ANEXO I

TERMO DE REFERÊNCIA

1. OBJETO

Contratação de solução de coleta e correlação de logs e eventos de segurança (SIEM) integrada a serviços de inteligência de ameaças (*Threat Intelligence Feeds*), serviços de SOAR (*Security Orchestration, Automation, and Response*), gestão de operações e de resposta a incidentes de segurança da informação, serviços especializados de gerenciamento e monitoração de ativos de rede e de segurança da informação, através de um Centro de Operações de Segurança (SOC), com serviços de implantação, instalação, configuração, criação de políticas e processos no ambiente do Banco, além de atualizações de segurança, serviços de suporte e manutenção, e treinamentos nas soluções ofertadas, conforme especificações constantes do Edital e seus Anexos.

2. JUSTIFICATIVA DA CONTRATAÇÃO

O Ambiente de Segurança Corporativa busca continuamente a conformidade no aspecto legal relacionado à política de segurança, proteção de dados e sigilo bancário, conforme a resolução do Conselho Monetário Nacional (CMN), nº 4.893, a Lei Geral de Proteção a Dados Pessoais - LGPD (Lei nº 13.709) e a Lei do Sigilo bancário (Lei Complementar 105/2001), contratando novas soluções e criando novos processos que envolvam o suporte técnico da equipe terceirizada, cujo descumprimento das normas 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 da equipe terceirizada, assegurando o efetivo funcionamento de todos os dispositivos.

Além disso, tem-se a Resolução CMN 4.893/21, de 26 de fevereiro de 2021, publicada pelo Banco Central do Brasil, a qual 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 e proteção de dados.

A citada resolução obriga as instituições financeiras e demais instituições autorizadas a funcionar pelo Bacen a definir, implementar, divulgar e manter 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.

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*". No parágrafo 2º, do mesmo artigo, é definido que "*os procedimentos e os controles de que trata o inciso II do caput devem abranger, no mínimo, a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção de vulnerabilidades, a proteção contra softwares maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações*".

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 sob a luz dos objetivos definidos. Os avanços da tecnologia digital, a natureza das operações e a complexidade dos produtos, serviços, atividades e processos, estabelecem substanciais e contínuos desafios para o atendimento pleno desta exigência, de modo que a reavaliação de tecnologias, novos investimentos e, principalmente, a prospecção de pessoal qualificado estabelecem-se como ações imperativas.

Com o aumento permanente das ameaças, conhecer e gerenciar bem os riscos de segurança cibernética tornou-se uma das grandes preocupações dos líderes de empresas e governos. Cada vez mais, elas adotam modelos e tecnologias inovadoras, como a segurança cibernética baseada na nuvem, *Security Analytics, Machine Learning*, inteligência artificial e a autenticação avançada para reduzir riscos e melhorar seus programas de segurança, bem como a contratação de profissionais e empresas qualificadas para prestar o suporte especializado e consultivo ao ambiente cibernético corporativo.

Além disso, em 06/02/2020 foi aprovada a Estratégia Nacional de Segurança Cibernética - E-Ciber, conforme o disposto no inciso I do art. 6º do Decreto nº 9.637, de 26 de dezembro de 2018, onde está registrado que "*É de amplo conhecimento que toda organização, pública ou privada, deve possuir uma equipe de tratamento e resposta aos incidentes cibernéticos - ETIR, também conhecida pela sigla - CSIRT, de Computer Security Incident Response Team. Essa equipe deve ser capacitada, e deve dispor de ferramentas computacionais adequadas às suas necessidades, e de sistemas baseados em tecnologias emergentes, condizentes com os padrões internacionais*".

Buscando aderência aos requisitos mínimos de segurança cibernética, definidos pelo Banco Central do Brasil, através da Resolução 4.893, e da Estratégia Nacional de Segurança Cibernética - E-Ciber, além de dar continuidade ao serviço prestado através do contrato 2021/095, a aquisição desta nova solução e serviços tem o intuito de manter o serviço de identificação e trazer automação de respostas em tempo mais ágil possível para os incidentes de segurança que envolvem as outras ferramentas utilizadas pelo Banco do Nordeste do Brasil, e assim preservar os ativos corporativos (*hardware*, *software* e dados) do BANCO, de modo a elevar a segurança das informações institucionais, minimizar riscos operacionais e evitar prejuízos, tanto de ordem financeira como de imagem institucional.

3. DOTAÇÃO ORÇAMENTÁRIA

As despesas decorrentes da contratação correrão à conta de recursos previstos em dotação orçamentária própria, sob as rubricas: rubrica 291000032- OUTROS SERVIÇOS DE TI e 218000029- CESSÃO DIREITO SISTEMA DE TI – DESPESA ANTECIPADA para o item 1, referente à solução de segurança e licenças e sob a rubrica 291000032- OUTROS SERVIÇOS DE TI para os itens 2,3, 4, 5 e 6, referentes aos serviços de implantação, suporte técnico e manutenção de equipamentos, monitoração do ambiente e serviços de treinamento na solução ofertada, sendo realizadas seguindo o cronograma de desembolso estabelecido.

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:

ITEM	DESCRIÇÃO	QUANT.
1.0	**FERRAMENTA DE COLETA E CORRELAÇÃO DE EVENTOS DE SEGURANÇA (SIEM)**	**-**
1.1	Aquisição da solução (em nuvem).	1

1.2	Serviços de manutenção, suporte técnico e atualização de versões dos componentes, pelo período de 24 (vinte e quatro) meses, contados da data de emissão do TAD.	1
2.0	**SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO DE SIEM**	**1**
3.0	**SERVIÇO ESPECIALIZADO DE ADMINISTRAÇÃO E SUPORTE ÀS FERRAMENTAS OFERTADAS, pelo período de 24 (vinte e quatro) meses.**	**1**
4.0	**SERVIÇO DE MONITORAÇÃO E NOTIFICAÇÃO DE INCIDENTES DE SEGURANÇA, pelo período de 24 (vinte e quatro) meses.**	**1**
5.0	**SERVIÇO ESPECIALIZADO DE APOIO À GESTÃO DO SOC, pelo período de 24 (vinte e quatro) meses.**	**1**
6.0	**TREINAMENTOS**	**-**
6.1	Modulo I - Solução Integrada de SOC	4 turmas
6.2	Modulo II - *Security Analytics*	4 turmas
6.3	Modulo III – Tratamento de Incidentes de Segurança	4 turmas

Quadro 1

4. CRITÉRIOS PARA SELEÇÃO DO FORNECEDOR

4.1. Documentação complementar à Proposta de Preço:

4.1.1. planilha de características técnicas dos serviços cotados, 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. Planilha conforme exemplificada no Anexo denominado “Demonstrativo de Formação de Preços”, devidamente preenchida, contendo informações detalhadas de formação dos preços dos serviços ofertados, contendo discriminação de todos os insumos e custos unitários em atendimento ao acórdão 1432/2024 do Tribunal de Contas da União;

4.1.3. declaração que manterá em seu corpo funcional, durante todo o período de implantação das soluções contratadas, obedecendo o conteúdo do Anexo II - Especificações Técnicas, equipe especializada contendo, no mínimo:

4.1.3.1. dois profissionais de nível técnico qualificados para acompanhar o planejamento e a execução dos serviços de implantação e integração dos componentes da solução de SIEM;

4.1.3.1.1. os profissionais devem ser certificados na implantação da solução de SIEM ofertada e com experiência comprovada de 01 (um) ano na implantação de soluções de SIEM;

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

4.1.4. declaração que manterá em seu corpo funcional, durante todo o período de suporte contratado obedecendo o conteúdo do Anexo II - Especificações Técnicas, equipe especializada contendo, no mínimo:

4.1.4.1. dois profissionais certificados na administração da solução de SIEM ofertada e com experiência comprovada de 01 (um) ano na administração de soluções de SIEM;

4.1.4.2. pelo menos um profissional qualificado para realizar as atividades de apoio à gestão do SOC, de forma remota, com as seguintes qualificações:

4.1.4.2.1. Formação Acadêmica: Curso Superior completo na área de informática ou Curso Superior completo em qualquer área de formação acrescido de pós-graduação na área de informática;

4.1.4.2.2. Experiência comprovada de 3 (três) anos de atuação em atividades de gestão de incidentes de segurança da informação;

4.1.4.2.3. Possuir certificação EC-Council's *Certified SOC Analyst* (CSA);

4.1.4.2.4. Possuir certificação EC-Council's *Certified Incident Handler* (E|CIH);

4.1.4.3. Pelo menos um dos profissionais do SOC deverá possuir certificação EC-Council's *Certified Threat Intelligence Analyst* (C|TIA).

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 e suporte à solução de coleta e correlação de logs e eventos de segurança (SIEM) integrada a serviços de inteligência de ameaças (ThreatIntelligenceFeeds), serviço de SOAR, plataforma para gestão de operações e de resposta a incidentes de segurança da informação, e serviços especializados de gerenciamento e monitoração de ativos de rede e de segurança da informação, através de um Centro de Operações de Segurança (SOC).

4.3. 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.

4.4. Fase de homologação técnica

4.4.1. 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.

4.4.1.1. 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.

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

4.4.2.1. 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;

4.4.2.2. O licitante deverá fornecer todos os recursos necessários para a comprovação dos requisitos técnicos obrigatórios, sem custo para a instituição;

4.4.2.3. 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;

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

4.4.3. A instalação da solução deverá ser feita na nuvem do fabricante de modo a abranger a ativação de todos os componentes fornecidos, resguardando as devidas proporções por considerarmos ser ambiente de homologação e não de produção.

4.4.3.1. 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.

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

4.4.3.3. 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.

4.4.4. Todos as despesas necessárias para o cumprimento dos requisitos da fase de homologação serão de responsabilidade do Licitante, que não poderá deixar de cumprir qualquer obrigação contratual, nem justificar acréscimos de valor em sua planilha de custos ou proposta.

4.4.5. Caso o sistema de gerenciamento necessite de infraestrutura diferente ou além da que será disponibilizada pelo Banco esta deverá ser provida pelo Contratado sem que isso incorra em qualquer tipo de ônus para o Banco, incluindo despesas decorrentes do licenciamento de software e da contratação de hardware.

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

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

4.4.8. 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.

4.4.9. 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.

4.4.10. 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. DESCRIÇÃO DOS SERVIÇOS

As especificações técnicas dos componentes da solução que integram o objeto da contratação estão descritas no **Anexo II - Especificações dos Serviços**.

6. PRAZO DE EXECUÇÃO DOS SERVIÇOS E VIGÊNCIA DO CONTRATO

O prazo de vigência do Contrato e execução dos serviços será de 30 (trinta) meses, sendo o período de até 6 (seis) meses referente aos serviços de implantação e 24 (vinte e quatro) meses referente aos demais serviços após a emissão do TAD, podendo ser prorrogado por igual período, mediante Aditivo Contratual, limitado a 60 (sessenta) meses.

7. PLANO DE 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.**

8. CONDIÇÕES DE PAGAMENTO

Os pagamentos serão efetuados 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, conforme abaixo:

Ferramenta de coleta e correlação de eventos de segurança – SIEM (ITENS 1.1 e 1.2 do Quadro 01 do Anexo I – Termo de Referência): o pagamento será realizado conforme o cronograma de desembolsos constante do quadro a seguir:

CRONOGRAMA DE DESEMBOLSO		PERCENTUAL DE DESEMBOLSO (%)
1.	Após a emissão do Termo de Entrega e Conferência (TEC).	30%
2.	Após a emissão do Termo de Aceitação Provisório 1 (TAP1).	10%
3.	Após a emissão do Termo de Aceitação Provisório 2 (TAP2).	10%
4.	Após a emissão do Termo de Aceitação Provisório 3 (TAP3).	10%

5.	Após a emissão do Termo de Aceitação Definitiva (TAD).	40%
TOTAL		**100%**

Serviços de instalação e configuração das soluções de SIEM (**ITEM 2** do **Quadro 01 do Anexo I - Termo de Referência**)**:** o pagamento integral será efetuado após a emissão do Termo de Aceitação Definitiva (TAD).

Serviço especializado de administração e suporte às ferramentas ofertadas (**ITEM 3** do **Quadro 01 do Anexo I - Termo de Referência**)**:** 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.

Serviço de monitoração e notificação de incidentes de segurança (**ITEM 4** do **Quadro 01 do Anexo I - Termo de Referência**)**:** 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.

Serviço especializado de apoio à gestão do SOC (**ITEM 5** do **Quadro 01 do Anexo I - Termo de Referência**)**:** 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.

Treinamentos (**ITENS 6.1, 6.2 e 6.3** do **Quadro 01 do Anexo I - Termo de Referência**)**:** o pagamento será efetuado após a conclusão de cada turma/treinamento.

9. REAJUSTE

Os preços dos serviços serão reajustados anualmente de acordo com a variação do Índice de Custos de Tecnologia da Informação – ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada (IPEA), podendo ser adotado, no caso de extinção, outro índice que venha a substituí-lo, em conformidade com a legislação em vigor, tomando-se por base o índice vigente no mês de apresentação da proposta.

10. GARANTIA CONTRATUAL

Para assegurar o integral cumprimento de todas as obrigações contratuais assumidas, o CONTRATADO deverá apresentar, no prazo de 10 (dez) dias úteis, prorrogável por igual período, a critério do BANCO, a contar do início da vigência do Contrato, comprovante de prestação de garantia de execução equivalente a 10% (dez por cento) do preço global contratado.

11. SANÇÕES ADMINISTRATIVAS

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

11.1.1. advertência;

11.1.2. multa de 5% (cinco por cento) aplicável sobre o valor do faturamento no mês da ocorrência da reincidência na aplicação de advertência de qualquer natureza no período de 4 (quatro) meses consecutivos;

11.1.3. multa de 1% (um por cento) por dia de atraso em qualquer uma das fases previstas no item 5 do Anexo III - Plano de Implantação do Edital, aplicável sobre o valor do faturamento do item em atraso;

11.1.3.1. 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;

11.1.4. 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);**

11.1.5. 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;

11.1.6. multa de 10% (dez por cento), aplicável sobre o valor mensal do Contrato, quando configuradas as situações abaixo descritas:

11.1.6.1. quebra de sigilo das informações do CONTRATANTE;

11.1.6.2. procedimentos executados de forma errada ou com não conformidades, ensejando a ocorrências de incidentes, interrupções, indisponibilidades e alterações nas configurações de equipamentos, serviços e recursos do BANCO, quando não solicitados por este;

11.1.7. multa de **10% (dez por cento),** aplicável sobre o valor apurado para pagamento quando se verificar a ocorrência faltosa, nas demais violações ou descumprimentos de cláusula(s) ou condição(ões) estipulada(s) no Contrato;

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

11.1.9. outros redutores de pagamento com respectivos percentuais, conforme descritos no Anexo IV - Níveis Mínimos de Serviços

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

12. REGIME DE EXECUÇÃO

Empreitada por preço global.

13. CRITÉRIO DE JULGAMENTO

Menor preço global.

14. UNIDADE RESPONSÁVEL PELA ELABORAÇÃO DO TERMO DE REFERÊNCIA E FISCALIZAÇÃO

Ambiente de Segurança Corporativa

GUSTAVO Sikora de Melo F159956
Gerente Executivo, e.e.
Célula de Segurança da Informação

LEOPOLDO Soares de Melo Junior F114162
Gerente de Ambiente