RNP

ORGANIZAÇÃO SOCIAL DO MCTI

Educação, Pesquisa
e Inovação em Rede

Termo de Referência (TR)

DATI - Diretoria-Adjunta de Tecnologia da Informação

RNP – Rede Nacional de Ensino e Pesquisa

CONTROLE DE VERSÕES

DATA	ALTERAÇÃO	RESPONSÁVEL
25/11/2024	Documento inicial	Luciana Brozios

Sumário

1. Sumário

2. Apresentação da RNP

A Rede Nacional de Ensino e Pesquisa (RNP) é uma instituição privada, sem fins lucrativos, com sede no Rio de Janeiro (RJ), qualificada pelo Governo Federal como Organização Social e contratada pelo Ministério da Ciência e Tecnologia (MCTI) para atender aos seguintes objetivos estratégicos:

- Promover o desenvolvimento tecnológico de novos protocolos, serviços e aplicações de redes;
- Prover serviços de infraestrutura de redes IP (Protocolo Internet) avançadas para atividades de pesquisa e desenvolvimento científico e tecnológico, educação e cultura;
- Promover a disseminação de tecnologias, através da implantação, em nível de produção de novos protocolos, serviços e aplicações de redes, da capacitação de recursos humanos e da difusão de informações; e
- Planejar e empreender projetos de tecnologia de informação e comunicação para o desenvolvimento e uso de aplicações e serviços inovadores.

A RNP promove o interesse público pelo desenvolvimento tecnológico da área de redes e suas respectivas aplicações, com o foco orientado para o suporte às ações estratégicas em educação, ciência, tecnologia e inovação, através de Programa Interministerial dos Ministérios da Ciência e Tecnologia e da Educação.

Para tanto, constitui-se como a infraestrutura de rede de comunicação e computação que garante o suporte à pesquisa brasileira, uma vez que propicia a integração de todo o sistema de pesquisa e ensino superior por uma rede nacional de alta capacidade, rica em serviços e aplicações. Nesta rede (ou backbone), também são realizadas pesquisas para o desenvolvimento e o teste de novas tecnologias de informação e comunicação (TIC). Estas tecnologias formam a base da nova Sociedade do Conhecimento, e seu domínio e uso são essenciais para o desenvolvimento do país. Neste sentido, a própria rede constitui-se em um laboratório nacional onde os experimentos de TIC são realizados, de modo que seus resultados possam beneficiar mais rapidamente nossos clientes: as universidades, os centros de pesquisa e as agências federais.

3. Objeto

A RNP – Rede Nacional de Ensino e Pesquisa, por meio deste Termo de Referência, descreve, especifica e define o objeto e demais elementos necessários para **aquisição, implantação e disponibilização** de uma **Plataforma para Recuperação de Desastres**, em substituição às atuais ferramentas utilizadas para Backup na organização.

4. Escopo

O escopo do projeto é a aquisição, implantação e disponibilização de uma Plataforma para Recuperação de Desastres para proteção dos serviços, sistemas e dados críticos da organização, incluindo arquivos de sistema, bancos de dados, arquivos de usuários e registros financeiros, abrangendo as seguintes infraestruturas de TI *on-premises* atualmente em funcionamento na RNP:

- **Nuvem Privada** corporativa, baseada na suíte VMware Cloud Foundation;
- **Infraestruturas de Virtualização Locais** em Escritórios e Pontos de Presença da RNP, baseadas no sistema de virtualização VMware vSphere;

Nestas infraestruturas de TI, estão presentes os seguintes tipos de ativos que devem ser protegidos por meio de Backup:

- Máquinas virtuais (VMs) na Nuvem Privada e nas Infraestruturas de Virtualização Locais.
- Sistemas de Gestão de Bancos de Dados (SGBDs) em funcionamento sobre estas VMs.

Além do escopo inicial deste projeto, é necessário que a Plataforma para Recuperação de Desastres ofertada tenha suporte para futuras expansões que podem englobar outros tipos de recursos em nuvem pública:

- Amazon Web Services (**AWS**);
- Google Cloud Platform (**GCP**);
- Microsoft **Azure**.

Nessas nuvens, estão presentes os seguintes tipos de ativos que devem ser protegidos por meio de Backup:

- Máquinas virtuais (VMs) na AWS, GCP e Azure;
- Sistemas de Gestão de Bancos de Dados (SGBDs), alguns gerenciados pelos provedores (exemplo: AWS RDS) e outros gerenciados pela própria RNP (instalados e gerenciados manualmente sobre o serviço de IaaS do provedor);
- Clusters Kubernetes;
- Espaços de armazenamento de objetos (Object Storage);
- Sistemas de arquivos de rede (NFS) gerenciados.

A Plataforma para Recuperação de Desastres deve garantir integridade, disponibilidade e segurança dos dados armazenados, bem como a recuperação em caso de falhas e perdas, suportando assim a estratégia de Recuperação de Desastres da RNP.

A Plataforma para Recuperação de Desastres deve ser acessada de maneira segura, pela Internet, e apenas por usuários autorizados. Seus requisitos funcionais, técnicos e de segurança da informação, e de privacidade e proteção de dados estão definidos neste documento.

A Plataforma para Recuperação de Desastres também é referenciada somente como “plataforma” ou “solução” neste documento.

O fornecedor vencedor deste processo deve ofertar à RNP uma solução de um fabricante que tenha um ou mais representantes ou parceiros no Brasil, que possuam certificações para atuar como consultoria especializada.

5. Etapas do Processo

O processo consiste em duas etapas, aqui definidas e detalhadas nas próximas seções deste documento.

5.1. Etapa 1: Compilação e envio das documentações obrigatórias

- Documentação cadastral (item 5);
- Atestado de capacidade técnica;
- **Evidências de conformidade dos Requisitos do Fornecedor e da Solução (item 0)** – é anexada a este documento uma planilha auxiliar elencando os requisitos obrigatórios e desejáveis (Anexo A), a fim de auxiliar na coleta e verificação da comprovação dos controles apresentados.
- Proposta comercial (item 7); Para a avaliação do atestado de capacidade técnica, o fornecedor deverá entregar no mínimo uma e no máximo três declarações de clientes (case de cliente) com os quais tenha prestado seus serviços, ofertado soluções, sistemas ou aplicações etc. Pede-se, ainda, que as declarações estejam em papel timbrado e assinada pelo responsável que contratou o sistema.

A planilha auxiliar deve ter todos os campos preenchidos; campos em branco serão considerados "não atende", o que para itens obrigatórios desclassifica o fornecedor e sua solução. O fornecedor deve analisar a planilha auxiliar do Anexo A, e preencher cada linha das abas "Negócio", "Segurança", "Privacidade" e "Gerais" conforme a explicação das colunas:

a. **"Atende/Atende Parcialmente/Não Atende":** deve ser escolhida uma das opções disponíveis;
b. **"Detalhamento da Resposta":** justificar a resposta do campo anterior, e observações quando necessário; e
c. **"Evidência Apresentada pelo Fornecedor":** quando a opção escolhida na coluna "a" for Atende ou Atende Parcialmente, o fornecedor deve indicar o nome da evidência apresentada para o item, e a evidência deve ser anexada e enviada para a RNP.

Como exemplo:

a. **"Atende" ou "Atende Parcialmente":** item referente à conexão da plataforma com solução de virtualização VMware vSphere;
b. **Detalhamento da Resposta:** é possível conectar a plataforma ao vCenter para realizar a leitura das máquinas virtuais e os processos de backup e recuperação por meio de agentes locais; e
c. **Evidência Apresentada pelo Fornecedor:** arquivo .pdf ou link da página pública do fornecedor com o passo a passo para a configuração a integração da solução.

As respostas apresentadas devem, no mínimo, observar os itens listados neste documento, visando atender as necessidades da RNP, porém não se limitando somente a estes itens.

Toda a documentação solicitada nesta etapa é obrigatória para habilitação do fornecedor neste processo, para que a RNP avalie os documentos obrigatórios para seleção da Etapa 2.

5.2. Etapa 2: Apresentação da Solução e Entrevista técnica

Os fornecedores selecionados na Etapa 1 deverão realizar uma apresentação da solução para um grupo de avaliadores da RNP, isto é, demonstrar o funcionamento dos sistemas, aplicações, funções e funcionalidades da solução ofertada pelo fornecedor, bem como, os requisitos de segurança da informação, privacidade e proteção de dados. A apresentação será agendada em data e horário estabelecido entre as partes.

Nesta etapa, serão avaliados os itens dispostos na proposta comercial em relação à solução apresentada e aderência dela com os requisitos da planilha (Anexo A). Também serão analisadas suas funcionalidades, usabilidades e compatibilidades dos sistemas e aplicações, além dos níveis de esclarecimento das dúvidas e o domínio do uso do(s) apresentador(es). Os fornecedores que não efetuarem a apresentação da solução ou não conseguirem evidenciar a aderência aos requisitos estabelecidos, serão incontestavelmente desclassificados.

A gestão e organização das apresentações práticas, com cada fornecedor, será realizada pela área de Compras da RNP. A apresentação prática terá duração máxima de 120 minutos, dos quais 60 minutos são disponibilizados para a apresentação da solução e 60 minutos para esclarecimento de dúvidas.

Caso a RNP entenda ser necessário, será realizada novas entrevistas para esclarecimentos de novas dúvidas.

Por último, as respostas e informações obtidas durante as etapas 1, 2 serão consideradas na decisão da solução contratada.

A realização da seleção de fornecedores **não obriga** a Rede Nacional de Ensino e Pesquisa a formalizar o contrato ou pedido de compra, podendo o mesmo ser desclassificado, sem que caiba direito aos participantes de pleitear qualquer indenização.

Realização da POC (Prova de Conceito)

As empresas classificadas na etapa 1 e 2, poderão ser convidadas pela RNP para realizada da POC

1. O fornecedor deve configurar a plataforma em sua infraestrutura, sem custo para a RNP, e entregar acessos para a equipe técnica designada validar os requisitos técnicos e funcionais da solução.
2. A equipe técnica designada terá o prazo de 30 dias úteis para analisar e tirar dúvidas com o fornecedor.
3. Ao final do prazo de 30 dias, a equipe técnica validará o funcionamento da solução, para classificação da Etapa comercial.

Ao final desta etapa, a empresa que tiver a melhor condição comercial aliada ao atendimento dos requisitos e da validação da RNP com base na Prova de Conceito será declarada como fornecedora vencedora do processo.

6. Documentação Cadastral

Os documentos obrigatórios para a realização do pré-cadastro e análise de homologação administrativa do fornecedor são:

- Contrato Social;
- Inscrição no Cadastro Geral de Contribuintes (CNPJ);
- Certidão de Débitos Relativos a Créditos Tributários Federais e à Dívida Ativa da União, expedida pela Receita Federal;
- Prova de regularidade com o Fundo de Garantia por Tempo de Serviço (FGTS), comprovada pela Certidão de Regularidade de Situação (C.R.S.).

7. Requisitos da Solução e do Fornecedor

A solução ofertada pelo fornecedor deve ter aderência aos requisitos aqui elencados. São definidos requisitos obrigatórios e desejáveis de negócio, segurança da informação, privacidade e proteção de dados e gerais. Anexado a este documento é disponibilizada uma planilha auxiliar, Anexo A, com os itens desta seção, a fim de apoiar no levantamento das documentações necessárias, identificar itens faltantes e incluir observações quando cabível.

7.1. Requisitos Técnicos e de Negócio

Requisitos obrigatórios:

1. A solução pode ser composta por uma ou mais ferramentas de modo a atender aos requisitos deste TR.
2. O fornecedor deve oferecer ferramentas que atendam este TR em sua totalidade, ou seja, não serão aceitas propostas com soluções parciais.
3. A solução deve ter suporte à proteção de VMs na suíte de nuvem privada VMware Cloud Foundation em versões a partir da 4.0.
4. A solução deve ter suporte à proteção de VMs na suíte de virtualização VMware vSphere em versões a partir da 6.0.
5. Inicialmente deve ser ofertado licenciamento ou subscrições para, no mínimo, 500 VMs em VMware;
6. Além de produtos VMware, que são o escopo inicial de licenciamento e implantação, a solução deve ter suporte para proteção futura de recursos em nuvem pública e/ou de outros tipos:
    - 6.1. Amazon Web Services (AWS).
        - 6.1.1. Suporte ao serviço de virtualização EC2.
        - 6.1.2. Suporte ao serviço de bancos de dados gerenciados RDS.
        - 6.1.3. Suporte ao serviço de armazenamento de objetos S3.
        - 6.1.4. Suporte ao serviço de sistemas de arquivos gerenciados EFS.
        - 6.1.5. Suporte ao serviço de clusters Kubernetes EKS.
    - 6.2. Google Cloud Platform (GCP).
    - 6.3. Microsoft Azure.
    - 6.4. Microsoft 365
        - 6.4.1. Suporte a backups do Exchange (Outlook Online), com proteção de e-mails, calendários, contatos, tarefas e arquivamento online;
        - 6.4.2. Suporte a backups do OneDrive, com proteção aos arquivos em todas as suas versões armazenadas;
        - 6.4.3. Suporte a backups do Teams, com proteção de Canais e Conversas;
        - 6.4.4. Suporte a backups do SharePoint, com proteção aos Sites (incluindo Sites de Equipe), Páginas, Listas e Bibliotecas de Arquivos, com todas as suas versões
        - 6.4.5. Suporte a backup do Microsoft Entra ID, com proteção a Usuários, Grupos, Administrative Units, Roles, Service Principals, App Registrations, Policies, Devices e Activity Logs.

6.5. Recursos em containers operando sobre *clusters* Kubernetes;

6.6. Sistemas de Gestão de Bancos de Dados (SGBDs) Microsoft SQL Server, MySQL, MariaDB e PostgreSQL não gerenciados por provedores de nuvem, ou seja, instalados pela própria RNP em VMs ou serviços de IaaS similares.

7. A solução deve ter licenciamento expansível, ou seja, deve ser possível adicionar mais licenças ou subscrições para cobertura e proteção de incrementos do número de VMs ou para adição de outros tipos recursos necessários para cobertura das tecnologias protegidas, informadas nos itens 6.1, 6.2, 6.3, 6.4, 6.5 e 6.6.
8. A solução deve permitir a configuração de múltiplas políticas de backup e múltiplos destinos para gravação dos dados, permitindo execução individual e/ou por agrupamento.
9. A solução deve suportar a gravação integral dos dados de backups em serviços de armazenamento de objetos (*object storage*) em nuvem pública AWS, GCP ou Azure.

   9.1. Não deve haver dependências com equipamentos de armazenamento (storages) instalados nas dependências da RNP, exceto para a máquina virtual responsável pela transferência dos dados entre as infraestruturas de TI próprias da RNP e a nuvem.
10. A solução deve permitir a restauração dos recursos completos e de arquivos granulares para tipos de recursos que deem este suporte, por exemplo, arquivos específicos dentro de VMs.
11. A solução deve ter acesso web para o grupo de analistas responsáveis pela sua gestão e operação, contendo recursos para:

    11.1. Visualização de informações consolidadas (dashboards);

    11.2. Criação e gestão de usuários;

    11.3. Visualização de registros (logs);

    11.4. Visualização de alarmes e alertas.

    11.5. Visualização em tempo real de status de backup e restauração.

    11.6. Gestão de políticas de backup;

    11.7. Gestão de trabalhos (*jobs*) de backup e restauração;
12. A solução deve possuir uma ou mais APIs documentadas e que permitam a integração com sistemas de monitoramento para conexão com APIs.
13. Extração de dados operacionais para compor relatórios gerenciais e aferição de indicadores.

Requisitos desejáveis:

14. A solução contar com gestão e operação completas, sendo ofertada em modalidade SaaS à RNP.
15. Permitir o consumo dos dados gerados pela solução para a construção de visualizações e *dashboards* em sistemas de BI.

7.2. Requisitos de Segurança da Informação

Requisitos obrigatórios:

16. Relação das opções de autenticação disponíveis, apresentando os fluxos de autenticação, aplicação de múltiplo fator de autenticação (MFA), integrações com SAML, LDAP, aplicação do controle de acesso baseado em funções (RBAC) e integração com um Vault (Cofre de Senhas) para o armazenamento de credenciais;
17. Ações de capacitação e conscientização em segurança da informação
18. Documentos e políticas relacionadas à segurança da informação:
    - Política de Segurança da Informação;
    - Normativo sobre Gestão de Acesso físico e lógico;
    - Normativo sobre Segurança física e do ambiente;
    - Declaração de cumprimento e revisão periódica das políticas/normas;
    - Política/Norma de Acesso;
    - Política/Norma de Senhas;
    - Outros documentos pertinentes ao âmbito da segurança da informação.
19. Descrição dos controles definidos na ISO 27001:27002 existentes;
20. Certificações relacionadas à segurança da informação e continuidade de negócios dentro do escopo da Plataforma para Recuperação de Desastres (se houver);
21. Certificado ou Declaração de Execução de Pentest informando o escopo da análise e periodicidade;
22. Documentos e políticas relacionados a gestão de incidentes e continuidade de negócios:
    - Plano de Comunicação de Incidentes;
    - Plano de Gestão de Continuidade de Negócios;
    - Plano de Resposta a Incidentes com a definição das atividades e responsabilidades;
    - Plano de Recuperação de Desastres;
    - Norma/Plano/Processo de Backup;
    - Normas/Processos de gerenciamento e retenção de logs;
    - Documento/Declaração que afirme a existência de execução de testes de continuidade, estudo de BIA e de RTO.
23. Declaração de controles e processos implementados para registro de acesso físico e lógico à infraestrutura, sistemas, aplicações, backup e seus componentes;
24. Evidência do sistema de monitoramento e acesso;
25. Documentação ou diagrama da arquitetura da solução, contemplando integrações, criptografia em trânsito e em repouso e protocolos de comunicação utilizados; e
26. Declaração ou certificação de desenvolvimento seguro, informando a aplicação das boas práticas de *security by design* e devsecops abrangendo todo o ciclo de vida da ferramenta.

27. Relatório com as ações de capacitação e conscientização em segurança da informação;

Requisitos desejáveis:

28. Certificação TIER do datacenter;
29. Práticas ou frameworks utilizados;
30. Documento que apresente o processo de análise e avaliação de riscos cibernéticos, a evidência da realização do processo e a comunicação dos riscos para a alta gestão;
31. Documento que apresente quais são as práticas ou frameworks (CIS, NIST, etc.) utilizados como baseline de segurança;
32. Resumo Executivo com controles aplicados ou Certificação ISO 22301 (Se houver); e
33. Detalhamento da Metodologia/Estratégia utilizada para realizações de SCA/SAST/DAST na aplicação e prazo para correções de vulnerabilidades.

A lista dos requisitos de segurança e o detalhamento das evidências quem devem ser apresentadas é encontrado na aba Segurança da Tabela do Anexo A. Caso algumas das evidências apresentadas atenda mais de um requisito solicitado, a mesma pode ser enviada uma única vez indicando quais controles se encontram na evidência.

7.3. Requisitos de Privacidade e Proteção de Dados

Requisitos obrigatórios:

34. Demonstração de implementação de controles relacionados à ISO 27701 aplicados nos processos e ativos que suportam a plataforma ou serviço;
35. Políticas corporativas Privacidade e Proteção de Dados corporativa e Aviso de Privacidade da Plataforma, demonstrando o compromisso da empresa e seus colaboradores com a aplicação da LGPD e boas práticas de mercado relacionadas à privacidade e proteção de dados ou desejável a apresentação de documentos normativos que evidenciem a aplicação de diretrizes relacionadas à privacidade e proteção de dados;
36. Documentação de formalização da indicação do Encarregado pelo Tratamento de Dados Pessoais, ou desejável, em casos de fornecedores que estejam enquadrados na definição de Agentes de Tratamento de Pequeno Porte, a indicação do responsável ou ponto focal de contato pelo tema de privacidade;
37. Documentação de formalização dos canais de contato com Encarregado de Dados e/ou Documentação do Plano de Resposta a Incidentes;
38. Relatório/parecer de análise de riscos em privacidade;
39. Evidências de que a plataforma ou serviço permite total gestão sobre dados pessoais pela RNP enquanto controlador;
40. Modelo do Termo de sigilo formalmente estabelecido;

41. Apresentação ou visualização dos contratos e/ou acordos estabelecidos com fornecedores terceiros (se necessário, sob compromisso de NDA por parte da RNP); e
42. Registro de ocorrência/relatório de tratamento de incidente (se necessário, sob compromisso de NDA por parte da RNP).

Requisitos desejáveis:

43. Evidências de que a plataforma ou serviço permite a criação de perfis com diferentes permissões de acesso a dados pessoais;
44. Evidências de que a plataforma ou serviço permite visualização/correção/edição de dados pessoais dos respectivos usuários através da interface;
45. Evidências de que a plataforma ou serviço permite realização de mascaramento e ocultação de conteúdos de dados pessoais do usuário através da interface;
46. Evidências de que a plataforma ou serviço permite gestão de consentimento (se aplicável) dos respectivos usuários através da interface;
47. Evidências de que a plataforma ou serviço permite inclusão de Termo de uso e Aviso de Privacidade para usuários da plataforma desenvolvidos pela RNP; e
48. Evidências de que a plataforma ou serviço realiza treinamentos periódicos sobre práticas de privacidade e proteção de dados à sua força de trabalho.

7.4. Requisitos Gerais

A solução deve ser fornecida com serviços de design, implantação, documentação, operação assistida, suporte técnico e treinamento.

Requisitos obrigatórios:

49. Devem estar inclusos na proposta todos os serviços necessários para design e implantação da solução, tais como planejamento, instalação e integração de todos os componentes, configuração e transferência de conhecimento;
    49.1. O prazo para entrega e implantação completa da solução é de 4 (quatro) meses corridos a partir da data de conclusão do processo de compra.
    49.2. Ao final do terceiro mês, a RNP deve ser capaz de realizar as ações de Backup e Restauração de recursos protegidos.
    49.3. Neste prazo de 4 meses, não são contados os 30 dias de operação assistida.
50. O fornecedor deve disponibilizar um gestor de projetos junto com os analistas e especialistas técnicos, para gestão da entrega com os requisitos e prazos definidos neste documento.
51. Antes do início da instalação da solução, o profissional do fornecedor deve elaborar, em conjunto com os analistas da RNP, um planejamento da implantação (design) contendo, pelo menos:
    51.1. Mapas lógicos com informações sobre a disposição de cada componente na arquitetura geral da solução.

51.2. Informações sobre hospedagem e infraestrutura dos servidores ou VMs que compõem a camada de administração da solução.

51.3. Informações sobre a resiliência da solução, capacidades de alta disponibilidade (HA) e recuperação de desastres (DR) na solução e nos seus componentes.

51.3.1. Os componentes devem contar com redundância com pelo menos 2 (dois) servidores ou VMs, em nuvem pública, para alta disponibilidade.

52. A instalação dos componentes de software pode ser realizada por meio de acesso remoto pelo profissional do fornecedor:

52.1. Caso seja feita por acesso remoto, deve ser feita por conferência (áudio e compartilhamento de tela) com acompanhamento de, pelo menos, 2 (dois) analistas do fornecedor;

52.2. As conferências devem ser gravadas para futura referência;

52.3. Cada operação realizada deve ser explicada aos analistas;

52.4. A definição das credenciais de acesso (usuários e senhas), quando necessárias, será feita pelos analistas do fornecedor e serão compartilhadas com o profissional da RNP;

52.5. Os componentes devem ter rotinas de backup configuradas, quando aplicável, em armazenamento a ser definido pelos analistas da RNP.

53. Após o término da instalação dos componentes de software, deve ser iniciada uma rotina, com, pelo menos:

53.1. Configuração completa de uma política de backup a escolha da RNP.

53.2. Conexão da solução com os sistemas de gestão da Nuvem Privada (VMware Cloud Foundation) e Infraestruturas de Virtualização Locais (VMware vSphere).

53.3. Conexão da solução com um espaço de armazenamento de objetos (object storage) em nuvem pública para armazenamento dos dados de backup.

53.4. Testes de backup de máquinas virtuais na Nuvem Privada e nas Infraestruturas de Virtualização Locais.

53.5. Testes de restauração e recuperação dos backups.

53.6. Visualização dos logs da solução e dos seus componentes.

54. Ao final da implantação e dos testes, o fornecedor deve entregar documentação completa da solução, contendo, pelo menos:

54.1. Diagramas de arquitetura geral da solução;

54.2. Diagrama de arquitetura de rede;

54.3. Diagrama de arquitetura de armazenamento;

54.4. Procedimentos de instalação do ambiente;

54.5. Procedimentos de recuperação de desastres;

54.6. Referências aos manuais de administração (*Administration Guides*) atualizados de cada componente da solução;

54.7. Informações sobre acesso a *backups*, *logs*, monitoramento e alertas de cada componente da solução;

54.8. Chaves de acesso e informações sobre licenças de *software* utilizadas na implantação.

55. A implantação se dará como concluída somente após assinatura de termo de aceite por parte de, pelo menos, 1 (um) analista e 1 (um) gerente designados pela RNP, obedecendo aos seguintes requisitos:

    55.1. A plataforma deverá estar instalada e configurada corretamente, atendendo a todos os requisitos técnicos.

    55.2. A plataforma deverá realizar backups e recuperações conforme os testes previamente definidos, sem falhas.

56. Deve estar inclusa na proposta uma etapa de operação assistida da plataforma por 30 (trinta) dias:

    56.1. A data de início do período de operação assistida será definida pela RNP em conjunto com o fornecedor;

    56.2. O profissional do fornecedor deverá estar de prontidão para atendimento imediato, em horário comercial (8h às 17h), caso haja alguma dúvida ou problema técnico, sem a necessidade de abertura de chamado;

    56.3. Deverão ser realizadas reuniões semanais com a equipe da RNP e o profissional do fornecedor para acompanhamento de atividades.

57. A plataforma deve ter suporte do fabricante durante todo o tempo de vigência das suas licenças ou subscrições;

    57.1. Devem estar cobertas todas as atualizações de versões de software.

58. O serviço de suporte técnico deve ser prestado a partir da data de assinatura do termo de aceite da implantação;
    58.1. O serviço de suporte técnico deve ser prestado em língua portuguesa;

    58.2. O serviço de suporte técnico deve contemplar toda a solução, com todos os componentes utilizados;

    58.3. O serviço de suporte técnico deve estar disponível em 24x7, ou seja, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

59. A RNP deve ter acesso à abertura e visualização de chamados a qualquer momento por meio do portal de relacionamento com o cliente, além de ter possibilidade de contato por telefone e e-mail;

    59.1. Imediatamente após a criação do chamado, a RNP deve receber o número do chamado. Por meio desse número de chamado a contratante poderá consultar informações sobre o chamado e também deverá ter acesso a toda a comunicação realizada com a equipe do suporte (portal, e-mail ou chat);

    59.2. Para chamados que relatem indisponibilidade parcial ou total da solução, o primeiro retorno deve ocorrer em até 30 (trinta) minutos e o atendimento deve ocorrer em até 2 (duas) horas após a abertura do chamado;

        59.2.1. Considera-se "indisponibilidade" quando um cliente ou usuário da solução não consegue ter acesso aos seus recursos e/ou dados armazenados, em decorrência de problemas que estejam ocorrendo em um ou mais componentes da solução.

60. O serviço de suporte técnico deve prever o desenvolvimento de correções de software para qualquer componente da solução;

61. O serviço de suporte técnico deve prever a possibilidade de escalonamento de chamados para atuação das equipes de engenharia;

62. O serviço de suporte técnico deve prever a atuação em regime de esforço contínuo para a solução de problemas e correções.

63. O fornecedor deve oferecer treinamento, em português, para a qualificação dos analistas indicados pela RNP responsáveis pela operação e administração da solução contratada:

    63.1. Devem estar inclusas apostilas de acompanhamento com todo o conteúdo programático, em português ou inglês;

    63.2. O treinamento deve ser ministrado para 1 (uma) turma de, pelo menos, 8 (oito) analistas;

    63.3. Devem ser fornecidos certificados de conclusão;

    63.4. O treinamento pode ser realizado, opcionalmente, por meio de conferência pela Internet.

64. O treinamento deve contemplar, no mínimo, os seguintes temas:

    64.1. Visão geral da solução;

    64.2. Criação de políticas de Backup;

    64.3. Procedimentos operacionais de Backup e Restauração;

    64.4. Relatórios de gestão e controles operacionais;

65. O treinamento deve contemplar, no mínimo, as seguintes atividades:

    65.1. Explicação teórica;

    65.2. Explicação da arquitetura definida na implantação da solução na RNP;

    65.3. Informações para uso das interfaces de gestão e monitoramento;

    65.4. Informações sobre possibilidades de automação de tarefas, acesso a APIs e informações relacionadas;

    65.5. Informações de diagnóstico e solução de problemas mais comuns (*troubleshooting*).

Requisitos desejáveis:

66. Quando aplicável, é desejável que sejam ofertados treinamentos oficiais do fabricante.

8. Proposta Comercial e Apresentação Institucional

A proposta comercial deverá conter uma breve apresentação do fornecedor e da solução ofertada, o escopo atendido, cronograma para implantação e disponibilização da solução, os custos conforme itens propostos a seguir, com prazo de validade da proposta de no mínimo 60 (sessenta) dias, contados a partir da sua entrega. A proposta deve ser assinada, digitalizada e enviada por e-mail – pode ser utilizada assinatura eletrônica, contanto que utilizados meios autênticos e passíveis de verificação e validação da assinatura.

Os custos devem ser detalhados na proposta comercial, minimamente, conforme cada item a seguir:

- **Licenciamento ou Assinatura Anual:** especificar os itens cobertos e se há diferentes opções de aquisição (exemplo: básico, intermediário, avançado).
- Especificar também os valores unitários de licenças não adquiridas inicialmente, porém que podem ser adquiridas em momentos futuros (por exemplo, licenças de suporte).

- **Arquitetura:** detalhar como a solução será disponibilizada e os recursos de infraestrutura física e lógica para sua instalação (exemplo: on-premises, SaaS, PaaS, IaaS etc.); inserir os valores fixos e ou recorrentes.
- **Implantação:** descrever as fases, com seu tempo médio de duração, para instalar, integrar, configurar.
- **Operação assistida:** por 30 dias da plataforma;
- **Atendimento e Suporte Técnico:** descrever canais, horários e níveis de atendimento disponíveis, acordo de nível de serviço (SLA), especificar se e quando há exceções ou cobranças adicionais, e se são disponibilizados relatórios dos atendimentos realizados com seus respectivos SLAs;
- **Treinamentos:** especificar o plano de treinamento; e
- Demais custos, se houver.

Os valores devem ser expressos em algarismos, com apenas duas casas decimais após a vírgula e por extenso, de forma legível. Em caso de divergência, prevalecerá o valor por extenso.

Os preços cotados serão irreajustáveis pelo prazo de 12 meses.

Além do que já está identificado neste Termo de Referência, devem ser inclusas na proposta quaisquer licenças, subscrições, equipamentos e/ou acessórios necessários para o funcionamento da solução como um todo.

Todas as propostas comerciais recebidas serão analisadas, e **não** serão consideradas aquelas que:

- Estiverem incompletas, pouco detalhadas, não conformes com as definições estabelecidas neste documento; e
- Imponham condições, ocasionem dúvidas quanto a seu teor, contenham preços excessivos ou manifestamente inexequíveis.

Deverá ser encaminhada também uma apresentação institucional da empresa.

9. Termo de Confidencialidade

A documentação de cada fornecedor enviada para a RNP será considerada matéria reservada, preservada a sua confidencialidade, e não será divulgada para os demais participantes, mesmo após a declaração da proposta vencedora, sendo divulgada apenas para os envolvidos no processo interno da RNP. Desta forma, as partes se comprometem, sob pena da lei, a manter a estrita confidencialidade das informações compartilhadas.

10. Aprovação

Após a conclusão de todas as etapas do processo, será contratada a solução que tenha atendimento tecnicamente a todos os requisitos desse processo e de menor preço, sendo encaminhado ao fornecedor vencedor o pedido de compra e, posteriormente a formalização do contrato.