	CNPEM **Centro Nacional de Pesquisa em Energia e Materiais**	Nun: 003/2024

OBJETIVO:

FORNECIMENTO DE LICENÇA DE SOFTWARE DE MANUTENÇÃO

TIPO DO DOCUMENTO:

ESPECIFICAÇÃO TÉCNICA

DEPARTAMENTO RESPONSÁVEL:

DMU – DIVISÃO DE MANUTENÇÃO E UTILIDADES

RESPONSÁVEL PELA SOLICITAÇÃO:

CLAUDIO JARRETA
claudio.jarreta@cnpem.br / 19.3512-1153

COLABORADORES:

- O proponente deverá realizar uma apresentação prévia da funcionalidade do software para equipe de manutenção CNPEM.
- As informações desta especificação técnica fará parte integrante do Contrato.

REVISÃO	DATA	EVENTO:
0	12/03/2024	EMISSÃO INICIAL

ÍNDICE

1. OBJETO

Contratação de empresa especializada para o fornecimento de licença de uso de software de gestão de manutenção (SSM), incluindo serviços de migração de dados, implantação, parametrizações e configurações, treinamento de usuários, suporte técnico e manutenção, com vigência inicial de 12 (doze) meses havendo possibilidade de prorrogação.

2. IDENTIFICAÇÃO

A prestação de serviço será realizada dentro das dependências do CNPEM - Centro Nacional de Pesquisa em Energia e Materiais, localizado à Rua Giuseppe Máximo Scolfaro, 10.000, Polo II de Alta Tecnologia. Campinas - SP. CEP: 13083-970.

3. ESCOPO

Contratação de empresa especializada para o fornecimento de licença de uso de software de gestão de manutenção (SSM), incluindo serviços de migração de dados e integrações (esta última conforme necessidade do contratante e disponibilidade técnica do fornecedor), implantação, parametrizações e configurações, treinamento de usuários, suporte técnico, manutenção, atualização e novos desenvolvimentos.

O sistema de gestão irá auxiliar no planejamento, controle e monitoramento das atividades de manutenção dos equipamentos e máquinas do CNPEM, a ser gerenciamento pela DMU (divisão de manutenção e utilidades).

3.1. Implantação:

A Contratada deverá apresentar cronograma detalhado das etapas do projeto, constando as atividades que serão realizadas, recursos de pessoal, prazos de desenvolvimento dos serviços de migração, implantação, treinamento e acompanhamento pós-implantação, contemplando todos os módulos e processos da solução.

As etapas para implantação do sistema seguirão da seguinte forma:

- Entrega, instalação e configuração dos módulos;
- Customizações iniciais dos módulos
- Parametrização inicial
- Migração dos dados existentes para o novo sistema;
- Estruturação dos níveis de acesso e habilitações dos usuários
- Treinamento operacional;
- GO Live, monitoramento, treinamento a usuários e implementação de melhorias.

O trabalho operacional de levantamento dos dados cadastrais e informações necessárias à implantação efetiva da solução é de responsabilidade do CNPEM.

3.2. Migração dos dados existentes

Esta etapa compreende a importação, reorganização e reestruturação dos dados existentes nos sistemas em uso pelo CNPEM, visando permitir a utilização plena destas informações. A empresa Contratada deverá providenciar a conversão dos dados existentes para os formatos e padrões exigidos pelos novos sistemas licitados, mantendo a integridade e segurança dos dados.

3.3. Características do sistema a ser contratado

A solução do software de gestão de manutenção deverá contemplar não menos que os seguintes módulos:

3.3.1 MÓDULO: Cadastros

3.3.1.1 Cadastro de ativos com campos editáveis, para inclusão e alteração de informações como: localização, fabricante, modelo, número de série e databook;

3.3.1.2 Cadastro e edição de planos de manutenção preventivo e preditivo com campos editáveis para periodicidade, criticidades etc.;

3.3.1.3 Cadastro e edição de plano de trabalho. (inclusão de tarefas / jobplan);

3.3.1.4 Cadastro e edição de itens de estoque de manutenção e controle de mínimo, máximo, ponto de ressuprimento e relatórios para definição da curva ABC;

3.3.1.5 Manter no banco de dados histórico dos equipamentos cadastrados ativos e

equipamentos desativados.

3.3.1.6 Cadastro de recurso (mão-de-obra técnica);

3.3.2 MÓDULO: Operação e Customização

3.3.2.1 Acesso a pessoas autorizadas a realizar customizações no ambiente de usuário;

3.3.2.2 Possibilitar customização do sistema para adequá-lo às necessidades do CNPEM;

3.3.2.3 Possibilitar inclusão de anexos (arquivos pdf, word e fotos) no cadastro do ativo e plano preventivo;

3.3.2.4 Gerar automaticamente as ordens de serviço preventivas baseado na periodicidade cadastrada;

3.3.2.5 Possibilitar a geração manual de ordens de serviço de manutenção preventiva;

3.3.2.6 Criação de ordens de serviço corretivos. As ordens de serviço devem conter as informações: Número sequencial, Descrição, Descrição do ativo, Prioridade, Tipo de Serviço;

3.3.2.7 Otimizar a rotina de trabalho, gerenciando as equipes e fornecedores;

3.3.2.8 Possibilitar direcionamento eletronico de preventivas programadas para equipe;

3.3.2.9 Realizar a gestão de recursos, com a possibilidade de avaliar o empenho de Homem Hora nas atividades;

3.3.2.10 Realizar controle do estoque, possibilitando o link da retirada de peças na ordem de serviço;

3.3.2.11 Disponibilizar banco de dados para pesquisa da equipe de manutenção;

3.3.2.12 Importar lista de ativos em formato .csv e/ou .xlsx

3.3.2.13 Possibilitar a comunicação com outros softwares, sensores, QR codes e inteligência artificial, para facilitar o gerenciamento e a execução das atividades de manutenção;

3.3.2.14 Possibilitar a impressão das ordens de serviço;

3.3.2.15 Realizar encerramento manual das ordens de serviços;

3.3.2.16 Alerta automatizado para preventivas de nível crítico (diferencial da proposta);

3.3.2.17 Alerta automatizado para solicitações de usuários classificadas como emergência (diferencial da proposta);

3.3.3 MODULO: Mobilidade

Possuir conectividade mobile para:

3.3.3.1 Realizar execução de serviços de manutenção online e offline (possibilitar registro off-line com atualização quando identificar rede);

3.3.3.2 Realizar o encerramento das ordens de serviço diretamente no mobile;

3.3.3.3 Realizar consulta de histórico de ativos e/ou ordens de serviço;

3.3.3.4 Possibilidade de criação de Ordens de Serviço e/ou Solicitação de Serviços;

3.3.3.5 Possuir rastreabilidade georreferenciada;

3.3.3.6 Realizar requisição de materiais diretamente ao almoxarifado;

3.3.3.7 Possuir interface intuitiva para facilitar o uso e o engajamento da equipe;

3.3.4 MODULO: Relatórios

3.3.4.1 Emissão de relatórios de itens de estoque;

3.3.4.2 Emissão de relatórios de ativos cadastrados;

3.3.4.3 Emissão de relatórios de manutenção preventivos;

3.3.4.4 Emissão de relatórios de SLA´s da equipe por ordem de serviço ou homem/hora.

3.3.4.5 Emitir relatórios com indicadores de KPIs da equipe com interface em Microsoft Power BI

3.3.5 MODULO: Help Desk

3.3.5.1 Possuir Interface intuitiva de comunicação entre usuário solicitante de serviço com o sistema de gerenciamento. (helpdesk);

3.3.5.2 Sistema deve fornecer por e-mail ao solicitante a atualização do status da

solicitação de serviço;

3.3.5.3 Solicitar automaticamente por e-mail a avaliação do usuário quando ocorrer o encerramento da solicitação de serviço;

3.3.5.4 Emitir relatórios com indicadores de SLA´s da equipe com interface em Microsoft Power BI;

3.3.5.5 Informar SLA do serviço solicitado ao usuário;

3.4. Responsabilidade da Contratada:

3.4.1 Fornecer SLA de atendimento corretivo com tempo de resposta de até 24 horas para chamados abertos em dias úteis.

3.4.2 Fornecer visitas periódicas para garantir a conformidade do software com os padrões e especificações.

3.4.3 Manter a gestão de versões do software para garantir a sua rastreabilidade e consistência.

3.4.4 Garantir que as demandas sejam extensivamente testadas previamente no ambiente de desenvolvimento antes da comunicação de entrada em homologação. A posterior publicação em produção deverá ocorrer somente após autorização;

3.4.5 Envio de relatórios periódicos detalhados (mensais e sob demanda) de acompanhamentos de demandas do Software;

3.4.6 Fornecer manuais de utilização do software.

3.4.7 Realizar revisões do software para adequações as necessidades do CNPEM.

3.4.8 Disponibilizar medições para avaliar a qualidade do software e identificar possibilidade de melhorias.

3.4.9 Espera-se um relacionamento colaborativo e flexível com fornecedor, sendo considerado diferencial para esta contratação os seguintes pontos, não se limitando à apenas estes:

3.4.10 Disponibilidade para reuniões presenciais e virtuais previamente

combinadas;

3.4.11 Canal único para comunicação, acompanhamento e gestão das demandas de garantia, suporte, manutenção e melhorias, tanto em período de garantia, quanto de suporte continuado;

3.4.12 Propor soluções e realizar pesquisa sob demanda sobre o comportamento do software, integrações e outras soluções;

3.4.13 Disponibilidade para apoio e alinhamento com outros fornecedores.

3.4.14 Auxiliar no desenvolvimento de uma nova ferramenta e/ou soluções de uma provável necessidade de integração com outros sistemas de gerenciamento e dispositivos sob gestão de outros fornecedores.

3.4.15 Disponibilizar treinamento para operação do software.

3.4.16 Fornecer assistência presencial e/ou remota para atendimentos relacionados a problemas do software.

3.4.17 Fazer levantamento e o refinamento de requisitos quando demandado.

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. Medidas de Segurança

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

4.1.1 Autenticação: O sistema deve possuir um mecanismo seguro de autenticação, garantindo que apenas usuários autorizados tenham acesso ao sistema.

4.1.2 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.

4.1.3 Criptografia: Dados confidenciais, como senhas e informações pessoais, devem ser armazenados e transmitidos de forma criptografada para evitar acesso não autorizado.

4.1.4 Prevenção de ataques: O sistema deve implementar mecanismos de detecção e prevenção de ataques.

4.1.5 Auditoria e rastreamento: Deve ser possível rastrear e auditar as atividades realizadas no sistema, registrando informações como data, hora, usuário e ação executada.

4.1.6 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.

4.1.7 Caso seja uma plataforma SaaS (Software as a Service) onde o fornecedor disponibiliza a ferramenta pela internet como um serviço, a contratada será responsável pela contínua atualização e manutenção da plataforma fornecida, abrangendo todos os aspectos do sistema, incluindo o sistema operacional.

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

4.2. Armazenamento em nuvem.

4.2.1 O sistema deverá ser implementado utilizando uma arquitetura baseada em nuvem, garantindo que todas as operações, dados e processos essenciais estejam hospedados em ambientes de nuvem confiáveis. Este requisito visa aproveitar os benefícios da computação em nuvem, proporcionando escalabilidade, disponibilidade, flexibilidade e manutenção simplificada.

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.

4.3.1 Análise de código:

Implementação das correções necessárias para as vulnerabilidades de segurança identificadas no código.

Revisão e análise de segurança de código pelos desenvolvedores.

4.3.2 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.

4.3.3 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.

4.3.4 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.

4.3.5 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.

4.3.6 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.

5. Qualidade do desenvolvimento e das entregas da contratada

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

5.1. 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.

5.1.1 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.

5.1.2 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.

5.1.3 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.