

ANEXO

REQUISITOS TÉCNICOS, REQUISITOS DE SEGURANÇA, REQUISITOS DO SERVIÇO EM NUVEM E MODO E CONDIÇÕES DE EXECUÇÃO DOS SERVIÇOS DE TREINAMENTO E SUPORTE TÉCNICO

Este documento descreve os requisitos técnicos e requisitos de segurança da ferramenta, os requisitos do serviço em nuvem e o modo e as condições de execução dos serviços de treinamento e suporte técnico.

1. REQUISITOS TÉCNICOS

- 1.1. Serviço a ser contratado deverá fornecer acesso via portal web que permita ao CONTRATANTE gerenciar as reuniões e outros materiais dos comitês e colegiados estatutários;
- 1.2. O portal deverá ser um local seguro com acesso somente a pessoas autorizadas através de um ID de usuário e senha exclusiva;
- 1.3. Deverão ser disponibilizados 120 (cento e vinte) acessos distribuídos entre os tipos Usuário e Administrador, sendo 90 (noventa) de usuários e 30 (trinta) de Administradores;
- 1.4. Permitir a convocação de reuniões, disponibilização do calendário de eventos e disponibilização da pauta e material das reuniões;
- 1.5. Permitir a interação com os membros dos colegiados e órgãos de governança por meio de envio de alertas, e-mails e votações on-line;
- 1.6. Possuir interface em português - Brasil;
- 1.7. Possibilitar a inclusão de organograma da empresa, estrutura societária, documentos societários, códigos, políticas, informações legais, informações financeiras e gerenciais das companhias;
- 1.8. Possuir ferramenta de busca que possibilite a pesquisa de conteúdo, conforme o perfil de acesso do usuário, inclusive do conteúdo dos materiais de reunião aos quais o usuário tenha acesso;
- 1.9. Possibilitar upload e download do conteúdo (textos, imagens e arquivos diversos) necessário à realização das reuniões e ao andamento dos trabalhos dos órgãos de governança;
- 1.10. Possibilitar gerenciamento do conteúdo: armazenamento, localização e recuperação de informações, inserção, edição e/ou exclusão de informações;
- 1.11. Possibilitar estruturação de pauta, disponibilização do material das reuniões (permitindo a inclusão de marca d'água nos documentos, contendo o nome do usuário e a data da consulta/impressão), envio de convites, convocações, boletins e informativos;
- 1.12. Possuir ambiente personalizado, incluindo elementos gráficos do BNB;
- 1.13. Possuir disponibilidade de armazenamento de conteúdo com capacidade ilimitada;
- 1.14. As informações processadas, armazenadas e transmitidas devem ser protegidas com uso de algoritmos públicos de criptografia, preferivelmente com a adoção de chaves criptográficas assimétricas. Possuir trilha de auditoria e rastreamento do histórico de acesso de usuários;
- 1.15. Possuir proteção contra vírus de software;
- 1.16. Possuir autenticação por múltiplos fatores distintos;

- 1.17. Ter mecanismo de proteção contra-ataques por força bruta (captcha ou delay progressivo na autenticação ou análogo);
- 1.18. Possibilitar ao BNB acesso às trilhas de auditoria do serviço;
- 1.19. Possibilitar ao BNB acesso a dados de reunião armazenados (pauta, itens, resultado de votação);
- 1.20. Prover meios para a exportação dos dados do BNB, com vistas a promover a continuidade dos processos de negócio do Banco, permitindo a migração de informações para outra solução ou outro provedor de serviços;
- 1.21. Possibilitar somente aos usuários do BNB o acesso aos dados armazenados na ferramenta;
- 1.22. A solução deverá permitir o carregamento de documentos e materiais dos comitês e colegiados estatutários e deverá permitir o acesso e visualização eletrônica através dos principais navegadores web disponíveis no mercado (Internet Explorer, Google Chrome, Microsoft Edge, Mozilla Firefox, Safari);
- 1.23. O sistema deve ser acessível por aplicativo próprio ou, alternativamente, deve ser compatível com os principais navegadores utilizados nessas plataformas;
- 1.24. No caso de dispositivos móveis, o acesso deverá ser por meio de aplicativos para dispositivos móveis compatível com as versões iOS 13 ou superior e Android 9 ou superior;
- 1.25. Deverá permitir configurar perfis de acesso com direitos de acesso definidos pelo CONTRATANTE, com no mínimo:
 - 1.25.1. Usuários: Usuários com capacidade de visualizar os documentos;
 - 1.25.2. Administradores: Usuários com capacidade de carregar, agrupar, imprimir, visualizar, aprovar e publicar documentos dos comitês e colegiados estatutários.
- 1.26. Deverá permitir a configuração e personalização do portal para utilização por administradores, incluindo:
 - 1.26.1. Reunião de planejamento de projeto, inclusive análise do fluxo de trabalho atual e identificação dos principais marcos, levando ao desenvolvimento de um plano de implementação que se ajuste às necessidades e prioridades do CONTRATANTE;
 - 1.26.2. Criação de configuração de contas de usuários;
 - 1.26.3. Definição de política de senha e de configuração de segurança;
 - 1.26.4. Configuração e instalação de recursos off-line no computador do administrador.
- 1.27. A ferramenta deverá possuir solução de backup e alta disponibilidade para garantir a continuidade do serviço em caso de falhas ou indisponibilidade;
- 1.28. Acessos online e off-line para os usuários:
 - 1.28.1. Enquanto estiverem conectados, os usuários poderão visualizar os documentos do cliente usando um navegador ou software específico fornecido pelo CONTRATADO;
 - 1.28.2. Cada usuário poderá acessar o portal da empresa com uma ID de Usuários e senha por meio de um software do cliente e navegadores da internet;

- 1.28.3. A funcionalidade off-line deverá permitir aos usuários baixar os materiais do site através da internet e visualizá-los usando o software do cliente quando não estiver com acesso à internet. A configuração desse recurso deverá incluir a capacidade para transferência de forma segura e armazenar de forma criptografada materiais a um computador designado ou dispositivo móvel compatível e permitir a visualização quando não estiver conectado à internet.
- 1.29. Ao final do contrato, a CONTRATADA não deverá ficar com nenhuma cópia dos dados, repassando-os para o BNB em meio digital antes da sua destruição;
- 1.30. Os servidores devem estar localizados em território brasileiro. Caso não estejam, devem estar em país com o qual o Brasil mantém acordo de cooperação de investigação de dados;
- 1.31. A ferramenta deverá possuir inteligência artificial para consultas, resumos e análises, e responder com base em conteúdo da organização armazenado na Plataforma, evitando alucinações e respeitando as permissões atribuídas a cada usuário;
- 1.32. O material adicionado à plataforma não será utilizado como fonte de dados para usuários externos à organização;
- 1.33. O sistema contará com componente de aplicação de formulários e questionários para avaliações e pesquisas entre os usuários;
- 1.34. Todo o tráfego de dados deverá utilizar protocolos criptográficos seguros (TLS 1.2 ou superior), com desativação de algoritmos obsoletos e validação rigorosa de certificados digitais;
- 1.35. A solução deverá manter trilhas de auditoria completas, imutáveis e exportáveis, abrangendo acessos, edições, votações, downloads, integrações e uso de funcionalidades de IA;
- 1.36. Em ambiente de nuvem, deverá ser assegurada segregação lógica (multitenancy), criptografia de dados em repouso e em trânsito e monitoramento contínuo de segurança;
- 1.37. Os dados institucionais do Banco não poderão ser reutilizados, compartilhados ou utilizados para treinamento externo de modelos de IA, devendo existir regras claras de retenção, descarte e portabilidade ao término do contrato;
- 1.38. Funcionalidades baseadas em inteligência artificial deverão possuir rastreabilidade, restrição de acesso, validação humana dos resultados e garantia de não utilização dos dados fora do escopo contratual;
- 1.39. Devem ser garantidos mecanismos formais de continuidade de negócio, incluindo backups, redundância, recuperação de desastres e SLAs compatíveis com a criticidade do serviço;

2. REQUISITOS DE SEGURANÇA E REQUISITOS DO SERVIÇO EM NUVEM

Elencam-se, abaixo, os requisitos de segurança e os requisitos do serviço em nuvem obrigatórios e desejáveis para a solução.

2.1. Requisitos de segurança:	Condição contratual
2.1.1. Autenticação por múltiplos fatores;	Obrigatório
2.1.2. Senha com avaliação de segurança e bloqueio por erro de tentativas;	Obrigatório
2.1.3. Possibilitar autenticação do serviço integrada com o Active Directory corporativo da contratante;	Desejável

2.1.4. Bloqueio de sessão por inatividade;	Obrigatório
2.1.5. E-mail de confirmação de login com revogação de acesso;	Desejável
2.1.6. Trilha de auditoria;	Obrigatório
2.1.7. Controle de acesso por grupo e usuário;	Obrigatório
2.1.8. Gerenciador de sessões, que permita derrubar sessões abertas em outros dispositivos;	Obrigatório
2.1.9. Impressão de marcas d'água nos documentos;	Obrigatório
2.1.10. Permitir o backup de dados pelo contratante;	Obrigatório
2.1.11. Sistemática de Pentest (teste de invasão) e report ao contratante;	Obrigatório
2.1.12. Planos de contingência para garantir a continuidade do serviço em caso de incidentes ou desastres;	Obrigatório
2.1.13. As informações processadas, armazenadas e transmitidas devem ser protegidas com uso de algoritmos públicos de criptografia, preferivelmente, com a adoção de chaves criptográficas assimétricas (AES-256, ou superior, por exemplo);	Obrigatório
2.1.14. Funcionar em arquitetura de segurança, composto por criptografia, firewalls, antimalware, sistemas de prevenção de invasões e demais práticas usualmente adotadas, para oferecer segurança e integridade do ambiente em geral, inclusive da documentação armazenada;	Obrigatório
2.1.15. Assegurar que a empresa adota controles que mitiguem os efeitos de eventuais vulnerabilidades na liberação de novas versões do aplicativo;	Obrigatório
2.2. Requisitos do serviço em nuvem:	Condição contratual
2.2.1. Nuvem em território nacional;	Desejável
2.2.2. Armazenagem dos dados criptografados (por AES-256, ou superior);	Obrigatório
2.2.3. Identificação do local do Datacenter;	Obrigatório
2.2.4. Estar alocado em Datacenter com disponibilidade mínima de 98,5%;	Obrigatório
2.2.5. Certificações para serviços em nuvem tais como CSA Star, ISO 27017 e 27018;	Desejável
2.2.6. Procedimentos para transferência dos dados ao contratante ou novo contratado e posterior destruição dos dados ao findar o contrato.	Obrigatório

3. MODO E CONDIÇÕES DE EXECUÇÃO DOS SERVIÇOS

3.1. TREINAMENTO

- 3.1.1. Sessões de treinamento destinadas aos Administradores e Usuários com instruções sobre as funcionalidades da ferramenta, procedimentos de login, uso de senha,

criação e construção de um arquivo/banco de dados do serviço, edição e alterações de arquivos em um formato que permita a fácil visualização pelos usuários;

- 3.1.2. Sessões individuais de treinamento com os usuários pela internet;
- 3.1.3. Treinamento sob demanda, totalizando 08 (oito) horas, incluindo treinamento para novos usuários, via web conferência;
- 3.1.4. Guias do usuário para referência rápida e fácil.

3.2. SUPORTE TÉCNICO

- 3.2.1. O CONTRATADO prestará os serviços de Suporte Técnico e de Atualização de Versões da ferramenta pelo prazo do Contrato, a contar da emissão do Termo de Aceitação Definitiva (TAD), conforme cronograma de implantação descrito no item 13.3 do Termo de referência;
- 3.2.2. O serviço de suporte técnico deverá ser provido 24h por dia, 7 dias por semana, e deverá fornecer um canal de comunicação direto para solução dos problemas, em caso de indisponibilidade de qualquer um dos produtos oferecidos pelo CONTRATADO;
- 3.2.3. O número de chamados para os serviços de atendimento remoto do CONTRATADO deverá ser ilimitado, sem restrições de horas de atendimento;
- 3.2.4. Para realizar o serviço de suporte técnico remoto, O CONTRATADO deverá disponibilizar, sem custo adicional para o BANCO, no mínimo, os seguintes canais de atendimento: site na Internet, telefone e e-mail, sendo todas as notificações de incidentes em língua portuguesa;
- 3.2.5. O CONTRATADO se obriga a manter, em ambiente computacional próprio, sistema informatizado para registro dos chamados de manutenção e suporte técnico, permitindo a abertura e o acompanhamento dos chamados pelo BANCO;
- 3.2.6. Os registros deverão conter, pelo menos, as informações de número (protocolo), data e hora do chamado, descrição do problema, situação do chamado, histórico de atendimento e ocorrências relacionadas;
- 3.2.7. O CONTRATADO deverá fornecer, mediante solicitação do BANCO, lista completa contendo as informações relativas aos chamados efetuados e atendidos, pendentes ou não de resolução, incluindo, no mínimo, acesso a todos os relatórios técnicos gerados. Essa lista deverá possibilitar a realização de consultas pelo BANCO, a qualquer momento, do status, do histórico e do andamento do atendimento às solicitações;
- 3.2.8. Ocorrendo problema na operação da ferramenta, em decorrência de mau funcionamento, o nível de severidade de um chamado ao serviço de suporte técnico determinará o prazo máximo que o CONTRATADO terá para apresentar uma solução para o problema a contar do chamado, conforme descrito abaixo:

Nível de Severidade	Impacto no Negócio	Prazo Máximo para a Solução de Contorno	Prazo Máximo para a Solução da Causa do Problema
I	A ferramenta está inoperante ou não possibilita que BANCO utilize a ferramenta com vistas à execução de seus serviços	3 (três) horas corridas	2 (dois) dias úteis

	ou ocasione impacto na realização das reuniões.		
II	A ferramenta está operando, porém com alguma funcionalidade ou módulo não operante que não prejudique a realização das reuniões.	6 (seis) horas corridas	5 (cinco) dias úteis

- 3.2.9. A solução somente será considerada restabelecida quando estiverem integralmente operacionais todas as funcionalidades impactadas em decorrência do evento que ocasionou chamado técnico;
- 3.2.10. Ficará a critério do BANCO o aceite das soluções implantadas;
- 3.2.11. O não cumprimento dos prazos estipulados acima implica nas penalidades especificadas no contrato;
- 3.2.12. Objetivando comprovar os níveis de serviço prestados, o CONTRATADO deverá fornecer relatórios mensais e anuais contendo a quantidade de chamados atendidos, por grau de severidade, a quantidade de chamados resolvidos dentro do prazo, a quantidade de chamados resolvidos fora do prazo e a quantidade de chamados não resolvidos;
- 3.2.13. Procedimentos de Inspeção
- 3.2.13.1. O Banco manterá internamente os registros dos chamados realizados ao CONTRATADO para resolução de incidentes;
- 3.2.13.2. Ficará registrado o tempo de envio da solução de contorno e definitiva, a efetividade das soluções fornecidas, a severidade do chamado e a disponibilidade da ferramenta para registro de chamados disponibilizada pelo CONTRATADO;
- 3.2.13.3. Os registros internos serão comparados com os relatórios fornecidos pelo CONTRATADO.

ANEXO I-B

DECLARAÇÃO DE NÃO OCORRÊNCIA DE REGISTRO DE OPORTUNIDADE

Ao Banco do Nordeste S/A,
Ref. Edital de Pregão Eletrônico nº. ____/2026

Objeto: Aquisição de Portal de Governança, com solução de gestão de reuniões, na modalidade SAAS, acessível em microcomputadores e dispositivo móveis, em modos *online* e *off-line*, em conjunto com os serviços de treinamento, implantação, manutenção, suporte técnico e licenciamento para 120 (cento e vinte) usuários.

Prezados Senhores,

O (LICITANTE), (qualificação), por meio de seu representante legal, **DECLARA**, que para a apresentação de proposta ao referido Edital, **NÃO** houve ocorrência de “**Registro de Oportunidade**”, de modo a garantir o princípio constitucional da isonomia e a seleção da proposta mais vantajosa para a Administração Pública, conforme disposto na Instrução Normativa Nº 1 de 4 de abril de 2019 e n art. 31 da Lei nº 13.303, de 2016.

Local: _____

Data: ____/____/____

Representante Legal:

(ASSINATURA) _____

RG: _____

CPF: _____