|  |  |
| --- | --- |
| **ID** | **TÍTULO DO CASO DE USO** |
| **UC-01** | **AUTENTICAR ACESSO AO PAINEL ADMINISTRATIVO** |
| **2 –ATOR(ES)** | |
| * Administrador * Gestor * Gerente * Operador | |
| **3 – PRÉ-CONDIÇÃO(OES)** | |
| * O usuário possuir um cadastro válido, previamente cadastrado. * Caso seja o primeiro cadastro do sistema, a equipe de projeto deve cadastrar na base de dados um usuário e senha para o administrador geral, tais informações serão utilizadas para cadastrar os demais usuários do sistema. | |
| **4 – CENÁRIO PRINCIPAL** | |
| 1. Ator acessa o sistema através da URL do sistema 2. Sistema exibe tela de login 3. Ator informa seus dados através do preenchimento dos campos de login e senha 4. Servidor valida os campos preenchidos 5. Sistema valida os dados informados pelo usuário buscando o cadastro no banco de dados [4.1] 6. Sistema redireciona o usuário para a dashboard do painel administrativo [5.1], [5.2] e [5.3] | |
| **5 – CENÁRIOS ALTERNATIVOS** | |
| **4.1. Campos obrigatórios não informados**   1. Sistema exibe mensagem informando o campo obrigatório que não foi preenchido. 2. Sistema volta para o passo 2.   **5.1. Dados informados são inválidos**   1. Sistema exibe mensagem informando que o usuário ou senha estão errados. 2. Sistema volta para o passo 2.   **5.2. Usuário bloqueado**   1. Sistema verifica que o usuário informado está bloqueado e não pode acessar o sistema. 2. Sistema exibe uma mensagem informando o motivo do bloqueio do usuário. 3. Sistema volta para o passo 2.   **5.3. Usuário com limite de quantidade de tentativas de acesso excedido**   1. Sistema verifica que o usuário existe, mas a senha está errada. 2. Sistema verifica a quantidade máxima de tentativas de acesso configurada no sistema. 3. Sistema verifica que usuário excedeu o limite máximo de tentativas de acesso. 4. Sistema realiza o bloqueio do usuário por exceder a quantidade máxima de tentativas de acesso. 5. Sistema exibe uma mensagem informando que o usuário foi bloqueado por exceder a quantidade máxima de tentativas de acesso permitidas. 6. Sistema volta para o passo 2. | |
| **6 – PÓS-CONDIÇÃO(ÕES)** | |
| Ator redirecionado para a tela inicial do painel. | |

|  |
| --- |
| **7 – REGRAS DE NEGÓCIO** |
| **Regra de quantidade máxima de tentativas de acesso com senha inválida**: O sistema deve bloquear um usuário caso o mesmo exceda o limite máximo de tentativas de acesso com senha inválida. Essa técnica tem por objetivo dificultar ataques de força bruta onde requisições de acesso poderiam ser realizadas initerruptamente até acertar a senha do usuário cadastrado. |

|  |
| --- |
| **8 – PROTÓTIPOS DE TELAS** |
| **C:\Users\Otávio\Desktop\print.png** |

|  |
| --- |
| **9 – DIAGRAMA DE SEQUÊNCIA** |
| **C:\Users\Otávio\Documents\Documentos extras TCC\diagrama1.png** |