CNPEM
Centro Nacional de Pesquisa
em Energia e Materiais

Especificação Técnica para Avaliação Competitiva

Integração de Plataforma de Cadastro de Itens 4MDG com ERP Protheus

Controle de Versão do Documento			
Versão	**Data**	**Responsável**	**Decrição**
1	18/08/2025	Luiz F. Rubin	Primeira versão

1. Objetivo / Declaração de Necessidade

Este documento apresenta os principais requisitos e orientações para a contratação de fornecedor especializado para a implantação e configuração de processo (API – Application Programming Interface) de integração entre a plataforma de cadastro e padronização de itens 4MDG e o ERP Totvs Protheus do CNPEM.

2. Orientações Gerais

2.1. Glossário e Conceitos

Seguem os principais termos, conceitos, sistemas e processos relevantes, para o melhor entendimento deste documento.

- **N/A**

2.2. CNPEM

O Centro Nacional de Pesquisa em Energia e Materiais (CNPEM) é uma organização social supervisionada pelo Ministério da Ciência, Tecnologia e Inovações (MCTI). Localizado em Campinas-SP, possui quatro laboratórios referências mundiais e abertos à comunidade científica e empresarial, como também a escola de ensino superior interdisciplinar em Ciência, Tecnologia e Inovação (Ilum). O Laboratório Nacional de Luz Síncrotron (LNLS) opera a única fonte de Luz Síncrotron da América Latina, o Sirius.

2.3. Fornecedor

Espera-se um relacionamento colaborativo e flexível com fornecedor, sendo considerado diferencial para esta contratação os seguintes pontos, mas o fornecedor pode acrescentar outros:

- Disponibilidade para reuniões presenciais previamente combinadas. Porém a maioria dessas deverão ser virtuais;
- Canal único para comunicação, acompanhamento e gestão das demandas de garantia, suporte, manutenção e melhorias, tanto em período de garantia, quanto de suporte continuado (por exemplo: Trello, Jira etc);
- Envio de relatórios periódicos detalhados de acompanhamentos de demandas, o seu progresso e a data estimada de conclusão;
- Propor soluções e realizar pesquisa sob demanda, como de componentes de software, integrações e outras soluções;
- Disponibilidade para apoio e alinhamento com outros fornecedores. Por exemplo, no desenvolvimento de uma nova ferramenta, pode haver a necessidade de integração com outros sistemas sob gestão de outros fornecedores.
- Realizar treinamentos sob demanda, conforme capacidade do fornecedor.
- Disponibilizar desenvolvedor dedicado, em relação às horas contratadas.
- Atender aos finais de semana e feriados quando necessário.
- Fazer levantamento e o refinamento de requisitos quando demandado.

3. Escopo da Contratação

3.1. Objetivo

O CNPEM deseja contratar um projeto de implementação de software para integração de plataformas, envolvendo os processos de levantamento de requisitos, desenvolvimento, testes de aceitação em ambientes de testes e implantação em ambiente produção.

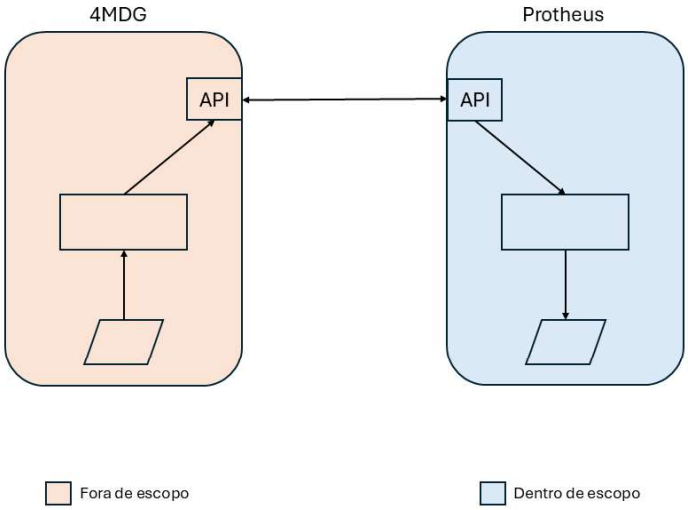
3.2. Detalhamento Técnico

3.2.1. O que será atendido

O projeto atenderá apenas à implementação do processo de integração relacionada com o ERP Totvs Protheus, ou seja, todo desenvolvimento será voltado para o recebimento de mensagens (requests) por web service do Protheus e o processamento das informações com atualização de tabelas no ERP Protheus.

3.2.2. O que não será atendido

O projeto não atenderá à implementação de customização da plataforma 4MDG para envio de informações (requests) para a plataforma ERP Totvs Protheus.



3.2.3. Informações técnicas

A implementação deverá seguir os princípios de design da arquitetura REST (REpresentational State Transfer), respeitando os métodos (POST, GET, PUT, DELETE), o conteúdo em formato JSON (Java Script Object Notation) e os códigos de status de resposta (HTTP Status Code), de acordo com normas e padrões de integração da plataforma ERP Totvs Protheus.

Para maiores detalhes de segurança, como autenticação, geração de token, chave e liberação de portas de acesso, a definição será feita após a contratação, através de detalhamento técnico entre a empresa contratada e a equipe técnica do CNPEM.

3.2.4. Tipos de Integração

Este projeto contemplará dois tipos de integração:

3.2.4.1. Criação de novo item

A API receberá um request de integração, contendo todos os campos necessários para o cadastro de um novo item no Protheus. Deverá retornar mensagem/status de erro caso esse item já exista, se algum campo obrigatório não seja informado, ou se houver alguma restrição de sistema.

3.2.4.2. Atualização de Item

A API receberá um request de integração, contendo todos os campos que devem ser atualizados no ERP

Protheus; deve retornar mensagem/status de erro caso o item a ser atualizado não exista no ERP Protheus ou haja alguma inconsistência em algum dos campos.

3.2.5. Envio de Dados

O envio de dados será realizado através de comandos POST (para criação de novos itens) ou de comandos PUT (para alteração de itens já existentes), com conteúdo em JSON com as informações indicadas na tabela abaixo. O endereço da URL e as informações para autenticação da integração serão informados ao fornecedor na fase de homologação da solução.

3.2.6. Informações Enviadas para Protheus

REF	Nome do campo	Exemplo	Informações adicionais	Tabela Protheus
1	Familia	MC	RM - NF Remessa de Material; PQ - Amostra para Pesquisa; EA- Energia Elétrica e Água;MC- Material de Consumo;ST- Serviços de Terceiros;VG- ViagensViagens, Eventos e Cursos;FD- Faturamento Direto;IV- Investimentos;PE- Pessoal	B1_ZZFAM
2	Codigo do Produto		Código Alfanumerico	B1_COD
3	Tipo de Produto	CT	CT-Custeio; IV-Investimento; PE-Pessoal	B1_TIPO
4	Tipo Mat	1	1=Material;2=Servico	B1_ZZTM
5	Grupo	MAC	RM-NF Remessa de Material; AMPQ-Amostra para Pesquisa; FEE-Energia Elétrica e Água; ALM-Alimentação; CED-Comunicação e Divulgação; INL-Insumos laboratoriais; **MAC-**Manutenção e Conservação; MTE-Material de expediente; MTI-Material de informática; SPO-Segurança Patrimonial e Ocupacional; ALM-Alimentação; CED-Comunicação e Divulgação; CAA-Consultorias, Assessorias e Auditoria; DAL-DESPESAS DE ALUGUEIS; MAC-Manutenção e Conservação; SPO-Segurança Patrimonial e Ocupacional; SAD-Serviços Administrativos; SIN-Serviços de Informática; TRG-Transportes em geral; EVE-Eventos;	B1_GRUPO

			VIA-Viagens; FD-Faturamento Direto; INFR-Equipamentos de Infraestrutura; LAB-Equipamentos de Laboratório; INFO-Informática; MAB-Material Bibliográfico;	
6	Subgrupo	06	06 = Material Manutenção	B1_ZZSUBGR
7	Desc. Comp		250 caracteres	B1_ZZDESCO
8	Descricao curta		60 caracteres	B1_DESC
9	Descricao Padronizada		3000 caracteres	B1_ZZCMP8
10	Unidade de Medida	UN	Ex: UN = Unidade	B1_UM
11	Tipo de Conversao da UM	M	M=Multiplicador;D=Divisor	B1_TIPCONV
12	Origem Cadastro	4MDG		B1_ZZORIG
13	Descricao em Ingles		Somente para produtos importados	B1_VM_I
14	Descricao da LI			B1_VM_GI
15	Aplicacao			B1_ZZAPLIC
16	Codigo Fabricante			B1_ZZPRTN
17	Fabricante			B1_FABRIC
18	Bloqueio de Tela	2	1=Sim;2=Nao	B1_MSBLQL
19	Atualiza Estoque	N	S=Sim; N=Nao	B1_ZZEST
20	Bloqueio Fluig	2	1=Sim;2=Nao	B1_ZZLIBUS
21	Numero Processo Ecm		Em branco	B1_ZZIDPRC
22	Anuente	2	1=Sim;2=Nao	B1_ANUENTE
23	Calcula INSS	N	S=Sim;N=Nao	B1_INSS
24	Retem PIS	2	1=Sim;2=Não	B1_PIS
25	Retem CSLL	2	1=Sim;2=Não	B1_CSLL
26	Retem COFINS	2	1=Sim;2=Não	B1_COFINS
27	Nomenclatura Ext.Mercosul	00000000	8 dígitos sem pontuação	B1_POSIPI
28	Origem do produto	0	0=Nacional;1=Importado;	B1_ORIGEM
29	Produto Importado	N	S=Sim;N=Nao	B1_IMPORT
30	Conta Contabil dn Prod		Em branco	B1_CONTA
31	Cta.Custo		Em branco	B1_ZZCTAC
32	Cta.Despesa		Em branco	B1_ZZCTAD
33	Cta.Orcamentaria		Em branco	B1_ZZCO
34	Cta.Convenio		Em branco	B1_ZZCTAZ
35	Foto do Produto			B1_BITMAP
36	Codigo de Serviço do ISS	12.03	Quando Tipo Mat = Serviço é realizado o preenchimento Ex: 14.01 ou 08.02 ou XX.XX	B1_CODISS
37	Segunda Unidade de Medida	PC	Ex: PC = PECA	B1_SEGUM

38	Controle RAD	1	1=Sim;2=Nao	B1_ZZCMP1
39	Controle PC	2	1=Sim;2=Nao	B1_ZZCMP2
40	Controle EX	2	1=Sim;2=Nao	B1_ZZCMP3
41	Controle PF	1	1=Sim;2=Nao	B1_ZZCMP4
42	Controle ANVISA	2	1=Sim;2=Nao	B1_ZZCMP5
43	Controle MAPA	2	1=Sim;2=Nao	B1_ZZCMP6
44	Controle IBAMA	1	1=Sim;2=Nao	B1_ZZCMP7

3.3. Exigências

A contratada deverá também:

- Atestar capacidade técnica de atendimento indicando trabalhos semelhantes e o contato de outros clientes de porte igual ou superior para averiguação do CNPEM.
- Concordar/assumir que todo conteúdo, código fonte e artefatos que fizerem parte das soluções sob gestão do fornecedor, mesmo que construído por ele, pertencem ao CNPEM;
- Manter a gestão de versão dos artefatos construídos no ambiente disponibilizado pelo CNPEM e na plataforma de versionamento de software do CNPEM (Gitlab);
- Disponibilizar seis meses de garantia (sem custo) a partir da entrada em produção dos desenvolvimentos especificados;
- Garantir que a demanda seja extensivamente testada previamente no ambiente de desenvolvimento antes da comunicação de entrada em homologação. A posterior publicação em produção deverá ocorrer somente após autorização;
- Envio de relatórios periódicos detalhados (semanais e sob demanda) de acompanhamentos de demandas, o seu progresso e a data estimada de conclusão;

4. Segurança da Informação e Privacidade dos Dados

A garantia da segurança do sistema é essencial para proteger a confidencialidade, integridade e disponibilidade dos dados e informações dos usuários, bem como para evitar danos e prejuízos decorrentes de violações de segurança. O desenvolvimento seguro deve ser incorporado em todas as fases do ciclo de vida do software, desde a análise de requisitos até o teste e a implantação, para garantir que o sistema atenda aos mais altos padrões de segurança.

1.1. O sistema deve ser projetado e implementado com medidas de segurança apropriadas para proteger os dados e as informações dos usuários. Isso inclui:

- Autenticação: O sistema deve possuir um mecanismo seguro de autenticação, garantindo que apenas usuários autorizados tenham acesso ao sistema.
- Controle de acesso: As permissões de acesso devem ser configuradas corretamente, garantindo que cada usuário tenha acesso apenas às funcionalidades e dados apropriados ao seu perfil.
- Criptografia: Dados confidenciais, como senhas e informações pessoais, devem ser armazenados e transmitidos de forma criptografada para evitar acesso não autorizado.
- Prevenção de ataques: O sistema deve implementar mecanismos de detecção e prevenção de ataques.
- Auditoria e rastreamento: Deve ser possível rastrear e auditar as atividades realizadas no sistema, registrando informações como data, hora, usuário e ação executada.
- Conformidade com regulamentações: O sistema deve estar em conformidade com as regulamentações e políticas de segurança relevantes, como a LGPD (Lei Geral de Proteção de Dados) ou outras regulamentações específicas do setor.

- Pró atividade na busca de atualizações de segurança que envolvem componentes da aplicação.

1.2. Testes de segurança – CNPEM:

O CNPEM irá realizar testes de vulnerabilidades e de penetração para identificar possíveis vulnerabilidades antes do lançamento do software no ambiente de produção, de forma periódica e para novas versões do sistema.

- Testes de vulnerabilidade:

Será disponibilizado relatório de análise de vulnerabilidades completo, documentando todas as vulnerabilidades identificadas e sua classificação de gravidade, sendo que os riscos estão classificados abaixo e com seus respectivos critérios de aceite:

Alto – Não Aceito
Médio – Não Aceito
Baixo – A ser avaliado pela equipe de cibersegurança do CNPEM
Informativo – Aceito

A contratada deverá providenciar a implementação de medidas corretivas para todas as vulnerabilidades identificadas como não aceitas durante a análise.
Após as ações tomadas pela contratada, o CNPEM irá realizar a revisão e aprovação do relatório de análise de vulnerabilidade por especialistas em segurança.

- Testes de penetração:

Será disponibilizado relatório de testes de penetração detalhado, incluindo todas as descobertas de vulnerabilidades identificadas, sendo que os riscos estão classificados abaixo e com seus respectivos critérios de aceite:

Alto – Não Aceito
Médio – Não Aceito
Baixo – A ser avaliado pela equipe de cibersegurança do CNPEM

A contratada deverá providenciar a documentação das ações tomadas para explorar as vulnerabilidades, demonstrando a eficácia das medidas de segurança implementadas, além de providenciar a correção de todas as vulnerabilidades identificadas durante os testes de penetração.
Após as ações tomadas pela contratada, o CNPEM irá realizar a revisão e aprovação do relatório de testes de penetração por especialistas em segurança.

1.3. Testes de segurança – Contratada:

A contratada deverá realizar as avaliações e testes abaixo, para identificar possíveis problemas antes do lançamento do software no ambiente de produção, de forma periódica.

- Análise de código:

Implementação das correções necessárias para as vulnerabilidades de segurança identificadas no código.
Revisão e análise de segurança de código pelos desenvolvedores.

- Teste de autenticação e autorização:

Verificação de que todos os mecanismos de autenticação e autorização estão funcionando corretamente.
Teste de diferentes cenários de autenticação e autorização, incluindo tentativas de acesso não autorizado.
Correção de quaisquer falhas ou vulnerabilidades identificadas durante os testes.

- Teste de criptografia:

Verificação de que todos os pontos relevantes do sistema estão utilizando criptografia de forma adequada.
Teste de transmissão de dados sensíveis para garantir a criptografia adequada.
Correção de quaisquer problemas relacionados à criptografia identificados durante os testes.

- Teste de manipulação de dados:

Verificação de que o sistema é robusto contra tentativas de manipulação de dados.
Correção de quaisquer vulnerabilidades ou falhas identificadas durante os testes de manipulação de dados.

- Teste de sessão e gerenciamento de estado:

Verificação de que as sessões de usuário são gerenciadas de forma segura.
Teste de diferentes cenários de sessão para garantir a autenticação adequada e o controle de estado.
Correção de quaisquer vulnerabilidades ou falhas identificadas durante os testes.

- Teste de recuperação de falhas:

Verificação de que o sistema é capaz de se recuperar adequadamente de falhas e interrupções inesperadas.
Teste de simulação de falhas e recuperação para verificar a eficácia das estratégias adotadas.
Correção de quaisquer problemas relacionados à recuperação de falhas identificados durante os testes.

2. Qualidade do desenvolvimento e das entregas da contratada

A qualidade das entregas dos itens desenvolvidos deverá seguir os seguintes testes e avaliações:

- Testes de sistema (ambiente de desenvolvimento): Os testes de sistema são executados para verificar se o sistema completo atende aos requisitos funcionais e de desempenho especificados. Esses testes são realizados em um ambiente semelhante ao de produção e podem incluir cenários de uso realistas para verificar se o software se comporta corretamente.
    - Obs.: Testes de aceitação (ambiente de homologação): Os testes de aceitação são realizados pelos stakeholders ou usuários finais para validar se o software atende aos critérios de aceite e requisitos do negócio. Esses testes são projetados para simular cenários reais de uso e verificar se o software atende às expectativas e necessidades dos usuários. Esses testes servirão como critério de aceite para a entrada de determinado item em ambiente de produção.
- Revisões de código: As revisões de código poderão ser realizadas por outros membros da equipe de desenvolvimento para identificar problemas de qualidade, como código mal estruturado, falta de comentários, uso inadequado de variáveis ou funções, entre outros. Essas revisões ajudam a garantir a qualidade e a consistência do código fonte.
- Monitoramento e registro de erros: Durante o uso do software em um ambiente de produção ou teste, é importante monitorar e registrar quaisquer erros, falhas ou comportamentos inesperados. Essas informações podem ser usadas para identificar problemas e melhorar a qualidade do software.

Campinas, 16 de setembro de 2025.

Luiz Fernando Rubin
SI – Sistemas de Informação

Cintia Barbosa Rodrigues Brites
GCAD – Gestão de Cadastros