CNPEM

Centro Nacional de Pesquisa
em Energia e Materiais

Especificação Técnica para Avaliação Competitiva

Saneamento e Padronização Descritiva de Materiais com Implantação de Central de Cadastro e Governança de Dados Própria

Controle de Versão do Documento			
Versão	**Data**	**Responsável**	**Decrição**
1	30/08/2024	Luiz Fernando Rubin/Cíntia Brites	Primeira versão

1. Objetivo / Declaração de Necessidade

Este documento apresenta os principais requisitos e orientações para a contratação de fornecedor especializado em saneamento e governança de dados de materiais e serviços, que possua plataforma/software para implantação e integração de processos de Padronização Descritiva de Materiais (PDM) e Serviços (PDS) na Central de Cadastro CNPEM.

2. Orientações Gerais

2.1. Glossário e Conceitos

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

- **Gestão de Materiais**: Governança de dados de materiais e serviços utilizados pelo CNPEM.
- **PDM:** Padronização Descritiva de Materiais. Método extremamente eficaz para a gestão de materiais.
- **PDS:** Padronização Descritiva de Serviços. Método extremamente eficaz para a gestão de serviços.
- **NCM:** Nomenclatura Comum do Mercosul.
- **Saneamento:** Higienização da base cadastral, com técnica de padronização de descrições, enriquecimento de dados, unificação, eliminação de duplicidades.

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).

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 referentes ao processo de saneamento de dados, o seu progresso e a data estimada de conclusão;
- Disponibilidade para apoio e alinhamento com outros fornecedores em caso de integrações com a plataforma ERP Totvs Protheus utilizada pelo CNPEM.
- Realizar treinamentos sob demanda, conforme capacidade do fornecedor.

3. Escopo da Contratação

3.1. Objetivo

O CNPEM deseja automatizar a atividade de cadastro de materiais e serviços, Central de Cadastro equipe própria, implantando plataforma de Padronização Descritiva de Materiais e Serviços, capaz de integrar com ERP Protheus, permitindo a centralização e sincronização de informações confiáveis entre sistemas, colaborando com a cadeia de suprimentos e demais processos. Também, objetiva contratar o saneamento terceirizado da base atual do CNPEM com mesmo fornecedor da plataforma.

Este documento foi assinado eletronicamente por Cibele de Souza Goncalves.
Para verificar as assinaturas vá ao site https://vertsign.portaldeassinaturas.com.br:443 e utilize o código 4985-8189-1F61-DED1.

Esses processos proveem os benefícios de melhoria da qualidade de dados, aumento da produtividade, embasamento para tomada de decisões e maior agilidade nos processos.

Para esse cenário, consideram-se os pontos abaixo:

- O fornecedor indicará opções contratuais de assinatura e licenciamento da solução/plataforma;
- O CNPEM escolherá a opção contratual que melhor se adeque às necessidades e demandas de serviço;
- O CNPEM pagará mensalmente pela utilização/assinatura da plataforma de acordo com a opção contratual escolhida.

3.2. Descrição das Funcionalidades e Requisitos

Abaixo a relação das funcionalidades e requisitos necessários para atendimento dessa proposta pelo fornecedor:

3.2.1 - Software

- Software de fácil usabilidade e interface intuitiva, que seja capaz de integrar com o Protheus e que tenha suporte oferecido pelo fornecedor;
- A plataforma deverá nos possibilitar trabalhar todas as informações necessárias de cadastro, tais como descrições e campos que serão integrados ao ERP Protheus. Recomenda-se que a escolha da plataforma seja da mesma empresa contratada para saneamento;
- Licença de Uso – Mínimo 100 licenças. A disponibilidade de acessos deve contemplar:
  - usuários chave solicitantes do cadastro
  - analistas
  - aprovadores

  De preferência que não tenha limite de licenças para que possamos definir o melhor recurso para o CNPEM; porém, caso haja limite, o fornecedor deve indicar as opções para o CNPEM definir qual se adequa às suas necessidades;
- Campos para informação – a plataforma deve contemplar:
  - campo para descrição informativa
  - aplicação
  - comentários adicionais
- Campo classificativo – possibilitar classificar a solicitação de cadastro:
  - Normal
  - Urgente
  - Urgentíssimo
- Campo de Descrição Padronizada – visualização dos campos de descrições curta (abreviada) e completa, conforme regras de PDM, e nos idiomas PT e EN, no mínimo;
- Pesquisa inteligente – Possibilitar diversas formas de pesquisas para identificação de itens cadastrados; o fornecedor deve indicar as diferentes opções/formas de pesquisa que a solução contempla;
- Duplicidade – deverá haver check de duplicidade, no momento da solicitação de cadastro de um novo item, conforme características preenchidas;
- Cadastro de PDM – Contemplar visão para inserir novo ou editar, definindo as regras necessárias, possibilitando criar árvore de categorias/subcategorias;
- Seleção de PDM – ser de fácil pesquisa e interface objetiva para características. Simples acesso quanto a opções dos valores, e que estes sejam selecionáveis.
  Contemplar campo aberto para inserir novo valor pelo usuário solicitante, caso não esteja disponível valor selecionável desejado, para que a central de cadastro possa verificar, validar e inserir; a nova opção deverá ficar em destaque até o aceite;

- Campos customizáveis – a ferramenta deverá contemplar os campos customizáveis e necessários do ERP Protheus, a serem mapeados.
  Desta forma, a possibilidade de trabalhar todas as informações em uma base única e realizar a integração por completo sem necessidade de editar e/ou preencher campos posteriormente, trará ganho em tempo e processo;
- Campo para Classificação Fiscal NCM – contemplar campo para classificar NCM, de modo selecionável (carregado com a tabela TIPI atualizada e que possa se manter atualizada), e que permita definir regras para PDM´s;
- Integração – o software deverá integrar com ERP Protheus. As integrações deverão ocorrer em tempo real. Após a integração, o código Protheus deverá ser retornado para o software. O fornecedor deverá informar como essa integração será realizada;
- Relatórios – disponibilizar relatórios/dashboards para acompanhamento e visualização geral do processo;
- Anexos – capacidade para inserir detalhes relacionados aos produtos, como fotos, especificações técnicas, desenhos e manuais. O fornecedor deverá informar a capacidade e formato dos arquivos anexados;
- Implantação – o software deve ser fácil e rápido de implantar. O fornecedor deverá informar estimava de prazo para este processo já contemplando a integração;
- Workflow – possibilitar a utilização de workflow personalizado para atender as demandas do CNPEM. Destacar se há limites de áreas;
- E-mail – contemplar disparo de e-mail informando status diário ou de conclusão do cadastro para os solicitantes e para áreas do processo de workflow;
- Gestão de Usuários – a plataforma deve permitir a criação de perfis de usuário com permissões específicas e funções diferenciadas;
- Segurança – garantir a segurança e a integridade dos dados, protegendo informações sensíveis contra acessos não autorizados;
- Backup – o fornecedor deverá informar a política de backup que o sistema possui;
- Desenvolvimento e homologação – o fornecedor deve prover a solução em diferentes ambientes para desenvolvimento, testes e homologação das soluções para o CNPEM, detalhando a política de utilização dos diferentes ambientes;
- Treinamento – o fornecedor deverá indicar como será realizado o treinamento dos usuários do sistema para a equipe do CNPEM;
- Manutenção – o fornecedor deverá detalhar o processo de manutenção e de atualização do sistema para os diferentes ambientes (desenvolvimento, homologação, produção) do CNPEM;
- Controle de Versão – garantir que a versão mais atualizada esteja em utilização;
- Documentos e guias – a plataforma deve possuir guias e manuais de utilização, solução de dúvidas mais frequentes e exemplos de configurações e definições de cadastros, assim como documentação técnica para configuração de processos de integração, como APIs, Web Hooks e Web Services;
- Diferenciais – descrever funcionalidades consideradas diferenciais, não citadas acima, que possam contribuir com o atendimento a futuras necessidades do CNPEM.

3.2.2 - Saneamento

- Setup – o fornecedor deverá informar como será realizado o processo de setup desta etapa;
- Categorização - O fornecedor deverá classificar os itens utilizando árvore de materiais 3 níveis;
- PDM´s - O fornecedor deverá elaborar e disponibilizar os PDM´s para padronização dos itens;
- Descrições - O fornecedor deverá padronizar as descrições conforme abaixo:

Este documento foi assinado eletronicamente por Cibele de Souza Goncalves.
Para verificar as assinaturas vá ao site https://vertsign.portaldeassinaturas.com.br:443 e utilize o código 4985-8189-1F61-DED1.

- Curta – contemplando as devidas abreviações e respeitando a quantidade de caracteres do campo conforme ERP Protheus;
- Longa – completa, detalhando as características e valores, sem limite de caracteres conforme padrão do ERP Protheus;

- Unidade de Medida – O fornecedor deverá revisar as unidades de medidas básica conforme descrição padronizada.
- Grupo de Mercadorias – O fornecedor deverá classificar o grupo de mercadorias, conforme níveis de categorização.
- Lista de PDM – O fornecedor deverá disponibilizar a lista dos PDM´s utilizados no processo de saneamento, com as devidas definições e regras, como bônus.
- Unificação/Duplicidades – O fornecedor deverá unificar as descrições e eliminar as duplicidades e/ou Multiplicidades;
- Obsolescência - O fornecedor deverá informar a existência de item obsoleto, utilizando como base referência/part number;
- Carga – O fornecedor disponibilizará as informações necessárias para carga no ERP Protheus.

3.3. Exigências

A contratada deverá também, relacionada a suporte e sustentação da solução:

- Apresentar SLA de atendimento, a ser aprovado e validado pelo CNPEM;
  - Ficam sugeridos os seguintes tempos de resposta para os chamados de suporte, de acordo com as seguintes severidades:
    - Crítica (sistema inoperante ou criticamente comprometido): 4 horas úteis.
    - Grave (sistema parcialmente inoperante): 8 horas úteis.
    - Relevante (sistema operante, com ocorrência de baixo impacto): 16 horas úteis.
    - Consulta (sistema operante, sem ocorrências, somente para consultas informativas): 24 horas úteis.
  - O tempo de resposta corresponde ao tempo máximo de resposta em horas úteis (horas precedentes ao horário comercial em dias úteis) ao chamado aberto.
  - A contratada será obrigada a cumprir o SLA, responder a todos os chamados de suporte abertos ao longo do contrato.

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.

4.1. 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.

Este documento foi assinado eletronicamente por Cibele de Souza Goncalves.
Para verificar as assinaturas vá ao site https://vertsign.portaldeassinaturas.com.br:443 e utilize o código 4985-8189-1F61-DED1.

- 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.
- Atualização e manutenção do sistema (exceto sistema operacional – este é de responsabilidade do CNPEM para plataformas "on premise")
- Pró atividade na busca de atualizações de segurança que envolvem componentes da aplicação.

4.2. 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.

4.3. 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.

Este documento foi assinado eletronicamente por Cibele de Souza Goncalves.
Para verificar as assinaturas vá ao site https://vertsign.portaldeassinaturas.com.br:443 e utilize o código 4985-8189-1F61-DED1.

- 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.

Campinas, 30 de agosto de 2024.

Luiz Fernando Rubin
SI – Sistemas de informação

Cintia Barbosa Rodrigues Brites
DPA – Especialista de Cadastro

Cibele de Souza Gonçalves
DPA – Gerente de Processos Administrativos

Este documento foi assinado eletronicamente por Cibele de Souza Goncalves.
Para verificar as assinaturas vá ao site https://vertsign.portaldeassinaturas.com.br:443 e utilize o código 4985-8189-1F61-DED1.

PROTOCOLO DE ASSINATURA(S)

O documento acima foi proposto para assinatura digital na plataforma Portal Vertsign. Para verificar as assinaturas clique no link: https://vertsign.portaldeassinaturas.com.br/Verificar/4985-8189-1F61-DED1 ou vá até o site https://vertsign.portaldeassinaturas.com.br:443 e utilize o código abaixo para verificar se este documento é válido.

Código para verificação: 4985-8189-1F61-DED1

Hash do Documento

C723E2582E5D492A8165D15A8458FE47E75E04F4B0AEF272D992CC3D19D5F19C

O(s) nome(s) indicado(s) para assinatura, bem como seu(s) status em 16/09/2024 é(são) :

☑ Cibele de Souza Goncalves - ***.919.308-** em 06/09/2024 10:05 UTC-03:00
Tipo: Assinatura Eletrônica

Evidências

Client Timestamp Fri Sep 06 2024 10:05:24 GMT-0300 (Horário Padrão de Brasília)
Geolocation Location not shared by user.
IP 201.82.181.184
Identificação: Autenticação de conta
Assinatura:

Hash Evidências:

FD0F22C2FCE15F5643BFDC4CFCC50E88FF358057872F2238EE8ED57EA27DD136