ANÁLISEDEREQUISITOS.com.br

ESPECIFICAÇÃO DE REQUISITOS

DOCUMENTO X-0001

NOME DO ANALISTA

ÚLTIMA ATUALIZAÇÃO: 03/11/2020

HISTÓRICO DE REVISÕES DO DOCUMENTO

DATA	VERSÃO	DESCRIÇÃO DA ALTERAÇÃO	AUTOR
23/03/2023	1	CRIAÇÃO DESTE DOCUMENTO	BERNARDO VIERO
24/03/2023	2	ALTERAÇÃO DO REQUISITO R1-1	BERNARDO VIERO

IDENTIFICAÇÃO DOS ENVOLVIDOS

PAPEL	NOME	EMAIL
ANALISTA DE REQUISITOS	Bernardo Viero	bernardo.viero@ufn.edu.br
PRODUCT OWNER	Bernardo Viero	bernardo.viero@ufn.edu.br
STAKEHOLDER	Bernardo Viero	bernardo.viero@ufn.edu.br
PATROCINADOR	UFN	bernardo.viero@ufn.edu.br

PROBLEMA DE NEGÓCIO

Crie uma funcionalidade de login que permita aos usuários acessar a plataforma. A funcionalidade deve incluir uma (tela)página de login com campos para nome de usuário e senha (Defina o tipo de de usuário - email, cpf, nome e critérios para uma senha forte), bem como opções para recuperar a senha em caso de esquecimento. Após o login bem-sucedido, o usuário deve ser redirecionado para a página inicial da plataforma. É importante que as senhas sejam criptografadas e armazenadas de forma segura no banco de dados da plataforma. A funcionalidade de login também deve incluir recursos de segurança, como prevenção de ataques de força bruta e bloqueio de contas após várias tentativas de login malsucedidas.

REQUISITOS DE SISTEMA[1]

R1 – CRIAR FUNCIONALIDA DE LOGIN

Criar um sistema web com a possibilidade de um usuário se 'logar' nesta página.

R1.1 – CRIAR TELA DE LOGIN

Primeiro, deve ser criada uma tela de login, com os campos para serem preenchidos de usuário e de senha.

R1.2 – VALIDAÇÃO DE LOGIN

Validar se os dados do usuário estão corretos, de acordo com as informações contidas no banco de dados.

R2 – FUNCIONALIDADE DE RECUPERAÇÃO DE SENHA

Permitir que o usuário solicite a troca de sua senha, ou que a receba através de uma validação.

R2.1 – VALIDAR ACESSO

Validar informações do usuário, para que seja feito a recuperação desta senha, através do seu e-mail.

R3 – SEGURANÇA DO SISTEMA

Bloquear usuários com várias tentativas de login malsucedidas, e fazer a criptografia de suas senhas no banco de dados.

R3.1 – BLOQUEAR USUÁRIOS

Não permitir que usuários realizem mais do que 5 tentativas de login. Caso isso aconteça e os dados não sejam corretos, esse usuário deve ser bloqueado por um determinado tempo.

R3.2 – CRIPTOGRAFAR SENHAS NO BANCO

Não deixar registrado de forma “aberta” as senhas dos usuários no banco de dados, inserindo algum tipo de criptografia.

WIREFRAMES PARA PROTOTIPAÇÃO DAS INTERFACES

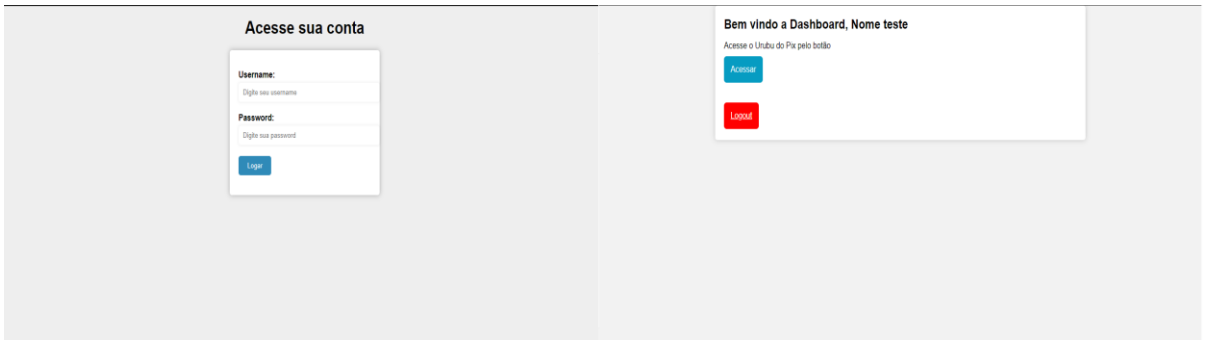

Figura 1 Exemplo de protótipo feito com figma.