



Teste de Regressão

ID	Descrição do Teste	Critérios de Aceitação	Requisitos Relacionados
TR01	Validar o login com diferentes perfis de usuários (usuário comum e administrador).	Login deve ser realizado com sucesso e o controle de permissões funcional para cada tipo de usuário, sem inconsistências.	RF9, RNF1
TR02	Verificar se o dashboard exibe corretamente as métricas de CPU, memória e I/O após alterações recentes.	Todas as métricas devem ser exibidas corretamente, sem inconsistências ou falhas, mesmo após atualizações no backend.	RF3, RNF2
TR03	Testar se os alertas configurados permanecem acionando corretamente após mudanças no código.	Alertas configurados antes de alterações no sistema devem continuar funcionando sem necessidade de reconfiguração.	RF4, RF8, RNF6
TR04	Garantir que os logs de acesso e atividades continuam sendo registrados após atualizações de segurança.	Logs devem ser armazenados corretamente com informações de data, hora, usuário e ação realizada.	RF11, RF12, RNF1
TR05	Validar a geração de relatórios de uso após adição de novos recursos no sistema.	Relatórios devem ser gerados corretamente, incluindo novos dados adicionados ao sistema, com formatos suportados.	RF6, RNF6
TR06	Testar se a coleta de dados continua	Dados devem ser coletados e atualizados	RF2, RF7, RNF6

	funcionando com a frequência configurada pelo usuário.	no banco de dados conforme o intervalo definido pelo usuário.	
TR07	Verificar a notificação de eventos críticos via e-mail e SMS após alterações na API de envio de mensagens.	Notificações devem ser enviadas corretamente, chegando ao usuário em tempo hábil, sem duplicidade ou atraso.	RF8, RNF6
TR08	Testar se o sistema suporta o aumento no número de LPARs monitoradas sem degradação de desempenho.	Sistema deve responder em menos de 2 segundos ao monitorar até 50 LPARs simultaneamente, sem falhas ou lentidões.	RNF2, RNF3
TR09	Validar que a interface continua funcional em navegadores modernos após atualizações de frontend.	Interface deve funcionar corretamente em navegadores modernos (Chrome, Firefox, Edge), sem erros visuais ou de interação.	RNF7
TR10	Testar se administradores ainda conseguem criar, editar e remover usuários após atualização de permissões.	Gerenciamento de usuários deve funcionar sem erros, e permissões devem ser aplicadas corretamente para cada perfil.	RF9, RNF1
TR11	Garantir que parâmetros globais podem ser configurados e aplicados após atualizações no backend.	Alterações feitas nos parâmetros globais devem ser salvas e aplicadas no sistema sem erros ou inconsistências.	RF10, RNF6
TR12	Verificar a confiabilidade dos dados históricos após alterações no banco de dados.	Dados históricos devem ser exibidos corretamente, sem perda de informações ou inconsistências.	RF5, RNF6
TR13	Testar a funcionalidade de exclusão de alertas	Alertas desativados ou removidos não devem	RF4, RNF6

	desnecessários após atualização do módulo de alertas.	aparecer na interface ou enviar notificações, mantendo consistência.	
TR14	Validar que a API do mainframe continua enviando dados no formato JSON correto após atualizações.	Dados extraídos do mainframe devem ser processados corretamente, sem erros de formatação ou estrutura.	RF1, RNF3
TR15	Testar a recuperação de falhas do sistema em caso de indisponibilidade da API do mainframe.	Sistema deve exibir mensagem amigável e continuar funcional para outras operações, sem comprometer a experiência do usuário.	RNF5, RNF6
TR16	Validar a escalabilidade do sistema com até 500 LPARs monitoradas.	Sistema deve manter estabilidade, exibir dados no dashboard e enviar alertas sem degradação perceptível.	RF3, RNF2
TR17	Testar a integração do dashboard com o backend após alterações nos endpoints da API.	Dashboard deve exibir os dados em tempo real sem falhas, mesmo após alterações nos endpoints do backend.	RF3, RNF4
TR18	Garantir consistência de logs em operações simultâneas realizadas por diferentes perfis de usuário.	Todos os eventos devem ser registrados corretamente, sem omissões ou duplicidade em cenários concorrentes.	RF11, RNF1