Mini Especificação de Requisitos (Demo)

Uso: validação do cenário QA/Engenharia de Requisitos no AuditDoc Engine

Este documento foi criado intencionalmente com ambiguidades, contradições e requisitos pouco testáveis para servir como 'golden test' do motor de auditoria. Ele descreve um módulo de Autenticação e Conta para um aplicativo web e mobile.

1. Escopo

- Usuário final: clientes que acessam o app via web e mobile.
- Objetivo: login, recuperação de senha, controle de sessão e segurança básica.
- Fora do escopo: pagamentos, cadastro de endereço, notificações por push.

2. Definições

- Conta: identidade única do usuário no sistema.
- Sessão: período autenticado entre login e logout/expiração.
- MFA: autenticação em 2 fatores (SMS ou app autenticador).

3. Requisitos Funcionais (RF)

- RF-01: O sistema deve permitir login por e-mail e senha.
- RF-02: O sistema deve permitir login por número de telefone e senha.
- RF-03: O sistema deve bloquear a conta após 5 tentativas de senha incorreta em um intervalo curto.
- RF-04: O bloqueio deve durar 15 minutos, mas o usuário deve poder tentar novamente imediatamente se solicitar 'Esqueci minha senha'.
- RF-05: O sistema deve oferecer recuperação de senha por e-mail em até 2 minutos.
- RF-06: O sistema deve oferecer recuperação de senha por SMS em até 30 segundos.
- RF-07: O sistema deve manter o usuário logado por um longo período, exceto quando houver risco.
- RF-08: O logout deve ocorrer automaticamente após 10 minutos de inatividade.
- RF-09: O sistema deve permitir que o usuário faça logout manual a qualquer momento.
- RF-10: O sistema deve registrar tentativas de login suspeitas e notificar o usuário rapidamente.

4. Requisitos Não Funcionais (RNF)

- RNF-01: O login deve ser muito rápido e não pode frustrar o usuário.
- RNF-02: A taxa de sucesso do login deve ser alta, mesmo com internet ruim.
- RNF-03: O sistema deve estar sempre disponível (24/7) e sem interrupções.
- RNF-04: As senhas devem ser armazenadas com criptografia forte e padrão de mercado.
- RNF-05: O sistema deve estar em conformidade com LGPD no que se refere a dados de autenticação.

5. Regras de Negócio e Restrições

- RB-01: Usuários com e-mail corporativo (domínio @empresa.com) não devem usar login por telefone.
- RB-02: Usuários com e-mail corporativo devem obrigatoriamente usar MFA.
- RB-03: Para demais usuários, MFA é opcional e deve ser sugerido de forma gentil.
- RB-04: Por segurança, a sessão deve expirar em 7 dias; entretanto, o app deve manter o usuário logado por 30 dias sempre que possível.

6. Critérios de Aceite (iniciais)

- CA-01: Usuário consegue logar com credenciais válidas.
- CA-02: Usuário não consegue logar com credenciais inválidas.
- CA-03: Recuperação de senha funciona.
- CA-04: Sessão expira corretamente.

Fim do documento.