1 OBJETO

Aquisição de solução de gestão de vulnerabilidades para o Banco do Nordeste, contemplando aquisição de licenças de uso, serviços de implantação, treinamento, assistência e suporte técnico para o período de 48 (quarenta e oito) meses.

2 JUSTIFICATIVA

O Ambiente de Segurança Corporativa busca, continuamente, a conformidade aos aspectos legais relacionados às questões de segurança cibernética, proteção de dados e sigilo bancário, em consonância com a resolução do Conselho Monetário Nacional (CMN), nº 4.893, a Lei Geral de Proteção de Dados Pessoais - LGPD (Lei nº 13.709/2018) bem como a Lei do Sigilo Bancário (Lei Complementar 105/2001), realizando aquisições de novas soluções de segurança e revisando e criando novos processos de trabalho, visando a prevenção e o tratamento dos incidentes de segurança. O descumprimento destas normas, vale ressaltar, pode ensejar sanções ao Banco do Nordeste. A observância estrita a essas exigências legais é viabilizada por meio de criterioso acompanhamento dos recursos de segurança, com o apoio de equipe contratada, assegurando o efetivo funcionamento de todas as soluções de segurança contratadas.

Cita-se, em especial, a Resolução CMN 4.893, de 26 de fevereiro de 2021, publicada pelo Banco Central do Brasil (BACEN), que dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras brasileiras. O objetivo dessa resolução é garantir que todas as instituições financeiras do país mantenham um padrão mínimo de segurança da informação, segurança cibernética e proteção de dados.

Esta citada resolução obriga as instituições financeiras e demais instituições autorizadas a funcionar pelo BACEN a definir, implementar, divulgar e manter uma política de segurança cibernética formulada a partir de princípios e diretrizes que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados. Desta forma, introduz-se a relatividade sobre o aspecto da sensibilidade dos dados e informações dentro da visão associada aos riscos operacionais e de imagem, e a privacidade de dados, imputando responsabilidade às instituições.

O inciso II do Art. 3º da supracitada resolução define que "*A política de segurança cibernética deve contemplar, no mínimo, os procedimentos e os controles adotados para reduzir a vulnerabilidade da instituição a incidentes e atender aos demais objetivos de segurança cibernética*". Já no inciso II, do parágrafo único do Artigo 6º, é definido que o plano de ação e de resposta a incidentes deve abranger, no mínimo, "*as rotinas, os procedimentos, os controles e as tecnologias a serem utilizados na prevenção e na resposta a incidentes, em conformidade com as diretrizes da política de segurança cibernética.* "

Nesse mister, a política deve contemplar a capacidade da instituição financeira de prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados ao ambiente cibernético, demandando reavaliação de procedimentos e controles internos à luz dos objetivos definidos. Considerando os avanços da tecnologia digital, a natureza das operações e a complexidade dos produtos, serviços, atividades e processos, o atendimento pleno desta exigência regulatória torna-se grande desafio. Os procedimentos e controles existentes, bem como aqueles a serem construídos, vão implicar em reavaliação de tecnologias, novos investimentos e, principalmente, necessidade de pessoal qualificado.

Destacando o Decreto nº 10.222, de 5 de fevereiro de 2020, do Governo Federal, que aprova a Estratégia Nacional de Segurança Cibernética, observando os requisitos e controles estabelecidos no documento, a seção 1.3, "Proteção Estratégica", define uma proteção para infraestruturas

críticas, no qual o sistema financeiro se insere, e destaca que as organizações necessitam de meios para identificar, proteger, detectar, avaliar, responder, recuperar e assim gerenciar o risco das ameaças cibernéticas, e também de ferramentas de automação de segurança que usam inteligência artificial e aprendizado de máquina, que permitam analisar, identificar e conter os ataques cibernéticos.

Diante deste cenário, e considerando a exposição que uma instituição financeira pode representar para os cibercriminosos, implementar um sistema de gestão de vulnerabilidades, além de atender as conformidades regulatórias aplicando práticas robustas de segurança, é primordial para proteção contra ciberataques. Além disso, adquirindo esse tipo de ferramenta é possível identificar, corrigir ou mesmo mitigar vulnerabilidades nas diversas aplicações e sistemas antes que estas possam ser exploradas, de maneira proativa e eficaz, reduzindo assim os riscos de incidentes de segurança. A velocidade com que essas vulnerabilidades são detectadas e como são corrigidas são cruciais para evitar interrupções de serviços, perda de dados e incidentes graves de segurança que possam levar a perdas financeiras e danos à imagem e à reputação.

Um sistema de gestão de vulnerabilidades permite uma visão abrangente das superfícies de ataque, evidenciando e classificando as vulnerabilidades com base em sua gravidade e potencial impacto, auxiliando a tomada de decisões de forma estratégica com foco na priorização das correções das vulnerabilidades mais críticas, reduzindo o risco de exploração. Oferece também a capacidade de realizar verificações regulares e automáticas em base de dados robusta, além oferecer relatórios customizáveis e completos que possibilitam: avaliar a postura de conformidade regulatória, analisar dados históricos para identificar padrões e tendências em vulnerabilidades, analisar ativos e vulnerabilidades específicas de modo que permite realizar ações de remediação de ameaças, comparar a postura de segurança cibernética da organização com outras do mesmo setor.

Ante o exposto, e considerando, sobretudo, a necessidade de conformidade com o arcabouço legal atualmente vigente (Resolução 4.893/2021, Lei 13.709/2018, Lei Complementar 105/2001 e Decretos 10.222/2020 e 9.637/2018), o Banco do Nordeste deve implementar métodos de segurança da informação que protejam as informações pessoais e corporativas, prevenindo ou mitigando os impactos de incidentes e ataques cibernéticos avançados, garantindo a continuidade de seus negócios.

3 DOTAÇÃO ORÇAMENTÁRIA E QUANTIDADES

3.1 O dispêndio total desta aquisição correrá à conta dos recursos previstos na programação do Plano de Dispêndio Global do Banco (PDG) para 202?, em dotação orçamentária própria, sob a rubrica 218000029-CESSÃO DIREITO SISTEMA DE TI – DESPESA ANTECIPADA, referente à entrega da solução de Gestão de Vulnerabilidades e sob a rubrica 291000032- OUTROS SERVIÇOS DE TI para os itens referentes aos serviços de instalação e configuração da solução, serviços de manutenção e atualização, serviços de administração e suporte, serviço de consultoria e treinamento, seguindo o cronograma de desembolso estabelecido na PLC.

3.2 A(s) quantidade(s) para contratação encontra(m)-se discriminada(s) no quadro apresentado abaixo e o detalhamento de cada item se encontra no **ANEXO II - Especificações Técnicas**:

Tabela 1

ITEM	SUBITEM/ MÓDULOS	DESCRIÇÃO	PREVISÃO DE UTILIZAÇÃO

1	1	**Solução de Gestão de Vulnerabilidades para Endpoints**, baseada e com análise contínua e adaptável de riscos e confiança.	**4875**
	2	**Solução de Gestão de Vulnerabilidades para FQDNs** Internos e Externos dos ativos de tecnologia da informação, baseada e com análise contínua e adaptável de riscos e confiança.	**105**
	3	**Solução de Gestão de Vulnerabilidades e Visibilidade de Ataques em tempo real para Estrutura de Diretório de Usuários** baseada e com análise contínua e adaptável de riscos e confiança.	**23.500**
2		Implantação **(ANEXO III – PLANO DE IMPLANTAÇÃO)**	1
3		Suporte e Assistência Técnica **(ANEXO IV – Suporte e Assistência Técnica)**	48 meses
4		Serviço de Treinamento	1

4 CRITÉRIOS PARA SELEÇÃO DO FORNECEDOR

4.1 Juntamente com a proposta de preços, o licitante deverá encaminhar:

4.1.1 planilha de características da solução cotada, obedecendo ao formato e conteúdo do **Anexo II - Especificações Técnicas**, acrescida de coluna indicando, para cada item (características técnicas), o documento ou manual e número da página, na documentação técnica fornecida, que permita a verificação das características técnicas obrigatórias, devendo toda e qualquer referência às características dos produtos cotados ser comprovadas, anexando documentação oficial do fabricante, que ateste o atendimento da correspondente especificação, entendendo-se por documentação do fabricante:

4.1.1.1 documentos públicos que possam ser obtidos no sítio oficial de cada fabricante; ou

4.1.1.2 documentos extraídos de consultas realizadas ao sítio oficial do fabricante na Internet, com informação do endereço eletrônico do fabricante e página onde consta a informação ou característica técnica cotada e data em que foi realizada a impressão;

4.1.2 **declaração** que manterá em seu corpo funcional, durante todo o período de contratação de serviço gerenciado que concerne a fase de implantação, obedecendo o conteúdo do **Anexo II - Especificações Técnicas**, equipe especializada contendo, no mínimo:

4.1.2.1 dois profissionais com perfil técnico, com certificação na ferramenta de gestão de vulnerabilidades, qualificado para conduzir o planejamento e a execução dos serviços de implantação e integração dos componentes da solução contratada;

4.1.2.2 um profissional com certificação PMP – *Project Management Professional* do PMI – *Project Management Institute* ou possuir MBA – *Master of Business Administration* em Gerência de Projetos;

4.1.2.3 um profissional com perfil de consultor, com certificação ISO/IEC 27001 – *Information Security Foundation* ou *ITIL Foundation Certified,* e certificação na ferramenta de gestão de vulnerabilidades, qualificado para conduzir os serviços de consultoria em mapeamento e avaliação de vulnerabilidades, ameaças e riscos, direcionamento de aplicação de configurações baseadas no mercado e nas regras de negócio do Banco, auxílio na estruturação de processo de gestão de vulnerabilidade com indicação de melhores práticas de segurança a serem adotadas com o uso da solução, e repasse de conhecimento para equipe técnica do Banco;

4.1.3 **declaração** que manterá em seu corpo funcional, durante todo o período de contratação de serviço gerenciado que concerne a fase de implantação e estruturação do processo obedecendo o conteúdo do **Anexo III – PLANO DE IMPLANTAÇÃO**, equipe especializada contendo, no mínimo:

4.1.3.1 **3 (três)** profissionais qualificados para conduzir o planejamento e a execução dos serviços de implantação e repasse de conhecimento para equipe técnica do Banco na solução de gestão de vulnerabilidades

4.1.3.2 **1 (um)** Analista de Processos de Análise de Vulnerabilidade nos primeiros 12 meses de contrato, contados da emissão do TAD (Termo de Aceitação Definitiva);

4.2 Para comprovação da qualificação técnica (habilitação), o licitante deverá apresentar atestado(s) de capacidade técnica, expedido(s) por pessoa(s) jurídica(s) de direito público ou privado, que comprove(m) aptidão técnica do licitante no desempenho de atividades pertinentes, compatíveis e de natureza semelhante em características com o objeto desta licitação.

4.2.1 Será considerado compatível com o objeto desta licitação o fornecimento, implantação, administração e suporte a solução de Gestão de Vulnerabilidades e prestação de serviços de consultoria em mapeamento e classificação da informação.

4.2.2 O(s) atestado(s) deverá(ão) conter o nome(s) da(s) empresa(s) declarante(s), a identificação do nome e a assinatura do responsável, bem como o número de telefone para contato.

4.3 Fase de homologação técnica

4.3.1 No prazo de **20 (vinte) dias úteis**, contados da data da solicitação do Pregoeiro no sistema eletrônico, o licitante provisoriamente classificado em primeiro lugar deverá apresentar a solução cotada, a ser demonstrada ao Banco, no CAPGV.

4.3.1.1 A apresentação da solução destinar-se-á à comprovação do atendimento de, pelo menos, 70% (setenta por cento) dos requisitos obrigatórios constantes do **Anexo II - Especificações Técnicas**, escolhidos aleatoriamente pelo BANCO.

4.3.2 Serão de responsabilidade do licitante as atividades e gastos relacionados com a instalação e configuração da solução no ambiente computacional do Banco.

4.3.2.1 Todos os componentes e materiais relativos à solução deverão ser do mesmo modelo e versão da proposta apresentada pelo licitante, identificados e conferidos pelo BANCO;

4.3.2.2 O licitante deverá fornecer todos os recursos de *software* necessários para a comprovação dos requisitos técnicos obrigatórios, sem custo para a instituição;

4.3.2.3 No teste de bancada, deverão ser comprovados, pelo menos, 70% (setenta por cento) dos requisitos obrigatórios constantes do **Anexo II - Especificações Técnicas**, escolhidos aleatoriamente pelo BANCO;

4.3.2.4 A instalação será realizada por técnico(s) do licitante com o devido acompanhamento de técnico(s) do BANCO;

4.3.3 A instalação da solução deverá ser feita de modo a abranger a ativação de todos os componentes de *software* fornecidos, resguardando as devidas proporções por considerarmos ser ambiente de homologação e não de produção.

4.3.3.1 Caberá ao licitante disponibilizar infraestrutura necessária, bem como designar técnico(s) para realizar os procedimentos de instalação e configuração da solução, apresentando a respectiva documentação técnica, deixando-a em plenas condições para homologação pela equipe do BANCO.

4.3.3.2 Todos os componentes e materiais relativos à solução deverão ser disponibilizados de acordo com a proposta apresentada pelo licitante, identificados e conferidos pelo BANCO.

4.3.3.3 No prazo máximo de 2 (dois) dias úteis, a contar da conclusão da instalação dos componentes em perfeito funcionamento da solução no ambiente de homologação, o BANCO procederá à verificação para comprovação da adequação da solução aos requisitos especificados no **Anexo II - Especificações Técnicas**.

4.3.4 Os testes para homologação da solução deverão contar com o devido suporte e acompanhamento presencial de técnico(s) do licitante.

4.3.5 O licitante deverá comunicar formalmente ao BANCO quaisquer dificuldades surgidas durante o processo de homologação.

4.3.6 Não caberá ao Banco do Nordeste, sob qualquer hipótese, o pagamento de nenhum tipo de indenização causada pela rejeição da amostra que não esteja em conformidade com os requisitos estabelecidos nas especificações do Edital.

4.3.7 Havendo conformidade das especificações da solução apresentada com a proposta do licitante e com as definidas no **Anexo II - Especificações Técnicas** do Edital, será confirmada sua classificação em primeiro lugar.

4.3.8 Caso não seja verificada a conformidade das especificações da solução apresentadas com a proposta do licitante e com as definidas nos anexos informados, o licitante terá sua proposta desclassificada, sendo convocado o licitante que apresentar o menor preço seguinte na classificação das demais propostas.

5 VIGÊNCIA DO CONTRATO

O prazo de vigência do Contrato será de 48 (quarenta e oito) meses.

6 CONDIÇÕES DE ENTREGA E IMPLANTAÇÃO

Os requisitos referentes às condições de entrega e aos serviços de implantação a serem observados pelo CONTRATADO estão descritos no **Anexo III - Plano de Implantação.**

7 ESPECIFICAÇÕES E QUANTITATIVOS

Os quantitativos e especificações técnicas dos componentes da solução que integra o objeto da contratação estão descritos no **Anexo II - Especificações Técnicas.**

SERVIÇOS DE ASSISTÊNCIA TÉCNICA E SUPORTE TÉCNICO

Os serviços de assistência e suporte técnico serão realizados conforme o Anexo IV – Requisitos de Assistência e Suporte Técnico

8 CONDIÇÕES DE PAGAMENTO

O pagamento será efetuado mediante crédito em conta corrente indicada pelo CONTRATADO, **não sendo admitida cobrança por meio de boleto bancário**, ficando sua liberação condicionada à total observância do Contrato, nas condições descritas abaixo:

9.1. **Solução de Gestão de Vulnerabilidades:** o pagamento será realizado conforme o cronograma de desembolsos constante do quadro a seguir:

Tabela 2

CRONOGRAMA DE DESEMBOLSO		PERCENTUAL DE DESEMBOLSO (%)
1.	Após a emissão do Termo de Entrega e Conferência (TEC).	25% do valor da implantação
2.	Após a emissão do Termo de Aceitação Provisório 1 (TAP).	25% do valor da implantação
3.	Após a emissão do Termo de Aceitação Definitiva (TAD).	50% do valor da implantação
TOTAL		**100%**

As licenças serão pagas mediante uso, dado o regime de contratação Empreitada por preço unitário, que deverão ser aferidas e pagas de acordo com as medições, até o 10º dia útil de cada mês após a emissão do TAD.

9.2. Suporte e Assistência Técnica (**ITEM 3 da Tabela 01**)**:** o pagamento será efetuado mensalmente, até o 10º (décimo) dia útil do mês subsequente ao da prestação dos serviços, de acordo com as condições estabelecidas no Contrato e demais anexos.

9.3. **Serviço de treinamento** (**ITEM 4** da **Tabela 01**)**:** o pagamento será efetuado após a conclusão do treinamento.

9 REAJUSTE

Os preços dos serviços serão reajustados, anualmente, de acordo com a variação do Índice de Preços ao Consumidor Amplo – IPCA/IBGE, em conformidade com a legislação em vigor, tomando-se por base o índice vigente no mês de apresentação da proposta ou do orçamento a que essa se referir.

10 GARANTIA CONTRATUAL

O CONTRATADO deverá apresentar, no prazo de 10 (dez) dias úteis, prorrogável por igual período, a critério do BANCO, a contar da assinatura do Contrato, comprovante de prestação de garantia de execução equivalente a 5% (cinco por cento) do preço global contratado.

11 SANÇÕES ADMINISTRATIVAS

12.1. Pela inexecução total ou parcial do objeto do Contrato, o BANCO poderá, garantida a prévia defesa, aplicar ao CONTRATADO as seguintes sanções:

12.1.1. advertência;

12.1.2. multa de **1% (um por cento)** por dia de atraso em qualquer uma das fases previstas no **item 4 do Anexo III - Plano de Implantação do Edital,** aplicável sobre o valor do faturamento do item em atraso;

12.1.2.1. após o 30º (trigésimo) dia de atraso e, a critério do BANCO, poderá ocorrer a não aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença;

12.1.3. multa de **0,1% (um décimo por cento)**, aplicável sobre o preço global contratado, por dia de atraso, pela inobservância do prazo fixado para apresentação ou reposição da garantia contratual, limitado a **2% (dois por cento);**

12.1.4. multa de **3% (três por cento)**, aplicável sobre o valor apurado para pagamento no mês em que se verificar a ocorrência faltosa, para o Nível de impacto Alto do subitem **2.7** do **Anexo IV – Requisitos de Assistência e Suporte Técnico.**

12.1.5. multa de **2% (dois por cento)**, aplicável sobre o valor apurado para pagamento no mês em que se verificar a ocorrência faltosa, pelo não atendimento dos níveis de serviços relacionados à assistência e suporte técnico de impacto médio, previsto no subitem 2.7 do **Anexo IV – Requisitos de Assistência e Suporte Técnico**;

12.1.6 multa de **1% (um por cento)** por ocorrência, aplicável sobre o valor apurado para pagamento no mês em que se verificar a ocorrência faltosa, pelo não atendimento dos níveis de serviços relacionados à assistência e suporte técnico de impacto baixo, previsto no subitem 2.7 do **Anexo IV – Requisitos de Assistência e Suporte Técnico**

12.1.7. multa compensatória correspondente a **5% (cinco por cento),** aplicável sobre o preço global do Contrato, caso não seja garantido absoluto sigilo sobre todos os processos, rotinas, objetos, informações, documentos e quaisquer outros dados fornecidos pelo BANCO, além das cominações previstas na legislação, podendo o BANCO rescindir o Contrato;

12.1.8. multa de **5% (cinco por cento),** aplicável sobre o preço global do Contrato, no caso de ocorrência de ações danosas ou criminosas cometidas por empregados, prepostos do CONTRATADO, empresas ou pessoas por ele contratadas ou designadas, no exercício das atividades previstas no Contrato que ocasionem prejuízos ao BANCO, a seus clientes/usuários de serviços bancários, devidamente comprovados através de decisão judicial (transitada em julgado), mais o valor correspondente ao valor do prejuízo apurado;

12.1.9. multa de **10% (dez por cento)**, aplicável sobre o preço global contratado, nas demais violações ou descumprimentos de cláusula(s) ou condição(ões) estipulada(s) no Contrato;

12.1.10. multa de **10% (dez por cento),** aplicável sobre o preço global contratado, em caso de inexecução total do Contrato;

12.1.11. suspensão temporária de participar em licitação e impedimento de contratar com o BANCO pelo prazo de até 2 (dois) anos.

12 TIPO DE JULGAMENTO

O tipo de julgamento será menor preço global.

13 REGIME DE EXECUÇÃO

O regime de execução será empreitada por preço unitário.

14 RESPONSÁVEL PELO TERMO DE REFERÊNCIA E PELA FISCALIZAÇÃO

Ambiente de Segurança Corporativa.