CNPEM
Centro Nacional de Pesquisa
em Energia e Materiais

Especificação Técnica para Avaliação Competitiva

Cadastro e Homologação de Fornecedores

Controle de Versão do Documento			
Versão	**Data**	**Responsável**	**Decrição**
1	10/09/2024	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 gestão de cadastro e homologação de fornecedores, que possua plataforma/software para implantação e integração de processos da 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 Fornecedores**: Governança de dados utilizados pelo CNPEM. Processo essencial para garantir que a empresa obtenha os melhores produtos e serviços de seus fornecedores, mantendo a qualidade, eficiência e custo-benefício.
- **Homologação:** Processo de avaliação e aprovação de fornecedores para garantir que eles atendam aos requisitos e definições do CNPEM.
- **Monitoramento:** Verificações e atualizações contínuas dos fornecedores para garantir que eles mantenham as definições acordadas.

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 fornecedores implantando ferramenta de Gestão e Homologação de Fornecedores capaz de gerir, armazenar documentos e integrar com ERP Protheus, permitindo a centralização, monitoramento e sincronização de informações confiáveis entre sistemas, colaborando com a qualificação e análise de tomada de decisão da cadeia de suprimentos e demais processos.
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:

- A contratada 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 pela contratada;
    - A plataforma deverá nos possibilitar trabalhar todas as informações necessárias de cadastro, tais como dados cadastrais e campos que serão integrados ao ERP Protheus. E deverá ser a forma única de solicitação de cadastro.
- Pré-cadastro – a contratada deverá disponibilizar link público, para inclusão no site do CNPEM, possibilitando que potenciais fornecedores realizem o pré-cadastro e o grupo de compras possa acessá-los. O potencial fornecedor deverá ter acesso as categorias.
- Solicitação/ Requisição – Todas as solicitações de cadastro deverão ser realizadas através da plataforma, que deverá disponibilizar:
    - Seleção Tipo de Fornecedor
        - Nacional PJ – campo chave CNPJ; os dados básicos cadastrais já deverão ser carregados automaticamente; Diferencial: possibilitar pesquisa por CNPJ ou razão social, indicando a existência na base.
        - Nacional PF – campo chave CPF, nome completo e campos necessários do ERP Protheus;
        - Internacional – Razão social, TIN-Tax Information Number (de forma opcional) e campos necessários do ERP Protheus;
    - Campos configuráveis – possibilitar inclusão de campos necessários para classificação do fornecedor e direcionamento de fluxo de validações;
    - Convite ao Fornecedor – contemplar envio de convite ao processo de cadastro e homologação via Portal do Fornecedor. Caso a categoria selecionada contemple apenas consulta publicas automáticas, o envio do convite ao fornecedor não se fará necessário;
    - Portal do fornecedor:
        - permitir configurar com a identidade visual (Razão social, imagens) do CNPEM para facilitar a identificação e confiabilidade pelo fornecedor.
        - Possibilitar suporte ao fornecedor para acesso e dúvidas quanto a funcionalidade do portal.
- Homologação – garantir a qualificação dos fornecedores através de fluxo definido pelo CNPEM, contemplando:
    - Categorias – permitir inclusão de categorias customizadas para definição de documentos, consultas públicas de validação automáticas e/ou documentos do fornecedor com validação interna. Possibilitar autonomia para configurações e atualizações das categorias pelo responsável CNPEM;
    - Consultas Públicas – disponibilizar lista das consultas públicas automáticas que serão realizadas para CNPJ;
    - Campos configuráveis – possibilitar:

        - configurar pontuação dos documentos por importância/relevância, para definição de score do fornecedor para tomada de decisão;
        - agrupar documentos por área validadora;
        - customizar documentos e questionamentos aos fornecedores, configurando conforme necessidade de anexos, justificativas, escolha, múltipla escolha etc.
    - Fluxos de aprovação/workflow – permitir configurações customizadas para atendimento as necessidades do CNPEM.
        - por exceção – permitir envio de fluxo para avaliação por exceção, podendo escalar a validação de forma estratégica.
        - automático – as áreas validadoras deverão receber automaticamente, via e-mail, alerta para tomada de ação.
    - Bloqueio de cadastro – possibilitar o bloqueio ou desbloqueio do fornecedor, integrando a decisão ao ERP Protheus;
    - Histórico – deverá registrar todo o processo de relacionamento e comunicação com o fornecedor, tais como notificações, atualizações, aprovações e que possibilite rastreamento e auditoria.
    - Relatório – permitir emissão de relatórios do processo de homologação, podendo também considerar pesquisas inteligentes através de filtros (categoria, status, solicitantes etc.);
- Monitoramento – a plataforma deverá controlar, automaticamente, atualizações e vencimentos de documentos com data definida. Deverá disparar alertas de pendências antecipados ao vencimento, com envio de e-mails ao fornecedor e solicitante CNPEM. Também deverá permitir que o CNPEM solicite regularização manualmente e/ou justificativa da pendência aos fornecedores para avaliação interna.
- Performance do fornecedor – possibilitar avaliar a performance dos fornecedores, permitindo customização conforme necessidade CNPEM.
- Indicadores/Dashboards – a ferramenta deverá disponibilizar indicadores/dashboards, permitindo exportações das informações. A contratada deverá informar formato.
- Gestão de Usuários – possibilitar a liberar, bloqueio, exclusão de usuários pelo responsável CNPEM. Permitir agrupar por área e perfil. Informar se há limite de acessos. A ferramenta deverá garantir os acessos das áreas somente em suas respectivas responsabilidades.
- Segurança - garantir a segurança e a integridade dos dados, protegendo informações sensíveis contra acessos não autorizados.
- Integração – o software deverá integrar com ERP Protheus, contemplando os novos cadastros e atualizações. As integrações deverão ocorrer em tempo real. Após a integração, o código Protheus deverá ser retornado para o software. A contratada deverá informar como essa integração será realizada;
- Implantação – deverá informar o prazo para implantar a plataforma no CNPEM e estimar o prazo considerando a integração.
- Carga base atual de fornecedores – a contratada deverá auxiliar com o carregamento dos fornecedores na plataforma. Especificar qual formato e processo.
- Backup – o fornecedor deverá informar a política de backup que o sistema possui;
- Desenvolvimento e homologação – a contratada 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 – a contratada deverá indicar como será realizado o treinamento dos usuários do sistema para a equipe do CNPEM;
- Manutenção – a contratada deverá detalhar o processo de manutenção e de atualização do sistema para os diferentes ambientes (desenvolvimento, homologação, produção) do CNPEM;

- Atualizações Sistêmicas – a plataforma deverá manter-se atualizada, conforme tendencia do mercado, permitindo insights e possibilitando estar em conformidade com as legislações e exigências documentais.
- 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, tais como verificação automática de dados bancários, análise ESG, Single Sign-On (SSO) etc.

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.
- 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 politicas 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.

- 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, 10 de setembro de 2024.

Luiz Fernando Rubin
SI – Sistemas de informação

Cíntia Barbosa Rodrigues Brites
DPA – Especialista de Cadastro

Cibele de Souza Gonçalves
DPA – Gerente de Processos Administrativos