



Especificação Técnica para contratação de ferramenta de *Due Diligence*

1. Objetivo

Contratação de licença de uso de solução tecnológica, disponibilizada em ambiente web (*Software as a Service – SaaS*), destinada à realização de consultas, pesquisas e análises de due diligence e background check de pessoas físicas e jurídicas, incluindo atualização das bases de dados, suporte técnico e manutenção da solução durante toda a vigência contratual.

2. Detalhamento do serviço a ser contratado

A empresa contratada deverá disponibilizar solução tecnológica, em ambiente web (*Software as a Service – SaaS*), destinada à realização de consultas, pesquisas e análises para apoio às atividades de due diligence, background check e avaliação de riscos relacionados a pessoas físicas e jurídicas.

A solução deverá permanecer disponível durante toda a vigência contratual, contemplando o licenciamento de uso, atualização contínua das bases de dados, manutenção da plataforma e suporte técnico aos usuários designados pelo CNPEM. A solução deverá possibilitar a realização de consultas e pesquisas por meio de diferentes parâmetros de busca, incluindo, no mínimo:

- CPF;
- CNPJ;
- nome da pessoa física;
- razão social;
- nome fantasia;
- sócios e administradores;
- outros identificadores disponíveis na plataforma.

As consultas deverão disponibilizar, sempre que legalmente permitido e tecnicamente disponível, informações relacionadas a:

2.1 Identificação Cadastral

- situação cadastral;
- dados cadastrais básicos;
- histórico cadastral, quando disponível;
- informações de registro da pessoa física ou jurídica.

2.2 Estrutura Societária

- quadro societário;
- administradores;
- participações societárias;





- empresas relacionadas;
- vínculos societários e empresariais;
- beneficiário final, quando disponível.

2.3 Processos Judiciais e Administrativos

- processos judiciais;
- ações cíveis;
- ações trabalhistas;
- ações tributárias;
- execuções;
- processos administrativos sancionadores;
- outras informações processuais disponíveis nas bases consultadas.

2.4 Integridade e Conformidade

A solução deverá disponibilizar informações que apoiem a avaliação de riscos de integridade, incluindo, sempre que disponíveis:

- sanções administrativas;
- cadastros restritivos de órgãos públicos;
- pessoas expostas politicamente (PEPs);
- listas nacionais e internacionais de sanções;
- impedimentos para contratar com a Administração Pública;
- registros públicos relacionados à integridade e conformidade.

2.5 Informações Econômico-Financeiras

Sempre que disponíveis, a solução deverá disponibilizar informações relacionadas a:

- recuperação judicial;
- falência;
- insolvência;
- restrições cadastrais;
- outras informações públicas relevantes para avaliação de risco.

2.6 Mídia adversa

A solução deverá permitir a pesquisa de notícias e informações públicas relacionadas à pessoa física ou jurídica consultada, incluindo referências em veículos de comunicação, quando disponíveis, possibilitando a identificação de potenciais riscos reputacionais e de integridade.

2.7 Relatórios

A solução deverá possibilitar:

- visualização dos resultados das consultas;
- geração de relatórios;
- exportação dos resultados em formato eletrônico;
- impressão das consultas realizadas.

2.8 Atualização das bases





As bases de dados utilizadas pela solução deverão ser atualizadas periodicamente pela empresa contratada, de modo a assegurar a atualidade, consistência e confiabilidade das informações disponibilizadas.

2.9 Disponibilidade da solução

A solução deverá permanecer disponível durante toda a vigência contratual, ressalvadas as interrupções programadas para manutenção previamente comunicadas ao CNPEM.

2.10 Suporte técnico

A empresa contratada deverá disponibilizar suporte técnico aos usuários indicados pelo CNPEM para atendimento de dúvidas, resolução de incidentes, esclarecimentos sobre funcionalidades e demais necessidades relacionadas à utilização da solução. Sempre que houver atualização relevante da plataforma ou inclusão de novas funcionalidades, a empresa contratada deverá disponibilizar orientações de uso ou treinamento aos usuários, sem ônus adicional para o CNPEM, quando previsto na proposta comercial.

3. Vigência

O contrato terá vigência de 36 (trinta e seis) meses, contados da data de sua assinatura, podendo ser prorrogado, mediante justificativa e observadas as disposições do Regulamento de Compras e Contratações do CNPEM.

Durante toda a vigência contratual, a contratada deverá assegurar o pleno funcionamento da solução, incluindo o acesso às funcionalidades contratadas, a atualização das bases de dados, a manutenção da plataforma e a prestação de suporte técnico aos usuários autorizados pelo CNPEM.

4. 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.

5. 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;
- 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.
- Atender aos finais de semana e feriados quando necessário.

6. 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.
 - * <detalhes técnicos> e outros requeridos pelo <nome do sistema>;
- 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 e emitir relatório mensal de atividades com identificação do chamado e horas consumidas.

7. 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.





7.1. 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.

Campinas, 16 de julho de 2026.

Michelle Pereira Guimarães

Michelle Guimarães
Gerente de Compliance
Assessoria de Compliance

Antonio Jose Roque Da Silva

Antonio José Roque da Silva
Diretor-Geral
Diretoria-Geral

