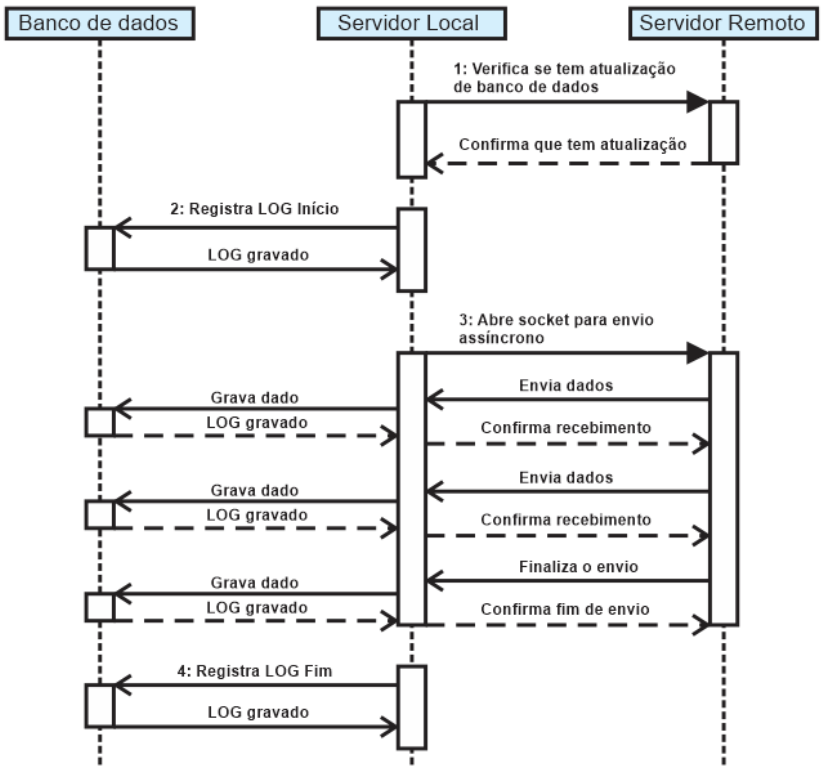
Figura 4 – Sequência de operação



Fonte: O autor (2022)

3.2.2. Sincronização de dados com servidor externo

Figura 5 – Sequência de sincronização de banco de dados



Fonte: O autor (2022)

4. Modelo de arquitetura do sistema

A arquitetura do sistema é uma mistura de várias arquiteturas pois o produto é composto por um hardware cliente, um servidor de operação e sistema web para configuração e monitoramento, este servidor também é cliente de um servidor de sincronização de dados externo.

4.1. Arquitetura Catracas

Baseada na arquitetura Cliente-Servidor, com baseados em transações, pois possibilita que os servidores possam ser distribuídos através de uma rede.

4.2. Arquitetura Servidor WEB

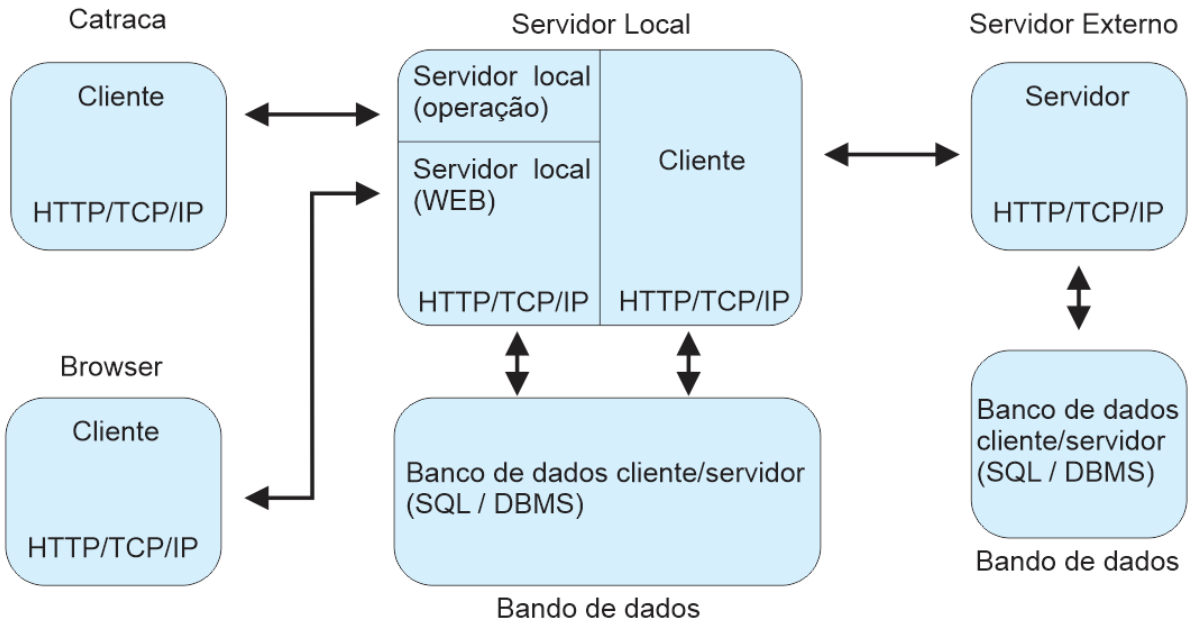
Baseado na arquitetura Cliente-Servidor, Sistema de informação, e em camadas (MVC), possibilitando desenvolvimento da parte WEB de forma incremental, sendo possível o lançamento de novas funcionalidades e correções, com acesso via browser, além de isolar as camadas de modelo, visão e controlador facilitando o gerenciamento da equipe de desenvolvimento.

4.3. Arquitetura Servidor de dados

Essa arquitetura foi definida como Cliente-Servidor sendo que o mesmo servidor de dados local será cliente deste servidor, sendo baseado também em transações e em camadas (MVC).

4.4. Diagrama de blocos da arquitetura

Figura 6 – Diagrama de bloco de integração do sistema



Fonte: O autor (2022)

5. Testes

Todo o desenvolvimento do sistema será dirigido a testes, a fim de documentação e facilidade na validação dos requisitos do projeto.

O sistema pode ser quebrado em componentes e os componentes possuem funcionalidades especificas, sendo assim, serão utilizadas as metodologias de testes listadas abaixo para validação do sistema.

Na parte de serviço WEB, será implementada metodologia de desenvolvimento incremental, sendo implementados também **testes de release**, sendo disponibilizados versões de **testes de usuários** em caráter BETA.

Para validação do sistema, será realizado o **teste de aceitação** e registro da aprovação.

5.1. Teste Unitário

Usado para validar cada funcionalidade específica, nesta etapa é validado cada parte do hardware eletrônico, como microcontrolador, fonte, cristal oscilador, entrada de sinal de sensor. Na parte de software (API) cada rota possuirá funções que devem ser testadas isoladamente.

5.2. Teste de Componente

Cada componente do sistema deve ser testado separadamente para garantir o seu funcionamento antes de integração. Podendo ainda separar em testes de hardware, API e banco de dados, e sincronia de dados.

5.3. Teste de Sistema

Após a validação dos componentes será necessário testar as integrações das partes, visto que todas devem comunicar para o funcionamento correto do produto.

6. Apêndices

Norma para Engenharia de software - Qualidade deproduto ISO9126-1: https://jkolb.com.br/wp-content/uploads/2014/02/NBR-ISO_IEC-9126-1.pdf

Norma para grau de proteção para invólucors de equipamentos elétricos: https://document.onl/documents/abnt-nbr-iec-60529-2009pdf.html

7. Controle de revisão

Revisão	Publicação	Desenvolvido por
1.0	26/04/2022	Bruno Silva Daniel; Diego Vieira Minatto; Filipi Bitencourt Piucco; Jonas Pereira Geremias; Leonardo Cechella Velho; Thiago Spíndola Rossi.
	Modificações: • Primeira revisão.	
1.1	18/06/2022	Bruno Silva Daniel; Diego Vieira Minatto; Filipi Bitencourt Piucco; Jonas Pereira Geremias; Leonardo Cechella Velho; Thiago Spíndola Rossi.
	Modificações: • Alterado documento de Elicitação de documentos (ER-0001) para Relatório de projeto (RP-0001). • Adicionado índice no documento para facilitar a busca de informação. • Adicionado tópico sobre a descrição do cenário; • Adicionado tópico sobre a análise de riscos; • Movido diagrama de casos de uso para tópico de modelagem do sistema; • Criado diagrama de sequência; • Criado modelo de arquitetura para o sistema; • Criado método de teste para o sistema;	