

ANEXO I

TERMO DE REFERÊNCIA

1. OBJETO

1.1. Contratação de serviços especializados de suporte à segurança da informação e cibernética, de prevenção e combate a fraudes e de prevenção e combate à lavagem de dinheiro, em modo presencial e híbrido, em conformidade com as especificações constantes do Edital e seus anexos.

2. JUSTIFICATIVA DA CONTRATAÇÃO

2.1. O Banco do Nordeste mantém o contrato 2020/229 com a empresa WIPRO DO BRASIL SERVIÇOS LTDA para a prestação de serviços técnicos especializados de Suporte à Segurança da Informação, cuja vigência é 31/12/2024.

2.2. Apesar das reiteradas tentativas promovidas por este Ambiente para viabilizar a continuidade do contrato 2020/229, considerando a possibilidade de prorrogação até 30/06/2025, a empresa WIPRO, por questões estritamente particulares, firmou posicionamento pela impossibilidade de prolongamento do pacto.

2.3. Sendo assim, diante da iminência do final da atual vigência do contrato, e descartada a possibilidade de prorrogação, faz-se necessário iniciar novo processo licitatório visando evitar a descontinuidade dos serviços contratados. As atividades atualmente exercidas pela equipe contratada estão divididas entre dois importantes processos:

2.3.1. Suporte Técnico à Segurança da Informação, ao Combate a Fraudes e Prevenção a Lavagem de Dinheiro; e

2.3.2. Resposta a Incidentes de Segurança da Informação (GRIS-I)¹.

2.4. A seguir são enumeradas as principais atividades desempenhadas pela equipe contratada, de acordo com os eixos:

2.4.1. Eixo 1 - Equipe de suporte técnico à segurança da informação, prevenção e combate a fraudes e a lavagem de dinheiro

2.4.1.1. apoio na prospecção de novas soluções e técnicas de proteção ou melhoria daquelas existentes, envolvendo identificação de vulnerabilidades, ameaças, ataques e legislação relacionada a crimes digitais e tendências relativas à segurança cibernética e da informação;

2.4.1.2. apoio, consultoria e suporte na implantação, desenvolvimento e utilização dos controles e das soluções de segurança cibernética e da informação;

2.4.1.3. auxílio na definição de políticas, normas, controles, padrões e requisitos de segurança;

2.4.1.4. apoio no gerenciamento dos recursos e soluções de segurança ora implantados;

2.4.1.5. auxílio na definição de parâmetros de controle, regras e procedimentos nos recursos e soluções de segurança cibernética e da informação;

2.4.1.6. apoio na análise e tratamento de incidentes de segurança cibernética e da informação;

¹ Equipe conhecida como GRIS-I - Grupo de Resposta a Incidentes de Segurança da Informação, serviço que é prestado há 20 anos.

- 2.4.1.7. auxílio na elaboração de materiais relativos à educação em segurança cibernética e da informação.
- 2.4.2. Eixo 2 - Grupo de Resposta a Incidentes de Segurança da Informação (GRIS-I)
- 2.4.2.1. auxílio na implantação de parâmetros de controle, regras e procedimentos nos recursos e soluções de segurança cibernética e da informação;
 - 2.4.2.2. monitoramento dos recursos e soluções de segurança cibernética e da informação;
 - 2.4.2.3. monitoramento da segurança da infraestrutura de rede do Banco;
 - 2.4.2.4. monitoramento de segurança em recursos e serviços bancários;
 - 2.4.2.5. apoio na detecção, análise e tratamento de incidentes de segurança cibernética e da informação.
- 2.5. 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.
- 2.6. 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.
- 2.7. 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.
- 2.8. 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”.
- 2.9. 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.

- 2.10. Com o aumento permanente das ameaças e a atual posição do Banco, 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 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.
- 2.11. A fim de atender ao exigido pela Resolução nº 4.893, este Ambiente de Segurança Corporativa destaca a necessidade de contratação de serviços especializados de Suporte à Segurança da Informação, englobando além dos perfis já atuantes, outros perfis, como: “perfil voltado para tratamento de incidentes”, “perfil de análise de vulnerabilidades” e “perfil de análise de dados”, de forma a amparar as atividades compatíveis às exigências legais e regulamentares.
- 2.12. Para atendimento dos serviços propostos, há a necessidade de:
- 2.12.1. alocação de postos de serviço ininterruptos, escala (24x7x365), para operação de firewall, monitoramento, suporte especializado e tratamento de incidentes de segurança;
- 2.12.2. alocação de equipe técnica especializada por 40 (quarenta) horas técnicas semanais de serviço, no período de 8h-17h, de segunda-feira a sexta-feira, para suporte em gerenciamento de produtos e serviços de segurança da informação, Prevenção à Fraudes e Prevenção a Lavagem de Dinheiro, liderança e supervisão das atividades deste objeto.
- 2.13. A forma de contabilização dos serviços será de unidades de serviços (US) ou hora de serviço, com valores estimados a partir de planilha de custos e formação de preços, similar à existente no Anexo III da Instrução Normativa nº. 05/2017 do Ministério do Planejamento, com lucro e sem percentual de reserva técnica.
- 2.14. Considerando a quantidade mínima estimada para execução dos novos serviços de aproximadamente 73 profissionais, que totalizam cerca de 12.848 (doze mil oitocentos e quarenta e oito) horas de serviço.

3. DOTAÇÃO ORÇAMENTÁRIA

- 3.1. As despesas decorrentes da contratação correrão à conta de recursos previstos em dotação orçamentária própria, sob a rubrica 00000342/000032 - SISTEMA DE SEGURANÇA - SERVIÇOS DE TERCEIROS.

4. ESTIMATIVA DE QUANTIDADE DE SERVIÇO

- 4.1. As estimativas mínimas de consumo para o Contrato encontram-se discriminadas no quadro a seguir:

ESPECIALIDADES		PERFIL	QUANTIDADE MÍNIMA DE PROFISSIONAIS	QUANTIDADE ESTIMADA DE HORAS
US - 1	Serviço de Supervisão Técnica de Segurança da Informação e Cibernética	-	1	176
US - 2	Serviço de Liderança Técnica de Governança de Segurança da Informação	-	1	176

US - 3	Serviço de Liderança Técnica de Segurança da Informação e Cibernética (Operações de Segurança)	-	2	352
US - 4	Serviço de Liderança Técnica de Segurança da Informação e Cibernética (Operações Defensivas)	-	2	352
US - 5	Serviço de Liderança Técnica de Segurança da Informação e Cibernética (Operações Ofensivas)	-	1	176
US - 6	Serviço de Gerenciamento de Projetos e Melhorias	-	2	352
US - 7	Serviço de Gerenciamento do Conhecimento (Base de Conhecimento e Conscientização)	PERFIL I	1	176
		PERFIL II	1	176
		PERFIL III	1	176
US - 8	Serviço de Gerenciamento de Dados	-	2	352
US - 9	Serviço de Segurança da Informação e Cibernética (Operações de Segurança I)	-	3	528
US - 10	Serviço de Segurança da Informação e Cibernética (Operações de Segurança II)	-	3	528
US - 11	Serviço de Segurança da Informação e Cibernética (Operações de Segurança III)	-	3	528
US - 12	Serviço de Atendimento e Tratamento de Requisições e Resposta a Incidentes (Security Operations Center)	-	9	1584
US - 13	Serviço de Segurança da Informação e Cibernética (Operações Defensivas)	PERFIL I	9	1584
		PERFIL II	3	528
US - 14	Serviço de Segurança da Informação e Cibernética (Operações Ofensivas)	PERFIL I	3	528
		PERFIL II	2	352
US - 15	Serviço de Consultoria	PERFIL I	5	880
		PERFIL II	8	1408
US - 16	Serviço de Operações de Combate e Prevenção a Fraude	PERFIL I	2	352
		PERFIL II	3	528
		PERFIL III	2	352
US - 17	Serviço de Operações de Combate e Prevenção à Lavagem de Dinheiro	PERFIL I	2	352
		PERFIL II	2	352
TOTAL MENSAL			73	12.848
TOTAL 24 MESES			-	308.352

5. CRITÉRIOS PARA SELEÇÃO DO FORNECEDOR

- 5.1. Consulta ao Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e Cadastro Nacional de Empresas Punidas (CNEP) do Portal da Transparência (disponíveis em www.portaldatransparencia.gov.br, nos links “Ceis” e “CNEP”, respectivamente);
- 5.2. Consulta ao Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa do Conselho Nacional de Justiça - CNJ (disponível em www.cnj.jus.br/improbidade_adm/consultar_requerido.php);
- 5.3. Consulta à Lista de Inidôneos do TCU (disponível em: <http://portal.tcu.gov.br/responsabilizacao-publica/licitantes-inidoneas/>);
- 5.4. Comprovação da REGULARIDADE FISCAL E TRABALHISTA, conforme a seguir:

- 5.4.1. Prova de regularidade para com a Fazenda Federal, mediante apresentação de certidão expedida pela Secretaria da Receita Federal do Brasil - RFB e pela Procuradoria-Geral da Fazenda Nacional - PGFN, referente a todos os tributos federais e à Dívida Ativa da União - DAU por elas administrados;
- 5.4.2. Certificado de Regularidade do Fundo de Garantia por Tempo de Serviço - FGTS, emitido pela Caixa Econômica Federal;
- 5.4.3. Certidão Negativa de Débitos Trabalhistas - CNDT, ou Positiva com Efeito de Negativa, em cumprimento ao disposto na Lei n.º 12.440, de 7/7/2011;
- 5.5. Declaração de vedação ao Nepotismo;
- 5.6. Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, acompanhado de documentos comprobatórios da eleição de seus administradores, no qual deverá constar, dentre os objetivos sociais, a execução de atividades da mesma natureza ou compatíveis com o objeto da contratação;
- 5.7. Documentação complementar à Proposta de Preço:
- 5.7.1. Planilha de Composição de Custos, devidamente preenchida, na forma do Anexo IX do Edital;
- 5.7.2. Comprovação do Fator Acidentário de Prevenção (FAP), por meio de apresentação da GFIP atualizada ou de outro documento apto a evidenciá-lo;
- 5.7.3. A proposta do licitante não pode apresentar valores de remuneração inferiores aos previstos no quadro constante do item 5.8 deste Termo.
- 5.8. Julgamento das Propostas de Preços (exequibilidade) - Quanto à remuneração dos profissionais a serem alocados na prestação dos serviços, a proposta deverá usar como referência os valores mínimos descritos no quadro a seguir, para cada especialidade de prestação de serviços:

Unidades de Serviço	Perfil	Salário Estimado (R\$)
US-1 Supervisão de Segurança da Informação e Cibernética	-	R\$22.414,20
US-2 Liderança Técnica de Governança de Segurança da Informação	-	R\$15.186,37
US-3 Liderança Técnica de Segurança da Informação e Cibernética (Operações de Segurança)	-	R\$15.186,37
US-4 Liderança Técnica de Segurança da Informação e Cibernética (Operações Defensivas)	-	R\$15.186,37
US-5 Liderança Técnica de Segurança da Informação e Cibernética (Operações Ofensivas)	-	R\$15.186,37
US-6 Gerenciamento de Projetos e Melhorias	-	R\$15.366,71
US-7 Gerenciamento do Conhecimento (Base de Conhecimento e Conscientização)	Perfil I	R\$6.656,65
	Perfil II	R\$8.848,32
	Perfil III	R\$7.998,32
US-8 Gerenciamento de Dados	-	R\$10.237,29
US-9 Segurança da Informação e Cibernética (Operações de Segurança I) - (SIEM, Inteligência de Ameaças e Automação)	-	R\$9.399,51
US-10 Segurança da Informação e Cibernética (Operações de Segurança II) - (O365, DLP, CASB)	-	R\$9.399,51

US-11 Segurança da Informação e Cibernética (Operações de Segurança III) - (Certificados Digitais, HSM, Gestão de Identidades e Acesso)	-	R\$9.399,51
US-12 Atendimento e Tratamento de Requisições e Resposta a Incidentes (Security Operations Center)	-	R\$6.823,32
US-13 Segurança da Informação e Cibernética (Operações Defensivas) - (Redes, Firewall, SSE, GAV, EDR, WAF, SWG)	Perfil I	R\$9.399,51
	Perfil II	R\$11.857,84
US-14 Segurança da Informação e Cibernética (Operações Ofensivas) - (Hacker Ético e Análise de Vulnerabilidades)	Perfil I	R\$9.399,51
	Perfil II	R\$12.032,84
US-15 Consultoria	Perfil I	R\$13.485,52
	Perfil II	R\$13.485,52
US-16 Operações de Combate e Prevenção a Fraude	Perfil I	R\$6.823,32
	Perfil II	R\$9.399,51
	Perfil III	R\$11.857,84
US-17 Operações de Combate e Prevenção à Lavagem de Dinheiro	Perfil I	R\$10.237,29
	Perfil II	R\$13.570,62

5.9. Qualificação técnica (habilitação) - Para comprovação da qualificação técnica, o licitante deverá apresentar atestado(s) de capacidade técnica, expedido(s) por pessoa(s) jurídica(s) de direito público ou privado, em papel timbrado, que comprove(m) a aptidão para desempenho de atividades pertinente e compatível em características, quantidades e prazos com o objeto do Edital.

5.10. Para fins de verificação da qualificação técnica, será observado o disposto a seguir:

5.10.1. Será considerado compatível com o objeto do Edital a execução de serviços especializados de suporte à segurança da informação e cibernética e de prevenção e combate à fraudes de, no mínimo, 3 (três) anos, que sejam ou tenham sido prestados para instituições públicas ou privadas com pelo menos 7.000 (sete mil) colaboradores, de acordo com as características mínimas abaixo:

5.10.1.1. Prestação de serviços de segurança da informação e cibernética, incluindo o tratamento de incidentes de segurança;

5.10.1.2. Prestação de serviços de análise de vulnerabilidades, incluindo o monitoramento e tratamento das vulnerabilidades encontradas;

5.10.1.3. Prestação de serviços de suporte ou prestação de serviços de manutenção para: Firewall, Filtro de conteúdo WEB, SIEM (Security Information and Event Management), DLP (Data Loss Prevention), Microsoft Active Directory e Antivírus/Antispam em redes com, pelo menos, 2.500 (dois mil e quinhentos) ativos computacionais;

5.10.1.4. Prestação de serviços de consultoria especializada nas diversas disciplinas envolvendo os temas: segurança da informação e cibernética e prevenção e combate a fraudes, de, no mínimo, 6 (seis) mil horas anuais;

5.10.2. Não serão aceitos atestados emitidos pelo licitante, em seu próprio nome, ou em nome de fornecedor, fabricante ou distribuidor, nem qualquer outro em desacordo com as exigências do Edital. Serão aceitos apenas atestados assinados por empresas contratantes (clientes finais) dos serviços prestados;

- 5.10.3. Será admitido o somatório das quantidades descritas em um ou mais atestados apresentados para compor a quantidade especificada;
- 5.10.4. Será admitido o somatório de atestados para comprovação da experiência, entretanto, os períodos concomitantes serão computados uma única vez;
- 5.10.5. As comprovações de qualificação técnica exigidas no Edital equivalem a, no máximo, 50% (cinquenta por cento) da infraestrutura computacional atual do CONTRATANTE, bem como aos serviços que deverão ser prestados no âmbito da presente contratação;
- 5.10.6. O(s) atestado(s) de capacidade técnica deverá(ão) se referir a serviços prestados no âmbito de sua atividade econômica principal e/ou secundária, especificada no contrato social, devidamente registrado na junta comercial competente, bem como no cadastro de Pessoas Jurídicas da Receita Federal do Brasil - RFB;
- 5.10.7. Os licitantes deverão disponibilizar, quando solicitadas pelo Pregoeiro, todas as informações necessárias à comprovação da legitimidade do(s) atestado(s) de capacidade técnica apresentado(s), podendo, para tanto, o Pregoeiro solicitar cópia do instrumento que deu suporte à contratação, endereço atual do contratante e local em que foram prestados os serviços, dentre outros documentos.

JUSTIFICATIVAS: A quantidade exigida de, no mínimo, 3 (três) anos de experiência é necessária, por se tratar de atividade de alta complexidade e a fim de evitar possíveis perdas financeiras e de imagem ao Banco do Nordeste.

6. DESCRIÇÃO DOS SERVIÇOS

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

7. VIGÊNCIA DO CONTRATO

- 7.1. O prazo de vigência do Contrato será de 24 (vinte e quatro) meses, podendo ser prorrogado por iguais e sucessivos períodos de 12 (doze) meses, mediante Aditivo Contratual, limitado a 60 (sessenta) meses.

8. CONDIÇÕES DE PAGAMENTO

- 8.1. O pagamento será efetuado de acordo com as condições estabelecidas no Contrato e demais anexos, após a execução e validação dos serviços e o exato cumprimento das obrigações assumidas, mediante crédito em conta corrente indicada pelo CONTRATADO, não sendo admitida cobrança por meio de boleto bancário e atentando para as seguintes condições de prazos:
 - 8.1.1. o CONTRATADO deverá apresentar o Relatório Mensal de Nível de Serviço até o 5º (quinto) dia útil do mês subsequente ao da prestação dos serviços;
 - 8.1.2. o Banco deverá validar os serviços executados, bem como o Relatório Mensal de Nível de Serviço, até o 10º (décimo) dia útil após a entrega descrita no subitem 8.1.1;
 - 8.1.3. o CONTRATADO deverá apresentar ao Banco as notas fiscais/faturas até o 5º (quinto) dia útil após a validação descrita no subitem 8.1.2;

8.1.4. o BANCO deverá efetuar o pagamento até o 10º (décimo) dia útil do mês subseqüente à apresentação descrita no subitem 8.1.3.

9. REPACTUAÇÃO

9.1. Os preços dos serviços contratados poderão ser repactuados, desde que solicitado pelo CONTRATADO, mediante demonstração analítica da variação de todos os componentes dos custos, observado o interregno mínimo de 1 (um) ano, da data do orçamento a que a proposta se referir;

10. GARANTIA CONTRATUAL

10.1. Para assegurar o integral cumprimento de todas as obrigações contratuais assumidas, o CONTRATADO deverá prestar, no prazo máximo 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 5% (cinco por cento) sobre o preço global contratado.

11. SANÇÕES ADMINISTRATIVAS

11.1. 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 0,07% (sete centésimos 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);

11.1.3. multa de até 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, pessoas por ele contratadas ou designadas, no exercício das atividades previstas no Contrato que ocasionem prejuízos ao CONTRATANTE, a seus clientes/usuários, mais o valor correspondente ao valor do prejuízo apurado;

11.1.4. multa de 0,03% (três centésimos por cento), para cada dia de atraso, aplicável sobre o preço global do Contrato, no caso da ocorrência de não cumprimento dos prazos estipulados das Fases do período de Transição dos Serviços, conforme previsto no Anexo VI;

11.1.5. multa de até 2% (dois por cento), aplicável sobre o valor apurado para o pagamento mensal no mês em que se verificar a ocorrência faltosa, quando configurada a não alocação dos profissionais de acordo com o quantitativo mínimo exigido no Anexo IV - Perfis e Qualificações dos Profissionais do Contratado;

11.1.6. multa de 10% (dez por cento), aplicável sobre o valor apurado para pagamento no mês em que se verificar a ocorrência faltosa, em caso de não pagamento dos salários e/ou das verbas trabalhistas;

11.1.7. multa de 10% (dez por cento), aplicável sobre o valor apurado para pagamento no mês em que se verificar a ocorrência faltosa, em caso de não recolhimento das contribuições sociais, previdenciárias e para com o FGTS;

- 11.1.8. multa de 10% (dez por cento), aplicável sobre o valor mensal do Contrato, quando configuradas as situações abaixo descritas:
- 11.1.8.1. quebra de sigilo das informações do CONTRATANTE;
 - 11.1.8.2. violação ou não cumprimento de outras cláusulas ou condição estipulada no Contrato;
 - 11.1.8.3. 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;
- 11.1.9. 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;
- 11.1.10. multa de 10% (dez por cento) sobre o preço global do Contrato, em caso de inexecução total do Contrato;
- 11.1.11. suspensão temporária de participar em licitação e impedimento de contratar com o BANCO pelo prazo de até 2 (dois) anos.
- 11.1.12. outros redutores de pagamento com respectivas multas, conforme descritos no Anexo III - Níveis Mínimos de Serviços

12. REGIME DE EXECUÇÃO

- 12.1. Empreitada por preço global.

13. CRITÉRIO DE JULGAMENTO

- 13.1. Menor preço global apresentado.

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

- 14.1. Ambiente de Segurança Corporativa

Gustavo Sikora de Melo
Gerente Executivo, em exercício

Leopoldo Soares de Melo Júnior
Gerente de Ambiente