



INSTITUTO NACIONAL DO SEGURO SOCIAL

ANEXO V PROVA DE CONCEITO

1. DA PROVA DE CONCEITO (PoC)

- 1.1. Este documento tem como objetivo definir os procedimentos e critérios para a realização da Prova de Conceitos (PoC) do sistema *web*, conforme as premissas e requisitos de funcionalidade estabelecidos neste documento.
- 1.2. A participação nos testes da PoC ficará limitada a até 2 (dois) representantes de cada licitante, que precisam ser indicados num prazo de 1 (um) dia útil, de antecedência à realização dos testes, como definido neste documento, respeitando os parâmetros definidos no item 2 - Avaliação da PoC e seus subitens.
- 1.3. A licitante classificada e habilitada provisoriamente em primeiro lugar, convocada nos termos do item 13.1 do Termo de Referência, deverá realizar PoC, conforme critérios estabelecidos neste anexo.
 - 1.3.1. Os ritos desta PoC poderão serão realizados por meio de ferramenta de videoconferência, a ser definida em momento oportuno pelo INSS, com comunicação aos interessados no prazo de 2 (dois) dias úteis de antecedência à sua realização.
- 1.4. Acompanhamento da PoC:
 - 1.4.1. A PoC será conduzida por uma equipe técnica designada, responsável pela avaliação do atendimento aos requisitos estabelecidos neste documento.
 - 1.4.2. Outras licitantes podem acompanhar a PoC mediante registro formal junto ao(a) pregoeiro(a), com antecedência de até 1 (um) dia útil, de antecedência ao início dos testes, como definido neste documento.
 - 1.4.3. Todas as despesas relacionadas à participação ou acompanhamento da PoC serão de responsabilidade de cada licitante.
 - 1.4.4. No caso de realização desta PoC por meio de ferramenta de videoconferência, o acompanhamento também seguirá o mesmo formato, conforme disposto no item 1.3.1.
- 1.5. Relatório de Resultados
 - 1.5.1. A equipe técnica elaborará um relatório que informará se o sistema *web* está de acordo com os requisitos e funcionalidades estabelecidos.

1.5.2. Será considerado aprovado com ressalva o sistema *web* que, mesmo possuindo todas as funcionalidades previstas, apresentar falha durante o teste.

1.6. Correções de Não Conformidades

1.6.1. Caso o sistema *web* seja aprovado com ressalvas, a licitante terá 3 (três) dias úteis, a contar da data de ciência do relatório, para realizar os ajustes necessários e disponibilizar o sistema para testes complementares.

1.6.2. Se o novo relatório indicar a não conformidade das correções, a licitante será desclassificada do processo licitatório e a próxima licitante na ordem de classificação será convocada para apresentar sua solução, num prazo de no máximo 02 (dois) dias úteis.

1.7. Declaração de Vencedora

1.7.1. Se o sistema *web* estiver consoante as especificações, a licitante será considerada aprovada para prosseguimento dos trâmites licitatórios.

1.8. Desclassificação

1.8.1. Se o sistema *web* não atender aos requisitos mínimos da PoC, a licitante será desclassificada, e a próxima licitante mais bem classificada será convocada para apresentar sua solução, no prazo estabelecido no item 1.6.2 acima.

1.9. Prazo de Apresentação

1.9.1. O sistema *web* aprovado na PoC deverá ser entregue em até 30 (trinta) dias corridos a partir do fornecimento dos dados pela Contratante, sob pena das sanções previstas na legislação em vigor, sem prejuízo de eventual rescisão unilateral do contrato.

1.10. Dispensa da PoC

1.10.1. A PoC poderá ser dispensada, a critério do INSS e devidamente justificada, caso a solução ofertada já tenha sido implementada na administração pública federal e validada pelo Instituto, desde que comprovada pelo licitante que atenda aos requisitos de funcionalidade explicitados neste termo.

2. AVALIAÇÃO DA POC

2.1. Os itens de avaliação da PoC estão a seguir elencados:

Nº	Requisitos de Acessibilidade	Atende	Não Atende	Observação
1	Acesso ao sistema via <i>Apple Safari</i>			
2	Acesso ao sistema via <i>Google Chrome</i>			
3	Acesso ao sistema via <i>Microsoft Edge</i>			
4	Acesso ao sistema via <i>Mozilla Firefox</i>			
5	Interface de acordo com o tipo de usuário (solicitante, aprovador e administrador)			

6	Conformidade com as diretrizes de acessibilidade WCAG 2.1 nível AA			
6.1	Navegação completa por teclado			
6.2	Suporte a leitores de tela			
6.3	Contraste mínimo adequado			
6.4	Legendas, descrições alternativas e formulários acessíveis			
6.5	Recursos avançados: modo alto contraste, atalhos personalizados, síntese de voz			
Nº	Requisitos de Disponibilidade e Desempenho	Atende	Não Atende	Observação
7	O sistema deve ser escalável para suportar o acesso simultâneo, sem degradação significativa do desempenho, de todos os usuários abrangidos pela contratação.			
8	Disponibilidade do sistema <i>web</i> mínima de 96% durante o período da PoC			
9	O desempenho será medido por um teste de tempo de resposta (RESPONSE TIME TESTING), no qual o sistema deverá apresentar tempo médio de resposta inferior a 2 segundos por página. A simulação de carga deverá considerar a quantidade estimada de 100 (cem) usuários simultâneos utilizando o sistema			
Nº	Requisitos de Segurança	Atende	Não Atende	Observação
10	O sistema deve cumprir integralmente as regulamentações da LGPD, incluindo a proteção de dados pessoais e a notificação de violações de dados			
11	Gestão granular de bloqueios			
11.1	Bloqueio por localização geográfica			
11.2	Bloqueio por horário			
11.3	Bloqueio por dispositivo			
12	<i>Logs</i> imutáveis e anonimizados			
13	Integração com Entra ID (Azure AD) corporativo e/ou Certificado Digital			
14	Autenticação Multifator (<i>MFA</i>) obrigatória			
15	Controle de sessão com <i>timeout</i> de 30 minutos (<i>web</i>) e 15 minutos (<i>mobile</i>)			
16	Bloqueio de múltiplas sessões simultâneas			
17	Sítio de hospedagem com certificado <i>SECURE SOCKETS LAYER (SSL)</i>			
18	Sistema <i>web</i> resistente a <i>CROSS-SITE REQUEST FORGERY (CSRF)</i>			
19	Sistema <i>web</i> resistente a <i>CROSS-SITE SCRIPTING (XSS)</i>			
20	Sistema <i>web</i> resistente a SQL INJECTION e injeções de código em geral			
21	Sistema <i>web</i> resistente a <i>Brute force</i>			
22	Mecanismos de proteção anti-robô e segurança comportamental			
22.1	CAPTCHA inteligente (reCAPTCHA v3)			
22.2	Rate <i>limiting</i> por IP e usuário			
22.3	Detecção e bloqueio de <i>bots</i>			
22.4	Análise de comportamento de usuário			

22.5	<i>Fingerprinting</i> de dispositivos			
22.6	Respostas automáticas a ameaças, com bloqueio e notificação			
23	Controle de acesso às funcionalidades do sistema <i>web</i> de acordo com perfis de usuários (<i>Broken Authentiction and Session Management</i>) e protegido de <i>Insecure Direct Object References</i>			
24	Acesso ao log de dados do sistema web e log de dados para Auditoria			
24.1	Log completo de todas as ações com usuário, IP, <i>timestamp</i> e dispositivo			
24.2	Logs de Auditoria completos			
24.3	Logs estruturados e integrados ao SIEM corporativo			
25	Plano de recuperação de desastres e <i>backup</i> regular de dados			
25.1	<i>Recovery Point Objective (RPO)</i> : 24 horas			
25.2	<i>Recovery Time Objective (RTO)</i> : 4 horas			
Nº	Requisitos de Funcionalidade	Atende	Não Atende	Observação
26	Cadastramento e alteração de unidades administrativas			
27	Cadastramento de todos os perfis de usuários			
28	Customização da interface para uso de logos governamentais e banners			
29	Inclusão de pedidos pelo usuário de materiais de consumo e expediente			
30	Inclusão de pedidos pelo usuário de gêneros alimentícios			
31	Inclusão de pedidos híbridos pelo usuário			
32	Manutenção do carrinho de compras com os itens selecionados após o <i>logout</i> do usuário			
33	Aprovação (total ou parcial) ou reprovação de pedidos pelo Aprovador com campo para justificativa			
34	Ateste (total ou parcial) ou conteste de pedidos com campo para justificativa			
35	Bloqueio automático de pedidos que excedam o limite orçamentário da unidade ou não atinjam o valor mínimo			
36	Permissão para o Administrador bloquear itens do catálogo para todas as unidades ou somente para unidades específicas			
37	Acompanhamento do status do pedido em tempo real por todos os perfis de usuários			
38	Envio de notificações automáticas por e-mail a cada evento relevante do pedido (ex: aprovação, faturamento, ateste pendente)			
39	Geração de relatórios com filtros personalizáveis pelo usuário			
40	<i>Dashboards</i> interativos e relatórios avançados com análise de tendências			
41	Extração de relatórios nos formatos CSV, PDF, Excel (.xlsx), JSON e XML			
42	<i>Upload</i> e <i>download</i> de documentos			
43	Abertura e acompanhamento de chamados de suporte (<i>Help Desk</i>)			
44	<i>Endpoints</i> obrigatórios para as APIs RESTful			
44.1	CRUD completo (GET/POST/PUT/DELETE) para todas as entidades			
44.2	Autenticação via <i>Bearer Token</i> (JWT)			

44.3	<i>Rate limiting:</i> 1000 requisições/hora por cliente			
44.4	Versionamento de API (v1, v2...)			
44.5	Documentação via OpenAPI/Swagger			
44.6	Disponibilização de Webhooks para notificação de eventos críticos do sistema			