LICITAÇÃO ELETRÔNICA

Nº 0000037/2026

OBJETO: Aquisição de Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida, composta por hardware, software e demais serviços.

DATA DE ABERTURA: 17/04/2026

HORÁRIO DE ABERTURA: 10horas

VALIDADE DAS PROPOSTAS: Mínimo 60 (sessenta) dias

UNIDADE GESTORA: Unidade de Arquitetura Computacional

FASE EXTERNA

EDITAL DE LICITAÇÃO Nº 0000037/2026

DADOS INICIAIS

OBJETO: Aquisição de Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida, composta por hardware, software e demais serviços.

CRITÉRIO DE JULGAMENTO: Menor Preço Global

MODO DE DISPUTA: Aberto

ENQUADRAMENTO ME/EPP: Preferencial ME/EPP

RECEBIMENTO DAS PROPOSTAS: Até às 10h do dia 17/04/2026.

ABERTURA DAS PROPOSTAS: Às 10h do dia 17/04/2026.

INÍCIO DA DISPUTA: Às 10h15min. do dia 17/04/2026.

LOCAL DE ABERTURA: www.pregaobanrisul.com.br

REFERÊNCIA DE TEMPO: Para todas as referências de tempo será observado o horário de Brasília (DF)

FORMALIZAÇÃO DE CONSULTAS: banrisul_licitacoes@banrisul.com.br

HABILITAÇÃO: Exclusivamente no sistema eletrônico

RECURSO ADMINISTRATIVO: Exclusivamente no sistema eletrônico

SUMÁRIO

CONDIÇÕES GERAIS DA LICITAÇÃO

O **BANCO DO ESTADO DO RIO GRANDE DO SUL S.A.,** através de sua Gerência de Licitações, situada na Rua Caldas Júnior, nº108, 5º andar, Centro Histórico, Porto Alegre/RS, CEP 90010-260, telefone (51) 3215-4503**,** torna pública a realização do presente certame, na modalidade **Licitação Eletrônica, nº 0000037/2026**, adotado o critério de julgamento MENOR PREÇO, pelo modo de disputa **ABERTO, SEM INVERSÃO DE FASES**, lote único, regida pela Lei Federal nº 13.303 de 30 de junho de 2016 e legislação pertinente, no que dispõe a Lei Complementar nº 123, de 14 de dezembro de 2006, sujeitando-se às disposições da Lei Estadual nº 11.389 de 25 de novembro de 1999, Lei Estadual nº15.228, de 25 de setembro de 2018 e no Regulamento de Licitações e Contratos do BANCO DO ESTADO DO RIO GRANDE DO SUL S.A., disponível no endereço eletrônico www.banrisul.com.br, para a execução dos serviços indicados neste edital e seus anexos, mediante as seguintes condições:

I. DO OBJETO

1.1. O presente procedimento licitatório tem por objeto a aquisição de Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida, composta por hardware, software e demais serviços, de acordo com as especificações contidas nos anexos, partes integrantes do presente edital.

II. DAS CONDIÇÕES PARA PARTICIPAÇÃO

2.1. Somente poderão participar desta licitação as licitantes que satisfaçam as exigências deste edital, da Lei n° 13.303/2016 e do Regulamento de Licitações e Contratos do Banrisul.

2.2. Poderão participar da presente licitação os interessados que estejam credenciados junto ao Portal do Fornecedor do RS (https://portaldofornecedor.rs.gov.br//home#/home), que atenderem a todas as exigências constantes deste edital e seus anexos, sendo que o não atendimento de qualquer das condições implicará a inabilitação da licitante ou a desclassificação de sua proposta.

2.3. A licitante, para participar do certame, deverá declarar, em campo eletrônico, o pleno conhecimento e atendimento às exigências de habilitação.

2.3.1. O não atendimento ao presente item ensejará a desclassificação da proposta no sistema, com automático impedimento da participação na disputa.

2.4. A participação dos interessados no dia e hora determinados nos **Dados Iniciais** deste edital dar-se-á por meio da digitação da senha privativa da licitante e subsequente encaminhamento da proposta de preços exclusivamente por meio eletrônico.

2.5. A informação de dados para acesso deve ser feita na página inicial do site www.pregaobanrisul.com.br ou através do *link* no site www.banrisul.com.br.

2.6. Caso o objeto contemple execução de serviços com dedicação exclusiva de mão de obra, não será permitida a participação de cooperativas de mão de obra, de acordo com o **Termo de Compromisso de Ajuste de Conduta** de 21 de dezembro de 2005, e súmula 281 do TCU, considerando que os serviços objeto desta licitação envolvem necessidade de subordinação

jurídica, habitualidade e pessoalidade entre o trabalhador e a Contratada.

2.7. Enquanto perdurarem os motivos determinantes de punições ou até que seja promovida a reabilitação, não poderão participar da presente licitação as empresas ou profissionais que tenham sofrido penalidades resultantes de contratos firmados anteriormente com o Banco, na condição de prestadores de serviços, fornecedores, empreiteiros ou construtores, tais como suspensão, declaração de inidoneidade, bem como aqueles impedidos de operar com o Banco por determinação do Banco Central do Brasil.

2.8. A simples participação neste certame implica aceitação de todos os seus termos, condições, normas, especificações e detalhes.

III. DOS IMPEDIMENTOS À PARTICIPAÇÃO

3.1. Não poderão participar desta Licitação empresas que se encontrem em processo de falência, dissolução ou liquidação.

3.1.1. Agente econômico em recuperação judicial ou extrajudicial poderá participar desta Licitação, desde que atenda às condições para comprovação da capacidade econômica e financeira previstas no edital.

3.2. Estará impedida de participar da presente licitação, em qualquer fase do processo, e de ser contratada, a empresa que se enquadre em uma das hipóteses abaixo:

I. Cujo administrador ou sócio detentor de mais de 5% (cinco por cento) do capital social seja diretor ou empregado do Banrisul ou uma de suas Controladas;

II. Que esteja cumprindo penalidade de suspensão aplicada pelo Banrisul ou uma de suas Controladas;

III. Que tenha sido declarado inidônea pelo Banrisul e ou por órgãos da administração pública direta e/ou indireta do Estado do Rio Grande do Sul, enquanto perdurarem os efeitos da sanção;

IV. Que seja constituída por sócio de empresa que estiver suspensa, impedida ou que tenha sido declarada inidônea pelo Banrisul ou uma de suas Controladas ou que tenha sido declarada inidônea pelo Estado do Rio Grande do Sul;

V. Cujo administrador seja sócio de empresa suspensa, impedida ou que tenha sido declarada inidônea pelo Banrisul ou uma de suas Controladas ou que tenha sido declarada inidônea pelo Estado do Rio Grande do Sul;

VI. Constituída por sócio que tenha sido sócio ou administrador de empresa suspensa, impedida ou que tenha sido declarada inidônea pelo Banrisul ou uma de suas Controladas ou que tenha sido declarada inidônea pelo Estado do Rio Grande do Sul, no período dos fatos que deram ensejo à sanção;

VII. Cujo administrador tenha sido sócio ou administrador de empresa suspensa, impedida ou que tenha sido declarada inidônea pelo Banrisul ou uma de suas Controladas ou que tenha sido declarada inidônea pelo Estado do Rio Grande do Sul, no período dos fatos que deram ensejo à sanção;

VIII. Que tiver, nos seus quadros de diretoria, pessoa que participou, em razão de vínculo de mesma natureza, de empresa declarada inidônea.

3.3. A vedação prevista no item anterior deste edital também se aplica para as seguintes situações:

I. À contratação de empregado ou dirigente do Banrisul ou de uma de suas Controladas, como pessoa física, bem como à participação dele em procedimentos licitatórios, na condição de licitante;

II. A quem tenha relação de parentesco, até o terceiro grau civil, com:

a) Dirigente do Banrisul ou de uma de suas Controladas;

b) Empregado do Banrisul ou de uma de suas Controladas cujas atribuições envolvam a atuação na área responsável pela licitação ou contratação;

c) Autoridade do ente público a que o Banrisul ou uma de suas Controladas está vinculado.

III. Empresa cujo proprietário, mesmo na condição de sócio, tenha terminado seu prazo de gestão ou rompido seu vínculo com o Banrisul ou uma de suas Controladas há menos de 6 (seis) meses.

3.4. Em se tratando de licitação para obras e/ou serviços de engenharia, é vedada, também, a participação direta ou indireta:

I. De pessoa física ou jurídica que tenha elaborado o anteprojeto ou o projeto básico da presente licitação;

II. De pessoa jurídica que participar de consórcio responsável pela elaboração do anteprojeto ou do projeto básico da presente licitação;

III. De pessoa jurídica da qual o autor do anteprojeto ou do projeto básico desta licitação seja administrador, controlador, gerente, responsável técnico, subcontratado ou sócio, neste último caso quando a participação superar 5% (cinco por cento) do capital votante;

3.5. Somente será permitida a participação das pessoas jurídicas e da pessoa física de que tratam os incisos II e III do item acima do presente edital, durante a licitação ou na execução do contrato, como consultor ou técnico, nas funções de fiscalização, supervisão ou gerenciamento, exclusivamente a serviço do Banrisul e de suas Controladas.

IV. DA PARTICIPAÇÃO DE MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE

4.1. Receberão tratamento diferenciado e favorecido nos termos da Lei Complementar Federal nº 123/2006 as licitantes que declararem, eletronicamente, em campo próprio, o enquadramento social de que trata esta seção, quando do envio da proposta inicial, devidamente comprovado conforme estabelece o presente Edital.

4.2. A ausência dessa declaração, no momento do envio da proposta, implicará na desistência da microempresa ou empresa de pequeno porte ao direito de utilizar-se das prerrogativas a elas concedidas pela Lei Complementar Federal nº 123/2006.

4.3. Será assegurada, como critério de desempate, preferência de contratação de Microempresas e Empresas de Pequeno Porte, conforme a Lei Complementar Federal nº 123/2006.

4.3.1. O Sistema Eletrônico de Compras informará às empresas que se enquadrarem no subitem anterior.

4.3.2. Entende-se por empate aquelas situações em que as propostas apresentadas pelas Microempresas e Empresas de Pequeno Porte sejam iguais ou até 10% (dez por cento) superiores à proposta mais bem classificada.

4.3.3. Não ocorrerá empate se a proposta mais bem classificada já for de Microempresa ou Empresa de Pequeno Porte.

4.3.4. Ocorrendo o empate, a Microempresa ou Empresa de Pequeno Porte mais bem classificada poderá apresentar proposta de preço inferior àquela considerada vencedora do certame. A proposta deverá ser apresentada no prazo máximo de 05 (cinco) minutos a partir da solicitação do Agente de Licitação sob pena de preclusão.

4.3.5. No caso de equivalência dos valores apresentados pelas Microempresas e Empresas de Pequeno Porte que se enquadrem no intervalo estabelecido como empate, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.

4.3.6. Não ocorrendo a contratação da Microempresa ou Empresa de Pequeno Porte, conforme subitens anteriores, serão convocadas as remanescentes de mesmo enquadramento social, na ordem classificatória, para exercício do mesmo direito.

4.4. Não ocorrendo a contratação nos termos previstos nos subitens acima, o objeto licitado será adjudicado em favor da proposta originalmente vencedora do certame, ou seja, da empresa que não se enquadra como Microempresa ou Empresa de Pequeno Porte que apresentou a melhor proposta.

4.5. Na hipótese de não haver mais empresas de mesmo enquadramento social, o objeto da licitação será adjudicado para a empresa originalmente vencedora.

4.6. As microempresas ou empresas de pequeno porte deverão apresentar os documentos de habilitação, mesmo que estes apresentem alguma restrição relativa à regularidade fiscal e trabalhista, sob pena de inabilitação.

4.7. A microempresa ou empresa de pequeno porte que apresentar documentos com restrições quanto à regularidade fiscal e trabalhista tem assegurado o prazo de 5 (cinco) dias úteis, a partir da declaração de vencedor da licitação, prorrogável por igual período, a critério do Banrisul, para apresentar as respectivas certidões de regularidade.

4.8. A não regularização da documentação implicará decadência do direito à contratação, sem prejuízo da aplicação das sanções previstas neste edital, podendo o Banrisul retomar a licitação com a convocação da segunda classificada, e assim sucessivamente, para apresentação da PROPOSTA DE PREÇOS FINAL e demais atos subsequentes.

V. DA SUBCONTRATAÇÃO

5.1. Somente será permitida subcontratação total ou parcial do objeto licitado caso haja previsão e apenas nos termos apresentados no Termo de Referência anexo a este edital.

5.1.1. Caso permitida a subcontratação, fica vedada a participação de pessoa jurídica como subcontratada em propostas de diferentes licitantes. De mesmo modo, um mesmo profissional não poderá figurar em mais de uma proposta de diferentes licitantes.

5.2. Em caso de subcontratação, deverá ser apresentada a documentação da(s) subcontratada(s) que comprove sua habilitação e qualificação técnica necessária à execução da parcela do serviço subcontratado, na forma exigida neste edital.

5.3. A subcontratação não exclui a responsabilidade da LICITANTE VENCEDORA perante a Administração Pública quanto à qualidade técnica do serviço prestado.

5.3.1. A LICITANTE VENCEDORA deverá providenciar e apresentar, por ocasião da assinatura do instrumento contratual, a cópia do contrato celebrado com sua(s) SUBCONTRATADA(S), devendo a(s) mesma(s) manter as condições exigidos para fins de habilitação.

VI. DA PARTICIPAÇÃO DE EMPRESAS EM CONSÓRCIO

6.1. Será permitida a participação de empresas em consórcio somente se houver previsão tal no Termo de Referência, anexo a este edital.

6.2. Caso permitida a participação de empresas em consórcio, as pessoas jurídicas que participarem organizadas em consórcio deverão apresentar, além dos demais documentos exigidos neste Edital, compromisso de constituição do consórcio, por escritura pública ou documento particular registrado em Cartório de Registro de Títulos e Documentos, discriminando a empresa líder e estabelecendo responsabilidade solidária dos integrantes pelos atos praticados pelo consórcio.

6.3. As empresas jurídicas organizadas em consórcio deverão apresentar as mesmas comprovações de habilitação requeridas na **seção DA HABILITAÇÃO DA PROPOSTA DA LICITANTE VENCEDORA**.

VII. DO CREDENCIAMENTO

7.1. O credenciamento dos licitantes dar-se-á pelas atribuições de chave de identificação e de senha pessoal e intransferível para acesso ao sistema obtidas junto ao Portal do Fornecedor do RS (https://portaldofornecedor.rs.gov.br//home#/home).

7.2. O credenciamento e sua manutenção no respectivo cadastro dependerão de registro cadastral no Portal do Fornecedor do RS.

7.3. O credenciamento junto ao provedor do sistema implica responsabilidade legal da licitante ou de seu representante legal e na presunção de sua capacidade técnica para realização das transações inerentes ao certame.

7.4. O uso da senha de acesso pela licitante é de sua responsabilidade exclusiva, incluindo qualquer transação efetuada diretamente ou por seu representante, não cabendo à PROCERGS, à

CELIC, ou ao BANRISUL, responsabilidade por eventuais danos decorrentes do uso indevido da senha, ainda que por terceiros.

7.5. A perda da senha ou quebra do sigilo deverão ser comunicadas imediatamente ao Portal do Fornecedor do RS, para imediato bloqueio de acesso.

VIII. DA OPERACIONALIZAÇÃO DA LICITAÇÃO ELETRÔNICA

8.1. A partir do horário previsto neste edital, terá início a sessão pública de Licitação Eletrônica.

8.2. A sessão de Licitação Eletrônica será conduzida pelo Agente de Licitação, mediante a inserção e monitoramento de dados gerados ou transferidos no site www.pregaobanrisul.com.br.

8.3. A participação no certame dar-se-á por meio da digitação da senha pessoal e intransferível da licitante credenciada e subsequente encaminhamento da proposta, exclusivamente por meio do sistema eletrônico, observados data e horário estabelecidos neste Edital.

8.4. O encaminhamento da proposta pressupõe o pleno conhecimento e atendimento das exigências de habilitação previstas neste Edital.

8.5. Caberá à licitante acompanhar as operações no sistema eletrônico durante a sessão pública da licitação, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de qualquer mensagem emitida pelo sistema ou de sua desconexão.

8.6. Aberta a etapa competitiva, os representantes das licitantes deverão estar conectados ao sistema para participar da sessão de lances. A cada lance ofertado o participante será imediatamente informado de seu recebimento e respectivo horário de seu registro e valor.

8.7. No caso de desconexão com o Agente de Licitação, no decorrer da etapa competitiva do certame, o sistema eletrônico poderá permanecer acessível às licitantes para recepção de lances, retornando o Agente de Licitação, quando possível, sua atuação na Licitação Eletrônica, sem prejuízo dos atos realizados.

8.8. Quando a desconexão persistir por tempo superior a 10 (dez) minutos, a sessão da Licitação Eletrônica, poderá ser suspensa e terá reinício após comunicação expressa aos participantes.

8.9. No caso de desconexão da licitante, esta deverá de imediato, sob sua inteira responsabilidade, providenciar sua conexão ao sistema.

IX. DA SESSÃO DA LICITAÇÃO ELETRÔNICA

9.1. A partir da data e horário previstos neste edital, terá início a sessão pública da Licitação Eletrônica.

9.2. Para classificação das propostas será adotado o critério de menor preço, observados os prazos máximos para fornecimento, as especificações técnicas e parâmetros mínimos de desempenho e qualidade definidos no edital.

9.3. Durante a sessão pública, a comunicação entre o Agente de Licitação e as licitantes ocorrerá exclusivamente pelo sistema eletrônico.

9.4. Somente poderá participar da rodada de lances a licitante que, anteriormente, tenha encaminhado proposta de preços ou de percentual de desconto, dependendo do critério de julgamento adotado.

9.5. Os representantes das microempresas e empresas de pequeno porte deverão declarar no Sistema Eletrônico de Compras, em campo próprio, quando do envio da proposta inicial, que as respectivas empresas se enquadram nessa(s) categoria(s).

9.6. A ausência dessa declaração, neste momento, significará a desistência da microempresa ou empresa de pequeno porte de utilizar-se das prerrogativas a elas concedidas pela Lei Complementar Federal nº 123/2006, art. 44, conforme parágrafo anterior do presente edital.

9.7. Aberta a etapa competitiva, os representantes das licitantes deverão estar conectados ao sistema para participar da sessão de lances. A cada lance ofertado o participante será imediatamente informado de seu recebimento e respectivo horário de seu registro e valor.

9.8. Só serão aceitos lances cujos valores forem inferiores ao último lance da própria licitante que tenha sido anteriormente registrado(a) no sistema.

9.9. Durante o transcurso da sessão pública, os participantes serão informados, em tempo real, do valor do menor lance registrado. O sistema não identificará o autor dos lances aos demais participantes.

9.10. O Agente de Licitação verificará as propostas apresentadas e desclassificará, motivadamente, aquelas que não estejam em conformidade com os requisitos estabelecidos neste Edital.

9.11. Durante a fase de lances, o Agente de Licitação poderá excluir, justificadamente, lance cujo valor ou percentual de desconto, dependendo do critério de julgamento adotado, seja manifestamente inexequível.

9.12. A etapa de lances da sessão pública será encerrada mediante aviso de fechamento iminente dos lances, emitido pelo sistema eletrônico, após o que transcorrerá o período de tempo de até 30 (trinta) minutos, aleatoriamente determinado também pelo sistema eletrônico, findo o qual será automaticamente encerrada a recepção de lances.

9.13. O sistema informará a proposta de menor preço imediatamente após o encerramento da etapa de lances, quando for o caso, após negociação e decisão do Agente de Licitação acerca da aceitação do lance mais vantajoso, assegurada a preferência de contratação de Microempresas e Empresas de Pequeno Porte, conforme a Lei Complementar Federal nº 123/2006.

9.14. A classificação das propostas se dará em ordem crescente dos preços apresentados, sendo considerada vencedora a proposta que cotar o MENOR PREÇO.

9.15. Encerrada a etapa de lances da sessão pública, quando convocada pelo agente de licitação, a licitante detentora da melhor oferta deverá remeter, **via sistema**, no prazo máximo de duas horas, **os documentos** exigidos no instrumento convocatório (seção XI deste edital) bem como **a proposta** de acordo com a proposta final. A Administração se reserva o direito de solicitar documentos através de diligência caso necessário para dirimir dúvidas.

9.15.1. O Banco analisará, em separado, cada item (objeto) da licitação para julgamento sob o critério de menor preço. A Administração se reserva o direito de solicitar ajustes nos valores dos itens através de diligência, caso necessário, respeitando o valor global negociado em sessão.

9.16. Se a proposta ou lance de menor valor não for aceitável, ou se o fornecedor desatender às exigências habilitatórias, o Agente de Licitação examinará a proposta ou lance subsequente, verificando a sua compatibilidade e a habilitação do participante, na ordem de classificação e assim sucessivamente, até a apuração de uma proposta ou lance que atenda o edital. Também nesta etapa o Agente de Licitação poderá negociar com o participante para que seja obtido melhor preço.

9.17. É facultada ao Agente de Licitação, em qualquer fase da licitação, a promoção de diligência destinada a esclarecer ou a complementar a instrução do processo.

9.17.1. O Agente de Licitação, necessitando esclarecimentos de ordem técnica, poderá valer-se do parecer das áreas técnicas especializadas do Banco para aferição do atendimento das especificações contidas neste processo licitatório, no sentido de verificar a consistência dos dados ofertados pelos licitantes, considerando a veracidade de informações e circunstâncias pertinentes.

9.17.2. Será inabilitada a licitante que apresentar documentação de habilitação em descordo com o estabelecido na **seção "Da Habilitação da Proposta da Licitante Vencedora"** que trata dos documentos de habilitação, e será analisada a documentação de habilitação da licitante com a próxima proposta mais vantajosa na fase anterior.

9.18. A proposta mais vantajosa deverá estar assinada pela licitante ou seu representante legal, redigida em português de forma clara, não podendo ser manuscrita e nem conter rasuras ou entrelinhas e incluirá:

a) O(s) preço(s) unitário e **total**, expresso(s) em moeda corrente nacional. Em caso de conflito entre os valores propostos (unitário e **total**) será considerado o valor unitário, e entre os valores expressos em algarismos e por extenso, serão considerados estes últimos;
b) O prazo mínimo de validade da proposta de **60 (sessenta) dias**, a contar da data da sessão da Licitação. Se na proposta não constar o prazo de validade, subentende-se **60 (sessenta) dias**;
c) Razão Social completa da empresa, endereço atualizado, telefone/e-mail e nº do CNPJ.

9.19. Inexistindo manifestação recursal, o Agente de Licitação declara a licitante vencedora da licitação.

X. DA PROPOSTA

10.1. As propostas apresentadas neste certame terão o prazo de validade mínima de **60 (sessenta) dias** a contar da data marcada para sua abertura.

10.1.1. A proposta final negociada com o Agente de Licitação terá o prazo de validade mínimo de **60 (sessenta) dias** a contar da data da negociação desta.

10.2. O prazo de validade das propostas, se necessário, poderá ser prorrogado mediante concordância das licitantes.

10.3. Até o dia e horário agendados para a abertura da sessão, a licitante poderá retirar ou substituir a proposta anteriormente apresentada.

10.4. Após a abertura da sessão, não cabe desistência da proposta, salvo por motivo resultante de fato superveniente e aceito pelo Agente de Licitação.

10.5. A licitante será responsável por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras sua proposta e lances.

10.6. As licitantes deverão encaminhar proposta inicial até a data e hora marcadas para a abertura da sessão, exclusivamente no sistema eletrônico do site www.pregaobanrisul.com.br, quando se encerrará a fase de recebimento de propostas.

10.7. Será efetuada a verificação da efetividade da proposta mais vantajosa, nos termos do art. 56 da Lei n°13.303/2016.

10.8. Nos preços propostos expressos em moeda corrente nacional, e naqueles que, porventura, vierem a ser ofertados através de lances, deverão estar inclusos todos os custos necessários à execução do objeto licitado, bem como todos os impostos, encargos trabalhistas, previdenciários, fiscais, comerciais, taxas, fretes, seguros e quaisquer outros que incidam ou venham incidir sobre o mesmo.

10.9. As ofertas serão de exclusiva responsabilidade da licitante, não lhe assistindo o direito de pleitear qualquer alteração das mesmas, sob alegação de erro, omissão ou qualquer outro pretexto.

10.10. A proposta de preços prevista no edital deverá ser encaminhada em formulário eletrônico específico, devendo constar o preço total do(s) lote(s), ficando desclassificada a proposta que não atender a este item.

10.11. Serão desclassificadas as propostas que não atenderem às exigências do presente Edital, que forem omissas ou apresentarem irregularidades insanáveis.

10.12. A omissão de qualquer despesa necessária ao perfeito cumprimento do objeto deste certame será interpretada como não existente ou já incluída no preço, não podendo a licitante pleitear acréscimo após a abertura da sessão pública.

10.13. É de inteira responsabilidade da licitante obter dos órgãos competentes informações sobre a incidência ou não de tributos de qualquer natureza relativos ao objeto desta licitação, nos mercados interno e/ou externo, não se admitindo alegação de desconhecimento de incidência tributária, ou outras correlatas.

10.14. Caso a licitante não apresente lances, concorrerá com o valor de sua proposta inicial, conforme o critério de julgamento adotado.

10.15. O orçamento previamente estimado para a contratação será sigiloso, sem prejuízo da divulgação do detalhamento dos quantitativos e das demais informações necessárias para a elaboração das propostas.

10.16. A licitante deverá anexar à proposta eletrônica a **Planilha de Orçamento** conforme modelo anexo ao edital, devidamente preenchida.

10.16.1. Deverá compor a proposta comercial a planilha orçamentária detalhada, tendo por base o modelo entregue neste Edital, contendo as unidades, as quantidades, os preços parciais de material e mão de obra, preços totais e parciais por item, preço total geral, de forma que estejam computadas no preço global total as despesas necessárias à completa execução da obra, serviços e instalações;

10.17. Esta licitação é composta por 01 (um) único lote, devendo os licitantes orçarem todos os seus subitens.

10.18. As licitantes arcarão com todos os custos decorrentes da elaboração e apresentação de suas propostas.

10.19. A partir das 09 horas do dia da publicação do respectivo edital poderão ser encaminhadas as propostas de preços, exclusivamente por meio eletrônico.

10.20. O Agente de Licitação, após finalizados todos os procedimentos previstos para a classificação das propostas, negociará com a licitante que ofertou a proposta mais vantajosa, podendo, inclusive, a seu critério, suspender a sessão pública para avaliação da Licitante.

10.21. A licitante detentora do lance mais vantajoso terá o prazo estabelecido pelo agente de licitação para encaminhar, exclusivamente por meio eletrônico, a **Planilha de Orçamento** e o **Cronograma Físico-Financeiro,** quando previsto no Termo de Referência**,** com os valores adequados ao preço negociado em sessão, e verificará a aceitabilidade dos valores ofertados.

10.22. Sendo aceitável a proposta de preços da licitante classificada em primeiro lugar, passa-se à fase de habilitação. Caso a proposta não atenda às exigências editalícias, será feita negociação e efetuada a verificação da efetividade das propostas das licitantes remanescentes, respeitando a ordem de classificação.

XI. DA HABILITAÇÃO DA PROPOSTA DA LICITANTE VENCEDORA

11.1. Para fins de habilitação o autor da melhor proposta deverá encaminhar exclusivamente **via sistema, no campo próprio para documentos de habilitação**, no prazo máximo de 2 (duas) horas a partir da data e horário agendados pelo Agente de Licitação, os documentos a seguir elencados. A Administração se reserva o direito de solicitar documentos através de diligência, caso necessário para dirimir dúvidas.

a) **Certificado de Fornecedor do Estado – CFE**, comprovando registro na(s) família(s) correspondente(s), ou outro **Certificado de Registro Cadastral – CRC** ou ainda, **os documentos constantes no subitem 11.2** a seguir. O Certificado de Fornecedor do Estado – CFE emitido pela Central de Licitações – CELIC, ou outro Certificado de Registro Cadastral – CRC emitido por órgão da Administração Pública Federal ou Estadual, em vigor na data de abertura da licitação, compatível com o objeto licitado, no qual deverão estar mencionados, individualmente, os documentos relacionados no subitem 11.2 e a data do respectivo vencimento. Na falta de algum desses documentos no CRC ou no caso de estarem vencidos, fica obrigatória a apresentação da documentação complementar ou revalidadora;

b) Declaração da licitante de vinculação ao instrumento convocatório e que não emprega menor de dezoito anos em trabalho noturno, perigoso ou insalubre e não emprega menor de

dezesseis anos, ressalvado na condição de aprendiz, a partir de 14 anos, de acordo com a **Declaração de Sujeição ao Edital** anexa a este edital;

c) Declaração, sob as penalidades legais, firmada pelo representante legal da licitante, de inexistência de fato impeditivo de habilitação ocorrido supervenientemente a sua inscrição no cadastro apresentado, ou à última atualização da sua documentação junto a tal cadastro, obrigando-se a declarar qualquer ocorrência, conforme **Item 4 da Declaração de Sujeição ao Edital** anexa a este edital;

d) Declaração de que a proposta atende todas as exigências previstas no edital, considerando todas as especificações técnicas e despesas necessárias, e que está ciente que o não atendimento de qualquer exigência prevista no edital implicará sanções administrativas que podem ser desde advertência, multa, suspensão temporária de licitar com a Administração pelo período de até 2 (dois) anos conforme **Item 5 da Declaração de Sujeição ao Edital** anexa a este edital;

e) Declaração de idoneidade para licitar e contratar com a Administração Pública, conforme **Item 5 da Declaração de Sujeição ao Edital** anexa a este edital;

f) **Relação de Sócios e Administradores**, conforme modelo anexo a este edital;

a. Todos os sócios Pessoa Física, independentemente de exercerem a administração da empresa interessada no credenciamento ou da empresa sócia devem apresentar a “Declaração de Inexistência de Fato Impeditivo” e a “Declaração de Pessoa Politicamente Exposta (PEP)”.

g) **Declaração de Inexistência de Fato Impeditivo**, conforme modelo anexo a este edital;

h) **Declaração de Pessoa Politicamente Exposta (PEP)**, conforme modelo anexo a este edital;

i) Prova de enquadramento como Microempresa – ME ou Empresa de Pequeno Porte – EPP, registrada pela Junta Comercial ou Cartório de Registro Especiais, caso se tratar dessas espécies;

j) As Microempresas e Empresas de Pequeno Porte deverão apresentar os documentos, mesmo que estes apresentem alguma restrição (Lei Complementar nº 123/2006);

k) Apresentar a documentação referente a **qualificação técnica** conforme solicitado no item **21 do Termo de Referência** anexo a este edital.

11.2. No caso de a licitante não possuir o **Certificado de Fornecedor do Estado – CFE** referido anteriormente para habilitação, deverá apresentar a seguinte documentação:

11.2.1. Jurídica

a) Registro comercial, no caso de empresa individual;

b) Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, em se tratando de sociedades comerciais e, no caso de sociedade por ações, acompanhados de documentos que comprovem a eleição de seus administradores;

c) Comprovante de inscrição do ato constitutivo, no caso de sociedades civis, acompanhado de prova da composição da diretoria em exercício;

d) Decreto de autorização, em se tratando de empresa ou sociedade estrangeira em funcionamento no país, e ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir.

11.2.2. Fiscal

a) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ;

11.2.3. Qualificação Econômico-Financeira

a) Apresentação das Demonstrações Contábeis dos dois últimos exercícios sociais em uma das seguintes formas de apresentação, conforme previsto no Decreto Estadual nº 57.154 de 22/08/2023 e Instrução Normativa CAGE N 11 de 04/12/2023:

1.a.1. Quando não utilizam as Escriturações Contábeis via SPED deverão apresentar: cópias das páginas do livro diário nas quais estão transcritos os Termos de Abertura e de Encerramento, o Balanço Patrimonial (BP) e a Demonstração do Resultado do Exercício (DRE) devidamente autenticados pela Junta Comercial ou órgão competente, e assinados pelo responsável pela contabilidade e pelo representante legal da empresa;

1.a.2. Quando utilizam as Escriturações Contábeis via SPED deverão apresentar cópia do Recibo de Entrega do Arquivo SPED à Receita Federal do Brasil, cópias dos Termos de Abertura e Encerramento do Livro Digital e cópias dos relatórios do SPED em que constem o Balanço Patrimonial (BP) e a Demonstração do Resultado do Exercício (DRE), de acordo com as Normas Brasileiras e de Contabilidade expedidas pelo Conselho Federal de Contabilidade (CFC);

1.a.3. Para empresas que publicam as demonstrações contábeis: cópia da página em que foram publicadas as demonstrações contábeis contendo o Balanço Patrimonial (BP) e a Demonstração de Resultado do Exercício (DRE).

b) Apresentação com base nos parâmetros contábeis sobre o último exercício social, conforme parágrafo 1º do Art. 6 da Instrução Normativa CAGE nº 11 de 04/12/2023, dos índices de liquidez geral - ILG, de solvência geral - ISG, e de liquidez corrente - ILC, superiores a um, obtidos pelas seguintes fórmulas:

1.b.1. *Índice de Liquidez Geral (ILG) = (Ativo Circulante + Realizável a Longo Prazo) / (Passivo Circulante + Passivo Não Circulante)*;

1.b.2. *Índice de Solvência Geral (ISG) = (Ativo Total) / (Passivo Circulante + Passivo não Circulante)*; e

1.b.3. *Índice de Liquidez Corrente (ILC) = (Ativo Circulante) / (Passivo Circulante)*.

c) Nas licitações e nas contratações de compras para entrega futura e de execução de obras e serviços, caso o licitante apresente resultado inferior ou igual a um em qualquer dos índices referidos no inciso I, deverá para fins de habilitação apresentar:

1.c.1. Patrimônio líquido mínimo do licitante de dez por cento do valor estimado da contratação.

d) Conforme Instrução Normativa CAGE nº 11, o valor estimado da contratação, utilizado para efeito dos parâmetros contábeis será:

1.d.1. O valor da proposta final do licitante, na hipótese de julgamento de proposta anterior à fase de habilitação; ou o valor orçado da administração quando a disputa não envolver proposta financeiras;

1.d.2. Ajustado para o valor anual do contrato, na hipótese de serviços e fornecimentos contínuos com vigência superior a 1 (um) ano.

e) As demonstrações contábeis previstas na alínea "a" e seus respectivos subitens poderão ser substituídas por certificado expedido pela Contadoria e Auditoria-Geral do Estado (CAGE) que ateste a adequação do licitante aos parâmetros contábeis referidos na alínea "b";

f) Certidão Negativa de Falência, expedida pelo distribuidor judicial do foro da sede da matriz da pessoa jurídica e, subsidiariamente, expedida pelo distribuidor judicial do foro da filial da pessoa jurídica no caso desta ser a participante do certame, emitida há menos de 60 (sessenta) dias da data fixada para abertura da licitação.

11.3. Em caso de previsão de subcontratação no Termo de Referência, deverá ser apresentada a documentação da subcontratada que comprove sua habilitação e qualificação técnica necessária à execução da parcela do serviço subcontratado, na forma exigida neste edital.

XII. DA AMOSTRA/VERIFICAÇÃO

12.1. Caso haja previsão de fase de amostra ou verificação do objeto licitado no Termo de Referência, devem ser observadas as orientações que seguem:

12.1.1. A licitante provisoriamente classificada em primeiro lugar será convocada para que se iniciem os procedimentos de verificação para efeito de comprovação exigida neste edital, conforme **o item 18 do Termo de Referência** em anexo.

12.1.1.1. A licitante deverá apresentar o **Termo de Confidencialidade e Manutenção de Sigilo - Fase de Verificação**, conforme modelo anexo a este edital, devidamente assinado.

12.1.2. Verificada a conformidade do objeto e aceita pelo Banco, será emitido pela área técnica um parecer. Caso satisfatório, o resultado da licitação será adjudicado pelo Agente de Licitação quando for o caso, e homologado pela autoridade superior.

12.1.3. Caso insatisfatórias as verificações, será retomado o processo, sendo convocados os detentores das propostas que constarem da classificação definitiva (após a fase de lances) para uma nova sessão, na qual será verificada/analisada a documentação de habilitação daquele que ofertou a segunda melhor proposta, e assim sucessivamente, sem prejuízo da aplicação das sanções cabíveis, garantidos os direitos ao contraditório e à ampla defesa.

12.1.4. Em observância ao princípio da publicidade dos atos, da transparência, do contraditório e da ampla defesa, o acompanhamento da fase de amostras deve ser viabilizado à todos os licitantes interessados.

XIII. DA IMPUGNAÇÃO E ESCLARECIMENTOS AO EDITAL

13.1. As solicitações de **esclarecimentos** e pedidos de **impugnação** referentes ao presente certame deverão ser encaminhadas por meio eletrônico via internet, para o endereço banrisul_licitacoes@banrisul.com.br em até **05 (cinco) dias úteis** antes da data fixada para recebimento das propostas.

13.2. Caberá ao Agente de Licitação decidir sobre a petição no prazo de até **03 (três) dias úteis**, de acordo com § 1º do Artigo 87 da Lei Federal 13.303./2016.

13.3. Acolhida a petição contra ato convocatório, será designada nova data para a realização do certame.

13.4. As impugnações e consultas interpostas fora de prazo serão recebidas como mero exercício do direito de petição.

13.5. As consultas recebidas e as respectivas respostas produzidas em relação ao presente edital encontrar-se-ão à disposição dos interessados no site www.pregaobanrisul.com.br.

XIV. DO RECURSO ADMINISTRATIVO

14.1. Após a decisão do julgamento de habilitação publicada pelo Agente de Licitação, será facultado a qualquer dos demais licitantes manifestar, no **prazo improrrogável de 20 (vinte) minutos**, por meio de formulário eletrônico específico disponibilizado no sistema**, a intenção motivada de interpor recurso**.

14.2. Admitida a intenção de recorrer, será concedido o prazo de **5 (cinco) dias úteis**, contados da aceitação da manifestação, para que o licitante interessado apresente suas razões recursais, devidamente fundamentadas, exclusivamente por meio do sistema eletrônico utilizado para a realização do certame. Os demais licitantes serão, desde logo, considerados intimados para, querendo, apresentarem contrarrazões no mesmo prazo, contado do término do prazo conferido ao recorrente, sendo-lhes assegurado o acesso imediato aos elementos indispensáveis ao exercício do contraditório e da ampla defesa.

14.3. A ausência de manifestação nos prazos e formas estabelecidos neste Edital implicará a decadência do direito de recorrer.

14.4. O recurso interposto contra decisão do Agente de Licitação não terá efeito suspensivo, e seu eventual acolhimento ensejará a invalidação apenas dos atos que não possam ser aproveitados.

14.5. Concluído o julgamento dos recursos e verificada a regularidade dos atos praticados, a autoridade competente poderá proceder com a adjudicação e a homologação do resultado do certame.

14.6. Dos demais atos da administração decorrentes da aplicação da Lei 13.303/2016, caberão as medidas previstas na referida lei.

14.7. Os recursos interpostos fora de prazo serão recebidos como mero exercício do direito de petição.

XV. DA ADJUDICAÇÃO E HOMOLOGAÇÃO

15.1. Definida a licitante vencedora, inexistindo manifestação recursal, o objeto licitado lhe será adjudicado pelo Agente de Licitação, estando a licitação sujeita à homologação pela Autoridade Superior.

15.2. Além das hipóteses previstas no § 3º do art. 57 da Lei n°. 13.303, de 30 de junho de 2016, e no inciso II do § 2° do art. 75 da mesma lei, a Autoridade Superior poderá revogar a licitação por razões de interesse público decorrentes de fato superveniente que constitua óbice manifesto e

incontornável, ou anulá-la por ilegalidade, de ofício ou por provocação de terceiros, salvo quando for viável a convalidação do ato ou do procedimento viciado.

15.3. A anulação da licitação por motivo de ilegalidade não gera obrigação de indenizar, bem como induz à anulação do contrato dela decorrente.

15.4. Depois de iniciada a fase de apresentação de lances ou propostas, a revogação ou a anulação da licitação somente será efetivada depois de se conceder às licitantes que manifestem interesse em contestar o respectivo ato prazo apto a lhes assegurar o exercício do direito ao contraditório e à ampla defesa.

15.5. Da decisão que anular ou revogar a licitação, observado o disposto no subitem anterior, caberá **recurso administrativo**, no prazo de **05 (cinco) dias úteis**.

XVI. DA CONTRATAÇÃO

16.1. Após a homologação da licitação, observada a conveniência do contratante e a validade da proposta, o contrato será enviado para que seja devidamente assinado na forma digital, onde o licitante vencedor tem o prazo de até 10 (dez) dias para efetivá-lo.

16.2. No caso de a licitante vencedora recusar-se a assinar o instrumento contratual dentro do prazo de validade de sua proposta e não apresentar justificativa porque não o fez, o Agente de Licitação examinará as ofertas subsequentes e a qualificação das licitantes, na ordem de classificação, e assim sucessivamente, até a apuração de uma que atenda ao edital, sendo a respectiva licitante declarada vencedora, sem prejuízo da aplicação das sanções cabíveis, garantido o direito ao contraditório e à ampla defesa.

16.3. Por ocasião da celebração do instrumento contratual entre as partes, a licitante vencedora deverá disponibilizar as informações solicitadas no **Cadastramento de Fornecedores** anexo a este edital.

XVII. DA VIGÊNCIA

17.1. O prazo de vigência da contratação será de 60 (sessenta) meses, podendo sua duração ser prorrogada, nos termos do que dispõe a Lei Federal 13.303/2016 e o Regulamento de Licitações e Contratos do Banrisul.

XVIII. DAS OBRIGAÇÕES DA CONTRATADA E DO CONTRATANTE

18.1. As obrigações da contratada e do Banrisul são aquelas previstas **na minuta de Contrato** anexa ao presente edital.

XIX. DA GARANTIA DE EXECUÇÃO DO CONTRATO

19.1. Caso haja previsão no Termo de Referência anexo a este edital, a CONTRATADA deverá apresentar garantia por uma das modalidades previstas no art. 70, § 1º, da Lei Federal 13.303/2016, conforme **a cláusula décima oitava da minuta de Contrato** anexa ao presente edital, observado o disposto no artigo 98 do Regulamento de Licitações e Contratos do Banrisul.

XX. DA EXECUÇÃO DO OBJETO

20.1. O objeto deverá ser executado conforme **minuta de Contrato** anexa ao presente edital.

XXI. DA GARANTIA DO OBJETO

21.1. Em caso de previsão neste edital, o prazo de garantia do objeto contratado se dará conforme **a cláusula segunda da minuta de Contrato**.

XXII. DO PAGAMENTO

22.1. O valor acordado será pago **até o dia 15 (quinze) do mês subsequente ao da prestação dos serviços, conforme medição**, com o respectivo aceite do Gestor dos Serviços, em moeda corrente nacional, por meio de crédito em conta corrente mantida em qualquer agência do contratante em nome da contratada, conforme **a cláusula quarta da minuta de Contrato** anexa ao presente edital.

XXIII. DA ATUALIZAÇÃO MONETÁRIA

23.1. Os valores da contratação, não pagos na data do vencimento, poderão ser corrigidos desde então, até a data do efetivo pagamento, pela variação do IPCA ocorrida no período.

XXIV. DO REAJUSTE

24.1. Caso a contratação possua prazo de execução superior a 12 (doze) meses, após a periodicidade de um ano, o preço do contrato poderá ser reajustado anualmente, conforme descrito **na cláusula sexta da minuta de Contrato** anexa ao presente edital.

XXV. DAS SANÇÕES ADMINISTRATIVAS

25.1. A licitante que, convocado dentro do prazo de validade de sua proposta, não celebrar o contrato, deixar de entregar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução de seu objeto, não mantiver as propostas, falhar ou fraudar na execução do contrato, comportar-se de modo inidôneo, ou cometer fraude fiscal, ficará impedido de licitar e contratar com o Banco pelo prazo de até 2 (dois) anos, sem prejuízo das demais penalidades previstas no instrumento da contratação e demais cominações legais.

25.2. A empresa contratada sujeita-se às penalidades e multas previstas, conforme **a cláusula décima sexta da minuta de Contrato** anexa ao presente edital, garantida a defesa prévia, nos termos da Lei 13.303/2016.

XXVI. DA RESCISÃO

26.1. O contrato poderá ser rescindido nas hipóteses previstas **na cláusula décima sétima da minuta de Contrato** anexa ao presente edital.

XXVII. DAS DISPOSIÇÕES GERAIS

27.1. Fica desde logo esclarecido que todos os participantes desta licitação, pelo simples fato de nela licitarem, sujeitam-se a todos os seus termos, condições, normas, especificações e detalhes,

comprometendo-se a cumpri-la plenamente, independentemente de qualquer manifestação expressa ou tácita.

27.2. Caso a licitante vencedora não apresente situação regular no ato da assinatura do instrumento contratual, ou venha recusar-se a celebrá-lo, injustificadamente, dentro do prazo estabelecido e na vigência de sua proposta, sujeitar-se-á às sanções cabíveis, reservando-se ao Banrisul o direito de, independentemente de qualquer aviso ou notificação, revogar a licitação ou convocar os remanescentes, conforme art. 75 da Lei Federal 13.303/2016.

27.3. Na convocação dos remanescentes serão observados a classificação final da sessão originária da Licitação Eletrônica e o disposto nos itens 9.5 e 9.18.

27.4. Os concorrentes remanescentes convocados na forma do parágrafo anterior se obrigam a atender a convocação e a assinar o contrato respectivo, no prazo fixado pelo Banrisul, ressalvados os casos de vencimento das respectivas propostas, sujeitando-se às penalidades cabíveis, no caso de recusa ou de não atendimento das condições de habilitação.

27.5. Os proponentes são responsáveis pela fidelidade e legitimidade das informações e dos documentos apresentados em qualquer fase da licitação, inclusive a preparação e apresentação das propostas.

27.6. É facultada ao Agente de Licitação ou à autoridade superior, em qualquer fase da licitação, a promoção de diligência destinada a esclarecer ou complementar a instrução do processo.

27.7. O Banco, representado pelo Agente de Licitação ou pela autoridade superior, reserva-se o direito de proceder ao exame das informações e comprovantes, por visitas “in loco” ou por outras medidas adequadas.

27.8. Caso seja necessária a diligência pelo Agente de Licitação para a verificação da habilitação da licitante, a sessão poderá ser interrompida ou suspensa por ordem do mesmo, que determinará o reinício dos trabalhos em momento oportuno, após a realização das diligências necessárias.

27.9. É facultado ao Agente de Licitação relevar erros formais ou simples omissões em quaisquer documentos, para fins de habilitação e classificação dos proponentes, desde que sejam irrelevantes, não firam o entendimento da proposta e o ato não acarrete violação aos princípios básicos da licitação.

27.9.1. A não regularização da documentação no prazo previsto, implicará a decadência do direito à contratação, sendo facultado à administração convocar os licitantes remanescentes, na ordem de classificação, para a assinatura do instrumento contratual, ou revogar a licitação.

27.10. A administração do Banco poderá anular ou revogar, parcialmente ou na sua totalidade, esta licitação, observadas as disposições legais pertinentes

27.11. É facultado, ainda, ao Agente de Licitação, convocar as licitantes para quaisquer esclarecimentos que porventura sejam necessários ao entendimento de suas propostas, que uma vez intimadas, deverão fazê-lo no prazo determinado pelo Agente de Licitação, sob pena de desclassificação/inabilitação.

27.12. A Microempresa e Empresa de Pequeno Porte que apresentar documentos com restrições conforme seção VI deste edital, tem assegurado o prazo de 5 (cinco) dias úteis, a partir da

publicação da adjudicação da licitação, para apresentar as respectivas certidões negativas ou positivas com efeito de negativas.

27.13. Os casos omissos serão resolvidos pelo Agente de Licitação, que a eles aplicará as disposições da Lei 13.303/2016 e do Regulamento de Licitações e Contratos do Banrisul, e disposições supletivas, se couber, desde que não venha conflitar com a referida legislação.

27.14. O desatendimento de exigências formais não essenciais não importará no afastamento da licitante, desde que sejam possíveis a aferição da sua qualificação e a exata compreensão da sua proposta, durante a realização da sessão pública da licitação, e desde que não comprometa o interesse do Banrisul, bem como a finalidade e a segurança da futura contratação.

27.15. As normas que disciplinam esta licitação serão interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse do Banrisul e a segurança da futura contratação.

27.16. Vista a documentos que integram o dossiê do processo deverá ser solicitada formalmente através do e-mail banrisul_licitacoes@banrisul.com.br.

27.17. Os resultados dos julgamentos e demais procedimentos relativos ao certame (agendamentos de aberturas, recursos, contrarrazões e outros) serão divulgados de acordo com a legislação pertinente, bem como no *site* www.pregaobanrisul.com.br.

27.18. O presente Edital e seus anexos, bem como a proposta vencedora, farão parte integrante do instrumento contratual, como se nele estivessem transcritos.

XXVIII. DOS ANEXOS

28.1. Fazem parte integrante e complementar deste edital.

- Anexo I - Relação de Sócios e Administradores;
- Anexo II - Declaração de Inexistência de Fato Impeditivo;
- Anexo III - Declaração de Pessoa Politicamente Exposta (PEP);
- Anexo IV - Cadastramento de Fornecedores;
- Anexo V - Declaração de Sujeição ao Edital;
- Anexo VI - Termo de Referência;
- Anexo VII - Minuta de **Contrato** nº 0100037/2026;
- Anexo VIII - Planilha da Orçamentos;
- Anexo IX - Planilha de Especificações Técnicas;
- Anexo X - Especificação dos Testes de Bancada - Core de Segurança de Rede;
- Anexo XI - Termo de Compromisso de Homologação - Core de Segurança de Rede;
- Anexo XII - Termo de Recebimento - Core de Segurança de Rede;
- Anexo XIII - Termo de Aceitação Definitiva - Core de Segurança de Rede;
- Anexo XIV - Termo de Responsabilidade e de Manutenção de Sigilo.

XXIX. DO FORO DE ELEIÇÃO

29.1. Fica eleito o Foro da Comarca de Porto Alegre para dirimir quaisquer dúvidas oriundas desta licitação.

Porto Alegre, 25 de março de 2026.

_____

BANCO DO ESTADO DO RIO GRANDE DO SUL S/A
Unidade de Contratações e Pagadoria
Gerência de Licitações

ANEXOS

ANEXO I

RELAÇÃO DE SÓCIO(S) E ADMINISTRADOR(ES)

I. **RELAÇÃO DE SÓCIO(S) E DE ADMINISTRADOR(ES)**

Nome/Razão Social:	
CPF/CNPJ:	RG:
Endereço:	
Telefone:	E-mail:
Este sócio é o administrador da empresa? ☐Sim	**☐Não**
Qual o seu percentual de participação? _____%	

Nome/Razão Social:	
CPF/CNPJ:	RG:
Endereço:	
Telefone:	E-mail:
Este sócio é o administrador da empresa? ☐Sim	**☐Não**
Qual o seu percentual de participação? _____%	

Nome/Razão Social:	
CPF/CNPJ:	RG:
Endereço:	
Telefone:	E-mail:
Este sócio é o administrador da empresa? ☐Sim	**☐Não**
Qual o seu percentual de participação? _____%	

a. Caso o(s) administrador(es) não participe(m) da sociedade, preencher o quadro abaixo para tantos quantos forem aqueles que possuam poderes de administração da empresa:

Nome Completo:	
CPF:	RG:
Telefone:	E-mail:

b. Deverá ser apresentado um quadro de dados para cada sócio, independentemente do percentual de participação que possua;

c. Caso haja sócio(a) pessoa natural residente no exterior desobrigada de inscrição no CPF, na forma definida pela Secretaria da Receita Federal do Brasil, deverá ser informado o país emissor, o número e o tipo do documento de viagem da pessoa física em questão;

d. Caso haja sócio pessoa jurídica com domicílio ou sede no exterior desobrigada de inscrição no CNPJ, na forma definida pela Secretaria da Receita Federal do Brasil, deve ser informado o nome da empresa, o endereço da sede e o número de identificação ou de registro da empresa no respectivo país de origem;

e. Se dentre os sócios acima relacionados, algum for Pessoa Jurídica e possuir mais de 20% de participação societária, deverá ser informada a composição societária da empresa sócia, conforme seção II deste documento.

II. **COMPOSIÇÃO SOCIETÁRIA - PARA SÓCIO PESSOA JURÍDICA**

Nome/Razão Social:	
CPF/CNPJ:	RG:
Endereço:	
Telefone:	E-mail:
Este sócio é o administrador da empresa? ☐Sim	**☐Não**
Qual o seu percentual de participação? _____%	

Nome/Razão Social:	
CPF/CNPJ:	RG:
Endereço:	
Telefone:	E-mail:
Este sócio é o administrador da empresa? ☐Sim	**☐Não**
Qual o seu percentual de participação? _____%	

Nome/Razão Social:	
CPF/CNPJ:	RG:
Endereço:	
Telefone:	E-mail:
Este sócio é o administrador da empresa? ☐Sim	**☐Não**
Qual o seu percentual de participação? _____%	

a. Cada sócio (Pessoa Física) desta empresa sócia do licitante vencedor também deverá apresentar a Declaração de Pessoa Politicamente Exposta e Declaração de Impedimentos. Ambos os arquivos se encontram anexos ao edital;

b. Este documento deverá ser apresentado em papel timbrado da empresa.

____________________, _____ de _____________ de 20___.

____

Assinatura do Representante Legal da Licitante Vencedora

ANEXO II

DECLARAÇÃO DE INEXISTÊNCIA DE FATO IMPEDITIVO DOS SÓCIOS PARA LICITAR OU CONTRATAR COM O BANRISUL E SUAS CONTROLADAS

À

Gerência de Licitações

Edital de Licitação nº 000037/2026

Eu, Nome completo do sócio, portador do CPF nº nº do CPF e documento de identificação Escolher um item. sob nº nº do documento selecionado, **declara,** para fins legais, a inexistência de impedimento para licitar ou contratar com o Banrisul e suas controladas, ciente da obrigatoriedade de declarar ocorrências posteriores.

_____

(local e data)

_____

(assinatura do sócio declarante)

Observações:

I. Cada sócio deverá apresentar sua declaração de inexistência de impedimento.
II. A declaração deverá ser feita em papel timbrado do licitante.

ANEXO III

DECLARAÇÃO PESSOA EXPOSTA POLITICAMENTE (PEP) DOS SÓCIOS

Conforme estabelece a Circular 3.978 do Banco Central do Brasil, de 23 de janeiro de 2020, as instituições financeiras são obrigadas a identificar Pessoas Expostas Politicamente (PEPs), ou seja, os agentes públicos que desempenham ou tenham desempenhado, nos últimos cinco anos, no Brasil ou em outros países, cargos, empregos ou funções públicas relevantes, assim como seus representantes, familiares e outras pessoas de seu relacionamento próximo.

Assim sendo, para cumprimento da determinação legal acima, eu Nome completo do sócio, portador do documento de identificação Escolher um item. nº nº do documento selecionado , declaro que:

1. Exerço ou exerci nos últimos cinco anos cargo, emprego ou função pública relevante?

☐Sim ☐Não

Preencher somente se a resposta acima for “Sim”:

Cargo/Função: _____

Data de Início do Exercício: ___/___/_____

Data de Fim do Exercício: ___/___/_____

Empresa Pública/Órgão Público: _____

CNPJ (opcional): _____

2. Possuo relacionamento próximo ou familiar com pessoa exposta politicamente?

☐Sim ☐Não

Preencher somente se a resposta acima for “Sim”:

Nome da pessoa exposta politicamente: _____

CPF (opcional): _____

Cargo/Função: _____

Tipo de Relacionamento:

☐Cônjuge ☐Companheiro(a) ☐Mãe ☐Pai ☐Filho(a)

☐Enteado(a) ☐Irmão ☐Procurador ☐Representante Legal ☐Preposto

☐Outorgante ☐Assessor ☐Sócio

☐Beneficiário ou Remetente, habitual, de valores, sem justificativa aparente

As informações acima prestadas são verdadeiras, e fico ciente que eventuais alterações deverão ser por mim comunicadas de imediato.

_____, _____ de _____ de 20____.

_____
Assinatura do Sócio Declarante

Observações:

I. Cada sócio deverá apresentar sua declaração de inexistência de impedimento.

II. A declaração deverá ser feita em papel timbrado do licitante.

ANEXO IV

CADASTRAMENTO DE FORNECEDORES

Em atenção a Circular 3.978/2020 BACEN, o licitante vencedor deverá apresentar as informações e documentos quando solicitados pelo Contratante:

I. **FATURAMENTO**

O valor abaixo deve representar os valores fiscais apurados pela empresa nos últimos 12 (doze) meses e serão utilizadas no cadastramento e/ou atualização da base de dados de fornecedores do Contratante.

Faturamento Bruto Total (Últimos 12 Meses)	**R$**

(*) *Caso a empresa tenha menos de 12 meses de existência, deve-se multiplicar o faturamento médio mensal dos meses que está em funcionamento por 12.*

II. **DADOS BANCÁRIOS**

DADOS BANCÁRIOS DA EMPRESA		
Código do Banco	**Nº da Agência**	**Nº da Conta Corrente PJ**

c. A empresa possui tratamento tributário diferenciado (Simples Nacional, Isenções, Imunidades?
☐SIM ☐NÃO
Especificar: Indique aqui qual tratamento diferenciado a empresa possui

d. Caso a resposta acima seja SIM, a empresa deverá enviar, juntamente com este formulário, a documentação que comprove essa condição, tais como: certidões, decisões judiciais, decisões administrativas do Fisco, declaração de SIMPLES, legislação específica.

e. Este documento deverá ser apresentado em papel timbrado da empresa.

_____, ____ de _____ de 20___.

_____
Assinatura do Representante Legal da Empresa

ANEXO V

DECLARAÇÃO DE SUJEIÇÃO AO EDITAL

Ref.: (identificação da Licitação)

O signatário da presente, _____, inscrito no CNPJ nº _____, por intermédio de seu representante legal o(a) Sr(a) _____, portador(a) da Carteira de Identidade nº _____ e do CPF nº _____ DECLARA:

1. que conhece e concorda, na íntegra, com os termos do Edital de Licitação e com todos os documentos dele componentes;
2. que considerou que o edital e seus anexos permitem a elaboração de uma proposta satisfatória;
3. que não existe, no presente momento, pedido de falência em nome desta empresa e que a mesma se submete a automática desclassificação, caso tal venha a ocorrer durante o processo de licitação;
4. sob as penalidades cabíveis, a não superveniência de fato impeditivo da habilitação;
5. que a empresa é idônea e atende a todos os pré-requisitos do edital e às demais exigências contidas na Lei Federal 13.303/2016;
6. que não se enquadra nas hipóteses previstas no artigo 38 da Lei Federal 13.303/2016, atendendo às condições de participação do edital e legislação vigente;
7. que assume total responsabilidade pelas informações prestadas e, em qualquer tempo, exime o ora CONTRATANTE, de qualquer ônus civil e penal que lhe possa acarretar;
8. que fará prova de todas as informações ora declaradas, quando necessário ou quando solicitado;
9. que visitou os locais dos serviços e tem pleno conhecimento das condições dos mesmos, quando for solicitado;
10. para os fins do disposto no inciso XXXIII do art. 7 da Constituição Federal, que não emprega menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e não emprega menor de dezesseis anos.

10.1. Ressalva: emprega menor, a partir de 14 (quatorze) anos, na condição de aprendiz ( ).

(Observação: em caso afirmativo, assinalar a ressalva acima)

_____

(Data)

_____

(Representante Legal)

TERMO DE REFERÊNCIA
PROCEDIMENTO LICITATÓRIO

Nº DO PROCESSO: 0000037/2026

UNIDADE REQUISITANTE Unidade que elaborou o Termo de Referência	Unidade de Arquitetura Computacional
GESTOR DOS SERVIÇOS Unidade responsável pela execução do bjeto	Unidade de Arquitetura Computacional
GESTOR TÉCNICO Unidade com o conhecimento técnico do objeto a ser contratado	Unidade de Arquitetura Computacional

INFORMAÇÕES BÁSICAS

1. DA JUSTIFICATIVA DA PROPOSTA

No ambiente de Data Center do Banrisul, a principal estrutura de rede é chamada de Core de Rede, e, até o início do segundo semestre de 2024, operava em uma arquitetura tradicional. O Core de Rede é o conjunto de equipamentos que interliga toda a rede de comunicação do Banrisul: Data Centers, Rede de Agências, Caixas eletrônicos, Parceiros Comerciais, Banrisul Cartões, Consórcios, RSFN, Corretora de Valores, Unidades Administrativas e Acessos do banco para Internet assim como da Internet para canais e serviços disponibilizados pelo banco. Por meio desse ambiente é viabilizado o acesso a diversos serviços tais como Banrisul Digital, Home Banking, Office Banking, E-mail, Rede Vero, Telefonia, VPN, etc. O plantel de equipamentos do Core de Rede tem como missão crítica a transmissão e encaminhamento das comunicações, garantindo a efetividade do fluxo de informações para os sistemas e serviços do banco.

Contudo, além do encaminhamento do tráfego de comunicação no Core de Rede, é necessária uma camada de proteção que atenda à complexidade do ambiente de rede uma vez que os serviços não podem operar sem o nível adequado de segurança.

Dessa forma, essa camada de proteção conta com um segundo conjunto de equipamentos, funcionalidades e serviços (on-premise e em nuvem) como Next Generation Firewalls, Next Generation IPS, Gateways VPN, ZTNA, SD-WAN, entre outros, cujas funcionalidades têm como missão crítica garantir a operação com segurança, disponibilidade, visibilidade, inovação e resiliência, de modo a proteger a imagem e os negócios do Banrisul.

Esse conjunto de equipamentos e funcionalidades que é necessário para garantir a segurança do ambiente de Core de Rede possui tanto serviços que podem atuar localmente no Data Center do Banrisul como em nuvens públicas (AWS, Azure, GCP, etc) e compõe, portanto, uma Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida, objeto escopo desse estudo técnico para processo de edital, que doravante será chamado de CORE DE SEGURANÇA DE REDE.

O CORE DE SEGURANÇA DE REDE é vital para a operação de qualquer sistema de tecnologia do banco pois trata-se da camada de segurança que viabiliza o ambiente adequado de operação e disponibilidade dos serviços Banrisul. As atualizações, implementações de novos recursos, automações, assim como as manutenções, operação assistida e melhorias disponibilizadas periodicamente são de fundamental importância para garantir um processo de comunicação ágil, eficiente e seguro.

O núcleo principal de equipamentos da solução de segurança existente (ativos de NGFW), foi adquirido em conjunto com os equipamentos da antiga solução de Core de Rede no processo 0007/2018, tendo sua implementação concluída em fevereiro de 2019. Em 2023 foi realizado processo licitatório para manutenção e suporte da solução existente (0026/2023), buscando, além de dar continuidade à solução, prover disponibilidade e segurança no funcionamento da infraestrutura de rede, tanto para a parte de conectividade como para a parte

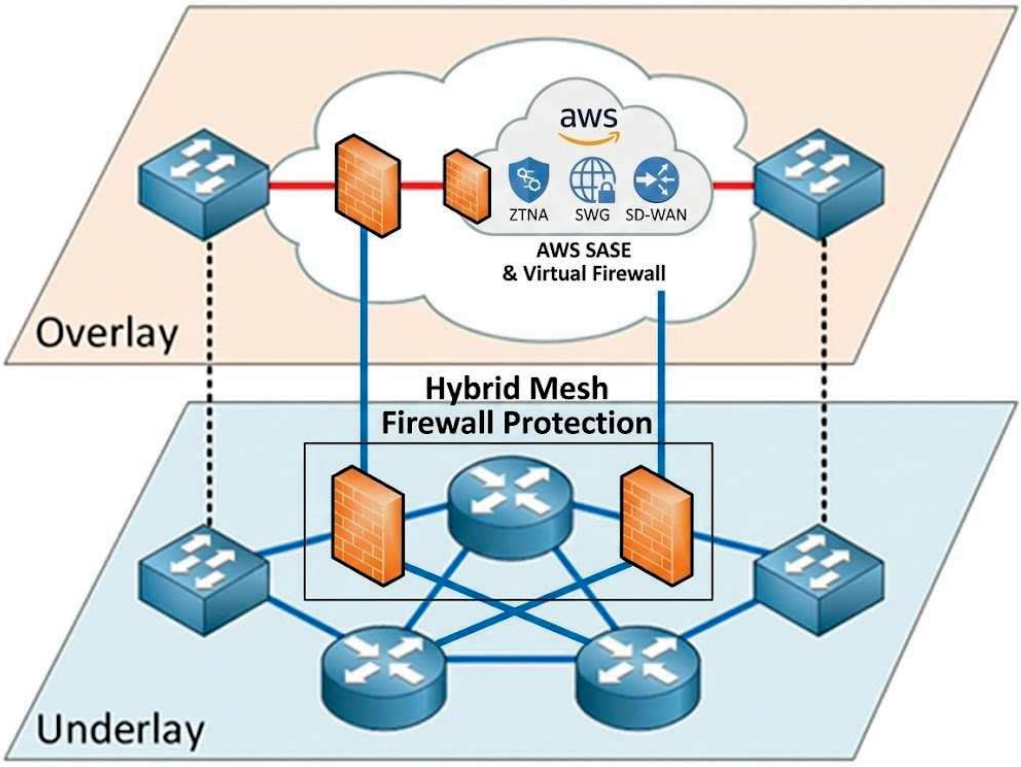
de segurança. Da mesma forma, existiram ainda os contratos de aquisição das soluções de NGIPS e VPN Lan-to-Lan (Cisco), contratos 100965/2018 e 100854/2017 que tiveram realizados, respectivamente, em sua sequência os contratos 101385/2023 e 100132/2023 para continuidade da manutenção e suporte das soluções de segurança existentes.

Na época em que essas soluções foram adquiridas, os estudo técnicos apontavam para a manutenção de um modelo de rede mais convencional e tradicional, e que fosse mais aderente a infraestrutura tecnológica implementada no Banrisul. Nos últimos anos o mercado vem evoluindo para metodologias de desenvolvimento ágeis, exigindo entrega e adequações de infraestrutura de conectividade de forma mais rápida, segura e sustentável, sem intervenção manual na rede a todo instante, e também, trazendo a necessidade de um nível de segurança capaz de se adaptar a esse novo formato. Tais metodologias se beneficiam de novas tecnologias com alto nível de integração e orquestração de infraestrutura, como o SDN (Software Defined Networking ou Rede Definida por Software), modelo de solução que foca em automatizar os processos de entrega de conectividade através da orquestração de recursos de hardware físicos e virtuais.

Esse modelo de conectividade definida por software foi implementado através do processo 1250/2023, tendo o final da sua implementação ao final do primeiro semestre de 2025, trazendo uma grande evolução no ambiente de rede, junto com uma quebra de paradigma.

Com a implementação da nova solução de Core de Rede através do Cisco ACI em 2025, parte da estrutura dos Data Centers Banrisul já está apta para atender a demanda trazida pelo novo paradigma, porém, devido ao tamanho e complexidade do projeto, não foi contemplada no mesmo certame a estrutura de segurança necessária para o atendimento desse novo cenário de rede, ocasião em que optou-se por conduzir a aquisição das linhas de conectividade e segurança em processos separados. Foi realizado então, durante a fase final de implementação da rede SDN, o arco final do estudo técnico referente ao novo ambiente de segurança que atenderia à nova estrutura de rede do Data Center, o CORE DE SEGURANÇA DE REDE.

Esse novo ambiente de segurança, portanto, é o projeto que continua a implementação do núcleo de rede do Data Center Banrisul (Core de Rede), de modo a atualizar as tecnologias de segurança de rede para adequada proteção desse novo cenário, viabilizando o acompanhamento da entrega de novos projetos, com o nível adequado de tecnologia, proteção e tempo de entrega.



Dado o exposto, se torna evidente a necessidade de atualização do CORE DE SEGURANÇA DE REDE do Banrisul para entrega ágil, segura e automatizada de estruturas de segurança de conectividade. A solução técnica avaliada e que está sendo proposta é da implantação de uma Estrutura de Segurança de Redes e Comunicações de Malha Híbrida, apta a proteger o novo ambiente de rede definida por software do Core de Rede, bem como os serviços de perímetro e Internet, ambientes operando em nuvem (ex.: AWS) e qualquer outro serviço de comunicação da rede Banrisul, suportando uma gama completa de funcionalidades além de possibilitar futuras expansões.

Nesta nova solução do CORE DE SEGURANÇA DE REDE estão contemplados, portanto, os equipamentos e funcionalidades de segurança de rede (Firewalls, IPS, VPN, ZTNA, etc), uma vez que os equipamentos de rede do Data Center já foram adquiridos em outro processo licitatório (1250/2023).

2. DO OBJETO

Aquisição de Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida, composta por hardware, software e demais serviços.

2.1. Especificações do Objeto

2.1.1. Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida, composta por hardware, software licenças, garantia, serviços de implementação da solução, suporte de hardware, suporte técnico e manutenção, operação assistida, e treinamentos;
2.1.2. O objeto é formado pelo(s) seguinte(s) iten(s):

LOTE	ITEM	DESCRIÇÃO
1	01	Gerenciamento do Projeto, Implementação da Solução e Treinamento Operacional
	02	Hardware e Software da Solução, sem incluir os valores de licenciamento definitivo

	03	Licenciamento Geral
	04	Licenciamento por Assinatura ou Subscrição
	05	Treinamentos Oficiais
	06	Suporte, Manutenção e Operação Assistida

2.1.3. As características do objeto são:
2.1.3.1. O objeto tem como principais premissas o provimento da segurança do ambiente de Core de Rede (Data Center), a atualização tecnológica gradual dos ambientes de segurança de redes e comunicações do CONTRATANTE (Rede Corporativa, Rede de Agências, Ambiente de Internet, VPN, Parceiros, seus serviços e funcionalidades), a visibilidade padronizada dos incidentes de segurança nas linhas de controle e monitoração, a integração da estrutura de segurança com as demais soluções de rede e comunicações (Cisco ACI, Aruba ClearPass, VMware, entre outros ambientes) e a iniciação do uso de Inteligência Artificial para apoio à atividades como configurações, diagnósticos, relatórios, troubleshooting, auditoria, compliance, manutenção corretiva e medidas protetivas através da aquisição de uma Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida, composta por hardware, software, licenças, garantia, serviços de implementação da solução, suporte de hardware, suporte técnico com acordo de nível de serviço (SLA) definido, operação assistida, manutenção dos equipamentos e treinamentos.
2.1.3.2. Esta solução deve permitir, em um universo de dois sites físicos de Data Center, que um equipamento ou conjunto de equipamentos possa assumir as operações de seus pares em caso de falha de algum nodo principal ou até mesmo assumir completamente a operação para garantir a continuidade do negócio com o nível adequado de segurança e disponibilidade, respeitando níveis de redundância equivalentes a um Data Center padrão Tier 4, considerando nível 2N+1, ou seja, dois conjuntos idênticos de equipamentos redundantes (por site físico) mais um componente extra de spare part para maior resiliência (equipamento para atendimento dos níveis críticos de SLA em caso de RMA).
2.1.3.3. A solução deve contemplar a entrega dos produtos especificados bem como serviços especializados de implementação e gerenciamento de projeto, treinamentos, profissionais dedicados para operação assistida, testes de aceitação, suporte técnico e manutenção, conforme o cronograma de entregas descrito neste edital e em conformidade com a Planilha de Especificações Técnicas.

2.2. Exigência de Marca/Modelo

O processo em questão não possui exigência de marca/modelo.

2.3. CRITÉRIOS DE SUSTENTABILIDADE DO OBJETO

I. Na presente contratação incidem critérios de sustentabilidade, em suas dimensões social ou ambiental?
[X] SIM. Especificar:

2.3.1 A Contratada deverá, sempre que acionada pelo Contratante, receber os equipamentos aofinal de sua vida útil, sem ônus ao Contratante, responsabilizando-se pelo descarte ambientalmente adequado dos mesmos, conforme a Lei 12.305/2010, que trata da Política Nacional de Resíduos Sólidos.
2.3.2 Os itens não poderão conter substâncias perigosas em concentração acima da recomendada na diretiva RoHS (Restriction of Certain Hazardous Substances), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr (VI)), cádmio (Cd), bifenilpolibromados (PBBs), éteres difenil-polibromados (PBDEs), conforme estabelece o art. 5º da Instrução Normativa 01/2010 da SLTI/MPOG.
2.3.3 As embalagens dos equipamentos deverão ser fabricadas com material reciclado, ou no caso de papelão das embalagens, quando não provenientes de material reciclado, deverão possuir certificação de origem florestal, tal como certificação FSC (Forest Stewardship Council), Cerflor ou similar, e serem recicláveis;

2.3.4 Os equipamentos deverão possuir a certificação de que trata a Portaria INMETRO nº 170, de 2012 ou certificação equivalente que deverá comprovar a segurança, compatibilidade eletromagnética e eficiência energética dos mesmos.

3. CLASSIFICAÇÃO DO OBJETO: EQUIPAMENTOS DE INFRAESTRUTURA

4. DO REGIME DE EXECUÇÃO OU FORMA DE FORNECIMENTO: EMPREITADA POR PREÇO GLOBAL

5. CONTRATANTE: BANCO DO ESTADO DO RIO GRANDE DO SUL S.A.

6. PARCELAMENTO DO OBJETO

I. A divisibilidade do objeto (em lotes) é possível? NÃO é possível a divisão do objeto em lotes, tecnicamente inviável e economicamente desvantajoso, conforme justificativa abaixo.

II. Justificativa pela inviabilidade de parcelamento do objeto: O suporte e manutenção precisam ser providos por uma única empresa, visando evitar a diluição de responsabilidades e o correto funcionamento da solução como um todo, assim como o hardware e software que compõem a solução.

CONDIÇÕES DA EXECUÇÃO

7. DETALHAMENTO DA FORMA DE EXECUÇÃO

7.1. REQUISITOS GERAIS

7.1.1. Serão exigidos perfis de profissionais durante a vigência do contrato, as exigências devem ser comprovadas mediante apresentação do certificado oficial emitido pelo fabricante, e experiência comprovada na instalação e configuração de equipamentos similares aos ofertados pela CONTRATADA, incluindo planejamento, adequação, execução, avaliação, mitigação e monitoramento da migração, os perfis e seus requisitos são:

7.1.2. A CONTRATADA disponibilizará pelo menos 2 (dois) profissionais que atendam aos requisitos de nível PROFISSIONAL DE SEGURANÇA para atuar na operação assistida de forma dedicada junto ao CONTRATANTE.

7.1.3. PROFISSIONAL DE SEGURANÇA

7.1.3.1. Planejar a manutenção regular da solução, suportar a resolução de problemas utilizando processos baseados na tecnologia e suas melhores práticas bem como as funcionalidades exigidas na planilha de especificações técnicas;

7.1.3.2. Possuir certificação do fabricante para o nível de ADMINISTRADOR / PROFISSIONAL DE SEGURANÇA DE REDES, ou nível técnico administrador equivalente;

7.1.3.3. Possuir pelo menos 2 (dois) anos de experiência prática no planejamento, adequação, execução, avaliação, mitigação e monitoramento de soluções de segurança de rede;

7.1.3.4. Ser capaz de definir e efetuar atualizações de software da solução, obter e instalar licenças, aplicar certificados/assinaturas digitais na solução de segurança;

7.1.3.5. Implementar acesso de gerência aos dispositivos via interface de linha de comando e/ou interface gráfica utilizando SSHv2, SSHv3, HTTPS, conforme as boas práticas de instalação, configuração e operação do fabricante;

7.1.3.6. Implementar serviços de gerenciamento como Simple Network Management Protocol versão dois e três (SNMPv2 e SNMPv3), criando visualizações, usuários, autenticação e encriptação;

7.1.3.7. Implementar e diagnosticar funcionalidades e protocolos de Autenticação, Autorização e Auditoria (AAA), RADIUS, LDAP e características de acesso baseado em perfis e Identidade;

7.1.3.8. Implementar NTP (Network Time Protocol);

7.1.3.9. Implementar e diagnosticar a exportação de SFLOW e SYSLOG;

7.1.3.10. Definir, Implementar e diagnosticar ACLs IPv4/IPv6, grupo de objetos, filtro de tráfego, filtro de aplicações, inspeção de protocolos, reações a eventos de rede, políticas de prevenção de intrusões;
7.1.3.11. Identificar e mitigar ameaças comuns diagnosticando também a origem, destino e os métodos das tentativas de ataques;
7.1.3.12. Implementar e diagnosticar funcionalidades de inspeção de telefonia celular;
7.1.3.13. Implementar, diagnosticar e analisar métodos de captura e redirecionamento de tráfego, regras de inspeção e controle, detecção de anomalias, ações de resposta e inspeção baseadas em reputação;
7.1.3.14. Implementar configurações, dimensionamento e otimização de inspeção para tráfego criptografado;
7.1.3.15. Implementar rotinas de API REST para funcionalidades de integração, automação, entre outros recursos;
7.1.3.16. Realizar a integração da solução ofertada com soluções de terceiros;

7.1.4. EXPERT DE SEGURANÇA

7.1.4.1. Deve possuir todos as características referenciadas no perfil PROFISSIONAL DE SEGURANÇA;
7.1.4.2. Possuir todas as características exigidas e conhecimentos aprofundados nos equipamentos/soluções de segurança de rede ofertados, comprovadas de forma prática através de exame prático (hands-on lab) e certificação do fabricante de NÍVEL MÁXIMO EM SEGURANÇA DE REDES;
7.1.4.3. Possuir pelo menos 3 (três) anos de experiência prática no planejamento, adequação, execução, avaliação, mitigação e monitoramento de soluções de segurança de rede;
7.1.4.4. Deve possuir conhecimento sobre os conceitos de segurança, tanto para redes IPv4 como para redes IPv6, assim como Dual-Stack, e suas aplicabilidades nos equipamentos da solução adotada;
7.1.4.5. Deve ser capaz de efetuar a implementação, configuração e verificação de serviços da Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida, de acordo com as boas práticas de instalação, configuração e operação do fabricante;
7.1.4.6. Implementar e diagnosticar serviços para visitantes (Guest Services), funcionalidades de BYOD (Bring Your Own Device), identificação transparente de usuários e customização de portais WEB;
7.1.4.7. Implementar e diagnosticar funcionalidades que forneçam maior segurança à camada de enlace (DHCP Snooping, Inspeção dinâmica de ARP, Storm Control, Port Security, MACsec) mitigando ataques de Spanning Tree, DHCP (Dynamic Host Configuration Protocol) rogue, VLAN hopping, MAC e ARP;
7.1.4.8. Implementar e diagnosticar funcionalidades de controle de uso e segurança WEB, filtros e redirecionamento de URLs, filtro de arquivos e políticas de decriptação;
7.1.4.9. Implementar, configurar e diagnosticar serviços de 802.1X em redes cabeadas e sem fio;
7.1.4.10. Implementar, configurar e diagnosticar serviços de VPN (OpenVPN, L2TP/IPsec, IKEv2/IPsec, WireGuard, SSL/TLS);
7.1.4.11. Configurar e realizar a manutenção de traduções de endereços de rede (NAT estático, NAT dinâmico, PAT, Policy NAT);
7.1.4.12. Configurar, diagnosticar e operacionalizar VPNs (Site-to-Site e Remote Access), aplicando técnicas como: Diffie-Hellman, IPsec – ESP, AH, IKEv2, Tunnel mode, Transport mode, Hairpinning, Split Tunneling, Always-on, NAT Traversal, SSL VPN Clientless;
7.1.4.13. Definir e implementar a arquitetura da solução de segurança nos modos "inline", "promiscuous" e "one armed / leg";
7.1.4.14. Definir e implementar a solução de segurança nos modos transparente e roteado, com características de Alta Disponibilidade, FailOver e Zoneamento de Segurança;
7.1.4.15. Implementar características de segmentação lógica do processamento de firewalls, criando instâncias distintas;

7.1.4.16. Definir e implementar políticas de segurança de e-mail (encriptação, anti-spam, inspeção de vírus, rastreamento de tráfego de mensagens, prevenção de perda de dados e Anti-malware);
7.1.4.17. Efetuar diagnóstico e resolução de problemas em configurações avançadas de firewall;
7.1.4.18. NOTA: O nível Expert de Segurança é o nível mais alto de consulta técnica nesta instância. Este é o profissional que tratará diretamente com problemas relacionados à serviços de missão crítica ligados diretamente ao Core de Rede, e para tanto, a equipe técnica da CONTRATANTE entende que este deve ser um profissional experiente, que já tenha tido a vivência prática nesse tipo de ambiente, conforme os quesitos referenciados para tal atividade.

7.1.5. GERENTE DE PROJETOS

7.1.5.1. Conhecimentos em melhores práticas do PMI;
7.1.5.2. Carga horária mínima de 360 (Trezentos e sessenta) horas em formação em gerência de projetos (Pós-Graduação/MBA Lato Sensu reconhecido pelo MEC) **ou** certificação PMP (PMI);
7.1.5.3. Experiência mínima de 360 (Trezentos e sessenta) horas em gerência de projetos;
7.1.5.4. Experiência comprovada na área de design de soluções de rede para atuar na integração de todo o projeto.
7.1.5.5. A CONTRATADA disponibilizará ao CONTRATANTE um profissional para gerenciar este projeto com o perfil de GERENTE DE PROJETOS.
7.1.5.6. O Gerente de Projetos deve possuir disponibilidade integral, ou seja, permanecer dedicado ao objeto e estar presente no local onde estiver sendo implementado o projeto, sempre que necessário durante todo o andamento das atividades do projeto, desde a assinatura do CONTRATO até a aceitação final (assinatura do Termo de Aceitação Definitiva).
7.1.5.7. O Gerente de Projetos será o ponto de contato com a equipe do CONTRATANTE. Estão inclusas nas responsabilidades:
7.1.5.8. Estabelecer objetivos claros para o projeto;
7.1.5.9. Monitorar e controlar as atividades de planejamento, prazo e escopo;
7.1.5.10. Integração da equipe e iniciativas necessárias para execução do trabalho definido;
7.1.5.11. Reportar diariamente ao CONTRATANTE sobre o status do projeto, andamento das atividades e cumprimento dos prazos;
7.1.5.12. Comunicação e gerenciamento das expectativas das equipes envolvidas no projeto;
7.1.5.13. Realizar o controle de mudanças;
7.1.5.14. Realizar reuniões semanais de alinhamento;

7.2. HARDWARE E SOFTWARE

7.2.1. A CONTRATADA deve fornecer uma solução completa de hardware, software, licenças e todos os serviços necessários para planejar, desenhar, configurar e suportar uma Estrutura de Segurança de Redes e Comunicações de Malha Híbrida capaz de prover segurança e atualização tecnológica gradual aos ambientes do CONTRATANTE;
7.2.2. Caso, no momento da assinatura do contrato, algum componente da solução esteja em alguma lista de descontinuidade (como "End of Life", "End of Support", "End of Sale" ou qualquer outra que acarrete o fim da prestação do suporte pelo fabricante), prevista para ocorrer em alguma data dentro do período de vigência do contrato, este componente deverá ser substituído pela CONTRATATADA, sem qualquer ônus para o CONTRATANTE, logo após a assinatura do contrato. A CONTRATADA terá um prazo de 90 dias corridos para a entrega dos componentes e 15 dias úteis para a instalação e configuração dos componentes que se enquadrarem nesta situação, contados a partir da assinatura do contrato. A instalação deverá ocorrer em dia e horário determinados pelo CONTRATANTE.
7.2.3. A CONTRATADA deve cumprir as especificações de hardware e software bem como demais questões técnicas referentes à estrutura a ser adquirida conforme descrito na PLANILHA DE ESPECIFICAÇÕES TÉCNICAS.

7.3. TESTES DE BANCADA

7.3.1. A CONTRATADA deve realizar testes de bancada conforme especificações constantes no ANEXO 01 – ESPECIFICAÇÃO DOS TESTES DE BANCADA deste edital;
7.3.2.

7.4. GESTÃO DO PROJETO

A CONTRATADA deve cumprir com, no mínimo, as seguintes entregas, não excluindo os serviços previamente mencionados:

7.4.1. Gerenciamento do Projeto:
7.4.1.1. Reunião de início do projeto com todo o time envolvido;
7.4.1.2. Reuniões semanais de atualização;
7.4.1.3. Testes de Bancada;
7.4.1.4. Entregas periódicas conforme cronograma;
7.4.1.5. Status Reports Periódicos.
7.4.1.6. Atas;
7.4.1.7. Reunião de encerramento do Projeto;
7.4.1.8. Termos de Abertura e Encerramento do Projeto.
7.4.2. Plano de Gerenciamento do Projeto (EAP - Estrutura Analítica do Projeto);
7.4.3. Plano de Projeto;
7.4.4. Cronograma.
7.4.5. Entrega dos Equipamentos;
7.4.6. Garantia de Hardware e Software;
7.4.7. Projeto Lógico e Plano de Migração;
7.4.8. Treinamentos Oficiais;
7.4.9. Implementação do Projeto;
7.4.10. Licenciamento;
7.4.11. Migração para o Novo Ambiente;
7.4.12. Acompanhamento da Migração.
7.4.13. Testes de Aceitação;
7.4.13.1. Termos de entrega e aceites.
7.4.14. Documentação Final do Projeto:
7.4.15. *High Level Design* (HLD);
7.4.15.1. Apresentações;
7.4.15.2. Documentação detalhadas da instalação.
7.4.15.3. Documentação detalhada das integrações.
7.4.15.4. Topologia Lógica.
7.4.15.5. Códigos fonte das integrações e respectiva documentação para manutenção.
7.4.15.6. Plano de Continuidade de Negócios (PCN).
7.4.15.7. Plano de Recuperação de Desastres (PRD);
7.4.15.8. Testes e Evidências da Validação do PRD;
7.4.15.9. *Health Check* da Solução implementada;
7.4.16. Treinamentos Operacionais;
7.4.17. Início da vigência do suporte e manutenção a hardware e software;
7.4.18. Profissionais Dedicados para Operação Assistida;
7.4.19. Termo de Aceitação Definitiva emitido pela CONTRATANTE;

7.5. PLANO DE PROJETO

7.5.1. A implementação da solução deve ser conduzida em formato de projeto para o qual a CONTRATADA executará e realizará todos os serviços pertinentes ao objeto desta especificação, obedecendo aos prazos estabelecidos, atuando em estrita concordância e obediência ao discriminado.
7.5.2. A CONTRATADA será responsável pela elaboração de um PLANO DE PROJETO que deve ser conduzido e validado juntamente à equipe do CONTRATANTE, balizando a fase de

implementação da solução com entregas documentadas, delimitadas e previstas em uma linha de tempo, buscando minimizar os riscos e impactos junto ao ambiente do CONTRATANTE.

7.5.3. A CONTRATADA realizará reunião inicial de alinhamento do projeto, envolvendo sua equipe participante do projeto e a equipe do CONTRATANTE para o detalhamento das atividades que compõem o projeto. Entende-se como:

7.5.3.1. Implantação: o recebimento de todos os equipamentos nas localidades, conferência física dos itens, instalação física de hardware e software adquiridos, energização e ativação dos equipamentos adquiridos pelo CONTRATANTE com as configurações previamente planejadas pelas equipes e seguindo o cronograma do projeto. Tais atividades não envolverão mudanças no ambiente que possam gerar riscos ou impacto ao ambiente em produção do CONTRATANTE.

7.5.3.2. Migração: a transferência das funcionalidades do ambiente atual, dentro do escopo da segurança de redes e comunicações, para o ambiente adquirido e implantado através da Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida. Estas atividades devem ser executadas prevendo o menor impacto e risco possíveis aos negócios do CONTRATANTE.

7.5.4. O PLANO DE PROJETO compreenderá todas as atividades individuais e suas durações, sendo o Gerente de Projetos responsável por detalhar tal plano, levando-se em conta as diferentes tecnologias que precisam ser implementadas.

7.5.5. O PLANO DE PROJETO deve respeitar as boas práticas em gerenciamento de projetos e deve apresentar, no mínimo, uma análise preliminar de escopo após o alinhamento das expectativas das partes interessadas, especificação dos recursos necessários, definição dos pré-requisitos do projeto, restrições de tempo definidas em conjunto e deve apresentar, em anexo, o detalhamento técnico da solução (incluindo o entendimento do ambiente atualmente em produção).

7.5.6. Após o detalhamento do plano de projeto, a CONTRATADA deve elaborar juntamente com o CONTRATANTE o cronograma de implementação com as atividades necessárias, seus pré-requisitos e o mapeamento das responsabilidades entre as equipes.

7.5.7. A CONTRATANTE participará ativamente, em conjunto com a CONTRATADA, da etapa de planejamento para os passos da migração e da própria migração de todo o ambiente, inclusive os serviços afetados.

7.6. PROJETO LÓGICO

7.6.1. A CONTRATADA é responsável pela elaboração de um documento de Projeto Lógico Preliminar, a ser entregue de forma digital ao CONTRATANTE, contendo o planejamento técnico, desenho da nova arquitetura e o plano de migração.

7.6.2. O Projeto Lógico Preliminar deve ser detalhado, contemplando informações completas sobre a solução, contendo no mínimo:

7.6.2.1. Especificação geral de todos os equipamentos que fazem parte da solução;
7.6.2.2. Descrição geral da arquitetura da solução;
7.6.2.3. Descrição do comportamento normal esperado da solução;
7.6.2.4. Topologia de rede física e lógica, de forma detalhada;
7.6.2.5. Diagrama de interconexão, descrevendo as regras e protocolos utilizados;
7.6.2.6. Manual de configuração, operação e manutenção de todos os itens da solução;
7.6.2.7. Estratégia de migração da solução atual para a nova solução, mencionando o funcionamento atual e pretendido após a mudança.

7.6.3. A CONTRATADA disponibilizará um profissional na função de líder técnico em SEGURANÇA para atuar no levantamento das configurações dos equipamentos atuais, planejamento das configurações, plano de migração e planejamento das atividades. O profissional “líder técnico em SEGURANÇA” deve possuir requisitos de nível EXPERT DE SEGURANÇA.

7.6.4. A atividade citada no item 7.6.3. poderá ser desempenhada pelo mesmo profissional EXPERT DE SEGURANÇA já mencionado anteriormente.

7.6.5. O Líder Técnico designado deve possuir disponibilidade integral, ou seja, permanecer dedicado ao objeto deste Contrato e estar presente no local onde estiver sendo implementado o

projeto, sempre que necessário e durante todo o andamento das atividades do projeto, desde início da vigência contratual até a assinatura do ANEXO 04 - TERMO DE ACEITAÇÃO DEFINITIVA.

7.6.6. A CONTRATADA disponibilizará também um segundo profissional com o mesmo perfil do Líder Técnico para acompanhar o projeto de forma passiva. Tal profissional deverá assumir todas as responsabilidades e atividades do Líder Técnico durante sua ausência, seja ela programada ou não prevista.

7.6.7. Os profissionais designados para o projeto poderão efetuar suas atividades de forma remota sempre que houver concordância formal do CONTRATANTE. A composição da escala de trabalho presencial e remota será definida pelo CONTRATANTE durante o andamento do projeto e poderá sofrer alterações com base nas necessidades do mesmo.

7.6.8. O CONTRATANTE deve possuir acesso/comunicação direta com os profissionais certificados a serem designados para este processo. Para tanto devem ser fornecidos os dados de contato dos mesmos. O CONTRATANTE poderá solicitar à CONTRATADA a qualquer momento da vigência contratual a revalidação das certificações exigidas.

7.6.9. Na etapa de planejamento, a CONTRATADA será responsável pelo entendimento do ambiente em produção do CONTRATANTE, para que sejam detalhados os passos necessários para a migração do ambiente. O entendimento do ambiente atual deve envolver todos os itens informados pela equipe técnica do CONTRATANTE no PLANO DE PROJETO.

7.6.10. Todas as informações referentes aos ambientes existentes envolvidos neste processo serão repassadas pelo corpo técnico do CONTRATANTE à CONTRATADA.

7.6.11. Será responsabilidade do CONTRATANTE, disponibilizar acesso às configurações dos equipamentos, bem como documentações existentes de topologia.

7.6.12. O CONTRATANTE possui em seu ambiente soluções de outros fabricantes (Cisco, VMWare, Redhat, Aruba, Fortinet, entre outros). Sempre que solicitado pelo CONTRATANTE, a solução deve prever a integração com outras soluções do CONTRATANTE.

7.6.13. A CONTRATADA será responsável pelo entendimento das necessidades técnicas do CONTRATANTE, a fim de customizar a configuração dos equipamentos de forma a obter a melhor performance, disponibilidade e segurança do ambiente.

7.6.14. A CONTRATADA é responsável pela elaboração da solução que melhor atenda às necessidades do CONTRATANTE.

7.6.15. A CONTRATADA é responsável pelo entendimento das necessidades, configuração e customização das ferramentas de gerência, de acordo com o que for especificado no PROJETO LÓGICO.

7.6.16. Todos os serviços necessários para o funcionamento da solução serão configurados para garantir a interoperabilidade do ambiente, alta disponibilidade, gerenciamento, e segurança exigida pelo CONTRATANTE.

7.6.17. O Projeto Lógico, bem como todos seus itens e equipamentos necessários, deve ter documentação de configuração e design aderentes ao PCI DSS (Payment Card Industry - Data Security Standard) vigente, ao longo de todo o período contratual, tendo em consideração as atualizações pelas quais esta norma passa ciclicamente.

7.6.18. A solução, ao ser implementada no escopo de adquirência do CONTRATANTE, deverá, obrigatoriamente, atender plenamente aos requisitos da norma PCI DSS vigente. Neste contexto, cita-se, mas não se limita a:

7.6.18.1. Manter aderência no que tange à segmentação de rede;
7.6.18.2. Utilizar apenas serviços e protocolos estritamente necessários e seguros;
7.6.18.3. Não manter contas genéricas ou default de usuários;
7.6.18.4. Configurar parâmetros de segurança de modo a prevenir mal uso;

7.6.19. Toda documentação do Projeto Lógico Preliminar deve ser validada pela equipe técnica do CONTRATANTE, contando com as melhores práticas de *design* para o respectivo ambiente.

7.6.20. Após o detalhamento técnico do Projeto Lógico Preliminar, a CONTRATADA deve atualizar juntamente com o CONTRATANTE o Cronograma de Implantação com as atividades necessárias, seus pré-requisitos e o mapeamento das responsabilidades entre as equipes.

7.7. IMPLANTAÇÃO E MIGRAÇÃO

7.7.1. A CONTRATADA disponibilizará pelo menos 02 (dois) analistas técnicos para atuar em campo responsáveis pela instalação dos equipamentos, implantação das configurações e parâmetros definidos no Plano Lógico Preliminar e execução de atividades em janelas de manutenção. Os profissionais devem possuir requisitos mínimo de nível PROFISSIONAL DE SEGURANÇA.
7.7.2. Toda configuração será realizada com acompanhamento e autorização prévia do CONTRATANTE.
7.7.3. A CONTRATADA será responsável pela implantação do novo ambiente de modo a cumprir as necessidades técnicas do CONTRATANTE devendo customizar a configuração dos equipamentos de forma a obter a melhor performance, disponibilidade e segurança do ambiente.
7.7.4. A solução contempla a Aquisição de Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida, composta por hardware, software, licenças, garantia, serviços de implementação da solução, suporte de hardware, suporte técnico com acordo de nível de serviço (SLA) definido, manutenção dos equipamentos e treinamento e todos os serviços necessários para configurar e suportar o ambiente de segurança de redes e comunicações junto aos equipamentos do Core de Rede e demais ambientes do CONTRATANTE incluindo a entrega dos produtos especificados no plano de projeto, os profissionais dedicados para operação assistida do ambiente e os testes de aceitação, conforme descrito neste edital.
7.7.5. A CONTRATADA também será responsável por conduzir, em conjunto com a equipe da CONTRATANTE, o processo de migração do ambiente existente para o escopo da nova Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida além de treinar os profissionais do CONTRATANTE para posterior fase de operação do ambiente.
7.7.6. A CONTRATADA executará os serviços sem qualquer interferência no funcionamento regular das atividades normalmente realizadas pelo CONTRATANTE, garantindo a continuidade dos serviços, ou seja, não poderá haver interrupção não programada do serviço de dados atual para a entrada do novo serviço. Desta forma, a CONTRATADA executará serviços em finais de semana, feriados e horário noturno sempre que houver necessidade para atendimento das condições expostas pelo CONTRATANTE nesta especificação.
7.7.7. A CONTRATADA informará ao CONTRATANTE ocorrências de fatos que possam interferir, direta ou indiretamente, na regularidade da prestação do objeto contratado, assim como, especificará de forma clara as responsabilidades que ficarem ao encargo do CONTRATANTE e que não foram descritas nesta especificação.
7.7.8. Os prazos estabelecidos para mudanças no ambiente poderão ser estendidos, a critério do CONTRATANTE e com aviso prévio de 05 (cinco) dias úteis, devido aos períodos de congelamento (*freezing*) definidos pelas áreas responsáveis pelo acesso aos Data Centers do CONTRATANTE. A CONTRATADA deve se adequar ao processo de mudanças do CONTRATANTE, visto que o mesmo é variável em atendimento aos acontecimentos de mercado.
7.7.9. A CONTRATADA poderá solicitar uma janela de manutenção emergencial para realizar o "*rollback*" (restauração) da configuração anterior.
7.7.10. Quaisquer alegações por parte da CONTRATADA relacionadas a instalações (ambiente inadequado, rede elétrica, rede lógica, etc.) ou usuários (mau uso, etc.) do CONTRATANTE, devem ser comprovadas tecnicamente através de laudos detalhados e conclusivos, emitidos pelo fabricante do equipamento. Não serão admitidas omissões baseadas em suposições técnicas sem fundamentação, "experiência" dos técnicos ou alegações baseadas em exemplos de terceiros. Enquanto não for efetuado o laudo e esse não demonstrar claramente os problemas alegados, a CONTRATADA deve prosseguir com o atendimento dos chamados.

7.8. ACEITAÇÃO FINAL

7.8.1. Após a migração, deve ser realizada uma reunião de encerramento do projeto, quando ao receber o ANEXO 04 - TERMO DE ACEITAÇÃO DEFINITIVA, a CONTRATADA deve entregar ao CONTRATANTE o *High Level Design,* documento que descreve o Plano Lógico Completo da solução implementada.
7.8.2. A CONTRATADA deve entregar/revisar o *High Level Design* (HLD) da solução juntamente ao termo de encerramento de projeto, e, além disso, uma atualização a cada 12 (doze) meses a

contar da entrega final do projeto ou após qualquer intervenção para solução de problemas ou mudanças no ambiente. O HLD é o documento que descreve detalhadamente a arquitetura e o desenho lógico da solução, bem como as configurações realizadas na fase de implementação. Além das atualizações refletindo as mudanças do ambiente, o documento deve contemplar:

7.8.2.1. Avaliação do *roadmap* (visão estendida do futuro apresentando uma coletânea de conhecimentos) de desenvolvimento do fabricante dos equipamentos, a fim de verificar novas funcionalidades e continuidade do uso da solução.

7.8.2.2. Continuidade do suporte técnico do fabricante (status de End Of Sale / End Of Life).

7.8.2.3. Validade de licenças.

7.8.2.4. Avaliação das tecnologias utilizadas contendo informações sobre:

7.8.2.5. Estado de uso.

7.8.2.6. Nível de obsolescência.

7.8.2.7. Representa a melhor opção quanto à segurança, desempenho e recursos.

7.8.2.8. Comprovação da inexistência de vulnerabilidades de segurança já catalogadas.

7.8.2.9. Arquitetura:

7.8.2.9.1. Se continua atendendo aos requisitos.

7.8.2.9.2. Se continua sendo a forma mais simples e mais eficaz de atender os requisitos.

7.8.2.9.3. Se atende ao crescimento do CONTRATANTE;

7.8.3. A CONTRATADA deve revisar o Plano Lógico da rede do CONTRATANTE a cada 12 (doze) meses, iniciando-se a contagem deste prazo logo no início da vigência contratual e após qualquer intervenção para solução de problemas e planos de mudanças relacionados à solução.

7.8.4. Ao final da implantação, o ambiente será considerado aceito e 100% funcional, finalizando o projeto com a assinatura do ANEXO 04 - TERMO DE ACEITAÇÃO DEFINITIVA.

7.9. RESPONSABILIDADES

7.9.1. A CONTRATADA deve viabilizar a execução de testes da solução, visando a identificação de vulnerabilidades no ambiente de TI que possam afetar o CONTRATANTE;

7.9.2. A CONTRATADA deve prover suporte e garantia a toda a Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida do CONTRATANTE, conforme especificado, durante todo o período contratual;

7.9.3. A CONTRATADA tem a responsabilidade de aplicar os controles necessários para corrigir quaisquer vulnerabilidades ligadas à solução que possam afetar a confidencialidade, integridade e disponibilidade dos serviços prestados ao CONTRATANTE;

7.9.4. Fica a critério do CONTRATANTE apresentar o detalhamento das análises e testes a serem realizados;

7.9.5. A CONTRATADA deve realizar o tratamento de vulnerabilidades identificadas sem ônus ao CONTRATANTE;

7.9.6. O CONTRATANTE realiza a classificação de vulnerabilidades de acordo com Common Vulnerability Scoring System (CVSS) na Versão 4 (quatro) ou superior;

7.9.7. As vulnerabilidades deverão ser corrigidas dentro dos prazos definidos pelo CONTRATANTE, de acordo com a severidade, definidos nos itens abaixo:

7.9.8. Vulnerabilidades de severidade CRÍTICA em até 10 (dez) dias corridos, a contar da data de encerramento dos testes;

7.9.9. Vulnerabilidades de severidade ALTA em até 30 (trinta) dias corridos, a contar de encerramento dos testes;

7.9.10. Vulnerabilidades de severidade MÉDIA em até 60 (sessenta) dias corridos, a contar da data de encerramento dos testes;

7.9.11. Vulnerabilidades de severidade BAIXA em até 90 (noventa) dias corridos, a contar da data de encerramento dos testes;

7.9.12. Para aquelas vulnerabilidades cuja severidade o cálculo do CVSS seja igual ou superior a 8.6 (oito ponto seis), a CONTRATADA deve iniciar o tratamento da vulnerabilidade imediatamente, incluindo medidas de mitigação e monitoramento de tentativas de exploração, e comunicar tempestivamente a CONTRATANTE;

7.9.13. As correções de vulnerabilidades serão registradas como tickets de Incidentes, associadas e integrantes do Acordo de Níveis de Serviços, no Nível de Severidade e no prazo contratual ajustado entre as PARTES, disto resultando na aplicação das respectivas penalidades em caso de não cumprimento;
7.9.14. O CONTRATANTE pode repassar as informações contidas na documentação para Órgãos Reguladores, Órgãos Fiscalizadores e Auditorias Externas;
7.9.15. As correções de vulnerabilidades por padrão fazem parte do escopo de suporte técnico e operação assistida já fornecidos pela CONTRATADA. As situações que necessitarem do estabelecimento de um projeto para tais correções devem ser conduzidas conforme acordo entre as partes, podendo ou não consumir o saldo de horas técnicas previsto em contrato, conforme o caso;
7.9.16. Acordado ou revisto formalmente a qualquer tempo, o projeto decorrente será classificado como uma Ordem de Serviço, vinculada a Requisição original, passando a ser considerado como integrante do Acordo de Níveis de Serviço, no Nível de Severidade e no prazo ajustado entre as PARTES, disto resultando a aplicação das respectivas penalidades pelo não cumprimento;
7.9.17. Caso a CONTRATADA tenha conhecimento de vulnerabilidades na solução ou na infraestrutura que trafega, processa ou armazena dados do CONTRATANTE, ou vulnerabilidades em outros ativos que possam afetar dados do CONTRATANTE, deve comunicar imediatamente o CONTRATANTE;
7.9.18. A Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida pode sofrer diversas mudanças ao longo do tempo e do seu ciclo de vida. Sempre que houver novas requisições de mudanças ou alterações nas configurações dos equipamentos cobertos pelo contrato atual, estas mudanças serão submetidas à Gerência de Mudanças do CONTRATANTE e passarão por processo de análise e validação pela equipe técnica da CONTRATADA antes de serem implementadas. A CONTRATADA terá 02 (dois) dias úteis para a validação após as propostas de mudanças serem submetidas;
7.9.19. A garantia de hardware e suporte a software deve abranger todo período contratual, no local de instalação dos equipamentos, para todos os equipamentos fornecidos;
7.9.20. A garantia deve prever a substituição de equipamentos que apresentem defeitos, bem como direito a atualização de software (minor releases) destes. Todo equipamento fornecido em substituição pela garantia deve ser acompanhado de Nota Fiscal da CONTRATADA. A CONTRATADA deve conceder o direito junto ao FABRICANTE para download de novos releases (minor releases) de software para os equipamentos cobertos pela garantia, em caso de problemas e/ou bugs registrados;
7.9.21. A garantia deve prever a atualização de licenças, inclusive as de subscrição, por todo o período contratual, para todo hardware e software que compõe a solução;
7.9.22. Se, durante a vigência do contrato houver o lançamento de um novo produto ou atualização de software que contenha no mínimo as mesmas funcionalidades do software contratado e fique caracterizado que este lançamento provocará uma descontinuidade na comercialização e suporte de qualquer software suportado por este contrato, a CONTRATADA deve efetuar o fornecimento e implantação deste novo software, sem ônus ao CONTRATANTE, mesmo que o referido produto contenha, adicionalmente, características e funcionalidades que originalmente não existiam no software contratado;
7.9.23. Nesse caso, o fornecimento e implantação do novo produto deve ocorrer em no máximo 120 (cento) dias corridos a contar da solicitação formal do CONTRATANTE, na qual serão apontadas evidências da descontinuidade na comercialização e suporte do software, hardware ou serviço suportado;
7.9.24. Ocorrendo a troca do produto, a CONTRATADA é obrigada a fornecer a quantidade de licenças necessárias para licenciar a infraestrutura da CONTRATANTE, previamente estipulada neste edital e no decorrer do contrato;
7.9.25. A CONTRATADA arcará com qualquer ônus referente à troca, licenciamento, migração, instalação e configuração de software, entre outros, ficando a CONTRATANTE livre de qualquer ônus diferente do acordado no contrato;
7.9.26. Caso a CONTRATADA identifique a necessidade de substituição de equipamentos que apresentem defeitos ou falhas, estes devem ser substituídos por produtos de qualidade e

características técnicas iguais ou superiores aos existentes, desde que compatíveis com todas as configurações necessárias ao seu funcionamento no ambiente do CONTRATANTE. O descarte dos equipamentos substituídos será de inteira responsabilidade da CONTRATADA, devendo respeitar as melhores práticas de sustentabilidade, conforme a Política Nacional de Resíduos Sólidos.

7.10. TREINAMENTOS OFICIAIS, OPERACIONAIS, EVENTOS e WORKSHOPS de Atualização

7.10.1. TREINAMENTOS OFICIAIS DO FABRICANTE

7.10.1.1. A CONTRATADA deve fornecer TREINAMENTOS OFICIAIS do fabricante que devem anteceder à finalização da etapa de planejamento da implementação do projeto (plano lógico preliminar) para que a equipe do CONTRATANTE possa receber o conhecimento amplo e necessário para entender e realizar a implementação da solução;

7.10.1.2. Os treinamentos oficiais dos fabricantes devem capacitar os colaboradores do CONTRATANTE para a realização de prova oficial de certificação do fabricante para o nível de ADMINISTRADOR / PROFISSIONAL DE SEGURANÇA DE REDES, ou nível técnico administrador equivalente, para todas as funcionalidades fornecidas na solução;

7.10.1.3. A CONTRATADA deve fornecer também os treinamentos oficiais que porventura sejam pré-requisitos dos treinamentos oficiais de nível administrador solicitados;

7.10.1.4. Os treinamentos oficiais dos fabricantes devem seguir no mínimo a carga horária informada na grade vigente dos cursos oficiais do fabricante em questão;

7.10.1.5. Para os TREINAMENTOS OFICIAIS, deve ser utilizada a ementa oficial dos cursos do fabricante, não serão aceitos treinamentos customizados;

7.10.1.6. A CONTRATADA deve prover treinamentos oficiais dos fabricantes dos equipamentos envolvidos na solução para 20 (vinte) colaboradores do CONTRATANTE, em duas turmas, no total de 10 (dez) pessoas por turma, em datas previamente acordadas com o CONTRATANTE;

7.10.1.7. Para todos os treinamentos previstos no presente termo deve haver intervalos de 15 minutos a cada duas horas de treinamento;

7.10.1.8. Para todos os treinamentos realizados no formato presencial, no intervalo de todos os treinamentos previstos no presente termo a CONTRATADA deve disponibilizar Coffee Break aos alunos de cada turma;

7.10.1.9. Os treinamentos devem ser realizados em Porto Alegre – RS, em local a ser definido pela CONTRATADA em comum acordo com o CONTRATANTE;

7.10.1.10. A CONTRATADA será responsável por providenciar os locais e os recursos necessários para os treinamentos oficiais;

7.10.2. TREINAMENTOS OPERACIONAIS

7.10.2.1. A CONTRATADA ministrará treinamentos demonstrando aspectos principais da configuração do produto após a implementação. Os treinamentos operacionais devem contemplar conhecimentos com relação aos equipamentos ofertados, especificamente conhecimento do hardware, seus módulos, conexões, protocolos suportados, configuração, operação e gerenciamento, assim como módulos de serviço ou soluções em nuvem, conforme as boas práticas de implementação utilizadas no projeto.

7.10.2.2. A CONTRATADA deve fornecer TREINAMENTOS OPERACIONAIS para passagem de conhecimento após a finalização da migração para o novo ambiente;

7.10.2.3. Os Treinamentos Operacionais visam passar uma visão geral de como foi implementada a solução no ambiente do CONTRATANTE e devem ser ministrados por um profissional da CONTRATADA envolvido no projeto e devidamente qualificado com a certificação técnica de grau máximo na solução ofertada.

7.10.2.4. A CONTRATADA deve ministrar os treinamentos operacionais, sem custo adicional ao CONTRATANTE para 20 (vinte) colaboradores, em duas turmas de 10 (dez) pessoas.

7.10.2.5. Os treinamentos deverão ser ministrados em português (salvo comum acordo com a CONTRATANTE para uso de língua estrangeira) e serão realizados presencialmente em Porto

Alegre – RS, em local a ser definido pelo CONTRATANTE, para duas turmas, no total de 10 (dez) pessoas por turma;
7.10.2.6. A carga horária mínima é de 30 (trinta) horas no total;
7.10.2.7. Deve haver intervalos de 15 minutos a cada duas horas de treinamento;
7.10.2.8. Nos intervalos dos treinamentos a CONTRATADA deve disponibilizar coffee break com itens variados aos alunos de cada turma, prevendo um total de 15 pessoas (alunos, instrutor e equipe de treinamento) por turma;
7.10.2.9. O CONTRATANTE informará à CONTRATADA com 15 (quinze) dias de antecedência a data de realização de todos os cursos previstos nos itens desta especificação;
7.10.2.10. Os treinamentos operacionais devem abordar, no mínimo, os seguintes tópicos gerais:
7.10.2.10.1. Descrição do escopo da solução e produtos envolvidos no projeto (overview da plataforma);
7.10.2.10.2. Instrumentação de todos os recursos da solução;
7.10.2.10.3. Apresentação de como ocorreu a migração para a solução;
7.10.2.10.4. Descoberta de ativos e inventário;
7.10.2.10.5. Relatórios e painéis interativos;
7.10.2.10.6. Avaliação dos desafios de rede (quais os problemas mais comuns);
7.10.2.10.7. Serviço de inspeção e monitoramento;
7.10.2.10.8. Propósitos da implementação e principais características;
7.10.2.10.9. Arquitetura e componentes;
7.10.2.10.10. Ferramentas de diagnóstico;
7.10.2.10.11. Funcionamento e problemas mais comuns;
7.10.2.10.12. Definições de grupos de usuários;
7.10.2.10.13. Entendendo o comportamento do tráfego;
7.10.2.10.14. Recursos de filtragem dos dados (condições lógicas, IP, porta, seção, outros);
7.10.2.10.15. Utilização em conjunto com outras soluções e tecnologias;
7.10.2.10.16. Estratégias e formas de incremento da solução no ambiente;
7.10.2.10.17. Estratégias para manutenção da solução;
7.10.2.10.18. Possíveis cenários de degradação;
7.10.2.10.19. Troubleshooting: Possíveis problemas e passo a passo para solucioná-los;
7.10.2.10.20. Hands-on da Operação e manuseio das ferramentas de administração;
7.10.2.10.21. Integração com outros fabricantes;
7.10.2.11. Os treinamentos serão divididos em fases ou agrupados, dependendo da escolha do público-alvo e disponibilidade de agendas, sendo essa definição pelo CONTRATANTE em fase de execução do projeto;
7.10.2.12. Mediante negociação e com o devido aceite do contratante, os treinamentos poderão ser realizados de forma remota, desde que todas as ferramentas necessárias para o bom andamento dos treinamentos sejam disponibilizadas pela CONTRATADA, sem ônus ao CONTRATANTE;
7.10.3. OUTROS TREINAMENTOS, EVENTOS E WORKSHOPS DE ATUALIZAÇÃO
7.10.3.1. A CONTRATADA deve realizar Workshops de Atualização de Conhecimentos e Tecnologia anualmente para até 10 (dez) colaboradores do CONTRATANTE;
7.10.3.2. Cada workshop deve ser concluído dentro do período de cada ciclo anual do contrato, considerando a data de assinatura do contrato como o início do primeiro ciclo anual, de acordo com cronograma estabelecido entre a Equipe Técnica do CONTRATANTE e a CONTRATADA;
7.10.3.3. Os workshops podem ser realizados nas dependências do CONTRATANTE e devem ser ministrados por instrutores preparados e certificados pelo fabricante dos produtos;
7.10.3.4. Os workshops previamente planejados devem ter carga horária mínima de 20 (vinte) horas, cobrindo conteúdo teórico e prático, em nível avançado e relacionado à solução fornecida, com foco nas atualizações aplicadas à solução durante cada ciclo anual, bem como em tópicos de interesse da equipe técnica do CONTRATANTE. Nesses casos, o workshop e o material didático deverão estar, preferencialmente, em língua portuguesa, ou, na sua impossibilidade, em língua inglesa;

7.10.3.5. Ainda dentro do período de cada ciclo anual do contrato, A CONTRATADA deve disponibilizar anualmente, 04 (quatro) vagas para colabores do CONTRATANTE para a participação de eventos de tecnologia do fabricante da solução ou em evento de tecnologia do qual o fabricante da solução esteja participando;
7.10.3.6. Caso os treinamentos, eventos ou workshops sejam realizados fora de Porto Alegre, as despesas com transporte (aéreo e local), hospedagem e alimentação deverão ser custeadas pela CONTRATADA;

7.11. MANUTENÇÃO, SUPORTE TÉCNICO E OPERAÇÃO ASSISTIDA DOS AMBIENTES

7.11.1. A CONTRATADA deve disponibilizar, sempre que necessário, profissionais para suporte às demandas da Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida.
7.11.2. Após a aceitação final do projeto, todos os profissionais mencionados acima devem possuir conhecimento pleno e detalhado da solução implementada no ambiente da CONTRATANTE.
7.11.3. A CONTRATADA deve garantir o acesso/comunicação direto do CONTRATANTE com os profissionais certificados a serem designados para este processo. Para tanto devem ser fornecidos os dados de contato destes profissionais.
7.11.4. O CONTRATANTE poderá solicitar à CONTRATADA a qualquer momento a revalidação das certificações anteriormente mencionadas.
7.11.5. A CONTRATADA é responsável pela elaboração da solução que melhor atenda às necessidades do CONTRATANTE. Todos os serviços de rede necessários para o funcionamento da solução serão configurados para garantir a interoperabilidade do ambiente, alta-disponibilidade, gerenciamento, balanceamento de carga e segurança desejada pelo CONTRATANTE.
7.11.6. A CONTRATADA deve elaborar o Plano de Continuidade de Negócios (PCN), embasado nas normas (ABNT NBR ISO 22301:2020 - Segurança e resiliência — Sistema de gestão de continuidade de negócios — Requisitos) ou boas práticas reconhecidas pelo mercado (Information Technology Infrastructure Library versão quatro – ITILv4, Control Objectives for Information and related Technology versão 2019 – COBIT 2019) para a Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida. O referido PCN e as evidências dos testes realizados deverão ser apresentados pela CONTRATADA ao CONTRATANTE na ocasião do encerramento da implementação, sendo atualizado anualmente ou sempre que solicitado. O Plano deve incluir:
7.11.6.1. PCN por Modelo de Equipamento: descrevendo cada equipamento, seus módulos, aplicação, serviços afetados em caso de falha, responsáveis pelos serviços, principais sintomas de incidentes e procedimentos de solução de contorno.
7.11.6.2. PCN por Cenário: descrevendo os principais cenários de quedas e paralisações de serviços de rede, baseando-se na topologia do CONTRATANTE, os principais sintomas e procedimentos de solução de contorno.
7.11.6.3. Plano de Testes para serem realizados após mudanças no ambiente.
7.11.7. O PCN deve ser revisado e atualizado a cada 12 (doze) meses a contar da entrega da primeira versão, a critério do CONTRATANTE, sempre que houver mudanças significativas na estrutura da solução e sempre que for solicitado.
7.11.8. O PCN apresentado pela CONTRATADA será analisado pelo CONTRATANTE, que poderá aceitar, rejeitar ou sugerir adequações de forma a atender aos requisitos do Acordo Níveis de Serviços. Em caso de rejeição ou havendo necessidade de ajustes a CONTRATADA terá mais 30 (trinta) dias corridos, a partir da comunicação do CONTRATANTE, para retornar o plano atualizado.

7.11.9. A CONTRATADA deve prover serviço de suporte técnico para execução de manutenção preventiva e corretiva dos equipamentos, que compõem a solução, instalados nos Data Center do CONTRATANTE. A CONTRATADA será a responsável direta pelos serviços de manutenção e suporte técnico, que serão pagos mensalmente.

7.11.10. O CONTRATANTE utiliza ferramenta padrão de mercado como meio de monitoramento proativo de falhas de todo o ambiente listado na planilha de especificações técnicas.
7.11.11. A CONTRATADA deve solicitar e sugerir customizações nas ferramentas de Gerência ao suporte técnico do CONTRATANTE a fim de auxiliar no cumprimento do SLA especificado neste documento.
7.11.12. Todos os equipamentos inseridos na solução devem ser passíveis de monitoração através da ferramenta "CA Spectrum".
7.11.13. Os serviços contemplam a substituição de peças e equipamentos em caso de falhas, atualizações de software e acesso ao "Centro de Assistência Técnica" (TAC - Technical Assistance Center) do fabricante dos equipamentos, através da CONTRATADA, e acesso ao "Ambiente Online do Fabricante" (AOF).
7.11.14. O acesso ao TAC e ao AOF será realizado através de usuário (identificador) e senha que permitam o acompanhamento de solicitações de serviço, bem como livre acesso às ferramentas e documentos técnicos disponibilizados pelo fabricante. A CONTRATADA deve controlar e fornecer as últimas versões dos softwares utilizados pelos equipamentos, contendo correções de bugs, atualizações ou novas funcionalidades suportadas, pelo equipamento em questão, bem como as respectivas licenças de uso.
7.11.15. A garantia deve prever a substituição de equipamentos que apresentem defeitos e o direito a atualização de software (*minor releases*) destes. Todo equipamento fornecido em substituição pela garantia deve ser acompanhado de Nota Fiscal da CONTRATADA. A CONTRATADA deve conceder o direito junto ao FABRICANTE para download de novos releases (minor releases) de software para os equipamentos cobertos pela GARANTIA, em caso de problemas e *bugs* registrados.
7.11.16. Caso a CONTRATADA identifique a necessidade de substituição de equipamentos que apresentem defeitos ou falhas, estes devem ser substituídos por produtos de qualidade e características técnicas iguais ou superiores aos existentes, desde que compatíveis com todas as configurações necessárias ao seu funcionamento no ambiente do CONTRATANTE.
7.11.17. O CONTRATANTE poderá abrir chamados técnicos com a CONTRATADA para consultoria técnica, participação do planejamento de novos projetos, configurações de novos serviços, aplicação de atualização de versões de software nos equipamentos, acompanhamento de janelas de manutenção programadas em qualquer horário e resolução de problemas (troubleshooting).
7.11.18. Para atendimento aos chamados dentro do SLA, o CONTRATANTE autorizará o acesso para os profissionais e equipamentos da CONTRATADA aos dois prédios de Data Center, dentro e fora do horário comercial. O CONTRATANTE também irá permitir o acesso remoto assistido à rede.
7.11.19. A abertura de chamados seguirá as melhores práticas descritas na última versão do ITIL quanto aos níveis de escalonamento. Para a resolução de problemas de maior complexidade devem ser envolvidos profissionais com maior capacitação.
7.11.20. O atendimento aos chamados poderá ser iniciado remotamente, de forma assistida até o registro de abertura do chamado.
7.11.21. Após o registro de abertura de um chamado e/ou contato telefônico com os representantes técnicos, o atendimento pode ocorrer nas dependências do CONTRATANTE em Porto Alegre/RS, a critério do CONTRATANTE.
7.11.22. Os chamados de suporte para manutenções preventivas, atualização de versão de softwares, adoção de novas tecnologias, adição de novas funcionalidades, aperfeiçoamento de configurações e alterações nas topologias da rede que envolvam os equipamentos, serão atendidos nas dependências do CONTRATANTE, em Porto Alegre/RS, em data e horário previamente acordado entre as partes.
7.11.23. Todo o suporte deve ser assistido por técnicos da CONTRATADA com qualificação comprovada pelo fabricante do equipamento, quando solicitado;
7.11.24. Os serviços prestados deverão ser realizados nas dependências da CONTRATANTE.

7.11.25. Os profissionais designados para atender aos chamados devem possuir conhecimento avançado de todos os elementos que irão compor a Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida adquirida pelo CONTRATANTE (Hardware, Software, Licenças, Protocolos, APIs, etc) bem como o conhecimento prévio da arquitetura implementada.

7.11.26. A CONTRATADA deve realizar *Health Checks* sob demanda, com o objetivo de verificar todos os aspectos relacionadas à solução, observando conformidade com as melhores práticas de configuração e segurança do fabricante, validação dos parâmetros em uso e identificação de funcionalidades disponíveis, porém não implementadas;
7.11.27. A CONTRATADA deve iniciar a execução do serviço em até 30 dias após a solicitação do CONTRATANTE.
7.11.28. A CONTRATADA deve apresentar uma proposta completa do *Heatlh Check* a ser realizado, contendo no mínimo o plano de ação para execução, cronograma e prazos, relação de itens a serem avaliados, e deve ter o prévio aceite do CONTRATANTE.
7.11.29. O CONTRATANTE reserva-se o direito de alterar o plano de ação conforme sua necessidade.
7.11.30. Como resultado do *Health Check*, a CONTRATADA deve apresentar ao CONTRATANTE, um relatório contendo, para o escopo avaliado:
7.11.30.1. Detalhamento da situação de cada item analisado;
7.11.30.2. As inconformidades da configuração atual, de acordo com as melhores práticas do fabricante;
7.11.30.3. As funcionalidades disponíveis na solução e não implementadas;
7.11.30.4. As vantagens, riscos, pré-requisitos, premissas, e custos atrelados a licenciamento, aquisição, configuração, e estimativa de horas necessárias;
7.11.30.5. Elaborar o plano de ação para atendimento dos itens apontados no relatório;
7.11.31. A CONTRATADA deve alocar 500 (quinhentas) horas técnicas por ano (em caráter limitador máximo, podendo variar de acordo com as necessidades do CONTRATANTE) para a prestação de serviços de suporte ao desenvolvimento, manutenção, implementação, projetos e especificações de segurança da informação com ênfase na solução ofertada, a serem executados nas dependências do CONTRATANTE, envolvendo:
7.11.31.1. Elaboração de novos projetos;
7.11.31.2. Suporte técnico no desenvolvimento e integração, relativos à solução ofertada;
7.11.31.3. Elaboração de material de apoio e documentação de novos projetos;
7.11.31.4. Elaboração de pareceres técnicos;
7.11.31.5. Orientação a analistas, desenvolvedores e programadores sobre aspectos relacionados à segurança da informação e a da solução ofertada;
7.11.32. Para a prestação dos serviços deste objeto a CONTRATADA vencedora do certame deve possuir:
7.11.32.1. Conhecimento sobre normas e regulamentações associadas a Segurança da Informação (ISO-27001, ISO-27002);
7.11.32.2. Comprovar conhecimento técnico através de pelo menos UMA das certificações profissionais constantes nos subitens a seguir:
7.11.32.2.1. CRISC (Certified in Risk and Information Systems Control – emitido pelo ISACA (Information Systems Audit and Control Association);
7.11.32.2.2. SECURITY+ (Certified by Computing Technology Industry Association USA - CompTIA);
7.11.32.2.3. CISM (Certified Information Security Manager) - emitido pelo ISACA (Information Systems Audit and Control Association);
7.11.32.2.4. CISSP (Certified Information System Security Professional) - emitido pelo ISC² (International Information Security System Certification Consortium);

7.11.33. A CONTRATADA deve disponibilizar para a Operação Assistida pelo menos 02 (dois) profissionais dedicados que atendam aos requisitos de nível PROFISSIONAL DE SEGURANÇA;

7.11.34. A CONTRATADA deve prover serviço de suporte técnico 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, no seguinte formato:
7.11.35. TRABALHO PRESENCIAL, através de profissionais dedicados, que no conjunto de suas escalas de trabalho, cubram a jornada regular inicialmente estabelecida das 07h30min às 19h30min, de segunda à sexta, para atuar na operação assistida de forma dedicada junto à equipe técnica do CONTRATANTE. O intervalo para jornada regular presencial a ser cumprida pode ser alterado conforme necessidade do CONTRATANTE, mantendo a carga horária individual por profissional dedicado prevista para 8 (oito) horas por dia;
7.11.36. TRABALHO REMOTO, em caráter de sobreaviso, através dos profissionais dedicados à operação assistida nos casos em que for necessária a atuação fora dos dias e horários de jornada regular definidos para o atendimento presencial, visando a execução do serviço de manutenção preventiva e corretiva dos equipamentos que compõem a Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida;
7.11.37. Cada profissional alocado para a operação assistida poderá realizar jornada de trabalho em formato híbrido através de escala mensal pré-definida em conjunto com a equipe técnica do CONTRATANTE, alternando entre formato presencial (dentro das instalações do CONTRATANTE) e remoto, estando sujeito a alterações, sem custos adicionais e de acordo com a escala de trabalho da equipe técnica do CONTRATANTE e com as suas políticas de teletrabalho;
7.11.38. A composição da escala da execução de trabalho presencial e remoto deve ser acordada entre as partes;
7.11.39. As horas realizadas em tarefas extraordinárias, fora da jornada de trabalho, seja em planos de mudança ou atendimento a incidentes, não serão contabilizadas para o atendimento ao tempo mínimo de escala presencial;
7.11.40. Em caso de alteração das políticas de teletrabalho, o CONTRATANTE deve comunicar formalmente à CONTRATADA o novo regramento, com antecedência de 30 (trinta) dias corridos, através de e-mail e/ou em reunião com o registro em ata;
7.11.41. O CONTRATANTE proverá os recursos administrativos (instalações, mesas, cadeiras, material de expediente, etc.) para atendimentos efetuados *in loco*;
7.11.42. O CONTRATANTE poderá, a qualquer momento, solicitar visita ao Centro de Operações e Suporte a Serviço da CONTRATADA, a fim de comprovar que a CONTRATADA possui estrutura de atendimento 24x7 para atendimento das demandas técnicas do CONTRATANTE;

7.12. ACORDO DE NÍVEIS DE SERVIÇO

7.12.1. O objetivo deste acordo é estabelecer as diretrizes para a entrega de serviços de alta qualidade para a Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida, de acordo com as necessidades do CONTRATANTE.
7.12.2. A cobertura dos serviços será integral, ou seja, 24 (vinte e quatro) horas por dia, nos 7 (sete) dias da semana, incluindo sábados, domingos, feriados e pontos facultativos. A abertura do chamado técnico ou solicitação de serviço será realizada através dos seguintes meios: Registro no sistema de Service Desk do CONTRATANTE, diretamente com os profissionais da CONTRATADA e via chamado telefônico DDG (0800);
7.12.3. 1.3. A CONTRATADA deve prover suporte e garantia a toda a Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida do CONTRATANTE, conforme especificado;
7.12.4. O CONTRATANTE utiliza ferramenta padrão de mercado como meio de monitoramento proativo de falhas de todo o ambiente listado na planilha de especificações técnicas (CA Spectrum). A CONTRATADA deve solicitar e sugerir customizações nas ferramentas de Gerência de Rede ao suporte técnico do CONTRATANTE a fim de auxiliar no cumprimento do SLA especificado neste documento. As informações contidas nos relatórios devem ser analisadas e apresentadas pela CONTRATADA sempre que solicitado pelo CONTRATANTE.
7.12.5. Os serviços contemplam a substituição de peças e equipamentos em caso de falhas, atualizações de software e acesso ao “Centro de Assistência Técnica” (TAC - Technical

Assistance Center) do fabricante dos equipamentos, através da CONTRATADA, e acesso ao "Ambiente Online do Fabricante" (AOF).

7.12.6. O acesso ao TAC e ao AOF será realizado através de usuário (identificador) e senha que permitam o acompanhamento de solicitações de serviço, bem como livre acesso às ferramentas e documentos técnicos disponibilizados pelo fabricante. A CONTRATADA deve controlar e fornecer as últimas versões dos softwares utilizados pelos equipamentos, contendo correções de bugs, atualizações ou novas funcionalidades suportadas, pelo equipamento em questão, bem como as respectivas licenças de uso;

7.12.7. A CONTRATADA deve fornecer o suporte do tipo solução junto ao fabricante, ou seja, o atendimento de chamados deve ocorrer através de uma equipe dedicada com nível técnico compatível com a complexidade do ambiente e processos de suporte coordenados, de modo a otimizar o tempo de resposta com o atendimento especializado. Esse nível de suporte visa resolver problemas mais rapidamente do que depender apenas do suporte padrão ao produto, prestando um nível avançado de atendimento e caso de chamados efetuados diretamente pelo CONTRATANTE junto ao fabricante, ou ainda por intermédio dos profissionais dedicados à operação assistida;

7.12.8. A CONTRATADA deve prestar as seguintes informações, por ocasião do início do contrato:

7.12.9. Procedimento descritivo ou ilustrativo de acesso ao TAC do fabricante pela Internet, para cadastro de usuários e abertura de registro por escrito referente a solicitações de assistência técnica (cases), bem como o acesso aos serviços de atualização de software e documentação técnica;

7.12.10. Número telefônico gratuito (serviço 0800) do TAC do fabricante da solução para o registro de solicitações de assistência técnica;

7.12.11. O CONTRATANTE poderá abrir requisições de serviço com a CONTRATADA para: consultoria técnica, participação do planejamento de novos projetos, configurações de novos serviços que envolvam o ambiente de segurança de rede e comunicações do CONTRATANTE, aplicação de atualização de versões de software nos equipamentos, acompanhamento de janelas de manutenção programadas em qualquer horário e resolução de problemas (troubleshooting);

7.12.12. As requisições de serviço por padrão fazem parte do escopo de suporte técnico e operação assistida já fornecidos pela CONTRATADA. As situações que necessitarem do estabelecimento de um projeto para tais requisições devem ser conduzidas conforme acordo entre as partes, podendo ou não consumir o saldo de horas técnicas previsto em contrato, conforme o caso;

7.12.13. A CONTRATADA deve possuir em sua equipe técnica profissionais com perfil do tipo PROFISSIONAL DE SEGURANÇA ou superior para atendimento de demandas realizadas via chamado técnico (0800) durante toda a sua operação (24x7);

7.12.14. Todo o suporte deve ser assistido por técnicos da CONTRATADA com qualificação comprovada pelo fabricante do equipamento, sempre que solicitado;

7.12.15. Os chamados de suporte para atualização de versão de softwares, adição de novas funcionalidades, aperfeiçoamento de configurações e alterações nas topologias da rede que envolvam risco de parada da continuidade do serviço prestado pela solução deverão ser atendidos nas dependências do CONTRATANTE, em Porto Alegre, em data e horário previamente acordado entre as partes.

7.12.16. A CONTRATADA reconhece que o não atendimento dos níveis de serviços contratados pode resultar em impacto adverso e relevante nos negócios e operações do CONTRATANTE;

7.12.17. Para atendimento aos chamados dentro dos prazos do SLA, o CONTRATANTE autorizará o acesso para os profissionais e equipamentos da CONTRATADA aos prédios de Data Center, dentro e fora do horário comercial, além do acesso remoto assistido à rede sempre que necessário;

7.12.18. A abertura de chamados seguirá as melhores práticas descritas na última versão do ITIL quanto aos níveis de escalonamento. Para a resolução de problemas de maior complexidade devem ser envolvidos profissionais com maior capacitação;

7.12.19. Após o registro de abertura de um chamado/incidente e/ou contato telefônico com os representantes técnicos, quando a natureza da ocorrência implicar em inoperância da solução ou afetar de forma significativa seu funcionamento, o atendimento deve ocorrer nas dependências do CONTRATANTE em Porto Alegre. Dentro dos horários de cobertura da operação assistida o atendimento poderá ser realizado inicialmente pela própria equipe local da CONTRATADA.
7.12.20. Os profissionais alocados na operação assistida responderão para a coordenação da área responsável pela Arquitetura de Segurança de Rede Corporativa do CONTRATANTE, limitando-se a executar atividades mediante anuência e aceite formal do CONTRATANTE;
7.12.21. Os profissionais alocados para a operação assistida devem apresentar vínculo profissional com a CONTRATADA;
7.12.22. Cada profissional deve possuir notebook, acesso próprio à internet e telefone celular, fornecidos e sob a responsabilidade da CONTRATADA, independente da infraestrutura fornecida pelo CONTRATANTE;
7.12.23. Os profissionais a serem destacados para atuar no CONTRATANTE devem possuir as seguintes atribuições:
7.12.24. Operação, arquitetura e administração de equipamentos e produtos da Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida;
7.12.25. Realização de suporte 1º e 2º nível para clientes internos e manutenções preventivas no ambiente de rede;
7.12.26. Atualização de documentações da rede do cliente, incluindo o Projeto Lógico, PCN, HLD, etc;
7.12.27. Inventário e identificação de equipamentos instalados;
7.12.28. Atualização de topologias;
7.12.29. Interação com operadoras de Telecom, mediante liberação pelos gestores técnicos do CONTRATANTE, para a resolução de problemas relacionados aos enlaces de longa distância (WAN);
7.12.30. Interação e comunicação com a equipe de Arquitetura de Segurança de Rede Corporativa do CONTRATANTE;
7.12.31. Realização de coleta de informações de rede, históricos (logs) e informações provenientes da equipe de TI do CONTRATANTE;
7.12.32. Apoiar as equipes do CONTRATANTE no controle das versões de software;
7.12.33. Aplicação de atualizações das versões de software nos equipamentos;
7.12.34. Configuração dos ativos da solução;
7.12.35. Desenvolvimento e manutenção de integrações dos dispositivos de rede junto a outros ambientes com uso de API REST;
7.12.36. Análise de informações coletadas, verificação de design e acompanhamento de arquitetura e recomendações;
7.12.37. Interagir na administração das ferramentas que o CONTRATANTE dispõe para a administração da solução, visando à agilidade dos diagnósticos e pronta resposta;
7.12.38. Acompanhamento de janelas de manutenção programadas em qualquer horário;
7.12.39. Identificar os componentes, peças, materiais ou software responsáveis pelo mau funcionamento dos equipamentos;
7.12.40. Ministrar treinamentos/passagem de conhecimento referentes aos equipamentos, protocolos e atividades realizadas nas dependências do CONTRATANTE;
7.12.41. Atualizar requisições e incidentes através da ferramenta de Service Desk do CONTRATANTE;
7.12.42. Em caso de ausência do profissional, por motivações previstas em lei ou não, a CONTRATADA deve disponibilizar um substituto com o mesmo perfil em no máximo 1 (uma) hora.

7.13. PRAZOS E PERIODICIDADE DA EXECUÇÃO

7.13.1. Os equipamentos devem ser entregues e instalados e os serviços devem ser prestados de acordo com o cronograma a seguir:

7.13.1.1. Atividade 1: ABERTURA e PLANO DE PROJETO
7.13.1.1.1. ABERTURA - Reunião inicial do projeto (kick-off com todo o time envolvido): Até 5 (cinco) dias úteis a contar do início da vigência do contrato;
7.13.1.1.2. Termo de Abertura do Projeto;
7.13.1.1.3. Reuniões semanais de atualização;
7.13.1.1.4. Gerenciamento do projeto: Desde o início da vigência do contrato até a entrega da documentação técnica final;
7.13.1.1.5. Apresentação do PLANO DE PROJETO completo: Até 15 (Quinze) dias úteis a contar da reunião inicial do projeto;
7.13.1.1.6. Plano de Gerenciamento de Projeto e EAP (Estrutura Analítica do Projeto);
7.13.1.1.7. Plano de Projeto (Atividades do Escopo);
7.13.1.1.8. Cronograma;

7.13.1.2. **Atividade 2: PLANEJAMENTO TÉCNICO PRELIMINAR E ENTREGA DOS EQUIPAMENTOS**: Até 45 (quarenta e cinco) dias corridos a contar do início da vigência do Contrato;
7.13.1.2.1. O ato de entrega dos equipamentos será considerado concluído após os testes iniciais de *"burn-in"* que consiste em ligar os equipamentos e validar o correto funcionamento de seus componentes e acesso à interfaces de gerenciamento e configuração.
7.13.1.2.2. Os testes iniciais devem ser acompanhados pelos profissionais da CONTRATADA;
7.13.1.2.3. Finalizados os testes de *"burn-in",* será emitido pelo CONTRATANTE o ANEXO 03 - TERMO DE RECEBIMENTO referente a etapa de entrega dos equipamentos;
7.13.1.2.4. Apresentação do **PLANEJAMENTO TÉCNICO PRELIMINAR**: Até que ocorra a entrega dos equipamentos. O Planejamento técnico preliminar inclui o projeto lógico e plano de migração com detalhamento de atividades para avaliação anterior à implementação do projeto;

7.13.1.3. Atividade 3: GARANTIA DE HARDWARE E SOFTWARE E TREINAMENTOS OFICIAIS:
7.13.1.3.1. INÍCIO DA VIGÊNCIA DA GARANTIA DE HARDWARE E SOFTWARE: Imediatamente após a entrega dos equipamentos;
7.13.1.3.2. TREINAMENTOS OFICIAIS: Devem ser concluídos antes de finalizar a MIGRAÇÃO PARA O NOVO AMBIENTE (Atividade 5);

7.13.1.4. **Atividade 4: IMPLEMENTAÇÃO INICIAL DO PROJETO:** Deve ser concluída até 120 (cento e vinte) dias a contar do início da vigência do Contrato;
7.13.1.4.1. Configurações da nova solução;
7.13.1.4.2. Licenciamento;

7.13.1.5. **Atividade 5: MIGRAÇÃO PARA O NOVO AMBIENTE**: Deve ser concluída até 180 (cento e oitenta dias) dias corridos a contar da conclusão da IMPLEMENTAÇÃO INICIAL DO PROJETO;
7.13.1.5.1. Migração dos ambientes existentes para a nova solução;
7.13.1.5.2. Acompanhamento da Migração;

7.13.1.6. Atividade 6: SUPORTE/MANUTENÇÃO A HARDWARE E SOFTWARE E PROFISSIONAIS DEDICADOS À OPERAÇÃO ASSISTIDA
7.13.1.6.1. INÍCIO DA VIGÊNCIA DO SUPORTE E MANUTENÇÃO A HARDWARE E SOFTWARE: Imediatamente após a IMPLEMENTAÇÃO INICIAL DO PROJETO (Atividade 4);
7.13.1.6.2. PROFISSIONAIS DEDICADOS À OPERAÇÃO ASSISTIDA: Em até 60 (sessenta) dias corridos a partir do início da MIGRAÇÃO PARA O NOVO AMBIENTE para a apresentação e início das atividades dos profissionais dedicados à operação assistida, de forma que estes participem da fase de IMPLEMENTAÇÃO INICIAL DO PROJETO;

7.13.1.6.3. O serviço de operação assistida deve ocorrer de segunda-feira a sexta-feira, exceto feriados, nacionais e municipais de Porto Alegre, das 07h30min às 19h30min através de dois profissionais dedicados, conforme seguintes horários:
7.13.1.6.4. Horário dos Profissionais de Operação Assistida:
7.13.1.6.4.1. PROFISSIONAL DE SEGURANÇA 01: 07h30min às 16h30min, com uma hora de intervalo nesse período;
7.13.1.6.4.2. PROFISSIONAL DE SEGURANÇA 02: 10h30min às 19h30min, com uma hora de intervalo nesse período;

7.13.1.7. Atividade 7: TESTES DE ACEITAÇÃO E TREINAMENTO OPERACIONAL:
7.13.1.7.1. TESTES DE ACEITAÇÃO: Em fases conforme as entregas parciais de migração, devendo ocorrer a conclusão (TERMO DE ACEITAÇÃO DEFINITIVA) em até 15 (quinze) dias úteis após a conclusão da MIGRAÇÃO PARA O NOVO AMBIENTE;
7.13.1.7.2. FINALIZAÇÃO DOS TREINAMENTOS OPERACIONAIS: Em até 60 (sessenta) dias corridos após a finalização da MIGRAÇÃO PARA O NOVO AMBIENTE;

7.13.1.8. **Atividade 8: ENTREGA DA DOCUMENTAÇÃO TÉCNICA FINAL E ENCERRAMENTO DO PROJETO:** Conclusão em até 15 (Quinze) dias úteis após os TESTES DE ACEITAÇÃO, que se dará com o TERMO DE ENCERRAMENTO DO PROJETO;
7.13.1.8.1. Termos de aceitação dos testes;
7.13.1.8.2. High Level Design (HLD);
7.13.1.8.3. Apresentações;
7.13.1.8.4. Documentação detalhadas da instalação;
7.13.1.8.5. Documentação detalhada das integrações;
7.13.1.8.6. Topologia Lógica;
7.13.1.8.7. Códigos fonte das integrações e respectiva documentação para manutenção;
7.13.1.8.8. Plano de Continuidade de Negócios (PCN).
7.13.1.8.9. Plano de Recuperação de Desastres (PRD);
7.13.1.8.10. Testes e Evidências da Validação do PRD;
7.13.1.8.11. Reunião de Encerramento de projeto;
7.13.1.8.12. Entrega das Atas em material compilado;
7.13.1.8.13. Aceite da Documentação Técnica Final;
7.13.1.8.14. Termo de Encerramento de Projeto;

7.13.2. A integração e a utilização do Service Desk do CONTRATANTE devem ocorrer até o prazo máximo de 180 (cento e oitenta) dias corridos a partir do início da vigência do contrato.
7.13.3. Em até 120 (cento e vinte) dias contados a partir da entrega dos equipamentos, a CONTRATADA deve comprovar que todos os equipamentos, bem como seus números de série estão cobertos por garantia do fabricante que atenda aos requisitos deste Contrato.

7.14. LOCAL DE ENTREGA / EXECUÇÃO

7.14.1. Os locais para prestação de serviços e entrega dos equipamentos, por padrão, concentram-se em dois endereços distintos:
7.14.1.1. DATACENTER DCCJ – Rua Caldas Junior, 120, 8º andar – Centro - Porto Alegre, RS – CEP 90018-900;
7.14.1.2. DATACENTER DCZS – Rua Eng. Ludolfo Boehl, 247 – Bairro: Teresópolis – CEP: 91720-150 - Porto Alegre/RS;
7.14.1.3. Eventualmente, serviços poderão ser realizados em outras unidades do CONTRATANTE na região metropolitana de Porto Alegre.
7.14.2. O recebimento dos equipamentos e serviços contratados pelo CONTRATANTE se efetivará por meio de termo de recebimento a ser emitido por representante do CONTRATANTE envolvido no projeto de aquisição e implementação.
7.14.3. Os Treinamentos Oficiais e Operacionais terão seu local ajustado entre o CONTRATANTE e a CONTRATADA.

7.15. OBRIGAÇÕES ESPECÍFICAS DA CONTRATADA

7.15.1. A CONTRATADA é a única responsável pelas ações realizadas por seus profissionais no ambiente do CONTRATANTE;

7.15.2. A CONTRATADA responderá por qualquer ação judicial, movida por profissional, referente ao atendimento do objeto deste contrato;

7.15.3. A CONTRATANTE estará à disposição da CONTRATADA para auxiliar, no caso de ocorrência citada acima;

7.16. DA GARANTIA AO OBJETO

A CONTRATADA deverá conceder garantia do objeto de, no mínimo, 60 (sessenta) meses, contados da data da execução, considerando todas as obrigações previstas na Lei nº 8.078/1990 – Código de Defesa do Consumidor – e alterações.

7.17. PROCEDIMENTOS DE TRANSIÇÃO E ENCERRAMENTO CONTRATUAL

Um ano antes do vencimento e até a data do efetivo término do contrato, a critério do CONTRATANTE, poderá ser definida uma data para início, de forma gradual, da transferência ordenada dos serviços ao CONTRATANTE ou a seu designado e cancelamento dos serviços.

8. DA VIGÊNCIA DA CONTRATAÇÃO

A vigência da contratação será de 60 (sessenta) meses, podendo sua duração ser prorrogada, conforme disposições do Art. 71 da Lei 13.303/2016.

a. Justificativa para a definição do prazo de vigência:

Considerando a análise econômico-financeira, administrativa e técnica, devido ao anúncio de fim de suporte e fim de ciclo de vida de produto de alguns dos dispositivos existentes no atual Core de Segurança, além da necessidade de atualização e expansão do ambiente, entende-se que é necessária a renovação de todo ambiente, que deve expandir para novas funcionalidades em uma única plataforma de segurança, unificando contratos. Ao final do prazo mencionado, será efetuado novo estudo para avaliar o estado da solução adquirida e da necessidade de uma nova contratação ou apenas renovação.

9. DA POSSIBILIDADE DE RESCISÃO

Caso alguma das partes tenha interesse na rescisão contratual, esta deverá fazer a solicitação à outra parte com antecedência mínima de 120 (cento e vinte) dias.

10. CONDIÇÕES DE PAGAMENTO

10.1. Os pagamentos estão organizados em atividades que possuem tarefas que podem ser conduzidas em conjunto como forma de otimização de prazos, dentro de uma cadência lógica de execução do projeto. Dessa forma cada atividade, após concluída, representa um ou mais percentuais dos valores constantes nos itens da PLANILHA DE ORÇAMENTOS.

10.2. Em virtude de vultuosidade, da complexidade e dos riscos envolvidos nesta contratação, os pagamentos serão efetuados de forma fracionada, somente após a entrega de cada atividade vinculada ao projeto.

10.3. Para cada atividade concluída, o CONTRATANTE fornecerá o referido termo de recebimento, conforme ANEXO 03 - TERMO DE RECEBIMENTO. Para algumas entregas dentro de cada atividade, poderá ser emitido um termo de recebimento específico.

10.4. Os pagamentos ocorrerão sempre até o dia 15 (quinze) do mês subsequente à prestação dos serviços/conclusão de cada etapa conforme descrito a seguir:

10.4.1. Entrega da Atividade 1 - ABERTURA E PLANO DE PROJETO: 10% do Item 01 - “Gerenciamento do Projeto, Implementação da Solução e Treinamento Operacional” constante na Planilha de Orçamentos. Entregáveis da Etapa:

10.4.1.1. Reunião inicial do projeto;

10.4.1.2. Termo de Abertura do Projeto;

10.4.1.3. Plano de Gerenciamento de Projeto com EAP;
10.4.1.4. Plano de Projeto (Atividades do Escopo);
10.4.1.5. Cronograma;

10.4.2. Entrega da Atividade 2 - PLANEJAMENTO TÉCNICO PRELIMINAR E ENTREGA DOS EQUIPAMENTOS: 10% do Item 01 - "Gerenciamento do Projeto, Implementação da Solução e Treinamento Operacional", 50% do Item 02 - "Hardware e Software da Solução, sem incluir os valores de licenciamento definitivo" constantes na Planilha de Orçamentos. Entregáveis da Etapa:
10.4.2.1. Projeto Lógico;
10.4.2.2. Plano de Migração com detalhamento de atividades para avaliação anterior à implementação do projeto;
10.4.2.3. Entrega dos Equipamentos, mediante fornecimento do ANEXO 03 - TERMO DE RECEBIMENTO pelo CONTRATANTE mencionando Entrega dos Equipamentos;

10.4.3. Entrega da Atividade 3 – GARANTIA DE HARDWARE E SOFTWARE E TREINAMENTOS OFICIAIS: 10% do Item 01 - "Gerenciamento do Projeto, Implementação da Solução e Treinamento Operacional" e 100% do Item 05 – "Treinamentos Oficiais" constantes na Planilha de Orçamentos. Entregáveis da Etapa:
10.4.3.1. Comprovação do registro da garantia contratada junto ao fabricante;
10.4.3.2. Conclusão dos Treinamentos Oficiais, mediante fornecimento do ANEXO 03 - TERMO DE RECEBIMENTO pelo CONTRATANTE mencionando a Entrega dos Treinamentos Oficiais;

10.4.4. Entrega da Atividade 4 – IMPLEMENTAÇÃO INICIAL DO PROJETO: 10% do Item 01 - "Gerenciamento do Projeto, Implementação da Solução e Treinamento Operacional", 10% do Item 02 - "Hardware e Software da Solução, sem incluir os valores de licenciamento definitivo", 40% do Item 3 - "Licenciamento Geral" e 40% do Item 4 - "Licenciamento por Assinatura ou Subscrição". Entregáveis da Etapa:
10.4.4.1. Configurações do Novo Ambiente (antes da migração);
10.4.4.2. Ativação dos Licenciamentos;

10.4.5. Entrega da Atividade 5 – MIGRAÇÃO PARA O NOVO AMBIENTE: 10% do Item 01 - "Gerenciamento do Projeto, Implementação da Solução e Treinamento Operacional", 20% do Item 02 - "Hardware e Software da Solução, sem incluir os valores de licenciamento definitivo", 50% do Item 3 - "Licenciamento Geral" e 50% do Item 4 - "Licenciamento por Assinatura ou Subscrição". Entregáveis da Etapa:
10.4.5.1. Migração dos ambientes existentes para a nova solução;

10.4.6. Entrega da Atividade 6 – SUPORTE/MANUTENÇÃO A HARDWARE E SOFTWARE E PROFISSIONAIS DEDICADOS À OPERAÇÃO ASSISTIDA: 20% do Item 01 - "Gerenciamento do Projeto, Implementação da Solução e Treinamento Operacional" e Início dos pagamentos mensais (pagamento mensal = montante do item/número de meses contratados) referentes ao Item 6 – "Suporte, Manutenção e Operação Assistida". Entregáveis da Etapa:
10.4.6.1. Início da vigência do suporte e manutenção a hardware e software (pós migração/projeto);
10.4.6.2. Início da vigência da operação assistida por profissionais dedicados;

10.4.7. Entrega da Atividade 7 – TESTES DE ACEITAÇÃO E TREINAMENTO OPERACIONAL: 20% do Item 01 - "Gerenciamento do Projeto, Implementação da Solução e Treinamento Operacional", 10% do Item 02 - "Hardware e Software da Solução, sem incluir os valores de licenciamento definitivo", 10% do Item 3 - "Licenciamento Geral" e 10% do Item 4 - "Licenciamento por Assinatura ou Subscrição". Entregáveis da Etapa:
10.4.7.1. Validação do funcionamento dos equipamentos;
10.4.7.2. Validação das configurações, operação e licenças habilitadas;

10.4.7.3. Finalização do Treinamento Operacional
10.4.7.4. Consolidado dos Termos de Recebimento/Conclusão de Atividade de todas as entregas realizadas;

10.4.8. Entrega da Atividade 8 – ENTREGA DA DOCUMENTAÇÃO TÉCNICA FINAL E ENCERRAMENTO DO PROJETO: 10% do Item 01 - "Gerenciamento do Projeto, Implementação da Solução e Treinamento Operacional" e 10% do Item 02 - "Hardware e Software da Solução, sem incluir os valores de licenciamento definitivo". Entregáveis da Etapa:
10.4.8.1. Entrega de toda documentação final conforme especificações técnicas (Inventário de Equipamentos, Manuais, Topologias, etc);
10.4.8.2. Termo de Encerramento de Projeto.

11. DO EQUILÍBRIO ECONÔMICO-FINANCEIRO

- REAJUSTE: Após a periodicidade de um ano, o preço do presente Contrato poderá ser reajustado anualmente, pela variação do IPCA (Índice de Preços ao Consumidor Amplo), apurado pelo Instituto Brasileiro de Geografia e Estatística (IBGE).

11.1. VARIAÇÃO CAMBIAL

I. O objeto está exposto com maior intensidade à variação cambial? SIM

Todo hardware e software é importado, portanto, pode sofrer principalmente com a variação do dólar.

12. DA GARANTIA CONTRATUAL

Deverá ser apresentada garantia de 5% do valor global contratado, conforme justificativa abaixo relacionada.

12.1. Justificativa para exigência de garantia

A exigência de garantia contratual tem por finalidade assegurar indenização ao contratante no caso de prejuízos causados pelo inadimplemento do particular contratado, incluindo, ainda, valores devidos em razão da aplicação de multas e do não cumprimento de outras obrigações previstas. Com relação ao percentual, optou-se pelo padrão de 5%, considerando que o objeto não se enquadra nos casos de grande vulto envolvendo alta complexidade técnica e riscos financeiros consideráveis.

13. DAS SANÇÕES – MULTAS

PERCENTUAL	BASE DE CÁLCULO	PERÍODO DE APLICAÇÃO	OCORRÊNCIA
0,20%	Valor total atualizado do contrato	Por hora de atraso	Descumprimento de prazo para a solução de ações corretivas (Incidentes) com rede de produção ou aplicação crítica parada ou seriamente degradada (2h).
0,05%	Valor total atualizado do contrato	Por hora de atraso	Descumprimento de prazo para a solução de ações corretivas (Incidentes) com rede de produção ou aplicação operando em contingência (Standby) (6h).
0,5%	Valor mensal do contrato	Por dia de atraso	Descumprimento de prazo para a solução de ações preventivas (Requisições de Serviços) para solicitação de avaliação técnica (48h).
5%	Valor mensal do contrato	Por dia de atraso	Descumprimento de prazo para a solução de ações preventivas (Requisições de Serviços) para substituição de hardware ou software utilizado em solução de contorno por peça definitiva da solução (15 dias).

0,05%	Valor total atualizado do contrato	Por dia de atraso	Descumprimento de prazo para a apresentação de solução definitiva para procedimento de contorno realizado.
0,010%	Valor total atualizado do contrato	Por dia de atraso	Descumprimento de prazo para a realização da reunião inicial do projeto.
0,010%	Valor total atualizado do contrato	Por dia de atraso	Reincidência no descumprimento de prazo para a entrega de ATA de reunião.
0,010%	Valor total atualizado do contrato	Por dia de atraso	Descumprimento de prazo para a entrega do plano de projeto.
0,010%	Valor total atualizado do contrato	Por dia de atraso	Descumprimento de prazo para a entrega do plano lógico preliminar.
0,010%	Valor total atualizado do contrato	Por dia de atraso	Descumprimento do prazo de entrega inicial dos softwares e equipamentos.
0,010%	Valor total atualizado do contrato	Por dia de atraso	Descumprimento do prazo de finalização dos Treinamentos Oficiais.
0,010%	Valor total atualizado do contrato	Por dia de atraso	Descumprimento do prazo de finalização da migração do ambiente.
0,010%	Valor total atualizado do contrato	Por dia de atraso	Descumprimento de prazo para a entrega da documentação final do projeto.
0,010%	Valor total atualizado do contrato	Por dia de atraso	Descumprimento do prazo de finalização dos Treinamentos Operacionais.
0,1%	Valor mensal do contrato	Por hora de atraso	Atraso do profissional para operação assistida ao local de trabalho.
0,5%	Valor mensal do contrato	Por dia de ausência	Ausência do profissional para operação assistida ao local de trabalho.
3%	Valor mensal do contrato	Evento	Execução de atividades sem anuência e aceite formal do CONTRATANTE que não impliquem na indisponibilidade ou degradação de desempenho do ambiente, sendo aplicada em dobro em caso de reincidência.
10%	Valor mensal do contrato	Evento	Execução de atividades sem submissão e aceite formal do CONTRATANTE que impliquem na indisponibilidade ou degradação de desempenho do ambiente.

ANÁLISES RELACIONADAS AO OBJETO

14. TRATAMENTO DIFERENCIADO ME/EPP – LEI 123/2006

I. O valor estimado do lote é inferior a R$ 80.000,00?
- LOTE 01: NÃO

15. UTILIZAÇÃO DO SERVICE DESK

I. Será utilizada a ferramenta Service Desk como ponto de contato sistêmico, para abertura, acompanhamento e gestão de incidentes, requisições de serviço e ocorrências? SIM
II. Caso a assertiva acima seja SIM, ocorreu avaliação e parecer favorável da Unidade de Logística e Operações de TI –Tecnologia Gestao Níveis de Serviço? SIM
III. Descrever a regra: Conforme abaixo:

15.1. MÉTODO DE ATENDIMENTO

15.1.1. O CONTRATANTE utiliza a ferramenta Service Desk como ponto único de contato sistêmico, para abertura, acompanhamento e gestão de todos os Incidentes, Requisições de Serviço e Ocorrências.
15.1.2. A CONTRATADA deve utilizar obrigatoriamente o Sistema Service Desk do CONTRATANTE para o controle dos Incidentes, Requisições de Serviço e Ocorrências, independentemente da utilização de ferramenta própria para controle interno.
15.1.3. O CONTRATANTE deve prover para a CONTRATADA o acesso ao seu Sistema de Service Desk para que a mesma acesse as informações sobre o andamento dos Incidentes, Requisições de Serviço e Ocorrências registrados.
15.1.4. O acesso ao console do Sistema Service Desk do CONTRATANTE será disponibilizado para a CONTRATADA via internet. Para cada contato será gerado um login e senha de acesso pessoal.
15.1.5. A CONTRATADA deve informar imediatamente o CONTRATANTE quando houver desligamento de algum usuário da empresa cadastrado no Service Desk, para inativação de seu acesso.
15.1.6. O Sistema Service Desk do CONTRATANTE estará disponível para uso da CONTRATADA em regime de 24 horas por dia, 07 dias da semana, podendo sofrer paradas para manutenção.
15.1.7. Se algum usuário da empresa ficar 60 dias sem acessar a ferramenta, seu cadastro será automaticamente inativado e ele perderá acesso.
15.1.8. A CONTRATADA deve prever o desenvolvimento do meio de integração com o Sistema Service Desk do CONTRATANTE dentro de regras já definidas e padronizadas, caso opte por também monitorar os Incidentes, Requisições de Serviço e Ocorrências sob sua responsabilidade através de ferramenta própria.
15.1.9. No momento que um Incidente, Requisição de Serviço ou Ocorrência for registrado, o Sistema Service Desk do CONTRATANTE enviará, automaticamente, uma notificação via e-mail para a CONTRATADA, alertando que um novo ticket foi direcionado para a empresa.
15.1.10. A notificação enviada segue um modelo padrão para todas as empresas externas; não serão feitas customizações.
15.1.11. A CONTRATADA deve registrar a solução do Incidente, Requisição de Serviço ou Ocorrência no Sistema Service Desk do CONTRATANTE imediatamente após executada, descrevendo a ação efetuada para normalizar a operacionalização do objeto contratado ou atender à requisição.
15.1.12. Após a resolução do Incidente, Requisição de Serviço ou Ocorrência pela CONTRATADA, o CONTRATANTE terá um prazo de 02 (dois) dias úteis para reabrir o chamado, caso identifique que a mesma falha voltou a ocorrer ou que a requisição não foi atendida adequadamente.

15.2. MÉTODO DE CONTROLE DE SLA

15.2.1. A CONTRATANTE estabelece que o método de controle de SLA será baseado em tickets de atendimento. Os prazos de atendimento e solução, respeitado o horário de atendimento, serão contados a partir da data/hora de transferência do ticket à CONTRATADA oriundo da ferramenta de Service Desk do CONTRATANTE; até a data/hora registrada na ferramenta de Service Desk do CONTRATANTE pela CONTRATADA.
15.2.2. A cobertura dos serviços será integral, ou seja, 24 (vinte e quatro) horas por dia, nos 7 (sete) dias da semana, incluindo sábados, domingos, feriados e pontos facultativos. Caso a ferramenta Service Desk não esteja disponível ou não seja possível efetuar a abertura do ticket junto ao Service Desk, a abertura do chamado técnico ou solicitação de serviço será realizada através de chamado telefônico DDG (0800) da CONTRATADA, sendo registrado posteriormente com uso de evidências telefônicas.
15.2.3. Os tickets de atendimento obedecerão às regras de Níveis de Serviço a seguir:

TIPOS DE SOLUÇÃO	DESCRIÇÃO

Solução de Contorno	Compreende a solução dada pela CONTRATADA que permita a continuidade operacional do objeto contratado, mesmo que não sejam utilizadas peças / configurações advindas do projeto original, podendo esta solução ser também definitiva se assim for aceito formalmente pelo CONTRATANTE.
Solução de Definitiva	Compreende a solução dada pela CONTRATADA que permita a continuidade operacional do objeto contratado, restabelecendo os serviços prestados de acordo com o projeto original.

15.2.4. Os tempos das soluções serão medidos desde o registro ou transferência até a solução do ticket na ferramenta Service Desk da CONTRATANTE. Cada um dos tickets de atendimento (Incidente, Requisição ou Ocorrência) levará em consideração o cenário da Falha, Ocorrência ou Circunstância, conforme abaixo classificado:

Perfil	Cenário	Tempo máximo de reparo (H)
Ações corretivas (Incidentes)	Com parada do negócio - Rede de produção ou aplicação crítica parada ou seriamente degradada em função de falha na solução, causando impacto crítico ou significante nas operações do negócio do CONTRATANTE.	2 horas corridas
	Sem parada do negócio - Rede de produção ou aplicação operando em contingência (Standby) devido a falha em parte da solução, sem qualquer impacto crítico ou significante nas operações do negócio do CONTRATANTE.	6 horas corridas
Ações preventivas (Requisições de Serviços)	Solicitação de avaliação técnica, instalações, atualizações de hardware/software, assistência para configurações, informações gerais sobre produtos, implementação de melhoria, atualização de documentações.	48 horas corridas, podendo ser estendido a critério do contratante.
	Substituição de hardware ou software utilizado em solução de contorno por peça definitiva da solução, incluindo o devido recebimento e operacionalização.	15 dias corridos, podendo ser estendido a critério do contratante.

15.2.5. Os atendimentos, e consequentemente os respectivos prazos do Acordo de Níveis de Serviço poderão ser paralisados nas seguintes situações:
15.2.5.1. Quando a CONTRATADA depender de informações e/ou recursos, por parte da CONTRATANTE, que inviabilizem a execução do atendimento;
15.2.5.2. Quando a ocorrência depender de retorno de informações da CONTRATADA mediante concordância da CONTRATANTE;
15.2.5.3. Quando a atendimento depender de agendamento para atendimento, onde fora acordada data/hora entre CONTRATADA e CONTRATANTE.
15.2.6. A pausa e retomada ocorre através da atualização do STATUS do ticket, exceto nos casos de agendamento em que a pausa ocorre quando preenchido campo DATA DE AGENDAMENTO na ferramenta de controle da CONTRATANTE. A retomada acontece automaticamente quando atingida a data/hora agendada.
15.2.7. Os status disponíveis para uso em Incidentes e Requisições, e que contemplam as situações acima citadas são: Aguardando Fornecedor, Aguardando cliente/usuário, Agendado; Em Homologação (somente para requisições); Em atendimento, Encaminhado, Homologado (somente para requisições), Não homologado (somente para requisições) e Reaberto;
15.2.8. Pausas e retomadas de tempo de atendimento só ocorrem quando o tempo total do SLA acordado para o atendimento ainda não foi excedido.
15.2.9. É vedada a transferência do ticket, salvo para correção de encaminhamento.

15.2.10. A CONTRATADA poderá atualizar o ticket a qualquer tempo.
15.2.11. Após a resolução do ticket pela CONTRATADA, a CONTRATANTE terá um prazo de 02 (dois) dias úteis para reabrir o ticket. Essa reabertura do ticket será considerada como continuação do atendimento anterior, ou seja, a contagem do prazo de atendimento será retomada e não haverá ônus financeiro para a CONTRATANTE em decorrência de uma possível caracterização de nova demanda.

16. ANÁLISE DE RISCO DE SERVIÇOS TERCEIRIZADOS E COMPUTAÇÃO EM NUVEM

a. O objeto desta contratação se enquadra para serviços terceirizados de **qualquer natureza**? SIM
b. O objeto desta contratação é um serviço de processamento **ou** armazenamento de dados **ou** de computação em nuvem **que utiliza recursos computacionais do prestador de serviços**? NÃO

17. PROTEÇÃO DE DADOS PESSOAIS (LGPD)

O objeto desta contratação prevê o compartilhamento e/ou acesso, com a/pela CONTRATADA, dos seguintes dados:

I. Dados Pessoais? NÃO
Informação relacionada a pessoa natural identificada ou identificável.

II. Dados Pessoais Sensíveis? NÃO
Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

CONDIÇÕES DO PROCEDIMENTO

18. EXIGÊNCIA DE AMOSTRA/VERIFICAÇÃO

I. Necessidade de amostra para verificação? SIM
II. Informar quais critérios objetivos serão analisados: Os critérios a serem analisados assim como outras informações de referência estão relacionados no ANEXO 01 – ESPECIFICAÇÃO DOS TESTES DE BANCADA constante neste edital.
III. Necessidade de assinatura de Termo de Sigilo? SIM
IV. Quantitativo da amostra pode fazer parte do objeto a ser entregue? SIM, desde que atendam todas as exigências do edital e mediante verificação da equipe do CONTRATANTE para atestar que os equipamentos são novos, sem qualquer tipo de uso e que estão em perfeito estado.
V. Regras para amostra/verificação:

18.1. Justificativa para exigência de amostra/verificação: A finalidade da amostra é permitir que a Administração, no julgamento da proposta, possa se certificar de que o bem proposto pelo CONTRATADA atende a todas as condições e especificações técnicas indicadas na sua descrição, tal como constante no edital. Com a verificação, pretende-se reduzir riscos e possibilitar a quem julga a certeza de que o objeto proposto atenderá à necessidade da Administração.

18.2. Realização dos Testes de Bancada:

18.2.1. Solicitação da Amostra: Após a declaração pelo agente de licitação, a CONTRATADA provisoriamente classificada em primeiro lugar deverá submeter-se a um processo de testes de bancada que validará as premissas da solução ofertada, para o qual deve disponibilizar o ambiente de testes para amostra e verificação em até 20 (vinte) dias úteis e, uma vez disponibilizado, deve realizar as validações por até 15 (quinze) dias úteis subsequentes, conforme definições no ANEXO 02 - TERMO DE COMPROMISSO DE HOMOLOGAÇÃO, que será formalizado previamente. O processo de amostra e verificação só se iniciará após a devida assinatura do referido termo.

18.2.2. Recepção da amostra: A entrega da amostra consiste em disponibilizar um ambiente pronto para a execução dos testes de bancada, processo para o qual a CONTRATADA poderá disponibilizar o ambiente, total ou parcialmente, em laboratório oficial do fabricante ou localmente na área de testes do Data Center do CONTRATANTE podendo fazer o uso de ambas as modalidades conforme a necessidade dos requisitos a serem validados, desde que cumpridos os prazos estipulados. Para o caso de fornecimento de equipamentos para validação local no Data Center do CONTRATANTE, estes devem ser entregues na Unidade de Arquitetura Computacional do CONTRATANTE em dois possíveis endereços: Rua Eng. Ludolfo Boehl, 247 – Bairro: Teresópolis – CEP: 91720-150 e Rua Caldas Junior, 120, 8º andar – Bairro: Centro – CEP 90018-900 – em Porto Alegre/RS, de segunda-feira à sexta-feira, das 09h45min às 16h00min em até 20 (vinte) dias úteis a contar da assimatura do ANEXO 02 - TERMO DE COMPROMISSO DE HOMOLOGAÇÃO. O não cumprimento do prazo para envio da amostra acarretará

na recusa da proposta da CONTRATADA provisoriamente classificada em primeiro lugar para o item. Não caberá a CONTRATADA ressarcimento do valor da amostra ou custo qualquer de apresentação da mesma. A CONTRATADA provisoriamente classificada em primeiro lugar arcará com todos os custos decorrentes da apresentação das amostras solicitadas e apresentadas, independentemente da condução ou resultado do processo.

18.2.3. Análise da amostra: A homologação da amostra consiste na execução de testes específicos e geração de evidências conforme critérios e referências relacionados no ANEXO 01 – ESPECIFICAÇÃO DOS TESTES DE BANCADA constante neste edital. A amostra será submetida à avaliação e o resultado será divulgado à CONTRATADA provisoriamente classificada em primeiro lugar em um prazo máximo de 35 (trinta e cinco) dias úteis a contar da recepção da amostra pelo CONTRATANTE. As amostras serão avaliadas mediante a realização de observações e/ou testes, quando for o caso, visando à comprovação da qualidade do produto quanto à correspondência entre a amostra e a especificação constante do Edital (medidas, quantidades, atendimento da finalidade), objetivando verificar a compatibilidade entre a especificação técnica e o material cotado.

18.2.4. Divulgação da análise: A aceitação da amostra é condição para adjudicação ou desclassificação do objeto do certame. Caso o objeto não seja aprovado mediante as condições pré-estabelecidas no procedimento de testes, a CONTRATADA provisoriamente classificada em primeiro lugar é desclassificada e a próxima é convocada, na ordem de classificação. Após a avaliação das amostras, o CONTRATANTE divulga seu parecer técnico de conclusão da avaliação do item, que passou por todos os testes necessários, informando o aceite definitivo ou a recusa. Este parecer permanecerá nos autos e poderá ser objeto de pedido de vistas. Caso o material não seja aprovado, a CONTRATADA provisoriamente classificada em primeiro lugar será informada sobre os motivos que levaram à reprovação do objeto e será imediatamente desclassificada. A CONTRATADA provisoriamente classificada em primeiro lugar será desclassificada quando ocorrer inconformidade do(s) material(is) entregue(s) com as especificações mínimas contidas no edital.

18.2.5. Devolução da amostra: A amostra será disponibilizada para retirada pela CONTRATADA provisoriamente classificada em primeiro lugar em até 15 (quinze) dias úteis a contar da divulgação das análises, sob pena de lhe ser dada outra destinação, a critério do Contratante.

18.2.6. Caso haja a intenção de utilizar os equipamentos da fase de homologação para composição da solução definitiva, a equipe do CONTRATANTE deverá atestar que os equipamentos são novos, sem qualquer tipo de uso e que estão em perfeito estado.

19. POSSIBILIDADE DE SUBCONTRATAÇÃO

Será permitida a subcontratação no que se refere à prestação de serviços de Operação Assistida e Treinamentos Oficiais.

19.1. Justificativa e regramento, caso seja permitido:

O mercado de prestação de serviços de Tecnologia da Informação trabalha constantemente com a contratação de pessoa jurídica para atendimento a demandas especializadas, sendo este um requisito básico de economicidade, visto que poderá haver aumento de custos e dificuldade na contratação destes profissionais se exigido vínculo empregatício com a CONTRATADA.

Será permitida subcontratação para os serviços de suporte com profissional para operação assistida e para os Treinamentos Oficiais do fabricante.

A subcontratação será permitida somente para a prestação dos serviços mencionados nesta cláusula, limitando-se ao valor máximo de 30% do valor total contratual para o somatório desses serviços.

As empresas subcontratadas devem ser especificadas e identificadas durante o processo licitatório e ao longo da vigência contratual, caso haja mudança.

20. POSSIBILIDADE DE PARTICIPAÇÃO EM CONSÓRCIO

Não será permitida a participação de empresas em consórcio.

21. DA QUALIFICAÇÃO TÉCNICA

As empresas participantes do processo deverão apresentar as seguintes comprovações quanto ao objeto licitado:

21.1. DOCUMENTAÇÃO TÉCNICA DA CONTRATADA

21.1.1. A CONTRATADA deve apresentar documentação que comprove relação de parceria com o fabricante da solução ofertada, atestando, portanto, o conhecimento sobre equipamentos e produtos ofertados bem como aptidão para a comercialização destes;
21.1.2. A CONTRATADA deve apresentar ATESTADOS DE CAPACIDADE TÉCNICA emitidos por pessoa jurídica de direito público ou privado que comprove sua aptidão para desempenho de atividades de implementação e suporte técnico de soluções de segurança de redes de modo que os atestados:
21.1.2.1. Comprovem, em seu somatório, tomando como base quantitativa apenas os equipamentos de firewall (de modo a haver o mesmo critério de comparação com soluções anteriores implementadas no mercado, sem incluir portanto equipamentos de *spare parts*, orquestradores ou outro tipo de equipamentos), a atuação no mercado com o mesmo fabricante ofertado no período dos últimos 02 (dois) anos havendo implementado pelo menos 50% (cinquenta por cento) da quantidade de ativos ofertados para o CENÁRIO A – CORE DE SEGURANÇA no presente objeto ou, com o mesmo ou outro fabricante de soluções de segurança de redes no período dos últimos 05 (cinco) anos havendo implementado pelo menos 80% (oitenta por cento) da quantidade de ativos ofertados para o CENÁRIO A – CORE DE SEGURANÇA no presente objeto, desde que, os equipamentos implementados no mercado correspondam, em termos de desempenho, a pelo menos 25% (vinte e cinco por cento) da capacidade dos equipamentos ofertados, considerando como referência os parâmetros de *NGFW Throughput, Threat Prevention Throughput* e *TLS Inspection Throughput;*
21.1.2.2. Evidenciem explicitamente a execução de objeto compatível ao objeto da presente proposta - contendo descrição adequada, clara e suficiente do(s) serviço(s) executado(s) ou em execução;
21.1.2.3. Contenham a identificação do(s) contrato(s) vinculado(s) e do(s) período(s) a que se referem os serviços executados, podendo considerar contratos já executados ou em execução;
21.1.2.4. Façam referência a serviços prestados no âmbito da atividade econômica principal ou secundária especificada no contrato social vigente do CONTRATADA;
21.1.2.5. Contenham a correta identificação do emissor e sejam emitidos sem rasuras, acréscimos ou entrelinhas;
21.1.3. No caso de atestados emitidos por empresas privadas, não serão admitidos aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da empresa CONTRATADA. São consideradas como pertencentes ao mesmo grupo empresarial as empresas controladas ou controladoras da CONTRATADA, ou que tenha pelo menos uma mesma pessoa física ou jurídica que seja sócia ou possua vínculo com a empresa emitente;
21.1.4. Com relação a capacidade operacional, a CONTRATADA deve fornecer atestados de capacidade técnica, conforme previsto no Regulamento de Licitações e Contratos do Banrisul (vide site www.banrisul.com.br), que, em seu somatório, comprovem experiência na execução de objetos de TIC (Tecnologia da Informação e Comunicação) com quantitativos de pelo menos 50% (cinquenta por cento) do objeto licitado no que se refere a valores;

21.2. DOCUMENTAÇÃO TÉCNICA DOS PROFISSIONAIS DA CONTRATADA

21.2.1. Serão exigidos perfis de profissionais durante toda vigência contratual. Para tanto, algumas das exigências devem ser comprovadas ainda em edital mediante apresentação de certificado oficial emitido pelo fabricante e/ou experiência comprovada, para os seguintes perfis já especificados neste edital:

21.2.1.1. A CONTRATADA deve apresentar documento comprovando certificação de, no mínimo, 01 (um) profissional com perfil do tipo EXPERT para SEGURANÇA;
21.2.1.2. A CONTRATADA deve apresentar documento comprovando certificação de, no mínimo, 02 (dois) profissionais com perfil do tipo PROFISSIONAL DE SEGURANÇA;

21.2.1.3. A CONTRATADA deve apresentar documento comprovando certificação de, no mínimo, 01 (um) profissional com perfil do tipo GERENTE DE PROJETOS;

21.3. COMPROVAÇÕES DE EXPERIÊNCIA:
A CONTRATADA deve apresentar as seguintes comprovações:

21.3.1. Para o Perfil EXPERT para SEGURANÇA:
21.3.1.1. Certificação Oficial do fabricante;
21.3.1.2. Carta de Experiência – comprovando participação em atividades de implementação (planejamento, instalação, configuração, adequação, execução, avaliação e monitoramento da migração) de equipamentos similares aos ofertados, tempo de experiência e todos os demais requisitos especificados na descrição do item "EXPERT DE SEGURANÇA", neste documento.

21.3.2. Para o Perfil PROFISSIONAL DE SEGURANÇA:
21.3.2.1. Certificação Oficial do fabricante;
21.3.2.2. Carta de Experiência – comprovando participação em atividades de implementação (planejamento, instalação, configuração, adequação, execução, avaliação e monitoramento da migração) de equipamentos similares aos ofertados, tempo de experiência e todos os demais requisitos especificados na descrição do item "PROFISSIONAL DE SEGURANÇA", neste documento.

21.3.3. Para o Perfil GERENCIAMENTO DE PROJETOS:
21.3.3.1. Certificado de conclusão de curso de formação em Gerenciamento de Projetos (360 horas) ou Certificação PMP;
21.3.3.2. Carta de Experiência – enumerando e comprovando a condução de projetos nos quais o profissional atuou (360 horas), tempo de experiência e todos os demais requisitos especificados na descrição do item "GERENTE DE PROJETO", neste documento;

DEMAIS INFORMAÇÕES

IDENTIFICAÇÃO DE CONTRATAÇÃO ANTERIOR:

I. Existiu contratação anterior com o mesmo objeto? SIM
II. Caso a assertiva acima seja SIM, informar: Parcialmente similar 0100007/2018

ASSINATURAS, LOCAL E DATA

Porto Alegre, 12 de janeiro de 2026

Arthur Trocesski Analista de TI Arquitetura TI de Rede Corporativa	ARTHUR SCHOLZ TROCESSKI:99853850044 Assinado de forma digital por ARTHUR SCHOLZ TROCESSKI:99853850044 Dados: 2026.02.20 12:17:26 -03'00'

Rafael Borba Gerente Executivo Gerência de Suporte à Plataforma Centralizada	RAFAEL BORBA MIRANDA:02097372040 Assinado de forma digital por RAFAEL BORBA MIRANDA:02097372040 Dados: 2026.02.20 13:20:54 -03'00'

CONTRATO DE AQUISIÇÃO DE SOLUÇÃO DE ESTRUTURA DE SEGURANÇA DE REDES E COMUNICAÇÕES DE MALHA HÍBRIDA, COMPOSTA POR HARDWARE, SOFTWARE E DEMAIS SERVIÇOS – Nº 0100037/2026

O CONTRATANTE, BANCO DO ESTADO DO RIO GRANDE DO SUL S.A., sociedade de economia mista, com sede na Rua Capitão Montanha, nº 177, Bairro Centro – CEP 90.010-040, em Porto Alegre/RS, inscrito no Cadastro Nacional de Pessoa Jurídica sob nº 92.702.067/0001-96, por seu representante legal no fim assinado,
e
A CONTRATADA, XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX, com sede na Rua XXXXXXXXXX, nº XXXX – Bairro XXXXXXXXX – CEP: XXXXXX – em XXXXXXXXX/XX, inscrita no CNPJ sob nº XXXXXXXXXXXXXXXXXX, por seu representante legal no fim assinado, têm como certo e ajustado o que adiante segue.

O presente Contrato tem seu respectivo fundamento e finalidade na consecução do objeto contratado, descrito abaixo, constante do Edital de Licitação nº 0000037/2026, regendo-se pela Lei Federal nº 13.303, de 30 de junho de 2016 e legislação pertinente, sujeitando-se às disposições da Lei Estadual nº 11.389, de 25 de novembro de 1999, pelos termos da proposta e pelas cláusulas a seguir expressas, definidoras dos direitos, obrigações e responsabilidades das partes.

CLAUSULA PRIMEIRA – DO OBJETO –

1.1. O objeto do presente contrato é a aquisição de Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida, composta por hardware, software e demais serviços.
1.2. Ficam fazendo parte do presente Contrato, para todos os fins e efeitos de direito, como se aqui estivessem transcritos, as Planilhas e Anexos integrantes do Edital de Licitação nº 0000037/2026.

CLÁUSULA SEGUNDA – DA EXECUÇÃO –

2.1. Especificações do Objeto:
2.1.1. Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida, composta por hardware, software licenças, garantia, serviços de implementação da solução, suporte de hardware, suporte técnico e manutenção, operação assistida, e treinamentos;
2.1.2. O objeto é formado pelo(s) seguinte(s) iten(s):

LOTE	ITEM	DESCRIÇÃO
1	01	Gerenciamento do Projeto, Implementação da Solução e Treinamento Operacional
	02	Hardware e Software da Solução, sem incluir os valores de licenciamento definitivo
	03	Licenciamento Geral
	04	Licenciamento por Assinatura ou Subscrição
	05	Treinamentos Oficiais
	06	Suporte, Manutenção e Operação Assistida

2.1.3. As características do objeto são:
2.1.3.1. O objeto tem como principais premissas o provimento da segurança do ambiente de Core de Rede (Data Center), a atualização tecnológica gradual dos ambientes de segurança de redes e comunicações do CONTRATANTE (Rede Corporativa, Rede de Agências, Ambiente de Internet, VPN, Parceiros, seus serviços e funcionalidades), a visibilidade padronizada dos incidentes de segurança nas linhas de controle e monitoração, a integração da estrutura de segurança com as demais soluções de rede e comunicações (Cisco ACI, Aruba ClearPass, VMware, entre outros ambientes) e a iniciação do uso de Inteligência Artificial para apoio à atividades como configurações, diagnósticos, relatórios, troubleshooting, auditoria, compliance, manutenção corretiva e medidas protetivas através da aquisição de uma Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida, composta por hardware, software, licenças, garantia, serviços de implementação da solução, suporte de hardware, suporte técnico com acordo de nível de serviço (SLA) definido, operação assistida, manutenção dos equipamentos e treinamentos.

2.1.3.2. Esta solução deve permitir, em um universo de dois sites físicos de Data Center, que um equipamento ou conjunto de equipamentos possa assumir as operações de seus pares em caso de falha de algum nodo principal ou até mesmo assumir completamente a operação para garantir a continuidade do negócio com o nível adequado de segurança e disponibilidade, respeitando níveis de redundância equivalentes a um Data Center padrão Tier 4, considerando nível 2N+1, ou seja, dois conjuntos idênticos de equipamentos redundantes (por site físico) mais um componente extra de spare part para maior resiliência (equipamento para atendimento dos níveis críticos de SLA em caso de RMA).

2.1.3.3. A solução deve contemplar a entrega dos produtos especificados bem como serviços especializados de implementação e gerenciamento de projeto, treinamentos, profissionais dedicados para operação assistida, testes de aceitação, suporte técnico e manutenção, conforme o cronograma de entregas descrito neste edital e em conformidade com a Planilha de Especificações Técnicas.

2.2. DETALHAMENTO DA FORMA DE EXECUÇÃO

2.2.1. REQUISITOS GERAIS

2.2.1.1. Serão exigidos perfis de profissionais durante a vigência do contrato, as exigências devem ser comprovadas mediante apresentação do certificado oficial emitido pelo fabricante, e experiência comprovada na instalação e configuração de equipamentos similares aos ofertados pela CONTRATADA, incluindo planejamento, adequação, execução, avaliação, mitigação e monitoramento da migração, os perfis e seus requisitos são:

2.2.1.2. A CONTRATADA disponibilizará pelo menos 2 (dois) profissionais que atendam aos requisitos de nível PROFISSIONAL DE SEGURANÇA para atuar na operação assistida de forma dedicada junto ao CONTRATANTE.

2.2.2. PROFISSIONAL DE SEGURANÇA

2.2.2.1. Planejar a manutenção regular da solução, suportar a resolução de problemas utilizando processos baseados na tecnologia e suas melhores práticas bem como as funcionalidades exigidas na planilha de especificações técnicas;

2.2.2.2. Possuir certificação do fabricante para o nível de ADMINISTRADOR / PROFISSIONAL DE SEGURANÇA DE REDES, ou nível técnico administrador equivalente;

2.2.2.3. Possuir pelo menos 2 (dois) anos de experiência prática no planejamento, adequação, execução, avaliação, mitigação e monitoramento de soluções de segurança de rede;

2.2.2.4. Ser capaz de definir e efetuar atualizações de software da solução, obter e instalar licenças, aplicar certificados/assinaturas digitais na solução de segurança;

2.2.2.5. Implementar acesso de gerência aos dispositivos via interface de linha de comando e/ou interface gráfica utilizando SSHv2, SSHv3, HTTPS, conforme as boas práticas de instalação, configuração e operação do fabricante;

2.2.2.6. Implementar serviços de gerenciamento como Simple Network Management Protocol versão dois e três (SNMPv2 e SNMPv3), criando visualizações, usuários, autenticação e encriptação;

2.2.2.7. Implementar e diagnosticar funcionalidades e protocolos de Autenticação, Autorização e Auditoria (AAA), RADIUS, LDAP e características de acesso baseado em perfis e Identidade;

2.2.2.8. Implementar NTP (Network Time Protocol);

2.2.2.9. Implementar e diagnosticar a exportação de SFLOW e SYSLOG;

2.2.2.10. Definir, Implementar e diagnosticar ACLs IPv4/IPv6, grupo de objetos, filtro de tráfego, filtro de aplicações, inspeção de protocolos, reações a eventos de rede, políticas de prevenção de intrusões;

2.2.2.11. Identificar e mitigar ameaças comuns diagnosticando também a origem, destino e os métodos das tentativas de ataques;

2.2.2.12. Implementar e diagnosticar funcionalidades de inspeção de telefonia celular;

2.2.2.13. Implementar, diagnosticar e analisar métodos de captura e redirecionamento de tráfego, regras de inspeção e controle, detecção de anomalias, ações de resposta e inspeção baseadas em reputação;

2.2.2.14. Implementar configurações, dimensionamento e otimização de inspeção para tráfego criptografado;
2.2.2.15. Implementar rotinas de API REST para funcionalidades de integração, automação, entre outros recursos;
2.2.2.16. Realizar a integração da solução ofertada com soluções de terceiros;

2.2.3. EXPERT DE SEGURANÇA
2.2.3.1. Deve possuir todos as características referenciadas no perfil PROFISSIONAL DE SEGURANÇA;
2.2.3.2. Possuir todas as características exigidas e conhecimentos aprofundados nos equipamentos/soluções de segurança de rede ofertados, comprovadas de forma prática através de exame prático (hands-on lab) e certificação do fabricante de NÍVEL MÁXIMO EM SEGURANÇA DE REDES;
2.2.3.3. Possuir pelo menos 3 (três) anos de experiência prática no planejamento, adequação, execução, avaliação, mitigação e monitoramento de soluções de segurança de rede;
2.2.3.4. Deve possuir conhecimento sobre os conceitos de segurança, tanto para redes IPv4 como para redes IPv6, assim como Dual-Stack, e suas aplicabilidades nos equipamentos da solução adotada;
2.2.3.5. Deve ser capaz de efetuar a implementação, configuração e verificação de serviços da Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida, de acordo com as boas práticas de instalação, configuração e operação do fabricante;
2.2.3.6. Implementar e diagnosticar serviços para visitantes (Guest Services), funcionalidades de BYOD (Bring Your Own Device), identificação transparente de usuários e customização de portais WEB;
2.2.3.7. Implementar e diagnosticar funcionalidades que forneçam maior segurança à camada de enlace (DHCP Snooping, Inspeção dinâmica de ARP, Storm Control, Port Security, MACsec) mitigando ataques de Spanning Tree, DHCP (Dynamic Host Configuration Protocol) rogue, VLAN hopping, MAC e ARP;
2.2.3.8. Implementar e diagnosticar funcionalidades de controle de uso e segurança WEB, filtros e redirecionamento de URLs, filtro de arquivos e políticas de decriptação;
2.2.3.9. Implementar, configurar e diagnosticar serviços de 802.1X em redes cabeadas e sem fio;
2.2.3.10. Implementar, configurar e diagnosticar serviços de VPN (OpenVPN, L2TP/IPsec, IKEv2/IPsec, WireGuard, SSL/TLS);
2.2.3.11. Configurar e realizar a manutenção de traduções de endereços de rede (NAT estático, NAT dinâmico, PAT, Policy NAT);
2.2.3.12. Configurar, diagnosticar e operacionalizar VPNs (Site-to-Site e Remote Access), aplicando técnicas como: Diffie-Hellman, IPsec – ESP, AH, IKEv2, Tunnel mode, Transport mode, Hairpinning, Split Tunneling, Always-on, NAT Traversal, SSL VPN Clientless;
2.2.3.13. Definir e implementar a arquitetura da solução de segurança nos modos "inline", "promiscuous" e "one armed / leg";
2.2.3.14. Definir e implementar a solução de segurança nos modos transparente e roteado, com características de Alta Disponibilidade, FailOver e Zoneamento de Segurança;
2.2.3.15. Implementar características de segmentação lógica do processamento de firewalls, criando instâncias distintas;
2.2.3.16. Definir e implementar políticas de segurança de e-mail (encriptação, anti-spam, inspeção de vírus, rastreamento de tráfego de mensagens, prevenção de perda de dados e Anti-malware);
2.2.3.17. Efetuar diagnóstico e resolução de problemas em configurações avançadas de firewall;
2.2.3.18. *NOTA: O nível Expert de Segurança é o nível mais alto de consulta técnica nesta instância. Este é o profissional que tratará diretamente com problemas relacionados à serviços de missão crítica ligados diretamente ao Core de Rede, e para tanto, a equipe técnica da CONTRATANTE entende que este deve ser um profissional experiente, que já tenha tido a vivência prática nesse tipo de ambiente, conforme os quesitos referenciados para tal atividade.*

2.2.4. GERENTE DE PROJETOS
2.2.4.1. Conhecimentos em melhores práticas do PMI;
2.2.4.2. Carga horária mínima de 360 (Trezentos e sessenta) horas em formação em gerência de projetos (Pós-Graduação/MBA Lato Sensu reconhecido pelo MEC) **ou** certificação PMP (PMI);
2.2.4.3. Experiência mínima de 360 (Trezentos e sessenta) horas em gerência de projetos;
2.2.4.4. Experiência comprovada na área de design de soluções de rede para atuar na integração de todo o projeto.
2.2.4.5. A CONTRATADA disponibilizará ao CONTRATANTE um profissional para gerenciar este projeto com o perfil de GERENTE DE PROJETOS.
2.2.4.6. O Gerente de Projetos deve possuir disponibilidade integral, ou seja, permanecer dedicado ao objeto e estar presente no local onde estiver sendo implementado o projeto, sempre que necessário durante todo o andamento das atividades do projeto, desde a assinatura do CONTRATO até a aceitação final (assinatura do Termo de Aceitação Definitiva).
2.2.4.7. O Gerente de Projetos será o ponto de contato com a equipe do CONTRATANTE. Estão inclusas nas responsabilidades:
2.2.4.8. Estabelecer objetivos claros para o projeto;
2.2.4.9. Monitorar e controlar as atividades de planejamento, prazo e escopo;
2.2.4.10. Integração da equipe e iniciativas necessárias para execução do trabalho definido;
2.2.4.11. Reportar diariamente ao CONTRATANTE sobre o status do projeto, andamento das atividades e cumprimento dos prazos;
2.2.4.12. Comunicação e gerenciamento das expectativas das equipes envolvidas no projeto;
2.2.4.13. Realizar o controle de mudanças;
2.2.4.14. Realizar reuniões semanais de alinhamento;

2.3. HARDWARE E SOFTWARE
2.3.1. A CONTRATADA deve fornecer uma solução completa de hardware, software, licenças e todos os serviços necessários para planejar, desenhar, configurar e suportar uma Estrutura de Segurança de Redes e Comunicações de Malha Híbrida capaz de prover segurança e atualização tecnológica gradual aos ambientes do CONTRATANTE;
2.3.2. Caso, no momento da assinatura do contrato, algum componente da solução esteja em alguma lista de descontinuidade (como "End of Life", "End of Support", "End of Sale" ou qualquer outra que acarrete o fim da prestação do suporte pelo fabricante), prevista para ocorrer em alguma data dentro do período de vigência do contrato, este componente deverá ser substituído pela CONTRATATADA, sem qualquer ônus para o CONTRATANTE, logo após a assinatura do contrato. A CONTRATADA terá um prazo de 90 dias corridos para a entrega dos componentes e 15 dias úteis para a instalação e configuração dos componentes que se enquadrarem nesta situação, contados a partir da assinatura do contrato. A instalação deverá ocorrer em dia e horário determinados pelo CONTRATANTE.
2.3.3. A CONTRATADA deve cumprir as especificações de hardware e software bem como demais questões técnicas referentes à estrutura a ser adquirida conforme descrito na PLANILHA DE ESPECIFICAÇÕES TÉCNICAS.

2.4. TESTES DE BANCADA
2.4.1. A CONTRATADA deve realizar testes de bancada conforme especificações constantes no ANEXO 01 – ESPECIFICAÇÃO DOS TESTES DE BANCADA deste edital;

2.5. GESTÃO DO PROJETO
A CONTRATADA deve cumprir com, no mínimo, as seguintes entregas, não excluindo os serviços previamente mencionados:
2.5.1. Gerenciamento do Projeto:
2.5.1.1. Reunião de início do projeto com todo o time envolvido;
2.5.1.2. Reuniões semanais de atualização;
2.5.1.3. Testes de Bancada;
2.5.1.4. Entregas periódicas conforme cronograma;

2.5.1.5. Status Reports Periódicos.
2.5.1.6. Atas;
2.5.1.7. Reunião de encerramento do Projeto;
2.5.1.8. Termos de Abertura e Encerramento do Projeto.
2.5.2. Plano de Gerenciamento do Projeto (EAP - Estrutura Analítica do Projeto);
2.5.3. Plano de Projeto;
2.5.4. Cronograma.
2.5.5. Entrega dos Equipamentos;
2.5.6. Garantia de Hardware e Software;
2.5.7. Projeto Lógico e Plano de Migração;
2.5.8. Treinamentos Oficiais;
2.5.9. Implementação do Projeto;
2.5.10. Licenciamento;
2.5.11. Migração para o Novo Ambiente;
2.5.12. Acompanhamento da Migração.
2.5.13. Testes de Aceitação;
2.5.13.1. Termos de entrega e aceites.
2.5.14. Documentação Final do Projeto:
2.5.15. *High Level Design* (HLD);
2.5.15.1. Apresentações;
2.5.15.2. Documentação detalhadas da instalação.
2.5.15.3. Documentação detalhada das integrações.
2.5.15.4. Topologia Lógica.
2.5.15.5. Códigos fonte das integrações e respectiva documentação para manutenção.
2.5.15.6. Plano de Continuidade de Negócios (PCN).
2.5.15.7. Plano de Recuperação de Desastres (PRD);
2.5.15.8. Testes e Evidências da Validação do PRD;
2.5.15.9. *Health Check* da Solução implementada;
2.5.16. Treinamentos Operacionais;
2.5.17. Início da vigência do suporte e manutenção a hardware e software;
2.5.18. Profissionais Dedicados para Operação Assistida;
2.5.19. Termo de Aceitação Definitiva emitido pela CONTRATANTE;

2.6. PLANO DE PROJETO

2.6.1. A implementação da solução deve ser conduzida em formato de projeto para o qual a CONTRATADA executará e realizará todos os serviços pertinentes ao objeto desta especificação, obedecendo aos prazos estabelecidos, atuando em estrita concordância e obediência ao discriminado.
2.6.2. A CONTRATADA será responsável pela elaboração de um PLANO DE PROJETO que deve ser conduzido e validado juntamente à equipe do CONTRATANTE, balizando a fase de implementação da solução com entregas documentadas, delimitadas e previstas em uma linha de tempo, buscando minimizar os riscos e impactos junto ao ambiente do CONTRATANTE.
2.6.3. A CONTRATADA realizará reunião inicial de alinhamento do projeto, envolvendo sua equipe participante do projeto e a equipe do CONTRATANTE para o detalhamento das atividades que compõem o projeto. Entende-se como:
2.6.3.1. Implantação: o recebimento de todos os equipamentos nas localidades, conferência física dos itens, instalação física de hardware e software adquiridos, energização e ativação dos equipamentos adquiridos pelo CONTRATANTE com as configurações previamente planejadas pelas equipes e seguindo o cronograma do projeto. Tais atividades não envolverão mudanças no ambiente que possam gerar riscos ou impacto ao ambiente em produção do CONTRATANTE.
2.6.3.2. Migração: a transferência das funcionalidades do ambiente atual, dentro do escopo da segurança de redes e comunicações, para o ambiente adquirido e implantado através da Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida. Estas atividades devem ser executadas prevendo o menor impacto e risco possíveis aos negócios do CONTRATANTE.

2.6.4. O PLANO DE PROJETO compreenderá todas as atividades individuais e suas durações, sendo o Gerente de Projetos responsável por detalhar tal plano, levando-se em conta as diferentes tecnologias que precisam ser implementadas.
2.6.5. O PLANO DE PROJETO deve respeitar as boas práticas em gerenciamento de projetos e deve apresentar, no mínimo, uma análise preliminar de escopo após o alinhamento das expectativas das partes interessadas, especificação dos recursos necessários, definição dos pré-requisitos do projeto, restrições de tempo definidas em conjunto e deve apresentar, em anexo, o detalhamento técnico da solução (incluindo o entendimento do ambiente atualmente em produção).
2.6.6. Após o detalhamento do plano de projeto, a CONTRATADA deve elaborar juntamente com o CONTRATANTE o cronograma de implementação com as atividades necessárias, seus pré-requisitos e o mapeamento das responsabilidades entre as equipes.
2.6.7. A CONTRATANTE participará ativamente, em conjunto com a CONTRATADA, da etapa de planejamento para os passos da migração e da própria migração de todo o ambiente, inclusive os serviços afetados.

2.7. PROJETO LÓGICO

2.7.1. A CONTRATADA é responsável pela elaboração de um documento de Projeto Lógico Preliminar, a ser entregue de forma digital ao CONTRATANTE, contendo o planejamento técnico, desenho da nova arquitetura e o plano de migração.
2.7.2. O Projeto Lógico Preliminar deve ser detalhado, contemplando informações completas sobre a solução, contendo no mínimo:
2.7.2.1. Especificação geral de todos os equipamentos que fazem parte da solução;
2.7.2.2. Descrição geral da arquitetura da solução;
2.7.2.3. Descrição do comportamento normal esperado da solução;
2.7.2.4. Topologia de rede física e lógica, de forma detalhada;
2.7.2.5. Diagrama de interconexão, descrevendo as regras e protocolos utilizados;
2.7.2.6. Manual de configuração, operação e manutenção de todos os itens da solução;
2.7.2.7. Estratégia de migração da solução atual para a nova solução, mencionando o funcionamento atual e pretendido após a mudança.
2.7.3. A CONTRATADA disponibilizará um profissional na função de líder técnico em SEGURANÇA para atuar no levantamento das configurações dos equipamentos atuais, planejamento das configurações, plano de migração e planejamento das atividades. O profissional "líder técnico em SEGURANÇA" deve possuir requisitos de nível EXPERT DE SEGURANÇA.
2.7.4. A atividade citada no item 2.7.3. poderá ser desempenhada pelo mesmo profissional EXPERT DE SEGURANÇA já mencionado anteriormente.
2.7.5. O Líder Técnico designado deve possuir disponibilidade integral, ou seja, permanecer dedicado ao objeto deste Contrato e estar presente no local onde estiver sendo implementado o projeto, sempre que necessário e durante todo o andamento das atividades do projeto, desde início da vigência contratual até a assinatura do ANEXO 04 - TERMO DE ACEITAÇÃO DEFINITIVA.
2.7.6. A CONTRATADA disponibilizará também um segundo profissional com o mesmo perfil do Líder Técnico para acompanhar o projeto de forma passiva. Tal profissional deverá assumir todas as responsabilidades e atividades do Líder Técnico durante sua ausência, seja ela programada ou não prevista.
2.7.7. Os profissionais designados para o projeto poderão efetuar suas atividades de forma remota sempre que houver concordância formal do CONTRATANTE. A composição da escala de trabalho presencial e remota será definida pelo CONTRATANTE durante o andamento do projeto e poderá sofrer alterações com base nas necessidades do mesmo.
2.7.8. O CONTRATANTE deve possuir acesso/comunicação direta com os profissionais certificados a serem designados para este processo. Para tanto devem ser fornecidos os dados de contato dos mesmos. O CONTRATANTE poderá solicitar à CONTRATADA a qualquer momento da vigência contratual a revalidação das certificações exigidas.
2.7.9. Na etapa de planejamento, a CONTRATADA será responsável pelo entendimento do ambiente em produção do CONTRATANTE, para que sejam detalhados os passos necessários

para a migração do ambiente. O entendimento do ambiente atual deve envolver todos os itens informados pela equipe técnica do CONTRATANTE no PLANO DE PROJETO.
2.7.10. Todas as informações referentes aos ambientes existentes envolvidos neste processo serão repassadas pelo corpo técnico do CONTRATANTE à CONTRATADA.
2.7.11. Será responsabilidade do CONTRATANTE, disponibilizar acesso às configurações dos equipamentos, bem como documentações existentes de topologia.
2.7.12. O CONTRATANTE possui em seu ambiente soluções de outros fabricantes (Cisco, VMWare, Redhat, Aruba, Fortinet, entre outros). Sempre que solicitado pelo CONTRATANTE, a solução deve prever a integração com outras soluções do CONTRATANTE.
2.7.13. A CONTRATADA será responsável pelo entendimento das necessidades técnicas do CONTRATANTE, a fim de customizar a configuração dos equipamentos de forma a obter a melhor performance, disponibilidade e segurança do ambiente.
2.7.14. A CONTRATADA é responsável pela elaboração da solução que melhor atenda às necessidades do CONTRATANTE.
2.7.15. A CONTRATADA é responsável pelo entendimento das necessidades, configuração e customização das ferramentas de gerência, de acordo com o que for especificado no PROJETO LÓGICO.
2.7.16. Todos os serviços necessários para o funcionamento da solução serão configurados para garantir a interoperabilidade do ambiente, alta disponibilidade, gerenciamento, e segurança exigida pelo CONTRATANTE.
2.7.17. O Projeto Lógico, bem como todos seus itens e equipamentos necessários, deve ter documentação de configuração e design aderentes ao PCI DSS (Payment Card Industry - Data Security Standard) vigente, ao longo de todo o período contratual, tendo em consideração as atualizações pelas quais esta norma passa ciclicamente.
2.7.18. A solução, ao ser implementada no escopo de adquirência do CONTRATANTE, deverá, obrigatoriamente, atender plenamente aos requisitos da norma PCI DSS vigente. Neste contexto, cita-se, mas não se limita a:
2.7.18.1. Manter aderência no que tange à segmentação de rede;
2.7.18.2. Utilizar apenas serviços e protocolos estritamente necessários e seguros;
2.7.18.3. Não manter contas genéricas ou default de usuários;
2.7.18.4. Configurar parâmetros de segurança de modo a prevenir mal uso;
2.7.19. Toda documentação do Projeto Lógico Preliminar deve ser validada pela equipe técnica do CONTRATANTE, contando com as melhores práticas de *design* para o respectivo ambiente.
2.7.20. Após o detalhamento técnico do Projeto Lógico Preliminar, a CONTRATADA deve atualizar juntamente com o CONTRATANTE o Cronograma de Implantação com as atividades necessárias, seus pré-requisitos e o mapeamento das responsabilidades entre as equipes.

2.8. IMPLANTAÇÃO E MIGRAÇÃO

2.8.1. A CONTRATADA disponibilizará pelo menos 02 (dois) analistas técnicos para atuar em campo responsáveis pela instalação dos equipamentos, implantação das configurações e parâmetros definidos no Plano Lógico Preliminar e execução de atividades em janelas de manutenção. Os profissionais devem possuir requisitos mínimo de nível PROFISSIONAL DE SEGURANÇA.
2.8.2. Toda configuração será realizada com acompanhamento e autorização prévia do CONTRATANTE.
2.8.3. A CONTRATADA será responsável pela implantação do novo ambiente de modo a cumprir as necessidades técnicas do CONTRATANTE devendo customizar a configuração dos equipamentos de forma a obter a melhor performance, disponibilidade e segurança do ambiente.
2.8.4. A solução contempla a Aquisição de Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida, composta por hardware, software, licenças, garantia, serviços de implementação da solução, suporte de hardware, suporte técnico com acordo de nível de serviço (SLA) definido, manutenção dos equipamentos e treinamento e todos os serviços necessários para configurar e suportar o ambiente de segurança de redes e comunicações junto aos equipamentos do Core de Rede e demais ambientes do CONTRATANTE incluindo a entrega dos produtos

especificados no plano de projeto, os profissionais dedicados para operação assistida do ambiente e os testes de aceitação, conforme descrito neste edital.

2.8.5. A CONTRATADA também será responsável por conduzir, em conjunto com a equipe da CONTRATANTE, o processo de migração do ambiente existente para o escopo da nova Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida além de treinar os profissionais do CONTRATANTE para posterior fase de operação do ambiente.

2.8.6. A CONTRATADA executará os serviços sem qualquer interferência no funcionamento regular das atividades normalmente realizadas pelo CONTRATANTE, garantindo a continuidade dos serviços, ou seja, não poderá haver interrupção não programada do serviço de dados atual para a entrada do novo serviço. Desta forma, a CONTRATADA executará serviços em finais de semana, feriados e horário noturno sempre que houver necessidade para atendimento das condições expostas pelo CONTRATANTE nesta especificação.

2.8.7. A CONTRATADA informará ao CONTRATANTE ocorrências de fatos que possam interferir, direta ou indiretamente, na regularidade da prestação do objeto contratado, assim como, especificará de forma clara as responsabilidades que ficarem ao encargo do CONTRATANTE e que não foram descritas nesta especificação.

2.8.8. Os prazos estabelecidos para mudanças no ambiente poderão ser estendidos, a critério do CONTRATANTE e com aviso prévio de 05 (cinco) dias úteis, devido aos períodos de congelamento (*freezing*) definidos pelas áreas responsáveis pelo acesso aos Data Centers do CONTRATANTE. A CONTRATADA deve se adequar ao processo de mudanças do CONTRATANTE, visto que o mesmo é variável em atendimento aos acontecimentos de mercado.

2.8.9. A CONTRATADA poderá solicitar uma janela de manutenção emergencial para realizar o "*rollback*" (restauração) da configuração anterior.

2.8.10. Quaisquer alegações por parte da CONTRATADA relacionadas a instalações (ambiente inadequado, rede elétrica, rede lógica, etc.) ou usuários (mau uso, etc.) do CONTRATANTE, devem ser comprovadas tecnicamente através de laudos detalhados e conclusivos, emitidos pelo fabricante do equipamento. Não serão admitidas omissões baseadas em suposições técnicas sem fundamentação, "experiência" dos técnicos ou alegações baseadas em exemplos de terceiros. Enquanto não for efetuado o laudo e esse não demonstrar claramente os problemas alegados, a CONTRATADA deve prosseguir com o atendimento dos chamados.

2.9. ACEITAÇÃO FINAL

2.9.1. Após a migração, deve ser realizada uma reunião de encerramento do projeto, quando ao receber o ANEXO 04 - TERMO DE ACEITAÇÃO DEFINITIVA, a CONTRATADA deve entregar ao CONTRATANTE o *High Level Design,* documento que descreve o Plano Lógico Completo da solução implementada.

2.9.2. A CONTRATADA deve entregar/revisar o *High Level Design* (HLD) da solução juntamente ao termo de encerramento de projeto, e, além disso, uma atualização a cada 12 (doze) meses a contar da entrega final do projeto ou após qualquer intervenção para solução de problemas ou mudanças no ambiente. O HLD é o documento que descreve detalhadamente a arquitetura e o desenho lógico da solução, bem como as configurações realizadas na fase de implementação. Além das atualizações refletindo as mudanças do ambiente, o documento deve contemplar:

2.9.2.1. Avaliação do *roadmap* (visão estendida do futuro apresentando uma coletânea de conhecimentos) de desenvolvimento do fabricante dos equipamentos, a fim de verificar novas funcionalidades e continuidade do uso da solução.

2.9.2.2. Continuidade do suporte técnico do fabricante (status de End Of Sale / End Of Life).

2.9.2.3. Validade de licenças.

2.9.2.4. Avaliação das tecnologias utilizadas contendo informações sobre:

2.9.2.5. Estado de uso.

2.9.2.6. Nível de obsolescência.

2.9.2.7. Representa a melhor opção quanto à segurança, desempenho e recursos.

2.9.2.8. Comprovação da inexistência de vulnerabilidades de segurança já catalogadas.

2.9.2.9. Arquitetura:

2.9.2.9.1. Se continua atendendo aos requisitos.

2.9.2.9.2. Se continua sendo a forma mais simples e mais eficaz de atender os requisitos.

2.9.2.9.3. Se atende ao crescimento do CONTRATANTE;
2.9.3. A CONTRATADA deve revisar o Plano Lógico da rede do CONTRATANTE a cada 12 (doze) meses, iniciando-se a contagem deste prazo logo no início da vigência contratual e após qualquer intervenção para solução de problemas e planos de mudanças relacionados à solução.
2.9.4. Ao final da implantação, o ambiente será considerado aceito e 100% funcional, finalizando o projeto com a assinatura do ANEXO 04 - TERMO DE ACEITAÇÃO DEFINITIVA.

2.10. RESPONSABILIDADES

2.10.1. A CONTRATADA deve viabilizar a execução de testes da solução, visando a identificação de vulnerabilidades no ambiente de TI que possam afetar o CONTRATANTE;
2.10.2. A CONTRATADA deve prover suporte e garantia a toda a Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida do CONTRATANTE, conforme especificado, durante todo o período contratual;
2.10.3. A CONTRATADA tem a responsabilidade de aplicar os controles necessários para corrigir quaisquer vulnerabilidades ligadas à solução que possam afetar a confidencialidade, integridade e disponibilidade dos serviços prestados ao CONTRATANTE;
2.10.4. Fica a critério do CONTRATANTE apresentar o detalhamento das análises e testes a serem realizados;
2.10.5. A CONTRATADA deve realizar o tratamento de vulnerabilidades identificadas sem ônus ao CONTRATANTE;
2.10.6. O CONTRATANTE realiza a classificação de vulnerabilidades de acordo com Common Vulnerability Scoring System (CVSS) na Versão 4 (quatro) ou superior;
2.10.7. As vulnerabilidades deverão ser corrigidas dentro dos prazos definidos pelo CONTRATANTE, de acordo com a severidade, definidos nos itens abaixo:
2.10.8. Vulnerabilidades de severidade CRÍTICA em até 10 (dez) dias corridos, a contar da data de encerramento dos testes;
2.10.9. Vulnerabilidades de severidade ALTA em até 30 (trinta) dias corridos, a contar de encerramento dos testes;
2.10.10. Vulnerabilidades de severidade MÉDIA em até 60 (sessenta) dias corridos, a contar da data de encerramento dos testes;
2.10.11. Vulnerabilidades de severidade BAIXA em até 90 (noventa) dias corridos, a contar da data de encerramento dos testes;
2.10.12. Para aquelas vulnerabilidades cuja severidade o cálculo do CVSS seja igual ou superior a 8.6 (oito ponto seis), a CONTRATADA deve iniciar o tratamento da vulnerabilidade imediatamente, incluindo medidas de mitigação e monitoramento de tentativas de exploração, e comunicar tempestivamente a CONTRATANTE;
2.10.13. As correções de vulnerabilidades serão registradas como tickets de Incidentes, associadas e integrantes do Acordo de Níveis de Serviços, no Nível de Severidade e no prazo contratual ajustado entre as PARTES, disto resultando na aplicação das respectivas penalidades em caso de não cumprimento;
2.10.14. O CONTRATANTE pode repassar as informações contidas na documentação para Órgãos Reguladores, Órgãos Fiscalizadores e Auditorias Externas;
2.10.15. As correções de vulnerabilidades por padrão fazem parte do escopo de suporte técnico e operação assistida já fornecidos pela CONTRATADA. As situações que necessitarem do estabelecimento de um projeto para tais correções devem ser conduzidas conforme acordo entre as partes, podendo ou não consumir o saldo de horas técnicas previsto em contrato, conforme o caso;
2.10.16. Acordado ou revisto formalmente a qualquer tempo, o projeto decorrente será classificado como uma Ordem de Serviço, vinculada a Requisição original, passando a ser considerado como integrante do Acordo de Níveis de Serviço, no Nível de Severidade e no prazo ajustado entre as PARTES, disto resultando a aplicação das respectivas penalidades pelo não cumprimento;
2.10.17. Caso a CONTRATADA tenha conhecimento de vulnerabilidades na solução ou na infraestrutura que trafega, processa ou armazena dados do CONTRATANTE, ou vulnerabilidades

em outros ativos que possam afetar dados do CONTRATANTE, deve comunicar imediatamente o CONTRATANTE;

2.10.18. A Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida pode sofrer diversas mudanças ao longo do tempo e do seu ciclo de vida. Sempre que houver novas requisições de mudanças ou alterações nas configurações dos equipamentos cobertos pelo contrato atual, estas mudanças serão submetidas à Gerência de Mudanças do CONTRATANTE e passarão por processo de análise e validação pela equipe técnica da CONTRATADA antes de serem implementadas. A CONTRATADA terá 02 (dois) dias úteis para a validação após as propostas de mudanças serem submetidas;

2.10.19. A garantia de hardware e suporte a software deve abranger todo período contratual, no local de instalação dos equipamentos, para todos os equipamentos fornecidos;

2.10.20. A garantia deve prever a substituição de equipamentos que apresentem defeitos, bem como direito a atualização de software (minor releases) destes. Todo equipamento fornecido em substituição pela garantia deve ser acompanhado de Nota Fiscal da CONTRATADA. A CONTRATADA deve conceder o direito junto ao FABRICANTE para download de novos releases (minor releases) de software para os equipamentos cobertos pela garantia, em caso de problemas e/ou bugs registrados;

2.10.21. A garantia deve prever a atualização de licenças, inclusive as de subscrição, por todo o período contratual, para todo hardware e software que compõe a solução;

2.10.22. Se, durante a vigência do contrato houver o lançamento de um novo produto ou atualização de software que contenha no mínimo as mesmas funcionalidades do software contratado e fique caracterizado que este lançamento provocará uma descontinuidade na comercialização e suporte de qualquer software suportado por este contrato, a CONTRATADA deve efetuar o fornecimento e implantação deste novo software, sem ônus ao CONTRATANTE, mesmo que o referido produto contenha, adicionalmente, características e funcionalidades que originalmente não existiam no software contratado;

2.10.23. Nesse caso, o fornecimento e implantação do novo produto deve ocorrer em no máximo 120 (cento) dias corridos a contar da solicitação formal do CONTRATANTE, na qual serão apontadas evidências da descontinuidade na comercialização e suporte do software, hardware ou serviço suportado;

2.10.24. Ocorrendo a troca do produto, a CONTRATADA é obrigada a fornecer a quantidade de licenças necessárias para licenciar a infraestrutura da CONTRATANTE, previamente estipulada neste edital e no decorrer do contrato;

2.10.25. A CONTRATADA arcará com qualquer ônus referente à troca, licenciamento, migração, instalação e configuração de software, entre outros, ficando a CONTRATANTE livre de qualquer ônus diferente do acordado no contrato;

2.10.26. Caso a CONTRATADA identifique a necessidade de substituição de equipamentos que apresentem defeitos ou falhas, estes devem ser substituídos por produtos de qualidade e características técnicas iguais ou superiores aos existentes, desde que compatíveis com todas as configurações necessárias ao seu funcionamento no ambiente do CONTRATANTE. O descarte dos equipamentos substituídos será de inteira responsabilidade da CONTRATADA, devendo respeitar as melhores práticas de sustentabilidade, conforme a Política Nacional de Resíduos Sólidos.

2.11. TREINAMENTOS OFICIAIS, OPERACIONAIS, EVENTOS e WORKSHOPS de Atualização

2.11.1. TREINAMENTOS OFICIAIS DO FABRICANTE

2.11.1.1. A CONTRATADA deve fornecer TREINAMENTOS OFICIAIS do fabricante que devem anteceder à finalização da etapa de planejamento da implementação do projeto (plano lógico preliminar) para que a equipe do CONTRATANTE possa receber o conhecimento amplo e necessário para entender e realizar a implementação da solução;

2.11.1.2. Os treinamentos oficiais dos fabricantes devem capacitar os colaboradores do CONTRATANTE para a realização de prova oficial de certificação do fabricante para o nível de ADMINISTRADOR / PROFISSIONAL DE SEGURANÇA DE REDES, ou nível técnico administrador equivalente, para todas as funcionalidades fornecidas na solução;

2.11.1.3. A CONTRATADA deve fornecer também os treinamentos oficiais que porventura sejam pré-requisitos dos treinamentos oficiais de nível administrador solicitados;
2.11.1.4. Os treinamentos oficiais dos fabricantes devem seguir no mínimo a carga horária informada na grade vigente dos cursos oficiais do fabricante em questão;
2.11.1.5. Para os TREINAMENTOS OFICIAIS, deve ser utilizada a ementa oficial dos cursos do fabricante, não serão aceitos treinamentos customizados;
2.11.1.6. A CONTRATADA deve prover treinamentos oficiais dos fabricantes dos equipamentos envolvidos na solução para 20 (vinte) colaboradores do CONTRATANTE, em duas turmas, no total de 10 (dez) pessoas por turma, em datas previamente acordadas com o CONTRATANTE;
2.11.1.7. Para todos os treinamentos previstos no presente termo deve haver intervalos de 15 minutos a cada duas horas de treinamento;
2.11.1.8. Para todos os treinamentos realizados no formato presencial, no intervalo de todos os treinamentos previstos no presente termo a CONTRATADA deve disponibilizar Coffee Break aos alunos de cada turma;
2.11.1.9. Os treinamentos devem ser realizados em Porto Alegre – RS, em local a ser definido pela CONTRATADA em comum acordo com o CONTRATANTE;
2.11.1.10. A CONTRATADA será responsável por providenciar os locais e os recursos necessários para os treinamentos oficiais;
2.11.2. TREINAMENTOS OPERACIONAIS
2.11.2.1. A CONTRATADA ministrará treinamentos demonstrando aspectos principais da configuração do produto após a implementação. Os treinamentos operacionais devem contemplar conhecimentos com relação aos equipamentos ofertados, especificamente conhecimento do hardware, seus módulos, conexões, protocolos suportados, configuração, operação e gerenciamento, assim como módulos de serviço ou soluções em nuvem, conforme as boas práticas de implementação utilizadas no projeto.
2.11.2.2. A CONTRATADA deve fornecer TREINAMENTOS OPERACIONAIS para passagem de conhecimento após a finalização da migração para o novo ambiente;
2.11.2.3. Os Treinamentos Operacionais visam passar uma visão geral de como foi implementada a solução no ambiente do CONTRATANTE e devem ser ministrados por um profissional da CONTRATADA envolvido no projeto e devidamente qualificado com a certificação técnica de grau máximo na solução ofertada.
2.11.2.4. A CONTRATADA deve ministrar os treinamentos operacionais, sem custo adicional ao CONTRATANTE para 20 (vinte) colaboradores, em duas turmas de 10 (dez) pessoas.
2.11.2.5. Os treinamentos deverão ser ministrados em português (salvo comum acordo com a CONTRATANTE para uso de língua estrangeira) e serão realizados presencialmente em Porto Alegre – RS, em local a ser definido pelo CONTRATANTE, para duas turmas, no total de 10 (dez) pessoas por turma;
2.11.2.6. A carga horária mínima é de 30 (trinta) horas no total;
2.11.2.7. Deve haver intervalos de 15 minutos a cada duas horas de treinamento;
2.11.2.8. Nos intervalos dos treinamentos a CONTRATADA deve disponibilizar coffee break com itens variados aos alunos de cada turma, prevendo um total de 15 pessoas (alunos, instrutor e equipe de treinamento) por turma;
2.11.2.9. O CONTRATANTE informará à CONTRATADA com 15 (quinze) dias de antecedência a data de realização de todos os cursos previstos nos itens desta especificação;
2.11.2.10. Os treinamentos operacionais devem abordar, no mínimo, os seguintes tópicos gerais:
2.11.2.10.1. Descrição do escopo da solução e produtos envolvidos no projeto (overview da plataforma);
2.11.2.10.2. Instrumentação de todos os recursos da solução;
2.11.2.10.3. Apresentação de como ocorreu a migração para a solução;
2.11.2.10.4. Descoberta de ativos e inventário;
2.11.2.10.5. Relatórios e painéis interativos;
2.11.2.10.6. Avaliação dos desafios de rede (quais os problemas mais comuns);
2.11.2.10.7. Serviço de inspeção e monitoramento;

2.11.2.10.8. Propósitos da implementação e principais características;
2.11.2.10.9. Arquitetura e componentes;
2.11.2.10.10. Ferramentas de diagnóstico;
2.11.2.10.11. Funcionamento e problemas mais comuns;
2.11.2.10.12. Definições de grupos de usuários;
2.11.2.10.13. Entendendo o comportamento do tráfego;
2.11.2.10.14. Recursos de filtragem dos dados (condições lógicas, IP, porta, seção, outros);
2.11.2.10.15. Utilização em conjunto com outras soluções e tecnologias;
2.11.2.10.16. Estratégias e formas de incremento da solução no ambiente;
2.11.2.10.17. Estratégias para manutenção da solução;
2.11.2.10.18. Possíveis cenários de degradação;
2.11.2.10.19. Troubleshooting: Possíveis problemas e passo a passo para solucioná-los;
2.11.2.10.20. Hands-on da Operação e manuseio das ferramentas de administração;
2.11.2.10.21. Integração com outros fabricantes;
2.11.2.11. Os treinamentos serão divididos em fases ou agrupados, dependendo da escolha do público-alvo e disponibilidade de agendas, sendo essa definição pelo CONTRATANTE em fase de execução do projeto;
2.11.2.12. Mediante negociação e com o devido aceite do contratante, os treinamentos poderão ser realizados de forma remota, desde que todas as ferramentas necessárias para o bom andamento dos treinamentos sejam disponibilizadas pela CONTRATADA, sem ônus ao CONTRATANTE;

2.11.3. OUTROS TREINAMENTOS, EVENTOS E WORKSHOPS DE ATUALIZAÇÃO
2.11.3.1. A CONTRATADA deve realizar Workshops de Atualização de Conhecimentos e Tecnologia anualmente para até 10 (dez) colaboradores do CONTRATANTE;
2.11.3.2. Cada workshop deve ser concluído dentro do período de cada ciclo anual do contrato, considerando a data de assinatura do contrato como o início do primeiro ciclo anual, de acordo com cronograma estabelecido entre a Equipe Técnica do CONTRATANTE e a CONTRATADA;
2.11.3.3. Os workshops podem ser realizados nas dependências do CONTRATANTE e devem ser ministrados por instrutores preparados e certificados pelo fabricante dos produtos;
2.11.3.4. Os workshops previamente planejados devem ter carga horária mínima de 20 (vinte) horas, cobrindo conteúdo teórico e prático, em nível avançado e relacionado à solução fornecida, com foco nas atualizações aplicadas à solução durante cada ciclo anual, bem como em tópicos de interesse da equipe técnica do CONTRATANTE. Nesses casos, o workshop e o material didático deverão estar, preferencialmente, em língua portuguesa, ou, na sua impossibilidade, em língua inglesa;
2.11.3.5. Ainda dentro do período de cada ciclo anual do contrato, A CONTRATADA deve disponibilizar anualmente, 04 (quatro) vagas para colabores do CONTRATANTE para a participação de eventos de tecnologia do fabricante da solução ou em evento de tecnologia do qual o fabricante da solução esteja participando;
2.11.3.6. Caso os treinamentos, eventos ou workshops sejam realizados fora de Porto Alegre, as despesas com transporte (aéreo e local), hospedagem e alimentação deverão ser custeadas pela CONTRATADA;

2.12. MANUTENÇÃO, SUPORTE TÉCNICO E OPERAÇÃO ASSISTIDA DOS AMBIENTES

2.12.1. A CONTRATADA deve disponibilizar, sempre que necessário, profissionais para suporte às demandas da Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida.
2.12.2. Após a aceitação final do projeto, todos os profissionais mencionados acima devem possuir conhecimento pleno e detalhado da solução implementada no ambiente da CONTRATANTE.
2.12.3. A CONTRATADA deve garantir o acesso/comunicação direto do CONTRATANTE com os profissionais certificados a serem designados para este processo. Para tanto devem ser fornecidos os dados de contato destes profissionais.
2.12.4. O CONTRATANTE poderá solicitar à CONTRATADA a qualquer momento a revalidação das certificações anteriormente mencionadas.

2.12.5. A CONTRATADA é responsável pela elaboração da solução que melhor atenda às necessidades do CONTRATANTE. Todos os serviços de rede necessários para o funcionamento da solução serão configurados para garantir a interoperabilidade do ambiente, alta-disponibilidade, gerenciamento, balanceamento de carga e segurança desejada pelo CONTRATANTE.
2.12.6. A CONTRATADA deve elaborar o Plano de Continuidade de Negócios (PCN), embasado nas normas (ABNT NBR ISO 22301:2020 - Segurança e resiliência — Sistema de gestão de continuidade de negócios — Requisitos) ou boas práticas reconhecidas pelo mercado (Information Technology Infrastructure Library versão quatro – ITILv4, Control Objectives for Information and related Technology versão 2019 – COBIT 2019) para a Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida. O referido PCN e as evidências dos testes realizados deverão ser apresentados pela CONTRATADA ao CONTRATANTE na ocasião do encerramento da implementação, sendo atualizado anualmente ou sempre que solicitado. O Plano deve incluir:
2.12.6.1. PCN por Modelo de Equipamento: descrevendo cada equipamento, seus módulos, aplicação, serviços afetados em caso de falha, responsáveis pelos serviços, principais sintomas de incidentes e procedimentos de solução de contorno.
2.12.6.2. PCN por Cenário: descrevendo os principais cenários de quedas e paralisações de serviços de rede, baseando-se na topologia do CONTRATANTE, os principais sintomas e procedimentos de solução de contorno.
2.12.6.3. Plano de Testes para serem realizados após mudanças no ambiente.
2.12.7. O PCN deve ser revisado e atualizado a cada 12 (doze) meses a contar da entrega da primeira versão, a critério do CONTRATANTE, sempre que houver mudanças significativas na estrutura da solução e sempre que for solicitado.
2.12.8. O PCN apresentado pela CONTRATADA será analisado pelo CONTRATANTE, que poderá aceitar, rejeitar ou sugerir adequações de forma a atender aos requisitos do Acordo Níveis de Serviços. Em caso de rejeição ou havendo necessidade de ajustes a CONTRATADA terá mais 30 (trinta) dias corridos, a partir da comunicação do CONTRATANTE, para retornar o plano atualizado.

2.12.9. A CONTRATADA deve prover serviço de suporte técnico para execução de manutenção preventiva e corretiva dos equipamentos, que compõem a solução, instalados nos Data Center do CONTRATANTE. A CONTRATADA será a responsável direta pelos serviços de manutenção e suporte técnico, que serão pagos mensalmente.
2.12.10. O CONTRATANTE utiliza ferramenta padrão de mercado como meio de monitoramento proativo de falhas de todo o ambiente listado na planilha de especificações técnicas.
2.12.11. A CONTRATADA deve solicitar e sugerir customizações nas ferramentas de Gerência ao suporte técnico do CONTRATANTE a fim de auxiliar no cumprimento do SLA especificado neste documento.
2.12.12. Todos os equipamentos inseridos na solução devem ser passíveis de monitoração através da ferramenta “CA Spectrum”.
2.12.13. Os serviços contemplam a substituição de peças e equipamentos em caso de falhas, atualizações de software e acesso ao “Centro de Assistência Técnica” (TAC - Technical Assistance Center) do fabricante dos equipamentos, através da CONTRATADA, e acesso ao “Ambiente Online do Fabricante” (AOF).
2.12.14. O acesso ao TAC e ao AOF será realizado através de usuário (identificador) e senha que permitam o acompanhamento de solicitações de serviço, bem como livre acesso às ferramentas e documentos técnicos disponibilizados pelo fabricante. A CONTRATADA deve controlar e fornecer as últimas versões dos softwares utilizados pelos equipamentos, contendo correções de bugs, atualizações ou novas funcionalidades suportadas, pelo equipamento em questão, bem como as respectivas licenças de uso.
2.12.15. A garantia deve prever a substituição de equipamentos que apresentem defeitos e o direito a atualização de software (*minor releases*) destes. Todo equipamento fornecido em substituição pela garantia deve ser acompanhado de Nota Fiscal da CONTRATADA. A CONTRATADA deve conceder o direito junto ao FABRICANTE para download de novos releases (minor releases) de software para os equipamentos cobertos pela GARANTIA, em caso de problemas e *bugs* registrados.

2.12.16. Caso a CONTRATADA identifique a necessidade de substituição de equipamentos que apresentem defeitos ou falhas, estes devem ser substituídos por produtos de qualidade e características técnicas iguais ou superiores aos existentes, desde que compatíveis com todas as configurações necessárias ao seu funcionamento no ambiente do CONTRATANTE.
2.12.17. O CONTRATANTE poderá abrir chamados técnicos com a CONTRATADA para consultoria técnica, participação do planejamento de novos projetos, configurações de novos serviços, aplicação de atualização de versões de software nos equipamentos, acompanhamento de janelas de manutenção programadas em qualquer horário e resolução de problemas (troubleshooting).
2.12.18. Para atendimento aos chamados dentro do SLA, o CONTRATANTE autorizará o acesso para os profissionais e equipamentos da CONTRATADA aos dois prédios de Data Center, dentro e fora do horário comercial. O CONTRATANTE também irá permitir o acesso remoto assistido à rede.
2.12.19. A abertura de chamados seguirá as melhores práticas descritas na última versão do ITIL quanto aos níveis de escalonamento. Para a resolução de problemas de maior complexidade devem ser envolvidos profissionais com maior capacitação.
2.12.20. O atendimento aos chamados poderá ser iniciado remotamente, de forma assistida até o registro de abertura do chamado.
2.12.21. Após o registro de abertura de um chamado e/ou contato telefônico com os representantes técnicos, o atendimento pode ocorrer nas dependências do CONTRATANTE em Porto Alegre/RS, a critério do CONTRATANTE.
2.12.22. Os chamados de suporte para manutenções preventivas, atualização de versão de softwares, adoção de novas tecnologias, adição de novas funcionalidades, aperfeiçoamento de configurações e alterações nas topologias da rede que envolvam os equipamentos, serão atendidos nas dependências do CONTRATANTE, em Porto Alegre/RS, em data e horário previamente acordado entre as partes.
2.12.23. Todo o suporte deve ser assistido por técnicos da CONTRATADA com qualificação comprovada pelo fabricante do equipamento, quando solicitado;
2.12.24. Os serviços prestados deverão ser realizados nas dependências da CONTRATANTE.
2.12.25. Os profissionais designados para atender aos chamados devem possuir conhecimento avançado de todos os elementos que irão compor a Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida adquirida pelo CONTRATANTE (Hardware, Software, Licenças, Protocolos, APIs, etc) bem como o conhecimento prévio da arquitetura implementada.

2.12.26. A CONTRATADA deve realizar *Health Checks* sob demanda, com o objetivo de verificar todos os aspectos relacionadas à solução, observando conformidade com as melhores práticas de configuração e segurança do fabricante, validação dos parâmetros em uso e identificação de funcionalidades disponíveis, porém não implementadas;
2.12.27. A CONTRATADA deve iniciar a execução do serviço em até 30 dias após a solicitação do CONTRATANTE.
2.12.28. A CONTRATADA deve apresentar uma proposta completa do *Heatlh Check* a ser realizado, contendo no mínimo o plano de ação para execução, cronograma e prazos, relação de itens a serem avaliados, e deve ter o prévio aceite do CONTRATANTE.
2.12.29. O CONTRATANTE reserva-se o direito de alterar o plano de ação conforme sua necessidade.
2.12.30. Como resultado do *Health Check*, a CONTRATADA deve apresentar ao CONTRATANTE, um relatório contendo, para o escopo avaliado:
2.12.30.1. Detalhamento da situação de cada item analisado;
2.12.30.2. As inconformidades da configuração atual, de acordo com as melhores práticas do fabricante;
2.12.30.3. As funcionalidades disponíveis na solução e não implementadas;
2.12.30.4. As vantagens, riscos, pré-requisitos, premissas, e custos atrelados a licenciamento, aquisição, configuração, e estimativa de horas necessárias;

2.12.30.5. Elaborar o plano de ação para atendimento dos itens apontados no relatório;
2.12.31. A CONTRATADA deve alocar 500 (quinhentas) horas técnicas por ano (em caráter limitador máximo, podendo variar de acordo com as necessidades do CONTRATANTE) para a prestação de serviços de suporte ao desenvolvimento, manutenção, implementação, projetos e especificações de segurança da informação com ênfase na solução ofertada, a serem executados nas dependências do CONTRATANTE, envolvendo:
2.12.31.1. Elaboração de novos projetos;
2.12.31.2. Suporte técnico no desenvolvimento e integração, relativos à solução ofertada;
2.12.31.3. Elaboração de material de apoio e documentação de novos projetos;
2.12.31.4. Elaboração de pareceres técnicos;
2.12.31.5. Orientação a analistas, desenvolvedores e programadores sobre aspectos relacionados à segurança da informação e a da solução ofertada;
2.12.32. Para a prestação dos serviços deste objeto a CONTRATADA vencedora do certame deve possuir:
2.12.32.1. Conhecimento sobre normas e regulamentações associadas a Segurança da Informação (ISO-27001, ISO-27002);
2.12.32.2. Comprovar conhecimento técnico através de pelo menos UMA das certificações profissionais constantes nos subitens a seguir:
2.12.32.2.1. CRISC (Certified in Risk and Information Systems Control – emitido pelo ISACA (Information Systems Audit and Control Association);
2.12.32.2.2. SECURITY+ (Certified by Computing Technology Industry Association USA - CompTIA);
2.12.32.2.3. CISM (Certified Information Security Manager) - emitido pelo ISACA (Information Systems Audit and Control Association);
2.12.32.2.4. CISSP (Certified Information System Security Professional) - emitido pelo ISC² (International Information Security System Certification Consortium);
2.12.33. A CONTRATADA deve disponibilizar para a Operação Assistida pelo menos 02 (dois) profissionais dedicados que atendam aos requisitos de nível PROFISSIONAL DE SEGURANÇA;
2.12.34. A CONTRATADA deve prover serviço de suporte técnico 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, no seguinte formato:
2.12.35. TRABALHO PRESENCIAL, através de profissionais dedicados, que no conjunto de suas escalas de trabalho, cubram a jornada regular inicialmente estabelecida das 07h30min às 19h30min, de segunda à sexta, para atuar na operação assistida de forma dedicada junto à equipe técnica do CONTRATANTE. O intervalo para jornada regular presencial a ser cumprida pode ser alterado conforme necessidade do CONTRATANTE, mantendo a carga horária individual por profissional dedicado prevista para 8 (oito) horas por dia;
2.12.36. TRABALHO REMOTO, em caráter de sobreaviso, através dos profissionais dedicados à operação assistida nos casos em que for necessária a atuação fora dos dias e horários de jornada regular definidos para o atendimento presencial, visando a execução do serviço de manutenção preventiva e corretiva dos equipamentos que compõem a Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida;
2.12.37. Cada profissional alocado para a operação assistida poderá realizar jornada de trabalho em formato híbrido através de escala mensal pré-definida em conjunto com a equipe técnica do CONTRATANTE, alternando entre formato presencial (dentro das instalações do CONTRATANTE) e remoto, estando sujeito a alterações, sem custos adicionais e de acordo com a escala de trabalho da equipe técnica do CONTRATANTE e com as suas políticas de teletrabalho;
2.12.38. A composição da escala da execução de trabalho presencial e remoto deve ser acordada entre as partes;
2.12.39. As horas realizadas em tarefas extraordinárias, fora da jornada de trabalho, seja em planos de mudança ou atendimento a incidentes, não serão contabilizadas para o atendimento ao tempo mínimo de escala presencial;
2.12.40. Em caso de alteração das políticas de teletrabalho, o CONTRATANTE deve comunicar formalmente à CONTRATADA o novo regramento, com antecedência de 30 (trinta) dias corridos, através de e-mail e/ou em reunião com o registro em ata;

2.12.41. O CONTRATANTE proverá os recursos administrativos (instalações, mesas, cadeiras, material de expediente, etc.) para atendimentos efetuados *in loco*;
2.12.42. O CONTRATANTE poderá, a qualquer momento, solicitar visita ao Centro de Operações e Suporte a Serviço da CONTRATADA, a fim de comprovar que a CONTRATADA possui estrutura de atendimento 24x7 para atendimento das demandas técnicas do CONTRATANTE;

2.13. ACORDO DE NÍVEIS DE SERVIÇO

2.13.1. O objetivo deste acordo é estabelecer as diretrizes para a entrega de serviços de alta qualidade para a Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida, de acordo com as necessidades do CONTRATANTE.
2.13.2. A cobertura dos serviços será integral, ou seja, 24 (vinte e quatro) horas por dia, nos 7 (sete) dias da semana, incluindo sábados, domingos, feriados e pontos facultativos. A abertura do chamado técnico ou solicitação de serviço será realizada através dos seguintes meios: Registro no sistema de Service Desk do CONTRATANTE, diretamente com os profissionais da CONTRATADA e via chamado telefônico DDG (0800);
2.13.3. 1.3. A CONTRATADA deve prover suporte e garantia a toda a Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida do CONTRATANTE, conforme especificado;
2.13.4. O CONTRATANTE utiliza ferramenta padrão de mercado como meio de monitoramento proativo de falhas de todo o ambiente listado na planilha de especificações técnicas (CA Spectrum). A CONTRATADA deve solicitar e sugerir customizações nas ferramentas de Gerência de Rede ao suporte técnico do CONTRATANTE a fim de auxiliar no cumprimento do SLA especificado neste documento. As informações contidas nos relatórios devem ser analisadas e apresentadas pela CONTRATADA sempre que solicitado pelo CONTRATANTE.
2.13.5. Os serviços contemplam a substituição de peças e equipamentos em caso de falhas, atualizações de software e acesso ao “Centro de Assistência Técnica” (TAC - Technical Assistance Center) do fabricante dos equipamentos, através da CONTRATADA, e acesso ao “Ambiente Online do Fabricante” (AOF).
2.13.6. O acesso ao TAC e ao AOF será realizado através de usuário (identificador) e senha que permitam o acompanhamento de solicitações de serviço, bem como livre acesso às ferramentas e documentos técnicos disponibilizados pelo fabricante. A CONTRATADA deve controlar e fornecer as últimas versões dos softwares utilizados pelos equipamentos, contendo correções de bugs, atualizações ou novas funcionalidades suportadas, pelo equipamento em questão, bem como as respectivas licenças de uso;
2.13.7. A CONTRATADA deve fornecer o suporte do tipo solução junto ao fabricante, ou seja, o atendimento de chamados deve ocorrer através de uma equipe dedicada com nível técnico compatível com a complexidade do ambiente e processos de suporte coordenados, de modo a otimizar o tempo de resposta com o atendimento especializado. Esse nível de suporte visa resolver problemas mais rapidamente do que depender apenas do suporte padrão ao produto, prestando um nível avançado de atendimento e caso de chamados efetuados diretamente pelo CONTRATANTE junto ao fabricante, ou ainda por intermédio dos profissionais dedicados à operação assistida;
2.13.8. A CONTRATADA deve prestar as seguintes informações, por ocasião do início do contrato:
2.13.9. Procedimento descritivo ou ilustrativo de acesso ao TAC do fabricante pela Internet, para cadastro de usuários e abertura de registro por escrito referente a solicitações de assistência técnica (cases), bem como o acesso aos serviços de atualização de software e documentação técnica;
2.13.10. Número telefônico gratuito (serviço 0800) do TAC do fabricante da solução para o registro de solicitações de assistência técnica;
2.13.11. O CONTRATANTE poderá abrir requisições de serviço com a CONTRATADA para: consultoria técnica, participação do planejamento de novos projetos, configurações de novos serviços que envolvam o ambiente de segurança de rede e comunicações do CONTRATANTE, aplicação de atualização de versões de software nos equipamentos, acompanhamento de janelas de manutenção programadas em qualquer horário e resolução de problemas (troubleshooting);
2.13.12. As requisições de serviço por padrão fazem parte do escopo de suporte técnico e operação assistida já fornecidos pela CONTRATADA. As situações que necessitarem do

estabelecimento de um projeto para tais requisições devem ser conduzidas conforme acordo entre as partes, podendo ou não consumir o saldo de horas técnicas previsto em contrato, conforme o caso;

2.13.13. A CONTRATADA deve possuir em sua equipe técnica profissionais com perfil do tipo PROFISSIONAL DE SEGURANÇA ou superior para atendimento de demandas realizadas via chamado técnico (0800) durante toda a sua operação (24x7);

2.13.14. Todo o suporte deve ser assistido por técnicos da CONTRATADA com qualificação comprovada pelo fabricante do equipamento, sempre que solicitado;

2.13.15. Os chamados de suporte para atualização de versão de softwares, adição de novas funcionalidades, aperfeiçoamento de configurações e alterações nas topologias da rede que envolvam risco de parada da continuidade do serviço prestado pela solução deverão ser atendidos nas dependências do CONTRATANTE, em Porto Alegre, em data e horário previamente acordado entre as partes.

2.13.16. A CONTRATADA reconhece que o não atendimento dos níveis de serviços contratados pode resultar em impacto adverso e relevante nos negócios e operações do CONTRATANTE;

2.13.17. Para atendimento aos chamados dentro dos prazos do SLA, o CONTRATANTE autorizará o acesso para os profissionais e equipamentos da CONTRATADA aos prédios de Data Center, dentro e fora do horário comercial, além do acesso remoto assistido à rede sempre que necessário;

2.13.18. A abertura de chamados seguirá as melhores práticas descritas na última versão do ITIL quanto aos níveis de escalonamento. Para a resolução de problemas de maior complexidade devem ser envolvidos profissionais com maior capacitação;

2.13.19. Após o registro de abertura de um chamado/incidente e/ou contato telefônico com os representantes técnicos, quando a natureza da ocorrência implicar em inoperância da solução ou afetar de forma significativa seu funcionamento, o atendimento deve ocorrer nas dependências do CONTRATANTE em Porto Alegre. Dentro dos horários de cobertura da operação assistida o atendimento poderá ser realizado inicialmente pela própria equipe local da CONTRATADA.

2.13.20. Os profissionais alocados na operação assistida responderão para a coordenação da área responsável pela Arquitetura de Segurança de Rede Corporativa do CONTRATANTE, limitando-se a executar atividades mediante anuência e aceite formal do CONTRATANTE;

2.13.21. Os profissionais alocados para a operação assistida devem apresentar vínculo profissional com a CONTRATADA;

2.13.22. Cada profissional deve possuir notebook, acesso próprio à internet e telefone celular, fornecidos e sob a responsabilidade da CONTRATADA, independente da infraestrutura fornecida pelo CONTRATANTE;

2.13.23. Os profissionais a serem destacados para atuar no CONTRATANTE devem possuir as seguintes atribuições:

2.13.24. Operação, arquitetura e administração de equipamentos e produtos da Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida;

2.13.25. Realização de suporte 1º e 2º nível para clientes internos e manutenções preventivas no ambiente de rede;

2.13.26. Atualização de documentações da rede do cliente, incluindo o Projeto Lógico, PCN, HLD, etc;

2.13.27. Inventário e identificação de equipamentos instalados;

2.13.28. Atualização de topologias;

2.13.29. Interação com operadoras de Telecom, mediante liberação pelos gestores técnicos do CONTRATANTE, para a resolução de problemas relacionados aos enlaces de longa distância (WAN);

2.13.30. Interação e comunicação com a equipe de Arquitetura de Segurança de Rede Corporativa do CONTRATANTE;

2.13.31. Realização de coleta de informações de rede, históricos (logs) e informações provenientes da equipe de TI do CONTRATANTE;

2.13.32. Apoiar as equipes do CONTRATANTE no controle das versões de software;

2.13.33. Aplicação de atualizações das versões de software nos equipamentos;

2.13.34. Configuração dos ativos da solução;
2.13.35. Desenvolvimento e manutenção de integrações dos dispositivos de rede junto a outros ambientes com uso de API REST;
2.13.36. Análise de informações coletadas, verificação de design e acompanhamento de arquitetura e recomendações;
2.13.37. Interagir na administração das ferramentas que o CONTRATANTE dispõe para a administração da solução, visando à agilidade dos diagnósticos e pronta resposta;
2.13.38. Acompanhamento de janelas de manutenção programadas em qualquer horário;
2.13.39. Identificar os componentes, peças, materiais ou software responsáveis pelo mau funcionamento dos equipamentos;
2.13.40. Ministrar treinamentos/passagem de conhecimento referentes aos equipamentos, protocolos e atividades realizadas nas dependências do CONTRATANTE;
2.13.41. Atualizar requisições e incidentes através da ferramenta de Service Desk do CONTRATANTE;
2.13.42. Em caso de ausência do profissional, por motivações previstas em lei ou não, a CONTRATADA deve disponibilizar um substituto com o mesmo perfil em no máximo 1 (uma) hora.

2.14. PRAZOS E PERIODICIDADE DA EXECUÇÃO

2.14.1. Os equipamentos devem ser entregues e instalados e os serviços devem ser prestados de acordo com o cronograma a seguir:

2.14.1.1. Atividade 1: ABERTURA e PLANO DE PROJETO

2.14.1.1.1. ABERTURA - Reunião inicial do projeto (kick-off com todo o time envolvido): Até 5 (cinco) dias úteis a contar do início da vigência do contrato;
2.14.1.1.2. Termo de Abertura do Projeto;
2.14.1.1.3. Reuniões semanais de atualização;
2.14.1.1.4. Gerenciamento do projeto: Desde o início da vigência do contrato até a entrega da documentação técnica final;
2.14.1.1.5. Apresentação do PLANO DE PROJETO completo: Até 15 (Quinze) dias úteis a contar da reunião inicial do projeto;
2.14.1.1.6. Plano de Gerenciamento de Projeto e EAP (Estrutura Analítica do Projeto);
2.14.1.1.7. Plano de Projeto (Atividades do Escopo);
2.14.1.1.8. Cronograma;

2.14.1.2. Atividade 2: PLANEJAMENTO TÉCNICO PRELIMINAR E ENTREGA DOS EQUIPAMENTOS: Até 45 (quarenta e cinco) dias corridos a contar do início da vigência do Contrato;

2.14.1.2.1. O ato de entrega dos equipamentos será considerado concluído após os testes iniciais de *"burn-in"* que consiste em ligar os equipamentos e validar o correto funcionamento de seus componentes e acesso à interfaces de gerenciamento e configuração.
2.14.1.2.2. Os testes iniciais devem ser acompanhados pelos profissionais da CONTRATADA;
2.14.1.2.3. Finalizados os testes de *"burn-in",* será emitido pelo CONTRATANTE o ANEXO 03 - TERMO DE RECEBIMENTO referente a etapa de entrega dos equipamentos;
2.14.1.2.4. Apresentação do **PLANEJAMENTO TÉCNICO PRELIMINAR**: Até que ocorra a entrega dos equipamentos. O Planejamento técnico preliminar inclui o projeto lógico e plano de migração com detalhamento de atividades para avaliação anterior à implementação do projeto;

2.14.1.3. Atividade 3: GARANTIA DE HARDWARE E SOFTWARE E TREINAMENTOS OFICIAIS:

2.14.1.3.1. INÍCIO DA VIGÊNCIA DA GARANTIA DE HARDWARE E SOFTWARE: Imediatamente após a entrega dos equipamentos;
2.14.1.3.2. TREINAMENTOS OFICIAIS: Devem ser concluídos antes de finalizar a MIGRAÇÃO PARA O NOVO AMBIENTE (Atividade 5);

2.14.1.4. Atividade 4: IMPLEMENTAÇÃO INICIAL DO PROJETO: Deve ser concluída até 120 (cento e vinte) dias a contar do início da vigência do Contrato;

2.14.1.4.1. Configurações da nova solução;
2.14.1.4.2. Licenciamento;

2.14.1.5. Atividade 5: MIGRAÇÃO PARA O NOVO AMBIENTE: Deve ser concluída até 180 (cento e oitenta dias) dias corridos a contar da conclusão da IMPLEMENTAÇÃO INICIAL DO PROJETO;
2.14.1.5.1. Migração dos ambientes existentes para a nova solução;
2.14.1.5.2. Acompanhamento da Migração;

2.14.1.6. Atividade 6: SUPORTE/MANUTENÇÃO A HARDWARE E SOFTWARE E PROFISSIONAIS DEDICADOS À OPERAÇÃO ASSISTIDA
2.14.1.6.1. INÍCIO DA VIGÊNCIA DO SUPORTE E MANUTENÇÃO A HARDWARE E SOFTWARE: Imediatamente após a IMPLEMENTAÇÃO INICIAL DO PROJETO (Atividade 4);
2.14.1.6.2. PROFISSIONAIS DEDICADOS À OPERAÇÃO ASSISTIDA: Em até 60 (sessenta) dias corridos a partir do início da MIGRAÇÃO PARA O NOVO AMBIENTE para a apresentação e início das atividades dos profissionais dedicados à operação assistida, de forma que estes participem da fase de IMPLEMENTAÇÃO INICIAL DO PROJETO;
2.14.1.6.3. O serviço de operação assistida deve ocorrer de segunda-feira a sexta-feira, exceto feriados, nacionais e municipais de Porto Alegre, das 07h30min às 19h30min através de dois profissionais dedicados, conforme seguintes horários:
2.14.1.6.4. Horário dos Profissionais de Operação Assistida:
2.14.1.6.4.1. PROFISSIONAL DE SEGURANÇA 01: 07h30min às 16h30min, com uma hora de intervalo nesse período;
2.14.1.6.4.2. PROFISSIONAL DE SEGURANÇA 02: 10h30min às 19h30min, com uma hora de intervalo nesse período;
2.14.1.7. Atividade 7: TESTES DE ACEITAÇÃO E TREINAMENTO OPERACIONAL:
2.14.1.7.1. TESTES DE ACEITAÇÃO: Em fases conforme as entregas parciais de migração, devendo ocorrer a conclusão (TERMO DE ACEITAÇÃO DEFINITIVA) em até 15 (quinze) dias úteis após a conclusão da MIGRAÇÃO PARA O NOVO AMBIENTE;
2.14.1.7.2. FINALIZAÇÃO DOS TREINAMENTOS OPERACIONAIS: Em até 60 (sessenta) dias corridos após a finalização da MIGRAÇÃO PARA O NOVO AMBIENTE;
2.14.1.8. Atividade 8: ENTREGA DA DOCUMENTAÇÃO TÉCNICA FINAL E ENCERRAMENTO DO PROJETO: Conclusão em até 15 (Quinze) dias úteis após os TESTES DE ACEITAÇÃO, que se dará com o TERMO DE ENCERRAMENTO DO PROJETO;
2.14.1.8.1. Termos de aceitação dos testes;
2.14.1.8.2. High Level Design (HLD);
2.14.1.8.3. Apresentações;
2.14.1.8.4. Documentação detalhadas da instalação;
2.14.1.8.5. Documentação detalhada das integrações;
2.14.1.8.6. Topologia Lógica;
2.14.1.8.7. Códigos fonte das integrações e respectiva documentação para manutenção;
2.14.1.8.8. Plano de Continuidade de Negócios (PCN).
2.14.1.8.9. Plano de Recuperação de Desastres (PRD);
2.14.1.8.10. Testes e Evidências da Validação do PRD;
2.14.1.8.11. Reunião de Encerramento de projeto;
2.14.1.8.12. Entrega das Atas em material compilado;
2.14.1.8.13. Aceite da Documentação Técnica Final;
2.14.1.8.14. Termo de Encerramento de Projeto;
2.14.2. A integração e a utilização do Service Desk do CONTRATANTE devem ocorrer até o prazo máximo de 180 (cento e oitenta) dias corridos a partir do início da vigência do contrato.
2.14.3. Em até 120 (cento e vinte) dias contados a partir da entrega dos equipamentos, a CONTRATADA deve comprovar que todos os equipamentos, bem como seus números de série estão cobertos por garantia do fabricante que atenda aos requisitos deste Contrato.

2.15. UTILIZAÇÃO DO SERVICE DESK

2.15.1. MÉTODO DE ATENDIMENTO

2.15.2. O CONTRATANTE utiliza a ferramenta Service Desk como ponto único de contato sistêmico, para abertura, acompanhamento e gestão de todos os Incidentes, Requisições de Serviço e Ocorrências.
2.15.3. A CONTRATADA deve utilizar obrigatoriamente o Sistema Service Desk do CONTRATANTE para o controle dos Incidentes, Requisições de Serviço e Ocorrências, independentemente da utilização de ferramenta própria para controle interno.
2.15.4. O CONTRATANTE deve prover para a CONTRATADA o acesso ao seu Sistema de Service Desk para que a mesma acesse as informações sobre o andamento dos Incidentes, Requisições de Serviço e Ocorrências registrados.
2.15.5. O acesso ao console do Sistema Service Desk do CONTRATANTE será disponibilizado para a CONTRATADA via internet. Para cada contato será gerado um login e senha de acesso pessoal.
2.15.6. A CONTRATADA deve informar imediatamente o CONTRATANTE quando houver desligamento de algum usuário da empresa cadastrado no Service Desk, para inativação de seu acesso.
2.15.7. O Sistema Service Desk do CONTRATANTE estará disponível para uso da CONTRATADA em regime de 24 horas por dia, 07 dias da semana, podendo sofrer paradas para manutenção.
2.15.8. Se algum usuário da empresa ficar 60 dias sem acessar a ferramenta, seu cadastro será automaticamente inativado e ele perderá acesso.
2.15.9. A CONTRATADA deve prever o desenvolvimento do meio de integração com o Sistema Service Desk do CONTRATANTE dentro de regras já definidas e padronizadas, caso opte por também monitorar os Incidentes, Requisições de Serviço e Ocorrências sob sua responsabilidade através de ferramenta própria.
2.15.10. No momento que um Incidente, Requisição de Serviço ou Ocorrência for registrado, o Sistema Service Desk do CONTRATANTE enviará, automaticamente, uma notificação via e-mail para a CONTRATADA, alertando que um novo ticket foi direcionado para a empresa.
2.15.11. A notificação enviada segue um modelo padrão para todas as empresas externas; não serão feitas customizações.
2.15.12. A CONTRATADA deve registrar a solução do Incidente, Requisição de Serviço ou Ocorrência no Sistema Service Desk do CONTRATANTE imediatamente após executada, descrevendo a ação efetuada para normalizar a operacionalização do objeto contratado ou atender à requisição.
2.15.13. Após a resolução do Incidente, Requisição de Serviço ou Ocorrência pela CONTRATADA, o CONTRATANTE terá um prazo de 02 (dois) dias úteis para reabrir o chamado, caso identifique que a mesma falha voltou a ocorrer ou que a requisição não foi atendida adequadamente.

2.16. MÉTODO DE CONTROLE DE SLA

2.16.1. A CONTRATANTE estabelece que o método de controle de SLA será baseado em tickets de atendimento. Os prazos de atendimento e solução, respeitado o horário de atendimento, serão contados a partir da data/hora de transferência do ticket à CONTRATADA oriundo da ferramenta de Service Desk do CONTRATANTE; até a data/hora registrada na ferramenta de Service Desk do CONTRATANTE pela CONTRATADA.
2.16.2. A cobertura dos serviços será integral, ou seja, 24 (vinte e quatro) horas por dia, nos 7 (sete) dias da semana, incluindo sábados, domingos, feriados e pontos facultativos. Caso a ferramenta Service Desk não esteja disponível ou não seja possível efetuar a abertura do ticket junto ao Service Desk, a abertura do chamado técnico ou solicitação de serviço será realizada através de chamado telefônico DDG (0800) da CONTRATADA, sendo registrado posteriormente com uso de evidências telefônicas.
2.16.3. Os tickets de atendimento obedecerão às regras de Níveis de Serviço a seguir:

TIPOS DE SOLUÇÃO	**DESCRIÇÃO**
Solução de Contorno	Compreende a solução dada pela CONTRATADA que permita a continuidade operacional do objeto contratado, mesmo que não

	sejam utilizadas peças / configurações advindas do projeto original, podendo esta solução ser também definitiva se assim for aceito formalmente pelo CONTRATANTE.
Solução de Definitiva	Compreende a solução dada pela CONTRATADA que permita a continuidade operacional do objeto contratado, restabelecendo os serviços prestados de acordo com o projeto original.

2.16.4. Os tempos das soluções serão medidos desde o registro ou transferência até a solução do ticket na ferramenta Service Desk da CONTRATANTE. Cada um dos tickets de atendimento (Incidente, Requisição ou Ocorrência) levará em consideração o cenário da Falha, Ocorrência ou Circunstância, conforme abaixo classificado:

Perfil	Cenário	Tempo máximo de reparo (H)
Ações corretivas (Incidentes)	Com parada do negócio - Rede de produção ou aplicação crítica parada ou seriamente degradada em função de falha na solução, causando impacto crítico ou significante nas operações do negócio do CONTRATANTE.	2 horas corridas
	Sem parada do negócio - Rede de produção ou aplicação operando em contingência (Standby) devido a falha em parte da solução, sem qualquer impacto crítico ou significante nas operações do negócio do CONTRATANTE.	6 horas corridas
Ações preventivas (Requisições de Serviços)	Solicitação de avaliação técnica, instalações, atualizações de hardware/software, assistência para configurações, informações gerais sobre produtos, implementação de melhoria, atualização de documentações.	48 horas corridas, podendo ser estendido a critério do contratante.

2.16.5. Os atendimentos, e consequentemente os respectivos prazos do Acordo de Níveis de Serviço poderão ser paralisados nas seguintes situações:

2.16.5.1. Quando a CONTRATADA depender de informações e/ou recursos, por parte da CONTRATANTE, que inviabilizem a execução do atendimento;

2.16.5.2. Quando a ocorrência depender de retorno de informações da CONTRATADA mediante concordância da CONTRATANTE;

2.16.5.3. Quando a atendimento depender de agendamento para atendimento, onde fora acordada data/hora entre CONTRATADA e CONTRATANTE.

2.16.6. A pausa e retomada ocorre através da atualização do STATUS do ticket, exceto nos casos de agendamento em que a pausa ocorre quando preenchido campo DATA DE AGENDAMENTO na ferramenta de controle da CONTRATANTE. A retomada acontece automaticamente quando atingida a data/hora agendada.

2.16.7. Os status disponíveis para uso em Incidentes e Requisições, e que contemplam as situações acima citadas são: Aguardando Fornecedor, aguardando cliente/usuário, Agendado; Em Homologação (somente para requisições); Em atendimento, Encaminhado, Homologado (somente para requisições), Não homologado (somente para requisições) e Reaberto;

2.16.8. Pausas e retomadas de tempo de atendimento só ocorrem quando o tempo total do SLA acordado para o atendimento ainda não foi excedido.

2.16.9. É vedada a transferência do ticket, salvo para correção de encaminhamento.

2.16.10. A CONTRATADA poderá atualizar o ticket a qualquer tempo.

2.16.11. Após a resolução do ticket pela CONTRATADA, a CONTRATANTE terá um prazo de 02 (dois) dias úteis para reabrir o ticket. Essa reabertura do ticket será considerada como

continuação do atendimento anterior, ou seja, a contagem do prazo de atendimento será retomada e não haverá ônus financeiro para a CONTRATANTE em decorrência de uma possível caracterização de nova demanda.

2.17. DA GARANTIA AO OBJETO

2.17.1. A CONTRATADA deverá conceder garantia do objeto de, no mínimo, 60 (sessenta) meses, contados da data da execução, considerando todas as obrigações previstas na Lei nº 8.078/1990 – Código de Defesa do Consumidor – e alterações.

2.18. LOCAL DE ENTREGA / EXECUÇÃO

2.18.1. Os locais para prestação de serviços e entrega dos equipamentos, por padrão, concentram-se em dois endereços distintos:
2.18.1.1. DATACENTER DCCJ – Rua Caldas Junior, 120, 8º andar – Centro - Porto Alegre, RS – CEP 90018-900;
2.18.1.2. DATACENTER DCZS – Rua Eng. Ludolfo Boehl, 247 – Bairro: Teresópolis – CEP: 91720-150 - Porto Alegre/RS;
2.18.1.3. Eventualmente, serviços poderão ser realizados em outras unidades do CONTRATANTE na região metropolitana de Porto Alegre.
2.18.2. O recebimento dos equipamentos e serviços contratados pelo CONTRATANTE se efetivará por meio de termo de recebimento a ser emitido por representante do CONTRATANTE envolvido no projeto de aquisição e implementação.
2.18.3. Os Treinamentos Oficiais e Operacionais terão seu local ajustado entre o CONTRATANTE e a CONTRATADA.

2.19. OBRIGAÇÕES ESPECÍFICAS DA CONTRATADA

2.19.1. A CONTRATADA é a única responsável pelas ações realizadas por seus profissionais no ambiente do CONTRATANTE;
2.19.2. A CONTRATADA responderá por qualquer ação judicial, movida por profissional, referente ao atendimento do objeto deste contrato;
2.19.3. A CONTRATANTE estará à disposição da CONTRATADA para auxiliar, no caso de ocorrência citada acima;

2.20. PROCEDIMENTOS DE TRANSIÇÃO E ENCERRAMENTO CONTRATUAL

Um ano antes do vencimento e até a data do efetivo término do contrato, a critério do CONTRATANTE, poderá ser definida uma data para início, de forma gradual, da transferência ordenada dos serviços ao CONTRATANTE ou a seu designado e cancelamento dos serviços.

2.21. COMPUTAÇÃO EM NUVEM: Fica vedada à CONTRATADA manter ou utilizar, mesmo que parcialmente, infraestrutura de hardware e software baseada em serviços de processamento ou armazenamento de dados em nuvem, para prestação dos serviços objeto deste Contrato.

2.22. SUSTENTABILIDADE: A contratada deverá observar os seguintes critérios de sustentabilidade durante a execução do objeto:
2.22.1. A Contratada deverá, sempre que acionada pelo Contratante, receber os equipamentos ao final de sua vida útil, sem ônus ao Contratante, responsabilizando-se pelo descarte ambientalmente adequado dos mesmos, conforme a Lei 12.305/2010, que trata da Política Nacional de Resíduos Sólidos.
2.22.2. Os itens não poderão conter substâncias perigosas em concentração acima da recomendada na diretiva RoHS (Restriction of Certain Hazardous Substances), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr (VI)), cádmio (Cd), bifenilpolibromados (PBBs), éteres difenil-polibromados (PBDEs), conforme estabelece o art. 5º da Instrução Normativa 01/2010 da SLTI/MPOG.

2.22.3. As embalagens dos equipamentos deverão ser fabricadas com material reciclado, ou no caso de papelão das embalagens, quando não provenientes de material reciclado, deverão possuir certificação de origem florestal, tal como certificação FSC (Forest Stewardship Council), Cerflor ou similar, e serem recicláveis;
2.22.4. Os equipamentos deverão possuir a certificação de que trata a Portaria INMETRO nº 170, de 2012 ou certificação equivalente que deverá comprovar a segurança, compatibilidade eletromagnética e eficiência energética dos mesmos.

CLÁUSULA TERCEIRA – DO PREÇO –
3.1. O preço do presente ajuste é de R$ XXXX (XXXX), pago por medição, constante da Proposta e aceito pela CONTRATADA, entendido como justo e suficiente para a total execução do presente objeto.
3.2. No preço acordado, estão inclusos todos os tributos ou outros ônus federais, estaduais ou municipais.
3.3. Todas as despesas de transporte, hospedagem e alimentação dos técnicos responsáveis pela realização dos serviços contratados, correrão por conta exclusiva da CONTRATADA.

CLÁUSULA QUARTA – DO PAGAMENTO –
4.1. Os pagamentos estão organizados em atividades que possuem tarefas que podem ser conduzidas em conjunto como forma de otimização de prazos, dentro de uma cadência lógica de execução do projeto. Dessa forma cada atividade, após concluída, representa um ou mais percentuais dos valores constantes nos itens da PLANILHA DE ORÇAMENTOS.
4.2. Em virtude de vultuosidade, da complexidade e dos riscos envolvidos nesta contratação, os pagamentos serão efetuados de forma fracionada, somente após a entrega de cada atividade vinculada ao projeto.
4.3. Para cada atividade concluída, o CONTRATANTE fornecerá o referido termo de recebimento, conforme ANEXO 03 - TERMO DE RECEBIMENTO. Para algumas entregas dentro de cada atividade, poderá ser emitido um termo de recebimento específico.
4.4. Os pagamentos ocorrerão sempre até o dia 15 (quinze) do mês subsequente à prestação dos serviços/conclusão de cada etapa, conforme descrito a seguir:

4.4.1. Entrega da Atividade 1 - ABERTURA E PLANO DE PROJETO: 10% do Item 01 - “Gerenciamento do Projeto, Implementação da Solução e Treinamento Operacional” constante na Planilha de Orçamentos. Entregáveis da Etapa:
4.4.1.1. Reunião inicial do projeto;
4.4.1.2. Termo de Abertura do Projeto;
4.4.1.3. Plano de Gerenciamento de Projeto com EAP;
4.4.1.4. Plano de Projeto (Atividades do Escopo);
4.4.1.5. Cronograma;

4.4.2. Entrega da Atividade 2 - PLANEJAMENTO TÉCNICO PRELIMINAR E ENTREGA DOS EQUIPAMENTOS: 10% do Item 01 - “Gerenciamento do Projeto, Implementação da Solução e Treinamento Operacional”, 50% do Item 02 - “Hardware e Software da Solução, sem incluir os valores de licenciamento definitivo” constantes na Planilha de Orçamentos. Entregáveis da Etapa:
4.4.2.1. Projeto Lógico;
4.4.2.2. Plano de Migração com detalhamento de atividades para avaliação anterior à implementação do projeto;
4.4.2.3. Entrega dos Equipamentos, mediante fornecimento do ANEXO 03 - TERMO DE RECEBIMENTO pelo CONTRATANTE mencionando Entrega dos Equipamentos;

4.4.3. Entrega da Atividade 3 – GARANTIA DE HARDWARE E SOFTWARE E TREINAMENTOS OFICIAIS: 10% do Item 01 - “Gerenciamento do Projeto, Implementação da Solução e Treinamento Operacional” e 100% do Item 05 – “Treinamentos Oficiais” constantes na Planilha de Orçamentos. Entregáveis da Etapa:

4.4.3.1. Comprovação do registro da garantia contratada junto ao fabricante;
4.4.3.2. Conclusão dos Treinamentos Oficiais, mediante fornecimento do ANEXO 03 - TERMO DE RECEBIMENTO pelo CONTRATANTE mencionando a Entrega dos Treinamentos Oficiais;

4.4.4. Entrega da Atividade 4 – IMPLEMENTAÇÃO INICIAL DO PROJETO: 10% do Item 01 - "Gerenciamento do Projeto, Implementação da Solução e Treinamento Operacional", 10% do Item 02 - "Hardware e Software da Solução, sem incluir os valores de licenciamento definitivo", 40% do Item 3 - "Licenciamento Geral" e 40% do Item 4 - "Licenciamento por Assinatura ou Subscrição". Entregáveis da Etapa:
4.4.4.1. Configurações do Novo Ambiente (antes da migração);
4.4.4.2. Ativação dos Licenciamentos;

4.4.5. Entrega da Atividade 5 – MIGRAÇÃO PARA O NOVO AMBIENTE: 10% do Item 01 - "Gerenciamento do Projeto, Implementação da Solução e Treinamento Operacional", 20% do Item 02 - "Hardware e Software da Solução, sem incluir os valores de licenciamento definitivo", 50% do Item 3 - "Licenciamento Geral" e 50% do Item 4 - "Licenciamento por Assinatura ou Subscrição". Entregáveis da Etapa:
4.4.5.1. Migração dos ambientes existentes para a nova solução;

4.4.6. Entrega da Atividade 6 – SUPORTE/MANUTENÇÃO A HARDWARE E SOFTWARE E PROFISSIONAIS DEDICADOS À OPERAÇÃO ASSISTIDA: 20% do Item 01 - "Gerenciamento do Projeto, Implementação da Solução e Treinamento Operacional" e Início dos pagamentos mensais (pagamento mensal = montante do item/número de meses contratados) referentes ao Item 6 – "Suporte, Manutenção e Operação Assistida". Entregáveis da Etapa:
4.4.6.1. Início da vigência do suporte e manutenção a hardware e software (pós migração/projeto);
4.4.6.2. Início da vigência da operação assistida por profissionais dedicados;

4.4.7. Entrega da Atividade 7 – TESTES DE ACEITAÇÃO E TREINAMENTO OPERACIONAL: 20% do Item 01 - "Gerenciamento do Projeto, Implementação da Solução e Treinamento Operacional", 10% do Item 02 - "Hardware e Software da Solução, sem incluir os valores de licenciamento definitivo", 10% do Item 3 - "Licenciamento Geral" e 10% do Item 4 - "Licenciamento por Assinatura ou Subscrição". Entregáveis da Etapa:
4.4.7.1. Validação do funcionamento dos equipamentos;
4.4.7.2. Validação das configurações, operação e licenças habilitadas;
4.4.7.3. Finalização do Treinamento Operacional
4.4.7.4. Consolidado dos Termos de Recebimento/Conclusão de Atividade de todas as entregas realizadas;

4.4.8. Entrega da Atividade 8 – ENTREGA DA DOCUMENTAÇÃO TÉCNICA FINAL E ENCERRAMENTO DO PROJETO: 10% do Item 01 - "Gerenciamento do Projeto, Implementação da Solução e Treinamento Operacional" e 10% do Item 02 - "Hardware e Software da Solução, sem incluir os valores de licenciamento definitivo". Entregáveis da Etapa:
4.4.8.1. Entrega de toda documentação final conforme especificações técnicas (Inventário de Equipamentos, Manuais, Topologias, etc);
4.4.8.2. Termo de Encerramento de Projeto.

4.5. O valor acordado será pago por medição, até o dia 15 (quinze) do mês subsequente ao da prestação dos serviços, com o correspondente aceite do Gestor dos Serviços, por crédito em conta corrente mantida em qualquer das Agências do CONTRATANTE, em nome da CONTRATADA.
4.6. A respectiva nota fiscal/fatura/duplicata deverá ser apresentada na Unidade de Contratações e Pagadoria da CONTRATANTE, situada na Rua Caldas Júnior, nº 108, 5º andar, Bairro Centro, em Porto Alegre, RS, CEP 90018-900, ou ainda, através do correio eletrônico para

nf_contratos@banrisul.com.br, com antecedência mínima de cinco dias úteis.

4.7. A nota fiscal/fatura deverá vir acompanhada do documento comprobatório de realização dos serviços (Ficha de Atendimento e/ou Ordem de Serviço) visado pelo representante do CONTRATANTE e do respectivo arquivo ".xml", este último, apenas quando se tratar de nota fiscal eletrônica.

4.8. Quando se tratar de prestação de serviços e, neste caso, estão incluídas as personalizações de objetos, deverá ser apresentada nota fiscal de serviços, uma para cada serviço contratado.

4.9. Deverão constar, obrigatoriamente, no corpo da nota fiscal/fatura/duplicata, as seguintes informações:

I. Tipo de serviço;
II. N° do Contrato;
III. N° do CNPJ do CONTRATANTE ou de suas filiais, conforme indicado pelo próprio;
IV. N° da Inscrição Estadual do CONTRATANTE;
V. Data do vencimento;
VI. Competência (mês e ano da efetivação dos serviços).
VII. Descrição dos materiais e/ou mão-de-obra fornecidos.

4.10. A nota fiscal deverá ser obrigatoriamente da CONTRATADA e, nos casos em que a emissão for de outro estabelecimento da empresa, o documento também deverá vir acompanhado de autorização para crédito em conta corrente mantida no nome da CONTRATADA.

4.11. A não observância do disposto na presente cláusula quanto ao preenchimento da nota fiscal e apresentação dos documentos exigidos, implicará na devolução do documento e na recontagem do prazo de pagamento, que reiniciará a partir da nova protocolização, sem nenhum tipo de ônus financeiro para o CONTRATANTE.

4.12. A CONTRATADA, caso optante pelo SIMPLES (Regime Especial Unificado de Arrecadação de Tributos e Contribuições), deverá apresentar, juntamente com a nota fiscal/fatura, a devida declaração, conforme modelo constante do Anexo IV da IN RFB nº 1.234 de 11 de janeiro de 2012, (original, atualizada e com reconhecimento de firma), a fim de não sofrer retenção de Imposto de Renda e Contribuições Sociais, de acordo com a legislação vigente.

4.12.1. Para fins de enquadramento do ISS (Imposto Sobre Serviços) de acordo com o SIMPLES NACIONAL, quando a legislação municipal assim permitir, será exigido o faturamento dos últimos 12 (doze) meses junto à referida Declaração.

4.13. O CONTRATANTE poderá exigir outros documentos comprobatórios (declarações de isenções tributárias, certidões, obrigações tributárias, etc.), a seu critério, para liberação do pagamento.

4.14. A glosa do pagamento durante a execução contratual, sem prejuízo das sanções cabíveis, poderá ocorrer quando o Contratado:

I. Não produzir os resultados, deixar de executar, ou não executar as atividades com a qualidade mínima exigida no Contrato; ou
II. Deixar de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizá-los com qualidade ou quantidade inferior à demanda.

4.15. Nas hipóteses em que for necessário o cancelamento da nota fiscal emitida, o CONTRATANTE deverá ser comunicado imediatamente sobre o fato, para que sejam adotados os procedimentos cabíveis, desde que não tenha ocorrido o pagamento.

4.15.1. O cancelamento do documento fiscal após o pagamento e/ ou recolhimento dos tributos devidos, sujeitará a CONTRATADA ao ressarcimento destes impostos, bem como das multas e encargos imputados ao CONTRATANTE, em função das correções nas informações fiscais, previamente enviadas aos órgãos arrecadadores, sem prejuízo da aplicação das multas contratuais.

CLÁUSULA QUINTA – DA ATUALIZAÇÃO MONETÁRIA –

Os valores do presente contrato, não pagos na data do vencimento, poderão ser corrigidos desde então, até a data do efetivo pagamento, pela variação do IPCA (Índice de Preços ao Consumidor Amplo), apurado pelo Instituto Brasileiro de Geografia e Estatística (IBGE), ou outro índice que vier a ser designado em sua substituição.

CLÁUSULA SEXTA – DO REAJUSTE –

Após a periodicidade de um ano, o preço do presente Contrato poderá ser reajustado anualmente, pela variação do IPCA (Índice de Preços ao Consumidor Amplo), apurado pelo Instituto Brasileiro de Geografia e Estatística (IBGE), ou outro índice que vier a ser designado em sua substituição.

CLÁUSULA SÉTIMA – DA VIGÊNCIA –

7.1. O prazo de vigência da contratação será de 60 (sessenta) meses, a contar de XX/XX/XXXX, podendo sua duração ser prorrogada, nos termos do que dispõe a Lei Federal 13.303/2016 e o Regulamento de Licitações e Contratos do Banrisul.

CLÁUSULA OITAVA – DOS DIREITOS E DAS OBRIGAÇÕES –

8.1. DOS DIREITOS:

Constituem direitos de o CONTRATANTE receber o objeto deste Contrato nas condições avençadas e da CONTRATADA perceber o valor ajustado na forma e no prazo convencionados.

8.2. DAS OBRIGAÇÕES:

8.2.1. Constituem obrigações do CONTRATANTE:

I. Efetuar o pagamento ajustado;

II. Dar à CONTRATADA as condições necessárias à execução do Contrato;

III. Designar formalmente um representante para fiscalizar e acompanhar o cumprimento do presente Contrato;

IV. Examinar a documentação exigida na contratação, verificando o integral cumprimento das obrigações trabalhistas e previdenciárias;

V. Efetuar as retenções tributárias devidas sobre o valor da fatura de serviços do contratado, nos termos da legislação vigente.

8.2.2. Constituem obrigações da CONTRATADA:

I. Prestar o serviço na forma ajustada;

II. Fornecer as ferramentas e materiais necessários à prestação dos serviços, responsabilizando-se pela perfeita execução;

III. Assumir inteira responsabilidade pelas obrigações sociais e trabalhistas relativamente aos seus empregados, correndo todas as obrigações e ônus de empregador por sua conta e, consequentemente, o pagamento das contribuições exigidas pela Previdência Social, seguro contra acidentes do trabalho e demais encargos da legislação vigente;

IV. Manter, durante toda a execução do Contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na contratação;

V. Apresentar, durante a execução do Contrato, quando solicitado, documentos que comprovem estar cumprindo a legislação em vigor quanto às obrigações assumidas na licitação e, em especial, encargos sociais, trabalhistas, previdenciários, tributários, fiscais e comerciais.

VI. Assumir inteira responsabilidade pelas obrigações fiscais decorrentes da execução do presente Contrato;

VII. Disponibilizar e informar ao CONTRATANTE, no ato da assinatura deste instrumento, o seu endereço eletrônico na Internet (e-mail), para o recebimento e envio de mensagens, relatórios gerenciais, planilhas, etc., o qual se estabelecerá como principal canal de comunicação entre as partes, especialmente no trato das demandas diárias;

VIII. Orientar seus empregados a manter sigilo absoluto quanto às informações contidas nos documentos ou materiais por ele manipulados ou acessados, dedicando especial atenção à sua guarda, arrumação ou descarte, quando for o caso;

IX. Fornecer pessoas especializadas para a execução dos serviços, devidamente identificadas, mantendo toda a documentação exigida pela legislação vigente;

X. Atender, imediatamente, solicitação de substituição de funcionário cuja atuação, permanência ou comportamento sejam julgados, pelo CONTRATANTE, prejudiciais, inadequados, inconvenientes ou insatisfatórios para a prestação dos serviços, sem que lhe assista qualquer direito ou reclamação;

XI. Responder por todo e qualquer dano que causar ao CONTRATANTE ou a terceiros praticado por seus prepostos, empregados ou mandatários, inclusive os de decisões judiciais, assegurando ao CONTRATANTE o direito de regresso, eximindo o Contratante de qualquer solidariedade ou responsabilidade;

XII. Identificar os empregados que executarão tarefas nas dependências do CONTRATANTE, mediante o alcance da relação nominal, qual contenha o(s) número(s) da(s) cédula(s) de identidade, uso de uniforme e crachá;
XIII. Dar imediato conhecimento, ao CONTRATANTE, de autuações ou notificações porventura lavradas pela fiscalização em geral, bem como erros e omissões, relativas aos serviços ou obras sob sua responsabilidade técnica ou fiscalização;
XIV. Corrigir gratuitamente os serviços que apresentem incorreção, imperfeição, sem prejuízo das multas contratuais;
XV. Não interromper a execução dos serviços sob alegação de inadimplemento por parte do Contratante, salvo nos casos previstos em lei;
XVI. A CONTRATADA deverá manter atualizado seu cadastro junto ao CONTRATANTE durante toda a execução do contrato, inclusive dados de contato como endereço, telefone, e-mail e dados completos do representante legal.
XVII. A atualização cadastral abrange a necessidade de comunicação de eventuais alterações como modificação do capital social, alteração do objeto social e/ou atividades, alteração da razão social, nome fantasia e/ou quadro societário, num prazo de até 10 (dez) dias do evento, devidamente acompanhado de documentação comprobatória.
XVIII. Cumprir e fazer cumprir todas as normas regulamentares sobre Medicina e Segurança do Trabalho, especialmente as normas NR-6 (uso de equipamentos de proteção individual), NR-8 (edificações), NR-10 (instalações e serviços de eletricidade) e NR-18 (obras de construção, demolição e reparos) da Portaria nº 3.214/78, aplicáveis aos empregados por ela contratados;
XIX. O atendimento e concordância à Resolução nº 4.557/17 do CMN, permitindo o acesso do Banco Central do Brasil a termos firmados, documentação e informações referentes aos serviços prestado e às dependências da CONTRATADA.

CLÁUSULA NONA – DA INDENIZAÇÃO –
Em decorrência das obrigações aqui assumidas, a CONTRATADA assume o compromisso de indenizar o CONTRATANTE por quaisquer importâncias que este seja compelido a desembolsar em favor dos empregados dela, seja a que título for, inclusive em se tratando de reclamatória trabalhista, promovida em função do presente ajuste.

CLÁUSULA DÉCIMA – DA RESPONSABILIDADE CIVIL –
10.1. A CONTRATADA assume exclusivamente a responsabilidade civil pelos atos praticados por seus empregados, quando na execução dos serviços contratados, e pelo atendimento às normas e regulamentos que disciplinam as atividades em foco.
10.2. A CONTRATADA assume a responsabilidade por eventuais danos causados por seus prepostos e empregados a bens ou pessoas.
10.3. A CONTRATADA responsabiliza-se, perante o CONTRATANTE, pela idoneidade das pessoas designadas aos serviços contratados.
10.4. As partes acordam que ao CONTRATANTE não cabe responsabilidade alguma em caso de ferimentos, seja de que natureza for, incapacidade parcial ou total, temporária, permanente ou morte de qualquer dos empregados da CONTRATADA designados à execução dos serviços contratados.

CLÁUSULA DÉCIMA PRIMEIRA – DA UTILIZAÇÃO DO CONTRATO COMO GARANTIA –
É vedado à CONTRATADA caucionar ou utilizar o presente Contrato como garantia para qualquer operação financeira.

CLÁUSULA DÉCIMA SEGUNDA – DA CONFIDENCIALIDADE –
12.1. A CONTRATADA garante manter sigilo sobre quaisquer dados, informações, documentos e especificações que sejam confiados ou que venham a ter acesso em razão dos serviços prestados, não podendo, sob qualquer pretexto, revelá-los, divulgá-los, reproduzi-los ou deles dar conhecimento a pessoas não formalmente autorizadas pelo CONTRATANTE, obedecendo ao TERMO DE CONFIDENCIALIDADE E SIGILO que é parte integrante deste instrumento e que será assinado pelo representante legal no ato da assinatura do presente Contrato.
12.2. O não cumprimento das cláusulas que tratam de Segurança da Informação e Sigilo, bem

como o TERMO DE CONFIDENCIALIDADE E SIGILO será considerado falta gravíssima.
12.3. A CONTRATADA garante que orientará seus agentes, representantes, especialistas, prestadores de serviço (internos ou externos), empregados, bem como todos aqueles autorizados formalmente a transmitir ou receber informações a seguirem as normas de Segurança da Informação estabelecidas pelo CONTRATANTE e a manter sigilo absoluto quanto às informações contidas nos documentos e materiais por eles manipulados ou acessados, dedicando especial atenção à sua guarda, arrumação ou descarte, quando for o caso.
12.4. A CONTRATADA deverá disponibilizar ao CONTRATANTE, sempre que solicitado, TERMO DE RESPONSABILIDADE E DE MANUTENÇÃO DE SIGILO, devidamente assinado por todos os seus agentes, representantes, especialistas, prestadores de serviços (internos ou externos), empregados, bem como todos aqueles autorizados formalmente a transmitir ou receber informações, que prestem serviços ao CONTRATANTE.
12.5. O CONTRATANTE poderá realizar auditorias em caso de fundada suspeita de descumprimento contratual e mediante notificação exclusivamente no ambiente do CONTRATANTE onde os serviços são desenvolvidos e com relação aos equipamentos nele existentes relacionados à execução do presente Contrato, de forma a se certificar do cumprimento das disposições de segurança e confidencialidade.

CLÁUSULA DÉCIMA TERCEIRA – DA CESSÃO E SUBCONTRATAÇÃO DO CONTRATO –
13.1. É proibida a cessão ou transferência total deste Contrato. A critério do CONTRATANTE poderá ser permitida a subcontratação parcial para o atendimento de necessidade específica que se verifique durante a execução dos serviços observado o seguinte:
I. Em caso de subcontratação, não será estabelecido qualquer vínculo entre o CONTRATANTE e a subcontratada, permanecendo a CONTRATADA responsável pelo integral cumprimento das obrigações estabelecidas neste instrumento;
II. A CONTRATADA deverá informar previamente ao CONTRANTE a subcontratação a ser realizada no curso da vigência deste Contrato, bem como qualquer substituição de subcontratado;
III. A CONTRATADA deverá diligenciar para a escolha de subcontratados que viabilizem o cumprimento das exigências estipuladas neste Contrato e respectivos anexos, devendo substituir qualquer subcontratado que impeça, dificulte ou prejudique a prestação dos serviços;
IV. A CONTRATADA se obriga a inserir, no Contrato de prestação de serviços que vier a celebrar com sua eventual subcontratada, cláusula estabelecendo responsabilidade solidária em relação à execução do serviço subcontratado.
13.2. Será permitida a subcontratação no que se refere à prestação de serviços de Operação Assistida e Treinamentos Oficiais, desde que a empresa subcontratada seja especificada e identificada na contratação, e considerado que seja apresentada a documentação necessária definida em Lei, no momento da contratação.
13.3. Para análise da empresa para a qual eventualmente for proposta a subcontratação relacionada acima, será exigida, anteriormente à manifestação do CONTRATANTE, a regularidade fiscal e jurídica, nos mesmos limites exigidos da licitante no item que trata de habilitação.
13.4. O CONTRATANTE verificará a regularidade da subcontratada em relação aos impedimentos de licitar e contratar, não sendo admitida a subcontratação no caso de impedimento.
13.5. No caso de subcontratação de outra empresa, a CONTRATADA não transferirá suas obrigações e responsabilidades, permanecendo, perante o CONTRATANTE, com total responsabilidade contratual.
13.6. Deve ser respeitado o limite máximo de 30% (trinta por cento) de subcontratação total em relação ao valor global contratado.
13.7. Para efeito de cálculo da subcontratação total em relação ao valor global contratado, serão somados/considerados mensalmente, a partir do início da prestação dos serviços por parte da(s) empresa(s) subcontratada(s):
I. Valores de eventuais pagamentos pelo CONTRATANTE relativos aos serviços subcontratados, os quais devem ser discriminados para fins de comprovação de respeito ao limite máximo de 30% (trinta por cento).
II. Os valores propostos, as regras contratuais relacionadas à forma de execução e aos prazos de solução e atendimento dos chamados não sofrerão quaisquer alterações em função da eventual

subcontratação destes serviços, nem tão pouco as obrigações e responsabilidades contratuais, que permanecerão com a CONTRATADA, respondendo está por quaisquer problemas ou irregularidades detectadas na execução dos serviços perante o CONTRATANTE.

13.8. Em caso de haver subcontratação de empresa, por parte da CONTRATADA, para realização de algum serviço integrante do objeto da presente contratação, aplicam-se à subcontratada as mesmas obrigações de confidencialidade exigidas neste instrumento, devendo ser firmado termo de sigilo e confidencialidade entre a CONTRATADA e a empresa subcontratada, que garanta a proteção das informações confidenciais do CONTRATANTE.

13.9. Cópia do termo de sigilo e confidencialidade firmado entre CONTRATADA e subcontratada poderá ser solicitado pelo CONTRATANTE a qualquer tempo, e quando houver esta solicitação, deve ser remetido de imediato pela CONTRATADA.

13.10. O CONTRATANTE pode, a qualquer tempo, solicitar outras informações sobre a empresa subcontratada que vier a realizar qualquer serviço integrante do presente objeto, em nome da CONTRATADA.

13.11. A CONTRATADA será solidariamente responsável pelos atos praticados por terceiros, por ela contratados, que tenham contato com informações confidenciais do CONTRATANTE.

CLÁUSULA DÉCIMA QUARTA – DAS ALTERAÇÕES –

14.1. Eventuais alterações contratuais reger-se-ão pela disciplina do art. 81 da Lei federal nº 13.303 de 30 de junho de 2016.

14.2. Poderão ser motivos para alterações contratuais, dentre outros:

I. Alteração dos prazos de início de etapas de execução, de conclusão e de entrega;

II. Superveniência de fato excepcional ou imprevisível, estranho à vontade das partes, que altere fundamentalmente as condições de execução do Contrato;

III. Aumento ou diminuição das quantidades inicialmente previstas no Contrato, nos limites permitidos pela Lei 13.303/2016; e,

IV. Modificação do projeto ou das especificações, para melhor adequação técnica aos objetivos.

14.3. As alterações deverão ser justificadas por escrito, previamente autorizadas pela autoridade competente e formalizadas mediante aditivo contratual.

CLAUSULA DÉCIMA QUINTA – DA UTILIZAÇÃO DO NOME DO CONTRATANTE –

A CONTRATADA não poderá utilizar o nome do CONTRATANTE, ou sua qualidade de CONTRATADA em quaisquer atividades de divulgação profissional como, por exemplo, em cartões de visita, anúncios diversos, impressos, etc., nem tampouco pronunciar-se em nome do CONTRATANTE à imprensa em geral sobre quaisquer assuntos relativos à atividade deste, bem como sua atividade profissional, sob pena de rescisão contratual, sem prejuízo das demais penalidades cabíveis.

CLÁUSULA DÉCIMA SEXTA – DAS PENALIDADES E MULTAS –

16.1. Serão aplicadas as seguintes sanções pelo não cumprimento de quaisquer das obrigações do presente Contrato à CONTRATADA, sem prejuízo de sua responsabilidade civil e da rescisão do mesmo, se for o caso:

16.1.1. Advertência, por escrito, sempre que ocorrerem pequenas irregularidades, para as quais haja concorrido;

16.1.2. Multa(s):

I. Afora as penalidades dispostas na presente cláusula, demais sanções estão previstas na Tabela de Sanções e Multas anexa ao presente documento;

II. **de 0,2% (dois décimos por cento)**, calculado sobre o valor total do Contrato, por dia de atraso, até o limite de 10% (dez por cento) do valor total do Contrato, pela inobservância do prazo fixado para apresentação da garantia, sem prejuízo da necessidade de apresentação da mesma;

III. **de 5% (cinco por cento) sobre o valor total atualizado do contrato,** no caso de descumprimento de cláusula contratual que não elencados nas hipóteses dos incisos anteriores, norma de legislação pertinente, execução imperfeita ou em desacordo com as especificações e/ou negligência na execução dos serviços contratados;

IV. de 10% (dez por cento), sobre o valor total atualizado da Contratação, quando ocorrer reincidência no cometimento de falta pela qual já houver sido a CONTRATADA advertida e/ou multada. Esta multa poderá ser aplicada independentemente da multa pelo atraso na entrega.
V. de 15% (quinze por cento), sobre o valor total atualizado da Contratação, no caso de descumprimento ou inexecução contratual parcial;
VI. de 30% (trinta por cento) sobre o valor total atualizado da contratação, no caso de descumprimento ou inexecução contratual total, desistência ou abandono da execução da contratação.
16.1.3. Suspensão do direito de licitar e contratar com o CONTRATANTE, pelo prazo de até dois anos, sem prejuízo do CONTRATANTE considerar rescindido este vínculo obrigacional e/ou adotar as demais medidas legais e judiciais cabíveis, quando ocorrer:
I. Apresentação de documentos falsos ou falsificados;
II. Reincidência de execução insatisfatória dos serviços contratados, acarretando prejuízos ao CONTRATANTE;
III. Atraso injustificado na execução dos serviços e retardamento na execução do Contrato, contrariando o disposto neste Contrato;
III.1. Configurar-se-á o retardamento da execução quando o contratado:
a) Deixar de iniciar, sem causa justificada, a execução do Contrato após 7 (sete) dias contados da data da ordem de serviço;
b) Deixar de realizar, sem causa justificada, os serviços definidos no Contrato por 3 (três) dias seguidos ou por 10 (dez) dias intercalados.
c) A falha na execução do Contrato estará configurada quando o contratado descumprir as obrigações e cláusulas contratuais, cuja dosimetria será aferida pela autoridade competente, de acordo com o que preceitua o subitem Multa(s) desta cláusula.
IV. Reincidência na aplicação das penalidades de advertência ou multa;
V. Irregularidades que ensejam a rescisão contratual;
VI. Ação no intuito de tumultuar a execução do Contrato;
VII. Práticas de atos ilícitos, demonstrando não possuir idoneidade para licitar ou contratar com a administração pública;
VIII. Condenação definitiva por praticar fraude fiscal no recolhimento de quaisquer tributos.
16.2. As multas mencionadas nesta cláusula são, individualmente, limitadas a 30% (trinta por cento) do valor da base de cálculo de sua incidência, por ocorrência, sem prejuízo da cumulação de multas, limitadas a 30% (trinta por cento) do valor total do Contrato.
16.3. A(s) multa(s) aplicadas(s) à CONTRATADA e os prejuízos por ela causados ao CONTRATANTE serão deduzidos de qualquer crédito devido à CONTRATADA ou serão cobrados judicialmente.
16.4. A(s) penalidade(s) de multa(s) não terá(ão) caráter compensatório, podendo ser aplicada cumulativamente com as demais sanções e a sua cobrança não tem intuito indenizatório, não isentando a CONTRATADA da obrigação de indenizar eventuais perdas e danos.
16.5. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.
16.6. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa, observando-se o procedimento previsto na Lei federal nº 13.303 de 30 de junho de 2016 e regulamento próprio do CONTRATANTE.
16.7. As sanções previstas nesta Cláusula não elidem a aplicação das penalidades estabelecidas na Lei Federal nº 12.846/2013, conforme o disposto no seu art. 30.

CLÁUSULA DÉCIMA SÉTIMA – DA RESCISÃO –
17.1. O presente Contrato poderá ser rescindido em caso de inadimplemento contratual de qualquer das partes contratantes, como nos exemplos citados abaixo, mas não se restringindo:Inexecução total do Contrato;
II. Execução imperfeita ou em desacordo com as especificações e/ou negligência na execução dos serviços contratados;
III. Não cumprimento de cláusulas contratuais, especificações, projetos ou prazos;

IV. Lentidão do seu cumprimento, levando a comprovar a impossibilidade da conclusão da obra, do serviço ou do fornecimento, nos prazos estipulados;
V. Atraso injustificado no início da obra, serviço ou fornecimento;
VI. Paralisação da obra, do serviço ou do fornecimento, sem justa causa e prévia comunicação;
VII. Subcontratação total ou parcial do seu objeto, a associação do contratado com outrem, a cessão ou transferência, total ou parcial, bem como a fusão, cisão ou incorporação, não admitidas no edital ou no Contrato;
VIII. Desatendimento das determinações regulares do CONTRATANTE decorrentes do acompanhamento e fiscalização do Contrato;
IX. Decretação de falência ou a instauração de insolvência civil;
X. Dissolução da sociedade ou o falecimento do contratado;
XI. Alteração social ou a modificação da finalidade ou da estrutura da empresa, que prejudique a execução do Contrato;
Ocorrência de caso fortuito ou de força maior, regularmente comprovada, impeditiva da execução do Contrato.
1.2.1. No caso de rescisão motivada por inadimplemento contratual previsto acima, a mesma será realizada com base na instauração de Processo Administrativo formal, no qual será oportunizado a ampla defesa ao contraditório.
1.3. O presente Contrato também poderá ser rescindido por acordo entre as partes, reduzido a termo no processo, desde que haja conveniência para CONTRATANTE e CONTRATADA.
1.4. O presente Contrato deverá ser rescindido em caso de determinação judicial.
1.5. O presente Contrato também poderá ser rescindido caso alguma das partes tenha interesse na rescisão contratual antecipada, devendo esta parte informar a outra com no mínimo 120 (cento e vinte) dias de antecedência.

CLÁUSULA DÉCIMA OITAVA – DA GARANTIA –
18.1. A CONTRATADA dá e se obriga a manter, durante toda a vigência do Contrato, garantia por uma das modalidades previstas no artigo 70, da Lei 13.303/2016, no valor equivalente a 5% (cinco por cento) do preço global contratado, devendo apresentar o respectivo comprovante em até 10 (dez) dias úteis, prorrogáveis por igual período, a critério do CONTRATANTE, contados da data de assinatura deste Contrato, sob pena de rescisão contratual e sanções administrativas cabíveis.
18.1.1. Nos contratos de serviço continuado com prazo de vigência superior a 12 meses (excluídos contratações por escopo ou empreitada), caso a CONTRATADA opte por garantia na modalidade **CAUÇÃO EM DINHEIRO**, a mesma poderá ser proporcionalizada para ao valor anual estimado do contrato. Devendo sempre ser mantida em valor compatível ao total anual do mesmo.
18.2. MODALIDADES DE SEGURO
I. NO CASO DE CAUÇÃO EM DINHEIRO:
a) O valor depositado em caução será administrado pelo CONTRATANTE e devolvido à CONTRATADA, até 03 (três) meses decorridos do término do Contrato ou da sua rescisão, desde que adimplidas todas as obrigações contratuais, trabalhistas, previdenciárias e fiscais;
b) O CONTRATANTE utilizará, a qualquer tempo, no todo ou em parte, o valor da garantia para cobrir os prejuízos eventualmente apurados, decorrentes do descumprimento de qualquer obrigação contratual ou falha dos serviços contratados, inclusive os motivados por greves ou atos dos empregados da CONTRATADA;
c) Utilizada a garantia, a CONTRATADA fica obrigada a reintegralizá-la no prazo de 10 (dez) dias úteis contados da data que for notificada formalmente pelo CONTRATANTE, sob pena de rescisão contratual;
d) O valor atualizado da garantia será devolvido à CONTRATADA, desde que a CONTRATADA não possua dívida com o CONTRATANTE e mediante expressa autorização deste.
II. NO CASO DE SEGURO GARANTIA:
a) O CONTRATANTE deverá ser indicado como beneficiário do seguro garantia;
b) A CONTRATADA obriga-se a apresentar a nova apólice em até 10 (dez) dias úteis após o vencimento da anterior e a comprovar o pagamento do prêmio respectivo em até dois dias úteis após o seu vencimento;

c) O descumprimento das obrigações previstas nos itens I e II, acima, constitui motivo para rescisão contratual;
d) O prazo de cobertura da apólice deverá abranger o período do Contrato, acrescido de 03 (três) meses;
III. NO CASO DE FIANÇA BANCÁRIA, deverá constar, no instrumento de fiança bancária:
a) Prazo de validade correspondente ao período de vigência deste Contrato, acrescido de 03 (três) meses;
b) Expressa afirmação do fiador de que, como devedor solidário e principal pagador, fará o pagamento, ao CONTRATANTE, dos prejuízos por este sofridos em razão do descumprimento das obrigações da CONTRATADA, independentemente de interpelação judicial;
c) Expressa renúncia do fiador ao benefício de ordem e aos direitos previstos nos artigos 827, 835 e 838 do Código Civil Brasileiro;
d) Cláusula que assegure a atualização do valor afiançado.
18.2.1. A garantia, qualquer que seja a modalidade escolhida, assegurará o pagamento de:
I. Prejuízos advindos do não cumprimento do objeto contratado e do inadimplemento das demais obrigações nele previstas;
II. Prejuízos causados ao CONTRATANTE ou a terceiro, decorrentes de culpa ou dolo durante a execução do Contrato;
III. Multas moratórias e punitivas aplicadas pelo CONTRATANTE à CONTRATADA;
IV. Obrigações trabalhistas, fiscais e previdenciárias de qualquer natureza, não adimplidas pela CONTRATADA.
18.3. A perda da garantia em favor do CONTRATANTE, por inadimplemento das obrigações contratuais, far-se-á de pleno direito, independentemente de qualquer procedimento judicial ou extrajudicial, sem prejuízo das demais sanções previstas no Contrato.
18.4. O garantidor não é parte interessada para figurar em processo administrativo instaurado pelo CONTRATANTE com o objetivo de apurar prejuízos e/ou aplicar sanções à CONTRATADA.
18.5. A garantia será considerada extinta com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia.
18.6. A garantia prevista nesta cláusula, somente será liberada ante a comprovação de que a CONTRATADA pagou todas as verbas rescisórias trabalhistas decorrentes da contratação, ou ainda, de que os empregados serão realocados em outra atividade de prestação de serviços, sem que ocorra a interrupção do Contrato. Caso tais comprovações não sejam apresentadas até o fim do segundo mês após o encerramento da vigência contratual, a garantia será utilizada para o pagamento dessas verbas trabalhistas diretamente pelo CONTRATANTE.
18.7. O atraso superior a 25 (vinte e cinco) dias para apresentação da garantia, autoriza o CONTRATANTE a promover a rescisão do contrato por descumprimento ou cumprimento irregular de suas obrigações, sem prejuízo da aplicação de multas, e a retenção do valor da garantia dos pagamentos eventualmente devidos pelo Contratante à Contratada, até que a garantia seja apresentada.
18.8. Não serão aceitas garantias que incluam outras isenções de responsabilidade que não as previstas nesta Cláusula.
18.9. Caso o pagamento de todas as obrigações trabalhistas e previdenciárias decorrentes da contratação não seja comprovado até o fim do segundo mês após o encerramento da vigência do Contrato, a garantia será utilizada para o pagamento dessas verbas.

CLÁUSULA DÉCIMA NONA – DA PROTEÇÃO DE DADOS PESSOAIS

19.1. As partes comprometem-se a observar e cumprir com os preceitos previstos na Lei 13.709/2018 (Lei Geral de Proteção de Dados).
19.2. Cada Parte é exclusivamente responsável pelo tratamento de dados que realizar no contexto deste Contrato, sendo que a responsabilidade entre as partes é limitada aos danos efetivamente sofridos.

CLÁUSULA VIGÉSIMA – DA MATRIZ DE RISCOS –

20.1. As Partes, tendo como premissa a obtenção do melhor custo contratual mediante a alocação do risco à parte com maior capacidade para geri-lo e absorvê-lo, identificam os riscos decorrentes

da relação contratual e, sem prejuízo de outras previsões contratuais, estabelecem os respectivos responsáveis na Matriz de Riscos anexa a este instrumento.
20.2. É vedada a celebração de aditivos decorrentes de eventos supervenientes alocados, na Matriz de Riscos, como de responsabilidade da Contratada.

CLÁUSULA VIGÉSIMA PRIMEIRA – DAS CONDIÇÕES GERAIS –
21.1. Qualquer modificação na rotina dos serviços deverá ser comunicada com antecedência mínima de setenta e duas horas e a expressa anuência da outra parte.
21.2. Qualquer tolerância ou concessão do CONTRATANTE ou da CONTRATADA, não constituem novações ou precedentes invocáveis por qualquer das partes.
21.3. Os casos fortuitos ou de força maior, previstos no artigo 393, parágrafo único, do Código Civil Brasileiro não constituem inadimplência.
21.4. Nos casos em que a CONTRATADA não comprovar o pagamento dos direitos trabalhistas e previdenciários dos empregados envolvidos na prestação dos serviços, o CONTRATANTE poderá utilizar os valores das faturas ou ainda da garantia apresentada pela CONTRATADA para realizar o pagamento diretamente aos trabalhadores.
21.5. As partes comprometem-se a observar os preceitos legais instituídos pelo ordenamento jurídico brasileiro no que tange ao combate à corrupção, em especial a Lei nº 12.846/2013.
21.6. A CONTRATADA declara, estar ciente acerca dos dispositivos contidos na Lei nº 12.846/2013 e se obriga a tomar todas as providências para fazer com que seus administradores, funcionários e representantes tomem ciência quanto ao teor da mencionada Lei.
21.7. As Partes declaram, sob as penas da Lei, que os signatários do presente instrumento são seus bastantes representantes/procuradores legais, devidamente constituídos na forma dos respectivos Estatutos/Contratos Sociais, com deveres para assumir as obrigações ora pactuadas.
21.8. As Partes reconhecem que o presente instrumento foi elaborado dentro dos mais rígidos princípios da boa-fé e da probidade, sendo fruto do mútuo consentimento expresso em cláusulas que atendem plenamente os seus recíprocos interesses comerciais. Declaram, outrossim, que leram e compreenderam integralmente o conteúdo avençado, tendo sido exercida em toda sua plenitude a autonomia da vontade das partes, reconhecendo que o presente ajuste é equânime e livre de ambiguidades e contradições.
21.9. Fica, desde já, convencionado, que caso haja alguma divergência entre as cláusulas do presente Contrato e as condições estabelecidas nos Anexos que o integram, serão consideradas como preponderantes as condições e disposições constantes neste Contrato. Em caso de dúvidas e divergências entre os Anexos, prevalecerá sempre o mais recente.
21.10. Qualquer comunicação pertinente ao contrato, a ser realizada entre Contratante e Contratada, inclusive para manifestar-se, oferecer defesa ou receber ciência de decisão sancionatória ou sobre rescisão contratual, deve ocorrer por e-mail, conforme informação a seguir:
a) E-mail da Contratada: XXXXXXXXXXXXX
21.10.1. A Contratada deve receber as comunicações referidas no caput desta cláusula pelo e-mail informado, declarando que se obrigam a verificá-lo a cada 24 (vinte e quatro) horas e que, se houver alteração de e-mail ou qualquer defeito técnico que impeça o acesso, deve comunicar ao Contratante no prazo de até 24 (vinte e quatro) horas.
21.10.2. Os prazos indicados nas comunicações iniciam em 2 (dois) dias úteis a contar da data de envio do e-mail referido no caput.
21.11. As cláusulas e condições pactuadas neste Contrato poderão ser alteradas a qualquer tempo, mediante assinatura de termo aditivo assinado pelos representantes autorizados das partes, respeitados os termos deste Contrato.
21.12. As Partes expressamente anuem, autorizam, aceitam e reconhecem que todos os documentos pertinentes ao contrato, inclusive o próprio instrumento de contrato e aditivos, todas as páginas de assinatura e eventuais anexos, podem ser assinados digitalmente, por meio de suas respectivas assinaturas mediante certificados eletrônicos, com autenticidade reconhecida pelo certificado digital ICP-Brasil, e enviados, entre as partes, por meio eletrônico, nos termos do art. 10, § 2º, da MP nº 2.220-2.

CLÁUSULA VIGÉSIMA SEGUNDA – DO FORO DE ELEIÇÃO –

As partes elegem o foro da Comarca de Porto Alegre, RS, para dirimir as questões relativas a este Contrato.

E, por estarem justos e contratados, firmam o presente em duas vias de igual teor e forma, para um só efeito, perante as testemunhas infra-assinadas.

_____

BANCO DO ESTADO DO RIO GRANDE DO SUL S/A

_____

XXXXXXXXXXXXXXX

TESTEMUNHAS:

_____ _____

MATRIZ DE RISCOS

MATRIZ DE RISCOS PARA CONTRATOS DE TIC – CORE DE SEGURANÇA DE REDE					
CATEGORIA	**RISCO**	**SITUAÇÃO FÁTICA**	**MATERIALIZAÇÃO**	**MITIGAÇÃO**	**ALOCAÇÃO DO RISCO**
Risco da Atividade	Atraso na execução do objeto contratual	Atraso na execução do objeto contratual por culpa do Contratado.	Aumento do custo do produto e/ou do serviço.	Diligência do Contratado na execução contratual.	CONTRATADA
Risco da Atividade	Elevação dos custos operacionais para o desenvolvimento da atividade empresarial em geral e para a execução do objeto em particular.	Necessidade de envolver outros recursos não previstos na proposta de serviço. Elevação de gastos com deslocamentos superiores ao estimado pela CONTRATADA.	Aumento do custo do produto e/ou do serviço.	Planejamento empresarial	CONTRATADA
Risco da Atividade	Elevação dos custos operacionais para o desenvolvimento da atividade empresarial em geral e para a execução do objeto em particular.	Fatos retardadores ou impeditivos da execução do Contrato que não estejam na sua área ordinária, tais como fatos do príncipe, caso fortuito ou de força maior, bem como o retardamento determinado pelo BANRISUL, que comprovadamente repercuta no preço da Contratada, desde que tais custos ultrapassem 30% acima do índice de reajuste estabelecido no contrato, e mediante manifestação e apresentação das comprovações por parte da contratada, conforme previsto na legislação.	Aumento do custo do produto e/ou do serviço.	Revisão de preço	CONTRATANTE
Risco da Atividade	Elevação dos custos operacionais para o desenvolvimento da atividade empresarial em geral e para a execução do objeto em particular.	Fatos retardadores ou impeditivos da execução do Contrato que não estejam na sua álea ordinária, tais como fatos do príncipe, caso fortuito ou de força maior, bem como o retardamento determinado pelo BANRISUL, que comprovadamente repercuta no preço da Contratada, desde que tais custos não ultrapassem 30% acima do índice de reajuste estabelecido no contrato.	Aumento do custo do produto e/ou do serviço.	Planejamento empresarial	CONTRATADA
Risco da	Danos a Terceiros	Danos causados a	Responsabilização	Contratação de	CONTRATADA

Atividade		terceiros durante a prestação do serviço. Roubos e furtos cometido por quadro funcional da CONTRATADA contra clientes e/ou patrimônio do CONTRATANTE.	por danos materiais, lucros cessantes e/ou lesões corporais. Aumento de prazo e custos.	Seguros	
Risco da Atividade	Quebra de sigilo.	Furto e/ou vazamento de banco de dados de clientes e/ou informações estratégicas cometido por quadro funcional da CONTRATADA.	Responsabilização pelo compartilhamento de dados sensíveis sem consentimento. Comprometimento da estratégia corporativa e/ou da segurança de sistemas internos.	Termo de responsabilidade e manutenção de sigilo. Termo de confidencialidade e sigilo.	CONTRATADA
Risco da Atividade	Infringência à Lei Geral de Proteção de Dados – LGPD	Violação de dados pessoais de terceiros identificados e identificáveis por falha de segurança técnica e administrativa da contratada na execução do contrato, por infringência à Lei Geral de Proteção de Dados – LGPD, falha de segurança técnica e administrativa ou descumprimento das orientações do contratante.	Aplicação das penalidades por infração legal	Cumprimento das obrigações contratuais e legais referente à proteção de dados pessoais.	CONTRATADA
Risco da Atividade	Modificações das especificações do objeto.	Modificação das especificações do objeto e/ou sua execução, ampliando ou reduzindo o escopo da contratação, por necessidade do Contratante.	Aumento do custo do produto e/ou do serviço. Aumento de prazo de execução.	Reajuste de preço. Aditivo contratual com prorrogação do prazo de execução.	CONTRATANTE
Risco da Atividade	Paralisação dos serviços por agentes e/ou eventos externos à relação contratual	Eventos ocorridos durante a contratualidade que impeçam o cumprimento do prazo ou aumentem seus custos, tais como desastres socioambientais, eventos que dizem respeito à saúde coletiva, sinistros, caso fortuito ou de força maior e/ou greves.	Aumento do custo do produto e/ou do serviço. Aumento de prazo de execução. Perda da qualidade de execução do objeto.	Planejamento empresarial	CONTRATADA
Risco de Mercado	Inflação. Flutuação de Câmbio.	Variação da taxa de câmbio	Aumento ou diminuição do custo do produto e/ou do serviço.	Revisão dos preços	CONTRATADA OU CONTRATANTE
Risco de Liquidez	Problemas de liquidez financeira.	CONTRATADA apresenta problemas de caixa, impossibilitando a continuação do contrato.	Aumento de prazo de execução. Perda da qualidade de execução do objeto.	Planejamento financeiro considerando a qualificação econômico-financeira	CONTRATADA

				adequada ao porte do objeto contratual.	
Riscos Trabalhista e Previdenciário	Falha ou fraude no pagamento de verbas trabalhistas e previdenciárias aos trabalhadores terceirizados.	Responsabilização do BANRISUL por verbas trabalhistas e previdenciárias dos profissionais da CONTRATADA alocados na execução do objeto contratual.	Geração de custos trabalhistas e/ou previdenciários para o BANRISUL, além de eventuais honorários advocatícios, multas e verbas sucumbenciais.	Ressarcimento, pela CONTRATADA, ou retenção de pagamento e compensação com valores a esta devidos, da quantia despendida pelo CONTRATANTE.	CONTRATADA
Risco Tributário e Fiscal	Falha no recolhimento tributário e/ou fiscal.	Responsabilização do CONTRATANTE por recolhimento indevido em valor menor ou maior que o necessário, ou ainda de ausência de recolhimento, quando devido, sem que haja culpa do CONTRATANTE.	Débito ou crédito tributário ou fiscal.	Ressarcimento, pela CONTRATADA, ou retenção de pagamento e compensação com valores a esta devidos, da quantia despendida pelo CONTRATANTE.	CONTRATADA
Risco Tributário e Fiscal	Falha no recolhimento tributário e/ou fiscal.	Alteração de enquadramento tributário, em razão do resultado ou de mudança da atividade empresarial, bem como por erro do Contratado na avaliação da hipótese de incidência tributária.	Aumento ou diminuição do lucro da Contratada	Planejamento tributário.	CONTRATADA
Risco Tributário e Fiscal	Alteração na alíquota tributária.	Ausência de requerimento por parte da CONTRATADA, tempestivamente, de revisão dos preços devido a majoração de alíquota tributária ocorrida entre a data da proposta e assinatura do contrato.	Débito ou crédito tributário ou fiscal (não tributário).	Planejamento tributário.	CONTRATADA
Risco Reputacional	Conduta comissiva ou omissiva da empresa CONTRATADA.	Práticas discriminatórias e/ou condutas abusivas praticadas pelo quadro funcional da CONTRATADA contra terceiros. Violação ou conduta contrária às exigências legais/regulatórias e/ou aos princípios e objetivos da Instituição.	Danos à imagem do Contratante, impactando a percepção de clientes e acionistas.	Cumprimento de condutas estabelecidas no Código de Ética e Políticas Institucionais. Legislação e normas pertinentes à contratação.	CONTRATADA
Risco Socioambiental	Execução de atividades potencialmente poluidoras e utilizadoras de recursos ambientais de	Descarte irregular de resíduos por parte da Contratada.	Responsabilização na mitigação de dano ou crime ambiental.	Logística reversa para descarte de insumos/ equipamento de TI, conforme legislação.	CONTRATADA

	forma não sustentável				
Risco de TI	Falha ou violação dos sistemas operacionais, de segurança ou de tecnologia	Concessão de perfis de acesso a sistemas de informação e a outros recursos a funcionários da contratada	Ocorrência de eventos nocivos ao Contratante, como vazamento de informações). Interrupção temporária dos negócios, aumentando custos e ocasionando perdas.	Criptografia de dados. Acesso lógico (perfil e senha). Log de trilhas de auditoria (rastreamento). Plano de Continuidade de Negócios.	CONTRATADA
Risco de TI	Falhas de segurança e/ou na integração entre plataformas internas e as da contratada	Falhas de segurança e/ou na integração entre plataformas internas e as da contratada, aumentando a exposição a infecções por vírus, softwares maliciosos e eventos mal-intencionados e violação de dados	Interrupção temporária dos negócios, aumentando custos e ocasionando perdas. Ocorrência de eventos nocivos ao Contratante. Danos à imagem do Contratante.	Acesso lógico (perfil e senha). Log de trilhas de auditoria (rastreamento). Plano de Continuidade de Negócios. Cumprimento das regras de Acordo de Níveis de Serviço.	CONTRATADA
Risco de TI	Obsolescência tecnológica, falta de inovação técnica ou deficiência de equipamentos.	Não aprimoramento dos sistemas de tecnologia da informação do prestador de serviço vinculados à operação do Contratante	Sobrecarga de servidor/sistema. Necessidade de adoção de nova solução. Retrabalhos por parte do Contratante. Aumento de prazo da execução e de custos.	Planejamento empresarial para adoção de ferramentas e materiais necessários à prestação dos serviços, responsabilizando -se pela perfeita execução.	CONTRATADA

TABELA DE SANÇÕES E MULTAS

PERCENTUAL	BASE DE CÁLCULO	PERÍODO DE APLICAÇÃO	OCORRÊNCIA
0,20%	Valor total atualizado do contrato	Por hora de atraso	Descumprimento de prazo para a solução de ações corretivas (Incidentes) com rede de produção ou aplicação crítica parada ou seriamente degradada (2h).
0,05%	Valor total atualizado do contrato	Por hora de atraso	Descumprimento de prazo para a solução de ações corretivas (Incidentes) com rede de produção ou aplicação operando em contingência (Standby) (6h).
0,5%	Valor mensal do contrato	Por dia de atraso	Descumprimento de prazo para a solução de ações preventivas (Requisições de Serviços) para solicitação de avaliação técnica (48h).
5%	Valor mensal do contrato	Por dia de atraso	Descumprimento de prazo para a solução de ações preventivas (Requisições de Serviços) para substituição de hardware ou software utilizado em solução de contorno por peça definitiva da solução (15 dias).
0,05%	Valor total atualizado do contrato	Por dia de atraso	Descumprimento de prazo para a apresentação de solução definitiva para procedimento de contorno realizado.
0,010%	Valor total atualizado do contrato	Por dia de atraso	Descumprimento de prazo para a realização da reunião inicial do projeto.
0,010%	Valor total atualizado do contrato	Por dia de atraso	Reincidência no descumprimento de prazo para a entrega de ATA de reunião.
0,010%	Valor total atualizado do contrato	Por dia de atraso	Descumprimento de prazo para a entrega do plano de projeto.
0,010%	Valor total atualizado do contrato	Por dia de atraso	Descumprimento de prazo para a entrega do plano lógico preliminar.
0,010%	Valor total atualizado do contrato	Por dia de atraso	Descumprimento do prazo de entrega inicial dos softwares e equipamentos.
0,010%	Valor total atualizado do contrato	Por dia de atraso	Descumprimento do prazo de finalização dos Treinamentos Oficiais.
0,010%	Valor total atualizado do contrato	Por dia de atraso	Descumprimento do prazo de finalização da migração do ambiente.
0,010%	Valor total atualizado do contrato	Por dia de atraso	Descumprimento de prazo para a entrega da documentação final do projeto.
0,010%	Valor total atualizado do contrato	Por dia de atraso	Descumprimento do prazo de finalização dos Treinamentos Operacionais.
0,1%	Valor mensal do contrato	Por hora de atraso	Atraso do profissional para operação assistida ao local de trabalho.
0,5%	Valor mensal do contrato	Por dia de ausência	Ausência do profissional para operação assistida ao local de trabalho.
3%	Valor mensal do contrato	Evento	Execução de atividades sem anuência e aceite formal do CONTRATANTE que não impliquem na indisponibilidade ou degradação

			de desempenho do ambiente, sendo aplicada em dobro em caso de reincidência.
10%	Valor mensal do contrato	Evento	Execução de atividades sem submissão e aceite formal do CONTRATANTE que impliquem na indisponibilidade ou degradação de desempenho do ambiente.

TERMO DE CONFIDENCIALIDADE E SIGILO

O CONTRATANTE, BANCO DO ESTADO DO RIO GRANDE DO SUL S.A., sociedade de economia mista, com sede na Rua Capitão Montanha, nº 177, Bairro Centro – CEP 90.010-040, em Porto Alegre/RS, inscrito no Cadastro Nacional de Pessoa Jurídica sob nº 92.702.067/0001-96, por seu representante legal no fim assinado,
e
A CONTRATADA, XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX, com sede na Rua XXXXXXXXXX, nº XXXX – Bairro XXXXXXXXX – CEP: XXXXXX – em XXXXXXXXX/XX, inscrita no CNPJ sob nº XXXXXXXXXXXXXXXXXX, por seu representante legal no fim assinado, têm como certo e ajustado o que adiante segue.

CLÁUSULA PRIMEIRA – DO OBJETO –
O presente TERMO DE CONFIDENCIALIDADE E SIGILO define os direitos, obrigações e responsabilidades das Partes em relação à Segurança da Informação e aos ativos envolvidos e necessários à execução do objeto deste Contrato e seus aditivos, doravante referido apenas como Contrato.

CLÁUSULA SEGUNDA – DAS DEFINIÇÕES –
2.1. Ativo: Qualquer coisa que tenha valor para as Partes, englobando:
I. Os ativos de informação, tais como, mas não se limitando a base de dados e arquivos, contratos e acordos, documentação de sistema, informações sobre pesquisa, manuais de usuário, material de treinamento, procedimentos de suporte ou operação, planos de continuidade do negócio, procedimentos de recuperação, trilhas de auditoria e informações armazenadas;
II. Os ativos de software, tais como, mas não se limitando a aplicativos, sistemas, ferramentas de desenvolvimento e utilitários;
III. Os ativos físicos, tais como, mas não se limitando a equipamentos computacionais, equipamentos de comunicação, mídias removíveis e outros equipamentos;
IV. Os serviços, tais como, mas não se limitando a serviços de computação e comunicações, utilidades gerais, por exemplo aquecimento, iluminação, eletricidade e refrigeração;
V. As pessoas e suas qualificações, habilidades e experiências;
VI. Os intangíveis, tais como, mas não se limitando a reputação e a imagem da Parte.
2.2. Confidencialidade e Sigilo: Garantia de que a informação é acessível somente a Pessoas Autorizadas.
2.3. Dado Pessoal: Qualquer informação relacionada a pessoa natural identificada ou identificável, de acordo com a Lei nº 13.709/18.
2.4. Informação: Significa toda e qualquer informação de natureza, mas não se limitando a comercial, técnica, financeira, jurídica, operacional ou mercadológica sobre, mas sem se limitar a análises, amostras, componentes, contratos, cópias, croquis, dados pessoais ou não pessoais, definições, desenhos, diagramas, documentos, equipamentos, especificações, estatísticas, estudos, experiências, fluxogramas, fórmulas, fotografias, ideias, instalações, invenções, mapas, métodos e metodologias, modelos, pareceres, pesquisas, planos ou intenções de negócios, plantas ou gráficos, práticas, preços, custos e outras informações comerciais, processos, produtos atuais e futuros, programas de computador, projetos, testes ou textos repassada na forma escrita, oral, armazenada em qualquer mídia tangível ou intangível.
2.5. Informações Confidenciais: São aquelas informações que a Parte Divulgadora deseja proteger contra o uso ilimitado, comunicação e ou divulgação indiscriminada ou competição e que sejam designadas como tal por meio de Contrato, especialmente para fins de celebração de acordo comercial referente aos projetos do BANRISUL.
2.6. Informação Liberada: Trata-se da informação identificada pela Parte Divulgadora com a expressão “INFORMAÇÃO LIBERADA” ou que:
I. Seja do conhecimento da Parte Receptora à época em que lhe for comunicada, desde que possa ser comprovado tal conhecimento prévio;
II. Antes de ser revelada, tenha se tornado do conhecimento do público através de fatos outros que não atos ilícitos praticados por uma das Partes ou por seus representantes ou empregados;

III. Tenha sido recebida legitimamente de terceiro sem restrição à revelação e sem violação à obrigação de sigilo direta ou indiretamente para com a Parte que as houver revelado;
IV. Tenha tido a divulgação autorizada por escrito pela Parte Divulgadora;
V. Tenha sido desenvolvida de forma independente por empregados ou por empresas do mesmo grupo da Parte Receptora, sem utilização direta ou indireta de Informações Confidenciais, desde que passível de comprovação;
VI. Toda e qualquer informação que não se enquadre nas hipóteses previstas acima deverá ser considerada confidencial e mantida sob sigilo pela Parte Receptora até que venha a ser autorizado, expressamente pela Parte Divulgadora, a tratá-la diferentemente.
2.7. Parte: Expressão utilizada para referir genericamente os signatários deste Termo de Confidencialidade e Sigilo.
2.8. Parte Receptora: É a Parte que recebe as informações Confidenciais.
2.9. Parte Divulgadora: É a Parte que divulga as informações Confidenciais.
2.10. Pessoa Autorizada: Agentes, representantes, especialistas, prestadores de serviço, internos ou externos, ou empregados dos signatários do Contrato ou deste Termo de Confidencialidade e Sigilo e aqueles autorizados formalmente a transmitir ou receber informações.
2.11. Sigilo: Condição nas quais dados sensíveis são mantidos em sigilo e divulgado apenas para as Pessoas Autorizadas.

CLÁUSULA TERCEIRA – DA PROTEÇÃO DAS INFORMAÇÕES –
Todas as informações relacionadas ao objeto do Contrato referido na cláusula primeira deste instrumento que forem transmitidas pela Parte Divulgadora à Parte Receptora devem ser consideradas e protegidas pela Parte Receptora como confidenciais, exceto se antes da divulgação for esclarecido expressamente que não são confidenciais.

CLÁUSULA QUARTA – DO TRATAMENTO DAS INFORMAÇÕES CONFIDENCIAIS –
As informações da Parte Divulgadora devem ser tratadas como confidenciais e serem protegidas pela Parte Receptora por período indeterminado, até ordem em contrário.

CLÁUSULA QUINTA – DAS AUTORIZAÇÕES PARA ACESSO ÀS INFORMAÇÕES CONFIDENCIAIS –
5.1. Para alcançar a condição de Pessoa Autorizada, os agentes, representantes, especialistas, prestadores de serviço, internos ou externos, ou empregados das Partes, envolvidos, direta ou indiretamente, com a execução do Contrato, deverão ser devidamente instruídos sobre a proteção e manutenção da Confidencialidade e Sigilo das Informações Confidenciais, bem como do teor deste Termo de Confidencialidade e Sigilo.
5.2. Concomitantemente, as Partes tomarão todas as providências para minimizar o risco de revelação de Informações Confidenciais, assegurando-se de que somente Pessoas Autorizadas tenham acesso a tais informações, na estrita medida do necessário.
5.3. Em qualquer caso, as Partes serão responsáveis por toda infração ao presente Termo de Confidencialidade e Sigilo que venha a ser cometida por qualquer Pessoa Autorizada sob sua responsabilidade e tomará todas as providências, inclusive judiciais, necessárias para impedi-los de revelar ou utilizar, de forma proibida ou não autorizada, as Informações Confidenciais.
5.4. Cada Parte fará a gestão das inclusões e exclusões de seus prepostos na condição de Pessoa Autorizada, devendo comunicar imediatamente à outra Parte as mudanças ocorridas.

CLÁUSULA SEXTA – DO USO –
6.1. As Informações Confidenciais reveladas serão utilizadas, exclusivamente, para os fins de execução do Contrato. Em hipótese alguma, poderão ser utilizadas para gerar benefício próprio exclusivo e/ou unilateral, presente ou futuro, ou para uso de terceiros.
6.1.1. A Parte Receptora concorda que:
I. Quaisquer informações confidenciais divulgadas de acordo com este instrumento devem ser usadas pela Parte Receptora tão somente com o propósito para o qual foram divulgadas;
II. Quaisquer informações confidenciais divulgadas de acordo com este documento permanecem em qualquer instância de propriedade da Parte Divulgadora;

III. Exceto nos casos de determinação judicial, a Parte Receptora não poderá usar, distribuir, divulgar ou disseminar informações confidenciais a quem quer que seja, salvo a seus empregados, incluindo os de sua controladora, subsidiárias controladas ou afiliadas, que necessitem ter conhecimento de tais informações ao alcance do propósito para o qual foram divulgadas, a não ser e até que tais informações:

a. Estejam disponíveis para o público por outros meios que não por quebra deste TERMO DE CONFIDENCIALIDADE E SIGILO;

b. Estejam de posse da Parte Receptora ou de seus empregados sem restrição, antes de qualquer divulgação feita segundo este TERMO DE CONFIDENCIALIDADE E SIGILO;

c. Sejam ou tenham sido divulgadas à Parte Receptora ou a seus empregados por terceiros, que não tenham sido empregados das Partes e desde que por meios legais tenham obtido conhecimento;

d. Sejam desenvolvidas independentemente pela Parte Receptora sem que as informações confidenciais, divulgadas segundo este TERMO DE CONFIDENCIALIDADE E SIGILO, tenham sido usadas direta ou indiretamente.

CLÁUSULA SÉTIMA – DA NÃO DIVULGAÇÃO –

7.1. A Parte Receptora garante que protegerá por todos os meios as informações confidenciais, comprometendo-se a protegê-las da forma e, no mínimo, no grau que protege suas próprias informações confidenciais.

7.2. A Parte Receptora concorda também em dar conhecimento a todos os seus empregados e demais colaboradores, de suas obrigações contratuais, que regem este instrumento e a todos que tiverem acesso às informações confidenciais.

7.3. A divulgação pela Parte Receptora de informações confidenciais, sem autorização expressa da Parte Divulgadora, sujeitará a infratora às penalidades legais e ou contratuais.

CLÁUSULA OITAVA – DA GUARDA DE INFORMAÇÕES CONFIDENCIAIS –

8.1. A Parte Receptora deverá manter procedimentos administrativos adequados à preservação de extravio ou perda de quaisquer Informações Confidenciais, principalmente os que impeçam a divulgação ou a utilização por seus agentes, funcionários, consultores e representantes, ou ainda, por terceiros não envolvidos com a execução do Contrato.

8.2. A CONTRATADA concorda também que tomará assinatura no TERMO DE RESPONSABILIDADE E DE MANUTENÇÃO DE SIGILO, de todos os seus empregados e colaboradores que vierem a ter acesso às informações confidenciais.

CLÁUSULA NONA – DAS CÓPIAS –

As Partes comprometem-se a não efetuar nenhuma gravação ou cópia das Informações Confidenciais recebidas.

CLÁUSULA DÉCIMA – DA PROPRIEDADE –

10.1. O presente TERMO DE CONFIDENCIALIDADE E SIGILO não implica a concessão, pela Parte Divulgadora à Parte Receptora, de nenhuma licença ou qualquer outro direito, explícito ou implícito, em relação a qualquer direito de patente, direito de edição ou qualquer outro direito relativo à propriedade intelectual.

10.2. Todas as anotações e compilações serão também consideradas Informações Confidenciais e serão havidos como de propriedade da Parte Divulgadora, não cabendo à outra Parte nenhum direito sobre tais, salvo acordo entre as mesmas, expresso e por escrito, em contrário.

CLÁUSULA DÉCIMA PRIMEIRA – DA VIOLAÇÃO –

As Partes informarão a outra Parte imediatamente sobre qualquer revelação não autorizada, esbulho ou mau uso, por qualquer pessoa, de qualquer Informação Confidencial, assim que tomar conhecimento, e tomará as providências necessárias ou convenientes para evitar qualquer violação futura de Informações Confidenciais.

CLÁUSULA DÉCIMA SEGUNDA – DO RETORNO DE INFORMAÇÕES CONFIDENCIAIS –
12.1. A pedido da Parte Divulgadora, a Parte Receptora deverá restituir imediatamente o documento (ou outro suporte) que contiver Informações Confidenciais.
12.2. A Parte Receptora deverá restituir espontaneamente a Parte Divulgadora as Informações Confidenciais que deixarem de ser necessárias, não guardando para si, em nenhuma hipótese, cópia, reprodução ou segunda via das mesmas.
12.3. A pedido da Parte Divulgadora, a Parte Receptora deverá prontamente emitir uma declaração assinada por seu representante legal, confirmando que toda Informação Confidencial foi restituída ou inteiramente destruída, comprometendo-se de que não foram retidas quaisquer reproduções (incluindo reproduções magnéticas), cópias ou segundas vias, sob pena de ser considerado falta gravíssima, conforme previsto no Contrato e ainda podendo ser, a CONTRATADA, responsabilizada por perdas e danos que porventura vierem a existir.

CLÁUSULA DÉCIMA TERCEIRA – DAS PENALIDADES –
O descumprimento de quaisquer cláusulas do presente Termo de Confidencialidade e Sigilo será considerado falta gravíssima conforme previsto no Contrato e ainda sujeitará a Parte, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos diretos sofridos pela outra Parte, excluindo-se danos indiretos, consequenciais ou lucros cessantes, bem como as de responsabilidade civil e criminal respectivas, que serão apuradas em regular processo judicial ou administrativo.

CLÁUSULA DÉCIMA QUARTA – DO PRAZO DE VIGÊNCIA –
O presente TERMO DE CONFIDENCIALIDADE E SIGILO terá a mesma vigência do Contrato e seus aditivos em consonância com a Cláusula Primeira. Não obstante o referido termo final de validade do Contrato, todas as obrigações previstas neste Instrumento, relacionadas às Informações já divulgadas, continuarão a ser observadas, notadamente a preservação da confidencialidade, por período indeterminado após a sua extinção.

CLÁUSULA DÉCIMA QUINTA – DA PUBLICIDADE –
Todas as declarações, anúncios públicos e/ou divulgações relativas ao Contrato e a este TERMO DE CONFIDENCIALIDADE E SIGILO deverão ser previamente comunicados e coordenados por ambas as Partes, dependendo a sua declaração, anúncio e/ou divulgação, do prévio e mútuo consentimento das mesmas.

CLÁUSULA DÉCIMA SEXTA – REVELAÇÃO POR ORDEM JUDICIAL –
Caso uma das Partes seja obrigada a revelar qualquer Informação Confidencial em virtude de ordem judicial, a mesma avisará a outra Parte imediatamente, para que a esta seja dada a oportunidade de opor-se à revelação. Caso a oposição da Parte não seja bem-sucedida, a Parte oposta somente poderá fazer a revelação na extensão exigida pela ordem judicial em questão e deverá exercer todos os esforços razoáveis para obter garantias confiáveis de que tais Informações Confidenciais tenham tratamento sigiloso.

CLÁUSULA DÉCIMA SÉTIMA – DISPOSIÇÕES GERAIS –
17.1. Falhas ou atrasos de qualquer uma das Partes no exercício de qualquer direito, poder ou privilégio não devem ser considerados como desistência, novação ou modificação dos direitos previstos neste TERMO DE CONFIDENCIALIDADE E SIGILO.
17.2. Fica entendido que este TERMO DE CONFIDENCIALIDADE E SIGILO não pretende e não vai obrigar as Partes a celebrar outros acordos ou contratos, ou ainda a realizar qualquer negócio, ficando, certo e ajustado que as Partes não têm exclusividade no recebimento das informações confidenciais a serem divulgadas.
17.3. Nada que esteja contido neste TERMO DE CONFIDENCIALIDADE E SIGILO deve ser tomado como garantia ou conferência de direitos de licença de uso das informações confidenciais divulgadas à parte Receptora.
17.4. Qualquer aditamento a este TERMO DE CONFIDENCIALIDADE E SIGILO deve ser por escrito e assinado por seus representantes legais.

TERMO DE RESPONSABILIDADE E DE MANUTENÇÃO DE SIGILO

Eu, _____, portador do documento de identidade

nº _____, expedido pela _____, CPF nº _____, comprometo-me a manter sigilo sobre dados, processos, informações, documentos e matérias que eu venha a ter acesso ou conhecimentos no âmbito do CONTRATANTE, em razão das atividades profissionais a serem realizados e ciente do que preceituam a Lei Complementar 105/2001 que trata do sigilo bancário; o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), nos Artigos 153, 154, 314, 325 e 327 e suas alterações promovidas pela Lei 9.983/2000 e Lei 6.799/1980; o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código do Processo Penal), no Artigo 207; a Lei Federal nº 13.105, de 16 de março de 2015 (Código de Processo Civil); a Lei nº 8.159, de 8 de janeiro de 1991 (Lei de Arquivos), nos Artigos 4, 6 e 25; e o Decreto nº 7.845, de 14 de novembro de 2012 (Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo e dispõe sobre o Núcleo de Segurança e Credenciamento).

Tenho ciência de que o não cumprimento do aqui estabelecido estará a Contratada incidindo em falta gravíssima em conformidade com o estabelecido no Termo de Confidencialidade e Sigilo e no Contrato propriamente dito.

E por estar de acordo com o presente Termo, assino-o na presença das testemunhas a seguir mencionadas.

_____
Assinatura do Colaborador da CONTRATADA

Testemunhas:

_____ _____

ORIENTAÇÕES AO FORNECEDOR

Prezado Fornecedor,

Visando padronizar o fluxo de envio da documentação e troca de informações, bem como agilizar os procedimentos para realização de pagamentos, se faz necessário o alinhamento sobre os pontos abaixo:

1. ATUALIZAÇÃO CADASTRAL

- Sempre mantenha seu cadastro atualizado junto ao contratante, incluindo dados de contato como endereço, telefone, e-mail e dados completos do representante legal. A atualização cadastral abrange a necessidade de comunicação de eventuais alterações como modificação do capital social, alteração do objeto social e/ou atividades, alteração da razão social, nome fantasia e/ou quadro societário, devidamente acompanhado de documentação comprobatória

2. GESTÃO DO CONTRATO

- Questionamentos a respeito do gerenciamento da contratação, tais como valores a receber, renovação, Termos Aditivos, prorrogações, reajuste de valores, controles de prazos e apresentação da garantia contratual, deverão ser direcionados para o endereço eletrônico **contratacoes_gestao_contratos@banrisul.com.br**.

3. GESTÃO DO PAGAMENTO

- Toda a documentação que se relaciona com o pagamento (nota fiscal, certidões de regularidade, certidões de isenção ou que demonstre condição tributária especial) deverá ser enviada para o endereço eletrônico **nf_contratos@banrisul.com.br**. Este e-mail é exclusivamente para o envio da documentação para pagamento. Mensagens que não se enquadrarem neste requisito serão desconsideradas.

- Questionamentos sobre pagamentos (dúvidas, previsão para pagamento, substituição tributária/ retenções efetuadas, etc.), deverão ser direcionados exclusivamente para o endereço eletrônico **pagadoria@banrisul.com.br**.

IMPORTANTE:

Informamos que, antes da emissão da nota fiscal, enviaremos as orientações necessárias para a correta emissão do documento (dados do tomador, enquadramento tributário, retenções na fonte, etc.).

A nota fiscal somente poderá ser emitida após a conformidade do Gestor demandante da contratação, confirmando a conclusão da prestação dos serviços/entrega do objeto, e que o mesmo está em conformidade com as exigências contratuais.

Agradecemos imensamente vossa atenção neste assunto e nos colocamos à disposição para maiores esclarecimentos por meio do endereço eletrônico, caso seja necessário: **contratacoes_pagadoria@banrisul.com.br**

Conheça o nosso **MANUAL DE RELACIONAMENTO COM FORNECEDORES**, documento que orienta sobre a conduta adequada na relação entre o Banrisul e seus fornecedores, bem como as informações gerais para o bom andamento deste relacionamento que ora se inicia, disponível na página de internet do Banrisul, na área de Transparência, no seguinte caminho: banrisul.com.br > Mais > Institucional > Transparência > Licitações e Contratos > MANUAL DE RELACIONAMENTO COM FORNECEDORES.

Conheça também nossa **APOSTILA TREINAMENTO DE TERCEIROS**, que em atendimento à regulação[1] vigente, está sendo disponibilizada de forma ampla e irrestrita, devendo os Fornecedores adotar medidas para que esta disposição seja levada a efeito junto a seus colaboradores, a qual se encontra disponível em: banrisul.com.br > Mais > Institucional > Transparência > Licitações e Contratos > Capacitação de Terceirizados - Res. 4557/2017.

Para maiores informações sobre procedimentos operacionais relacionados com a presente contratação, a contratada deverá consultar o **MANUAL DO FORNECEDOR DO BANRISUL**, documento que auxilia os fornecedores a conhecerem e entenderem os procedimentos que a empresa utiliza nas suas relações comerciais de aquisição de bens e prestação de serviços, disponível na página de internet do Banrisul, na área de Transparência, no seguinte caminho: banrisul.com.br > Mais > Institucional > Transparência > Licitações e Contratos > MANUAL DE FORNECEDORES DO BANRISUL.

Atenciosamente,

UNIDADE DE CONTRATAÇÕES E PAGADORIA

[1] Artigo 36 da Resolução CMN nº 4.557/2017, o qual define que a instituição deve se assegurar da adequada capacitação sobre risco operacional de todos as prestadores de serviços terceirizados relevantes, Artigo 7º da Resolução CMN nº 4.595/17, Inciso III, que estabelece a necessidade capacitação de todos os empregados e dos prestadores de serviços terceirizados relevantes, em assuntos relativos à conformidade; e Artigo 3º, Inciso I, da Carta Circular BCB nº 3.978/2020, que determina a promoção de cultura organizacional de prevenção à lavagem de dinheiro e ao financiamento do terrorismo, inclusive, aos prestadores de serviços terceirizados.

PLANILHA DE ORÇAMENTO – PROCESSO Nº 0000037/2026

1 . **OBJETO:** Aquisição de Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida, composta por hardware, software e demais serviços.

2 . **DEMAIS CONDIÇÕES:** Conforme Termo de Referência do processo.

ITEM	DESCRIÇÃO	PRODUTO/MODELO/SERVIÇO	QTD.	UN.	VALOR UN.	VALOR TOTAL
Item 1	**GERENCIAMENTO DO PROJETO, IMPLEMENTAÇÃO DA SOLUÇÃO E TREINAMENTOS OPERACIONAIS**	Descrição do Pacote de Serviços	1	Pct.		
1.1	Serviços de Gerenciamento do Projeto e Implementação da Solução	Descrição do Pacote de Serviços	1	Pct.		
1.2	Treinamentos Operacionais	Descrição do Pacote de Serviços	1	Pct.		
Item 2	**HARDWARE e SOFTWARE**	Descrição do Conjunto de Hardware e Software	1	CJ		
Item 3	**LICENCIAMENTO**	Descrição do Pacote de Serviços	1	Pct.		
3.1	Licenciamento Geral	Descrição do Pacote de Licenças	1	Pct.		
3.2	Licenciamento por assinatura ou subscrição	Descrição do Pacote de Licenças	1	Pct.		
Item 4	**TREINAMENTOS OFICIAIS**	Descrição do Pacote de Treinamento	1	Pct.		
Item 5	**GARANTIA, SUPORTE TÉCNICO, MANUTENÇÃO E OPERAÇÃO ASSISTIDA (pagamento mensal)**	Descrição do Pacote /Serviço	54	MÊS		
5.1	Pacote Mensal de Serviços de Suporte Técnico e Manutenção com nível de SLA definido	Descrição do Pacote /Serviço	54	MÊS		
5.2	Equipe de 02 (dois) Profissionais Dedicados à Operação Assistida	Descrição do Pacote /Serviço	54	MÊS		
VALOR FINAL						

3 . **REGRAMENTO DE PRECIFICAÇÃO:**

a) Nos preços propostos e naqueles que, porventura, vierem a ser ofertados através de lances, deverão estar inclusos todos os custos necessários à execução do objeto, bem como todos os impostos, encargos trabalhistas, previdenciários, fiscais, comerciais, taxas, fretes, seguros e quaisquer outros que incidam ou venham incidir sobre este.

b) O valor total do item “TREINAMENTOS OFICIAIS” informado na planilha de orçamentos deve ser inferior a 2% do valor total da proposta.

c) O valor total do item “GARANTIA, SUPORTE TÉCNICO, MANUTENÇÃO E OPERAÇÃO ASSISTIDA” deve ser superior a 25% do valor total da proposta.

d) Os subitens 3.1 e 3.2 referem-se a modalidades de licenciamento, e, conforme a composição da solução ofertada pela licitante podem variar em valor. Ex.: Se um determinado fabricante ofertar apenas licenciamento de subscrição, o item 3.1 aparecerá zerado. Licenças de caráter perpétuo ou que não sejam de subscrição, devem constar no item 3.1, já licenças de subscrição, no item 3.2.

4 . **DADOS DA PROPONENTE: RAZÃO SOCIAL; CNPJ; ENDEREÇO COMPLETO; TELEFONE; E-MAIL; DADOS BANCÁRIOS.**

5 . VALIDADE DA PROPOSTA: _____

PLANILHA DE ESPECIFICAÇÕES TÉCNICAS
Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida

1. DO OBJETO

1.1. Aquisição de Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida, composta por hardware, software, licenças, garantia, serviços de implementação da solução, suporte de hardware, suporte técnico com acordo de nível de serviço definido, operação assistida, manutenção dos equipamentos e treinamentos;

1.2. Especificações do Objeto

O objeto tem como principais premissas o provimento da segurança do ambiente de Core de Rede (Data Center), a atualização tecnológica gradual dos ambientes de segurança de redes e comunicações do CONTRATANTE (Rede Corporativa, Rede de Agências, Ambiente de Internet, VPN, Parceiros, seus serviços e funcionalidades), a visibilidade padronizada dos incidentes de segurança nas linhas de controle e monitoração, a integração da estrutura de segurança com as demais soluções de rede e comunicações (Cisco ACI, Aruba ClearPass, VMware, entre outros ambientes) e a iniciação do uso de Inteligência Artificial para apoio à atividades como configurações, diagnósticos, relatórios, troubleshooting, auditoria, compliance, manutenção corretiva e medidas protetivas.

Esta solução deve permitir, em um universo de dois sites físicos de Data Center, que um equipamento ou conjunto de equipamentos possa assumir as operações de seus pares em caso de falha de algum nodo principal ou até mesmo assumir completamente a operação para garantir a continuidade do negócio com o nível adequado de segurança e disponibilidade, respeitando níveis de redundância equivalentes a um Data Center padrão Tier 4, considerando nível 2N+1, ou seja, dois conjuntos idênticos de equipamentos redundantes (por site físico) mais um componente extra de *spare part* para maior resiliência (equipamento para atendimento dos níveis críticos de SLA em caso de RMA).

A solução deve contemplar a entrega dos produtos especificados bem como serviços especializados de implementação e gerenciamento de projeto, treinamentos, profissionais dedicados para operação assistida, testes de aceitação, suporte técnico e manutenção, conforme o cronograma de entregas descrito neste edital e em conformidade com a Planilha de Especificações Técnicas.

1.3. ESPECIFICAÇÕES TÉCNICAS PARA AQUISIÇÃO DE HARDWARE E SOFTWARE

1.3.1. CARACTERÍSTICAS GLOBAIS DA SOLUÇÃO

1.3.1.1. A CONTRATADA deve fornecer uma solução completa de hardware, software, licenças e todos os serviços necessários para planejar, desenhar, configurar e suportar uma Estrutura de Segurança de Redes e Comunicações de Malha Híbrida capaz de proteger os cenários de rede e comunicações do CONTRATANTE;

1.3.1.2. As especificações da solução a ser adquirida estão descritas ao longo deste documento;

1.3.1.3. A solução ofertada deve ter caráter híbrido, ou seja, ser composta por funcionalidades que atendam tanto situações de uso on-premise como em nuvem, de modo que respeite as melhores práticas de mercado e também as necessidades e limitações do ambiente do CONTRATANTE;

1.3.1.4. Em linhas gerais, a solução deve ser composta por pelo menos oito equipamentos (ou conjunto de equipamentos) físicos de grande porte que atendam às funcionalidades descritas no CENÁRIO A – CORE DE SEGURANÇA (NGFW, NGIPS, VPN entre outras) apoiadas por outras funcionalidades conforme descrito nos demais cenários, que, conforme o caso, poderão ser oferecidas no formato on-premise, virtualizado e/ou nuvem, por isso, sendo considerado uma solução de malha híbrida. Esses equipamentos de grande porte serão denominados “nodos”, e cada Data Center terá à sua disposição quatro deles, dois em um ambiente “X” e dois em um ambiente “Y”. Cada Data Center deve conter um nodo extra além dos mencionados para “*spare part*”;

1.3.1.5. A solução também deve contar com uma estrutura secundária de dois equipamentos físicos de menor porte, para atender a requisitos específicos de compliance do CONTRATANTE (um em cada Data Center);
1.3.1.6. Algumas funcionalidades devem estar presentes tanto no caso de uso on-premise como em nuvem, garantindo a coesão e consistência na aplicação de políticas de segurança na solução como um todo;
1.3.1.7. As principais premissas da solução são alta disponibilidade, visibilidade, segurança e integração, de modo que deve ser observada a relação entre os componentes ofertados para que haja uma intercomunicação entre as funcionalidades, de modo a compor uma linha de segurança na qual todas entidades participantes possam comunicar algum tipo de detecção para que, ao tomarem conhecimento da informação propagada, as outras entidades possam atuar em seu escopo de controle e inspeção;
1.3.2. Dado o exposto, para cada cenário especificado, a solução deve atender os requisitos a seguir:

1.3.2.1. CENÁRIO A – CORE DE SEGURANÇA
1.3.2.1.1. Ser composta por um conjunto de equipamentos individuais, ou um coletivo de conjuntos de equipamentos arranjados como uma unidade individual, cuja UNIDADE seja capaz de suportar toda a operação de um site ativo do CONTRATANTE, mesmo sem nenhum tipo de redundância pareada a essa unidade;
1.3.2.1.1.1. Cada unidade (sendo um equipamento único ou um conjunto de equipamentos arranjados como unidade única) capaz de manter toda a operação de um dos sites individualmente será nomeada ao longo da especificação como NODO.
1.3.2.1.2. Atender a infraestrutura de Data Centers do CONTRATANTE em conformidade com o nível de redundância (2N+1), ou seja, com dois sistemas independentes e totalmente espelhados, incluindo um terceiro sistema de *spare*, prontos para assumir a operação em caso de falha conforme referenciado em norma (ANSI/TIA-942) para Data Centers de TIER 4;
1.3.2.1.2.1. A principal premissa é o provimento de uma solução de alta disponibilidade, ou seja, ambientes com nível de redundância que contenham um segundo nodo paralelo por site, trabalhando de modo que possa assumir as operações do site por completo em caso de falha de um nodo principal ou, até mesmo, assumir completamente a operação para garantir a continuidade do negócio, com plena visibilidade dos ambientes e todos os recursos de inspeção disponíveis na linha de segurança;
1.3.2.1.3. Atender, independentemente do *design* e do conjunto de equipamentos recomendados pelo fabricante, a seguinte premissa básica de organização: Cada AMBIENTE (figura 1) deve atender DOIS SITES FÍSICOS. Para isso, deve minimamente conter um NODO operando em modo ativo e um segundo conjunto de equipamentos idênticos, por site, funcionando como *standby* para substituição em caso de falhas (ou seja, um nodo ativo e um novo *standby* para cada site). Esse mesmo arranjo deve estar disponível no site secundário, garantindo que toda a operação possa ser mantida com apenas um nodo em modo ativo. Assim, em caso de falha de um nodo, seu par dentro do mesmo site assume toda a operação. Caso o site inteiro apresente falhas, o outro site deve ser capaz de assumir completamente a operação, mantendo o mesmo modelo de funcionamento citado. Mesmo em uma situação crítica, na qual reste apenas um único nodo ativo por ambiente, a operação ainda assim deve ser sustentada em sua totalidade.

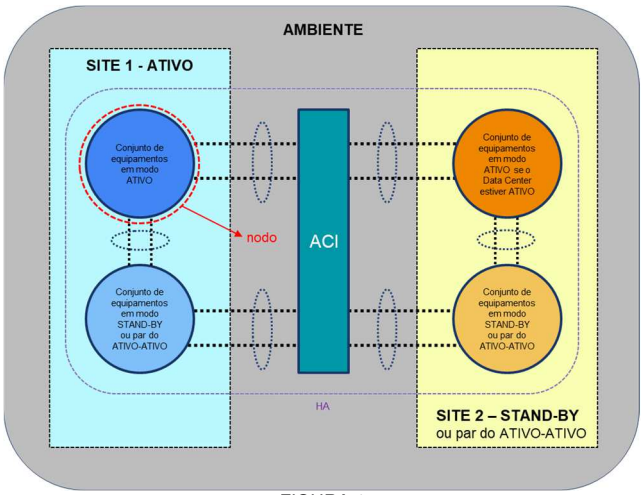


FIGURA 1

1.3.2.1.4. Conter minimamente os conjuntos de equipamentos necessários para atender a 2 (DOIS) AMBIENTES COMPLETOS, ou seja, 08 (oito) nodos no total, sendo 04 (quatro) nodos por ambiente e 02 (dois) nodos por site em cada ambiente (figura 2), de modo a respeitar as demais especificações técnicas para atender à operação dos Data Centers;

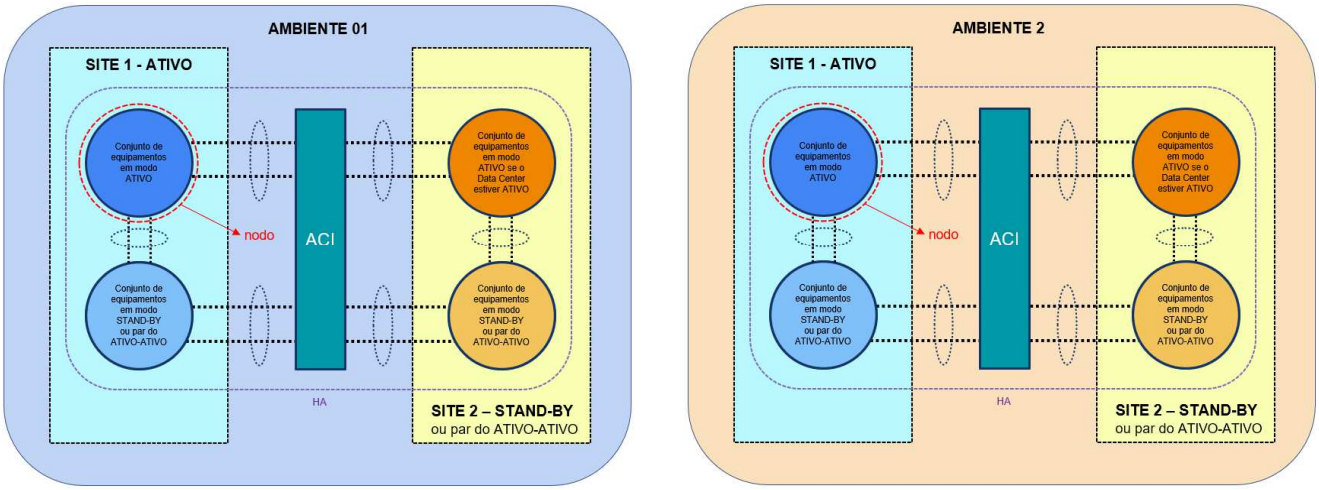


FIGURA 2

1.3.2.1.5. Ser composta pelo mesmo conjunto de equipamentos para cada nodo apresentado na premissa básica de organização de AMBIENTE citada anteriormente, de modo que o design sugerido pela LICITANTE apresente o mesmo hardware individual, ou conjunto de equipamentos, para cada nodo, buscando a padronização e organização da solução;

1.3.2.1.6. Possuir 02 (dois) nodos extras, um para cada Data Center, aptos para utilização em caráter de *spare part*, visando atender os níveis mais críticos de SLA em caso de falhas críticas que exijam substituição imediata de hardware;

1.3.2.1.7. Ter contrato de suporte ativo diretamente com o fabricante, para todos os componentes da solução ofertada, durante todo o período contratual;

1.3.2.1.8. Manter todos os serviços baseados em assinaturas ou subscrição disponíveis pelo tempo de duração do contrato;

1.3.2.1.9. Ser disponibilizada em hardware do próprio fabricante, não sendo aceitos hardwares de fabricantes terceiros, não sendo aceitos também hardwares homologados (quando o fabricante da

solução/software e do hardware são empresas diferentes) à exceção de servidores que visem prover a infraestrutura gerenciamento da solução ou ainda o apoio à consulta e análise de dados de outros ambientes ou de análises especializadas cujo processamento não possa ocorrer no ambiente de produção on-premise do CONTRATANTE;

1.3.2.1.10. Ser do tipo *appliance* físico (à exceção dos servidores de gerenciamento ou funcionalidades exclusivamente em nuvem) operando em alta disponibilidade com manutenção e compartilhamento dos estados de sessão TCP com seus nodos pares;

1.3.2.1.11. Possuir sistema operacional preparado (*hardened*) e embarcado para os *appliances* físicos;

1.3.2.1.12. Ter operação plenamente compatível com a solução Cisco ACI, que será utilizada como núcleo de rede dos ambientes do CONTRATANTE;

1.3.2.1.13. Permitir a implementação de alta disponibilidade, com a utilização de um segundo (ou mais) nodo(s) idêntico(s), podendo operar nos modos ativo/standby ou ativo/ativo;

1.3.2.1.14. Suportar a comunicação de ocorrências suspeitas com outras soluções que componham o ambiente de rede e comunicações do CONTRATANTE, de forma que, possa enviar mensagens para a linha de equipamentos de segurança (NGFW, NGIPS, NAC, EDR, SOC, SIEM, entre outras entidades de rede que possam atuar na mitigação de ameaças) para que outros cenários possam atuar na detecção, prevenção e tratamento de possíveis incidentes. Ex.: A equipe de SOC identifica uma situação em que entende ser necessário um bloqueio na linha de perímetro e envia, automaticamente, uma chamada para que os equipamentos de NGIPS (e outros) atuem nos níveis corretos de inspeção, ou ainda, uma das funcionalidades do ambiente de firewall detecta em alguma das camadas de inspeção que um usuário está com um comportamento suspeito e comunica a solução de NAC do CONTRATANTE que esse usuário precisa ser colocado em quarentena assim como outras correlações similares;

1.3.2.1.15. Prover todas as documentações e manuais técnicos completos necessários à instalação, configuração e operação dos equipamentos. Essa documentação deve estar em português ou inglês, preferencialmente nesta ordem;

1.3.2.1.16. Possuir gerenciamento centralizado para o cenário em um único console/painel de controle, unificando configuração, monitoramento, relatórios e auditoria;

1.3.2.1.17. Incluir recurso de armazenamento mínimo de 1,5 (um vírgula cinco) terabytes, dedicados ao armazenamento de logs e análise de dados, para cada nodo previsto na solução. Deve ser possível o upgrade futuro desse espaço de armazenamento sem afetar a solução em produção;

1.3.2.1.17.1. Caso os equipamentos fornecidos não possuam o referido hardware para armazenamento, A LICITANTE deve fornecer a infraestrutura de discos necessária para o atendimento do requisito de armazenamento de logs;

1.3.2.1.18. Utilizar discos de estado sólido para leitura, escrita e armazenamento de dados não sendo aceitos equipamentos com discos mecânicos;

1.3.2.1.19. Oferecer funcionalidades de NGFW e NGIPS de forma nativa, no mesmo nodo físico sem necessidade de *appliances* adicionais. O mecanismo de NGIPS deve estar integrado ao motor de inspeção do NGFW, permitindo aplicação de políticas conjuntas;

1.3.2.1.20. Prover inspeção profunda de pacotes DPI (Deep Packet Inspection), com capacidade de detecção e prevenção de ataques em tempo real;

1.3.2.1.21. Suportar, para o sistema de NGIPS, os modos de detecção e de prevenção, de forma que seja possível configurar o modo de atuação em nível de regras de filtragem;

1.3.2.1.22. Oferecer biblioteca de assinaturas constantemente atualizada para ataques como Exploits de sistemas operacionais e aplicações, Malware, Ransomware e variantes conhecidas, Ataques de rede DoS/DDoS, Varreduras, Buffer overflows, Injeções, Comunicação com botnets e C&C (Command & Control), entre outros;

1.3.2.1.23. Suportar detecção baseada em comportamento e anomalias;

1.3.2.1.24. Oferecer correlação de eventos entre NGIPS e demais módulos de segurança nativos (antimalware, filtragem web, sandbox, EDR/XDR, etc.);

1.3.2.1.25. Possibilitar a definição de ações automáticas para eventos críticos (bloqueio e alerta);
1.3.2.1.26. Permitir que uma única política de segurança combine: controle de aplicações, inspeção de conteúdo, NGIPS, antimalware e filtragem web;
1.3.2.1.27. Implementar NTP (Network Time Protocol), contemplando autenticação criptografada entre os peers;
1.3.2.1.28. Realizar integração com ferramentas de SIEM, SOAR, entre outras, permitindo exportação de logs e eventos via syslog, API ou outros protocolos padrão;
1.3.2.1.29. Possuir um sistema de NGIPS que opere em alta performance, com aceleração por hardware (ASICs, NPUs ou equivalentes) ou software otimizado;
1.3.2.1.30. Garantir *throughput* consistente com as especificações, mesmo com todos os recursos de segurança habilitados, sem degradação significativa de desempenho;
1.3.2.1.31. Suportar clusterização/alta disponibilidade (HA) e escalabilidade horizontal;
1.3.2.1.32. Estar integrado a uma rede global de inteligência de ameaças (Threat Intelligence) do fabricante;
1.3.2.1.33. Permitir a atualização de assinaturas e feeds de inteligência de forma automática e em tempo real, sem intervenção manual;
1.3.2.1.34. Suportar a importação de feeds de terceiros via formatos abertos (STIX/TAXII, etc.);
1.3.2.1.35. Gerar relatórios customizáveis por: usuário, aplicação, protocolo, evento e ameaça detectada;
1.3.2.1.36. Permitir trilhas de auditoria completas, atendendo requisitos de conformidade (LGPD, GDPR, PCI-DSS, ISO 27001);
1.3.2.1.37. Os equipamentos fornecidos para atender a solução devem:
1.3.2.1.37.1. Possuir Homologação na Anatel sempre que sejam passíveis de homologação compulsória pela referida agência reguladora;
1.3.2.1.37.2. Ser compatíveis com o padrão de fixação em rack(s) de 19" (dezenove polegadas) ou fornecidos na forma de módulos de outros equipamentos com fixação em rack(s) de 19”. Devem ser fornecidos kits de suporte específico para este fim. Eventuais ajustes na estrutura do rack (fixação de colunas, etc.) necessários para a instalação da solução deverão ser executados pela LICITANTE;
1.3.2.1.37.3. Possuir o fluxo do ar de frente para trás (front-to-back);
1.3.2.1.37.4. Implementar de forma nativa mecanismo de monitoramento e detecção de falhas em suas fontes de alimentação individuais;
1.3.2.1.37.5. Possuir fontes de alimentação redundantes do tipo hot-swap que sejam integradas ao equipamento. As fontes devem possuir tensão de alimentação de entrada 220 Volts CA 60 Hz;
1.3.2.1.37.6. Ser fornecidos juntamente com todos os cabos, tomadas, acessórios e softwares necessários à completa carga, instalação, configuração e operação dos equipamentos. Os cabos de energia deverão ter conectores no padrão IEC-320 C13-C14;
1.3.2.1.38. Todas as funcionalidades de gerência, exibição de opções e comandos, seja através de CLI, SSH, interface gráfica (GUI) ou Syslog devem estar obrigatoriamente em português ou inglês;
1.3.2.1.39. As licenças de hardware e software devem permitir a plena continuidade de utilização e operação simultânea de todas as funcionalidades mesmo após o término do contrato, de forma perpétua, à exceção das funcionalidades licenciadas mandatoriamente por subscrição, estas devem permanecer vigentes e operacionais durante todo o período contratual;
1.3.2.1.40. Todos os recursos especificados devem ser funcionais e não será aceito licença do tipo demonstração, ou recursos com prazo de expiração;
1.3.2.1.41. Todos os equipamentos devem ser novos, sem qualquer tipo de uso, estar em perfeito estado e não podem estar descontinuados no seu país de origem durante o período da implementação e da vigência do contrato;

1.3.2.1.42. Todos os equipamentos devem ter capacidade de processamento e memória suficientes para trabalhar com todas as capacidades e funções solicitadas neste termo de referência;
1.3.2.1.43. O número de série de cada equipamento deve ser obrigatório e único, afixado em local visível na parte externa do equipamento e na embalagem que o contém. Esse número deve ser identificado pelo fabricante, como válido para o produto entregue e para as condições do mercado brasileiro no que se refere à assistência técnica e garantia no Brasil;
1.3.2.1.44. Todos os equipamentos fornecidos pela LICITANTE deverão ser compatíveis com a solução CA Spectrum utilizada para o gerenciamento do BANRISUL. Estes devem suportar o protocolo SNMP, nas versões 2 e 3 (versões dois e três, em todos os tipos de criptografia definidos para a versão três);
1.3.2.1.45. Caso os equipamentos disponibilizem as informações para o gerenciamento de suas funcionalidades somente por meio de MIBS proprietárias, o fabricante deve apresentar comprovação de que os equipamentos, ou as MIBS utilizadas por estes, estão certificados na solução CA Spectrum. A relação de equipamentos e MIBS certificados podem ser consultadas no site https://netops-certification.broadcom.com/vendors(default-header:vendors);
1.3.2.1.46. Possuir documentação aderente à versão vigente do PCI DSS;
1.3.2.1.47. Qualquer problema na entrega e configuração dos equipamentos deve ser reportado imediatamente ao BANRISUL. Os problemas originados nos componentes que estão sendo fornecidos e ativados devem ser resolvidos pela LICITANTE dentro do prazo de 10 dias corridos;
1.3.2.1.48. Possuir sistema operacional preparado (*hardened*) e embarcado e ser capaz de oferecer todas as funcionalidades sem a necessidade de adicionar novos elementos de *hardware*;
1.3.2.1.49. Para fins de conectividade física e desempenho, a solução deve:
1.3.2.1.49.1. Possuir, para *uplink* de cada ambiente, no mínimo, 04 (quatro) portas QSFP-100 Gigabit Ethernet BASE BiDi por nodo, prontas para uso, já populadas com transceiver, independentemente das interfaces de gerenciamento;
1.3.2.1.49.1.1. Essas portas serão conectadas através de conectores LC ao fabric Cisco ACI existente no ambiente do CONTRATANTE;
1.3.2.1.49.1.2. Para tanto, devem ser fornecidos tanto os transceivers do lado da solução ofertada quanto os outros 04 (quatro) transceivers Cisco 100Gbps QSFP100 SR1.2 BiDi para o lado do ACI já existente no Data Center do CONTRATANTE;
1.3.2.1.49.2. Possuir, para tráfego de dados em cada nodo, no mínimo 8 (oito) portas 10G BASE-X SFP+ SR prontas para uso (porta + transceiver, se for o caso), independente das interfaces de gerenciamento;
1.3.2.1.49.3. Possuir, para gerenciamento em cada nodo, ao menos uma interface dedicada para gerenciamento out-of-band no padrão RJ45 Gigabit Ethernet;
1.3.2.1.49.4. Os equipamentos do tipo “spare part” também devem vir com as interfaces populadas com transceivers e prontas para uso, nos mesmos moldes que um equipamento ativo do nodo;
1.3.2.1.49.5. Implementar gerenciamento *out-of-band* via interface Ethernet RJ45. Esta interface não deve ser contabilizada para o atendimento daquelas originalmente especificadas para o equipamento;
1.3.2.1.49.6. Fornecer cabo de console compatível com a porta de console fornecida junto com o equipamento;
1.3.2.1.49.7. Suportar agregação de interfaces de rede de acordo com o padrão IEEE 802.3ad (LACP);
1.3.2.1.49.8. Implementar pelo menos 1.000 (mil) VLANs por ambiente;
1.3.2.1.49.9. Suportar pelo menos 3.000.000 (três milhões) de sessões simultâneas por nodo ou no mínimo 12.000.000 (doze milhões) de conexões simultâneas por nodo;
1.3.2.1.49.10. Suportar pelo menos 300.000 (trezentas mil) sessões de decriptografia concorrentes por nodo;
1.3.2.1.49.11. Implementar pelo menos, 250.000 (duzentas e cinquenta mil) novas conexões TCP por segundo por nodo;

1.3.2.1.49.12. Implementar Prevenção e Proteção contra Ameaças (Threat Prevention / Threat Protection) real, ou seja, realizando análise e inspeção completa de todo conteúdo dos pacotes, garantindo um *throughput* mínimo de 32 Gbps (trinta e dois gigabits por segundo) para cada nodo, com todas as funcionalidades e todas as assinaturas habilitadas simultaneamente, considerando pacotes TCP multiprotocolo em IPv4 e IPv6;
1.3.2.1.49.13. Implementar Inspeção TLS Completa, ou seja, atuar realizando abertura, análise e inspeção profunda completa de todo conteúdo dos pacotes criptografados e aplicando a esse tráfego as respectivas diretrizes de segurança, garantindo um *throughput* mínimo de 20 Gbps (vinte gigabits por segundo) para cada nodo, considerando chaves de criptografia de 2048 bits com hash SHA256 com pelo menos as seguintes funcionalidades habilitadas simultaneamente: NGIPS (Intrusion Prevention System), Anti-Malware, Anti-Virus em tráfego de Rede, Sandboxing, Advanced Malware Protection, DNS Filtering, Anti-Bot, Anti-C&C, URL/Web Filtering, Proteção contra Exploits e Zero-Day;
1.3.2.1.49.14. Suportar um *throughput* real de IPSec VPN de no mínimo 10 Gbps (dez gigabits por segundo) para cada nodo;
1.3.2.1.49.15. Gerar latência média igual ou inferior a 100 (cem) microssegundos considerando tráfego não criptografado;
1.3.2.1.50. Para demais funcionalidades, a solução deve:
1.3.2.1.51. Suportar transferência remota para atualização do sistema operacional;
1.3.2.1.52. Permitir a criação de regras de *Inspection Bypass*, permitindo ao administrador definir e decidir quais tráfegos não serão inspecionados;
1.3.2.1.53. Suportar, no mínimo, as versões v1.2 e v1.3 do protocolo TLS;
1.3.2.1.54. Construir registro de fluxos de dados relativos a cada sessão iniciada, armazenando para cada uma destas sessões informações tais como: endereços de origem e destino dos pacotes, portas TCP e UDP de origem e destino, bem como números de sequência dos pacotes TCP e UDP, status dos flags “ACK”, “SYN” e “FIN”, facilitando assim o controle de todo tráfego que passa pelo firewall e aplicação da política de segurança;
1.3.2.1.55. Permitir a “randomização” do número de sequência TCP, de modo a garantir que um host situado em uma interface considerada “externa” (insegura), sob o ponto de vista de política de segurança do firewall, nunca tenha acesso ao número de sequência TCP real do host seguro (interno ao firewall) em uma sessão estabelecida entre os referidos hosts;
1.3.2.1.56. Suportar agrupamento lógico de objetos (“*object grouping*”) para criação de regras de filtragem;
1.3.2.1.57. Implementar a contagem de passagem de fluxo para cada regra de filtragem (“*hit counts*” em ACLs) individualmente, independentemente do fato de a configuração da política ter utilizado o conceito de agrupamento lógico de objetos;
1.3.2.1.58. Implementar PIM Sparse Mode e PIM Source Specific Mode;
1.3.2.1.59. Implementar simultaneamente a criação de regras IPv4 e IPv6;
1.3.2.1.60. Permitir captura e armazenamento de pacotes em formato PCAP do *tcpdump*;
1.3.2.1.61. Realizar a monitoração de tráfego de ambientes de rede em modo transparente sem endereço IP;
1.3.2.1.62. Implementar instâncias virtuais de NGFW, de modo que sejam fornecidas no mínimo 20 (vinte) instâncias virtuais por nodo de hardware;
1.3.2.1.63. Ser capaz de inspecionar tráfego simétrico e assimétrico;
1.3.2.1.64. Suportar funcionalidades atualizadas de SD-WAN;
1.3.2.1.65. Suportar integração com Single Sign-on;
1.3.2.1.66. Disponibilizar, por todo o período de vigência do contrato, todos os serviços que forem baseados em assinaturas/subscrição;

1.3.2.1.67. Prover funcionalidades de prevenção de intrusão em seu modo padrão de fábrica (configuração básica) com regras ativas (habilitadas automaticamente quando uma nova política de segurança é criada, em modo bloqueio e com criação de notificação, conforme recomendações do fabricante);
1.3.2.1.68. Permitir a seleção de ações de resposta através das regras de filtragem bem como configurações condicionais, que permitam a definição de ações que alternam entre permitir e bloquear determinados fluxos de acordo com condições encontradas no ambiente (como por exemplo, permitir as 10 (dez) primeiras conexões de um único IP para determinado tráfego de rede. Nesse exemplo, após a conexão número 11 (onze), na mesma janela de tempo, a ação deve ser alternada para bloqueio ou quarentena;
1.3.2.1.69. Suportar assinaturas para proteção contra vulnerabilidades, detecção de exploits, roubo de informações, vírus, *malwares, ransonwares, spywares*, tentativas de reconhecimento de rede, entre outras técnicas de intrusão de modo que as assinaturas estejam organizadas e possam ser filtradas por categoria de ataque;
1.3.2.1.70. Possuir regras que implementem análise e controle comportamental do tráfego;
1.3.2.1.71. Ser capaz de detectar e bloquear ataques de reconhecimento de rede;
1.3.2.1.72. Implementar otimização de tráfego através de controle de banda;
1.3.2.1.73. Implementar *Rate Limiting* baseado em endereços IP, portas ou aplicação;
1.3.2.1.74. Suportar configuração de Autoridades Certificadoras Internas e Externas;
1.3.2.1.75. Possuir ferramenta para criação de filtros customizados, sendo que estes devem permitir a customização de parâmetros tais como:
1.3.2.1.75.1. Nome do filtro;
1.3.2.1.75.2. Descrição do filtro;
1.3.2.1.75.3. Protocolo ou serviço, permitindo a criação de filtros de proteção baseados em IPv4 e IPv6;
1.3.2.1.75.4. Severidade do filtro;
1.3.2.1.75.5. Customização da categoria do filtro;
1.3.2.1.75.6. Classificação do filtro;
1.3.2.1.75.7. Gatilhos de acionamento (triggers), nos quais dados contidos no streaming de rede possam ser utilizados como gatilho para validação de parâmetros adicionais da regra;
1.3.2.1.75.8. Detecção de *payload*, permitindo o uso de strings e expressão regular para detecção avançada de instruções no streaming de rede;
1.3.2.1.75.9. Detecção de payload, permitindo o uso de strings e expressão regular para buscar e validar a existência de informações no cabeçalho HTTP, distinguindo métodos GET, POST, OPTIONS, PUT, DELETE, TRACE, CONNECT, HEAD, LOCK, UNLOCK, PROPFIND. Também deve permitir a validação de dados específicos em URI, URI PATH, URI Target, Header e Payload;
1.3.2.1.75.10. Criação de customizações a nível TCP, sendo possível definir portas de origem e destino, além de validação de flags TCP;
1.3.2.1.76. Suportar processamento de tráfego assimétrico;
1.3.2.1.77. Possibilitar o uso no modo *bypass* total forçado;
1.3.2.1.78. Possuir controles de proteção contra ataques de DDOS, atuando como um SYN PROXY.
1.3.2.1.79. Possuir controles de proteção contra ataques de DDOS baseado em filtros;
1.3.2.1.80. Detectar e permitir o bloqueio de tunelamento de conexões DNS;
1.3.2.1.81. Possuir assinatura que permita a validação de requisições HTTP/2 e HTTP/3;
1.3.2.1.82. Bloquear nativamente a transferência de arquivos maliciosos via FTP;
1.3.2.1.83. Detectar ataques baseados em SSL, como por exemplo detectar o uso de certificados SSL/TLS maliciosos;

1.3.2.1.84. Prover estatísticas de vulnerabilidades, inclusive de dia zero, oferecendo suporte à mitigação de riscos de vulnerabilidades de dia zero e de riscos de segurança;
1.3.2.1.85. Suportar atualizações automáticas dos filtros/assinaturas;
1.3.2.1.86. Apresentar, sempre que a solução for atualizada, descritivo visualizável na própria solução (console local ou gerenciamento centralizado) indicando quais filtros foram incluídos, quais foram modificados e quais foram removidos (*release notes*). O mesmo deve ocorrer para os filtros de ameaças (*malwares*), sendo exigidos os mesmos parâmetros para permitir o acompanhamento e monitoramento dos novos filtros adicionados pela solução;
1.3.2.1.87. Permitir o bloqueio de tráfego baseado na reputação do endereço de IP de origem da conexão, de destino da conexão, através da reputação de IP, DNS e URLs;
1.3.2.1.88. Aplicar categorias para o serviço de reputação, tais como: *Malware, Botnet, Spyware, SPAM*, TOR, *Web Application Attackers*, P2P e *Network Worm;*
1.3.2.1.89. Criar exceções baseadas em domínio e endereços IP, assim como deve ser possível estabelecer as políticas de reputação individuais para cada instância em uso no ambiente;
1.3.2.1.90. Suportar IPv4 e IPv6 na base de reputação IP;
1.3.2.1.91. Implementar base de reputação IP do próprio fabricante, e também permitir o uso de bases de terceiros;
1.3.2.1.92. Implementar políticas de reputação que permitam a customização de ações tanto para bloquear ou permitir determinados acessos;
1.3.2.1.93. Possuir assinaturas de proteção específicas contra malwares. As assinaturas de malware deverão detectar a infiltração, exfiltração e comunicação com servidores de comando e controle através da inspeção do tráfego de rede;
1.3.2.1.94. Ser capaz de interromper atividades maliciosas tais como *ransomware*, fuga de dados, fraude de cliques, etc;
1.3.2.1.95. Ser capaz de bloquear ameaças do tipo *drive-by-downloads*;
1.3.2.1.96. Detectar atividades de comunicação com servidores de comando e controle de botnets;
1.3.2.1.97. Possibilitar a customização de filtros de NGIPS;
1.3.2.1.98. Suportar a importação de regras no padrão SNORT, podendo esta ocorrer de forma direta e nativa via interface de gerenciamento, ou então através de ferramenta de conversão, na qual o arquivo padrão SNORT deve ser importado e convertido para o padrão utilizado pela solução ofertada;
1.3.2.1.99. Identificar tipo de tráfego de rede gerado por dispositivos conectados no ambiente monitorado, incluindo tráfego malware e ataques associados;
1.3.2.1.100. Implementar e identificar a existência de malware em comunicações de entrada e saída;
1.3.2.1.101. Prover as funcionalidades de inspeção especializada em malwares, operando com filtro de ameaças avançadas e análise de execução em tempo real para pelo menos os seguintes tipos: *Command & Control,Vírus, Worms,* Cavalos de Tróia (*Trojans*), *Ransomwares, Adwares, Spywares, Rootkits, Keyloggers, Botnets, Cryptojacking* e *Malwares* sem arquivo;
1.3.2.1.102. Possuir capacidade para monitoração de ataques em tempo real;
1.3.2.1.103. Permitir o controle de arquivos e URLs em tempo real;
1.3.2.1.104. Permitir o controle e bloqueio de aplicações (protocolos, clientes e web) em tempo real;
1.3.2.1.105. Permitir o bloqueio de malwares em tempo real;
1.3.2.1.106. Implementar mecanismos de detecção e bloqueio de vazamento de informações sensíveis no ambiente, ao permitir a identificação de dados em arquivos (criptografados ou não) sendo enviados ou recebidos via protocolo HTTP, HTTPS, FTP e SMTP;
1.3.2.1.107. Possuir capacidade de implementar detecção de ataques que utilizem mecanismo de *exploit* em arquivos do pacote Microsoft 365, XML e PDF;

1.3.2.1.108. Implementar capacidade para detecção de explorações diretas, uso suspeito ou malicioso nas seguintes plataformas de aplicações: Oracle Java Runtime, SQL Server, Apache HTTP Server, Adobe Systems, MySQL, PostgreSQL, MongoDB, plataformas de sistema operacional como (Windows, Linux e MACOs) entre outras;
1.3.2.1.109. Implementar consulta automática a nuvem de inteligência de ameaças global para atualização de objetos, ameaças, vacinas, entre outras funcionalidades de segurança;
1.3.2.1.110. Possuir capacidade de realizar, de forma automática e periódica, consultas e atualizações de dados de reputação para identificação de tráfego associado a origens e destinos de malware, comando e controle, spam, bots, proxies abertos, relays abertos, *phishing* e TOR (The Onion Router), entre outras ameaças;
1.3.2.1.111. Possuir recursos que permitam o envio de informações de eventos para ferramentas de SIEM de fabricantes terceiros;
1.3.2.1.112. Realizar toda detecção e bloqueio de ataques de rede e malwares em tempo real, não sendo uma solução que necessita exclusivamente de tecnologia de virtualização para detecção de arquivos maliciosos e prevenção de malware na rede monitorada;
1.3.2.1.113. Possuir réplica da base de assinaturas atualizadas nos equipamentos on-premise, de modo que no caso de perda de comunicação com a nuvem de segurança do fabricante, a solução possa seguir atuando com as assinaturas armazenadas no repositório local;
1.3.2.1.114. Realizar análises em ambiente virtual controlado (*sandbox*);
1.3.2.1.115. Permitir filtrar tipos de arquivos previamente, para que, ao serem identificados pela solução sejam automaticamente enviados para análise utilizando um repositório *sandbox on-premise* ou tecnologia de virtualização em nuvem;
1.3.2.1.116. Possuir um recurso de análise para arquivos executáveis (MSEXE, MSI, COM, APK, JAR, SWF, etc) de modo a permitir a análise completa do comportamento do arquivo ou código malicioso;
1.3.2.1.117. Suportar análise de documentos do Microsoft 365 (DOC, DOCX, XLS, XLSX, PPT, PPTX, etc);
1.3.2.1.118. Suportar análise de documentos em formato PDF;
1.3.2.1.119. Suportar múltiplos idiomas nas imagens de sistema operacional utilizadas para análise pelos equipamentos, sendo no mínimo, português (brasileiro) e inglês (americano) os idiomas suportados;
1.3.2.1.120. Permitir a utilização das imagens de sistema operacional da CONTRATANTE para detecção de APTs;
1.3.2.1.121. Analisar dinamicamente arquivos compactados (ZIP, BZIP2, RAR, etc);
1.3.2.1.122. Analisar dinamicamente binários PE de 32-bits e de 64-bits;
1.3.2.1.123. Analisar dinamicamente bibliotecas dinâmicas (DLL);
1.3.2.1.124. Analisar dinamicamente arquivos binários;
1.3.2.1.125. Possuir tecnologia própria de análise de artefatos em sandboxing;
1.3.2.1.126. Possibilitar o uso da rede dedicada para a internet na análise de sandbox;
1.3.2.1.127. Analisar dinamicamente arquivos do Adobe Flash (SWF);
1.3.2.1.128. Detectar, caso uma ameaça faça o download de outra (enquanto inspecionada na sandbox) de modo que esta última também seja analisada num evento correlacionado;
1.3.2.1.129. Submeter uma amostra a sistemas operacionais diferentes, a fim de detectar ações específicas para um sistema;
1.3.2.1.130. Ter capacidade de integração via API com soluções de terceiros;
1.3.2.1.131. Identificar ameaças do tipo Ransonware por comportamento;
1.3.2.1.132. Identificar e executar arquivos de scripts no formato Visual Basic e Javascript inclusive quando estiverem ofuscados;

1.3.2.1.133. Disponibilizar acesso a base de dados externa do fabricante que possibilite a correlação entre informações geradas no ambiente com informações de outros clientes que foram afetados pelo mesmo padrão ou tipo de ameaça. Este acesso deve ser via web, e deve possuir referências e atalhos nos próprios relatórios e logs locais da solução;
1.3.2.1.134. Suportar os seguintes Padrões/Normas (Todos os padrões de RFC - Request For Comment - devem ser atendidos nas versões mencionadas neste documento de forma integral ou em sua versão superior (versão atualizada):
1.3.2.1.134.1. IEEE 802.3ad-2021 (Link Aggregation);
1.3.2.1.134.2. IEEE 802.1Q-2022 (VLANs);
1.3.2.1.134.3. Certificação “FIPS 140-2 ou superior”
1.3.2.1.134.4. RFC 1981, "Descoberta de Caminho MTU";
1.3.2.1.134.5. RFC 8200, "Especificação do Protocolo de Internet, Versão 6 (IPv6)";
1.3.2.1.134.6. RFC 2474, “Cabeçalhos IPv4 e IPv6”;
1.3.2.1.134.7. RFC 8415, “Protocolo de configuração dinâmica de hosts para IPv6 (DHCPv6)”;
1.3.2.1.134.8. RFC 4213, "Mecanismos de Transição Básicos para Hosts e Roteadores IPv6";
1.3.2.1.134.9. RFC 4861, "Descoberta de Vizinho IPv6";
1.3.2.1.134.10. RFC 4443, "ICMPv6";
1.3.2.1.134.11. RFC 4862, "SLAAC";
1.3.2.1.134.12. RFC 4301, “Segurança de Arquitetura do Protocolo da Internet”;
1.3.2.1.134.13. RFC 7296, "IPsec/IKEv2";
1.3.2.1.134.14. RFC 4303, “Segurança de Encapsulamento do Payload IP (ESP)”
1.3.2.1.134.15. RFC 4884, “ICMP estendido para oferecer suporte a mensagens com diversas partes”
1.3.2.1.134.16. RFC 7761, “PIM Sparse Mode”;
1.3.2.1.134.17. RFC 1997, “Atributos de Comunidades BGP”
1.3.2.1.134.18. RFC 9000, “QUIC: Um transporte multiplexado e seguro baseado em UDP”;
1.3.2.1.134.19. RFC 2597, "Encaminhamento QoS Assegurado";
1.3.2.1.134.20. RFC 1035, “Nomes de domínio - Implementação e especificação;
1.3.2.1.134.21. RFC 6147, “DNS64: Extensões DNS para tradução de endereços de rede de clientes IPv6 para servidores IPv4”;
1.3.2.1.134.22. RFC 4193, “Endereços Unicast IPv6 Locais Exclusivos;
1.3.2.1.135. Implementar os protocolos de roteamento RIPv2, OSPFv2, OSPFv3 e BGPv4;
1.3.2.1.135.1. Deve suportar autenticação MD5 entre os peers para RIPv2 e OSPFv2;
1.3.2.1.136. Implementar Inspeção *Stateful*;
1.3.2.1.137. Suportar Extensões DNS para IPv6;
1.3.2.1.138. Implementar a definição de VLAN *trunking* conforme padrão IEEE 802.1Q, a criação de interfaces lógicas associadas às VLANs e o estabelecimento de regras de filtragem (Stateful Firewall) entre as subredes associadas a estas VLANs;
1.3.2.1.139. Permitir pelo menos 10 (dez) usuários simultâneos para configurações de filtragem e funcionalidades de firewall.
1.3.2.1.140. Construir registros de fluxos de dados relativos a cada sessão iniciada, armazenando para cada uma destas sessões informações tais como: endereços de origem e destino dos pacotes, portas TCP, UDP e serviços de origem e destino, bem como números de sequência dos pacotes TCP e UDP, status dos flags “ACK”, “SYN” e “FIN”, facilitando assim o controle de todo tráfego que passa pelo firewall e aplicação da política de segurança.
1.3.2.1.141. Possibilitar o controle do tráfego para os protocolos GRE, SIP, H323, IGMP, IPSEC (AH e ESP) baseados nos endereços de origem e destino da comunicação.

1.3.2.1.142. Implementar a integração da solução com o Microsoft Active Directory (MSAD), permitindo a criação de políticas de filtragem baseados em usuários e grupos de usuários existentes na base MS-AD.
1.3.2.1.143. Implementar agrupamento lógico de objetos ("*object grouping*") para criação de regras de filtragem. Deve ser possível criar grupos de pelo menos os seguintes tipos de objetos: hosts, redes IP, serviços e lista de IPs. Deve ser possível verificar a utilização *("hit counts*") de cada regra de filtragem ("*Access Control Entry*") individualmente, independentemente do fato de a configuração da política ter utilizado o conceito de agrupamento lógico de objetos.
1.3.2.1.144. Suportar autenticação usando base local de usuários (interna ao equipamento);
1.3.2.1.145. Implementar a declaração dinâmica de objetos externos, via integração nativa ou API, possibilitando a consulta a objetos externos à solução de modo que estes possam ser utilizados como parâmetros das regras de filtragem ("*Access Control Entry*" / "*Access Control List* ") e sejam atualizados automaticamente (sem a necessidade de recompilar as regras de filtragem existentes, nem adicionar ou excluir objetos manualmente na solução quando for alterado no ambiente externo que originou os objetos) para pelo menos as seguintes fontes de objetos: Cisco ACI, Aruba ClearPass e Vmware;
1.3.2.1.146. Implementar listas de controle de acesso com no mínimo os seguintes campos: IP de Origem, Nome do Usuário/Grupo do AD, IP de Destino, Serviço de origem, Serviço de destino e Ação (permit/deny). O "nome de usuário" deve ser identificado de forma automática e transparente para o usuário final através de consultas à base MS-AD.
1.3.2.1.147. Implementar políticas de controle de acesso baseadas em informações de horário ("*time-based access control*");
1.3.2.1.148. Implementar *Stateful Failover*, ou seja, em caso de falha de uma das unidades, não poderá haver perda de nenhuma das conexões ativas e a transição destas conexões entre os dois nodos deve ser completamente transparente para o usuário final, inclusive para alta disponibilidade e para redes de roteamento / tráfego assimétrico.
1.3.2.1.149. Possuir mecanismo que possibilita o tráfego de serviços específicos em horários específicos;
1.3.2.1.150. Possuir capacidade de filtrar elementos web como JavaScript, HTML5, CSS3, Adobe Flash, Silverlight, JavaFX, WebSockets, WebGL, "applets" Java e controles ActiveX;
1.3.2.1.151. Possuir mecanismo de proteção contra-ataque de negação de serviço (DoS);
1.3.2.1.152. Possuir mecanismo contra-ataques de falsificação de endereços de origem (*IP Spoofing*);
1.3.2.1.153. Possuir proteção contra-ataque de *SYN Flood*, repassando somente as conexões estabelecidas entre os ambientes (*handshake* triplo do protocolo TCP completo);
1.3.2.1.154. Possuir capacidade de limitar o número de conexões TCP simultâneas por IP de origem (sem necessidade de especificar tal endereço);
1.3.2.1.155. Possuir capacidade de controlar conexões simultâneas por IP de origem (sem necessidade de especificar tal endereço);
1.3.2.1.156. Possuir capacidade de limitar o número de conexões TCP simultâneas para um endereço de origem ou de destino especificado;
1.3.2.1.157. Possuir mecanismo de conversão de endereços (NAT) direto e reverso;
1.3.2.1.158. Possibilitar que uma rede com endereços reservados acesse uma rede externa a partir de um único endereço IP e possibilitar também um mapeamento "um para um" de forma a permitir que serviços internos com endereços reservados sejam acessados externamente através de endereços válidos.
1.3.2.1.159. Possibilitar o NAT baseado em políticas definidas pelos endereços de origem, destino e portas TCP/UDP.
1.3.2.1.160. Implementar o serviço de PAT (Port Address Translation);
1.3.2.1.161. Ter a capacidade de implementar, no mínimo, 6.000 (seis mil) regras de NAT;

1.3.2.1.162. Possibilitar limitar o número máximo de conexões simultâneas (Rate Limiting) para cada instância de firewall;
1.3.2.1.163. Possibilitar, para cada instância, averiguar no mínimo os seguintes tipos de recursos: número conexões simultâneas, número de endereços IP traduzidos, número de sessões de gerenciamento simultâneas, número de endereços MAC;
1.3.2.1.164. Operar com independência de instâncias, de modo que a exaustão dos recursos alocados para uma dada instância de firewall não tenha influência sobre a operação das demais instâncias;
1.3.2.1.165. Permitir a operação nos modos roteamento (*Routing Mode*) e transparente (*Transparent Mode*, *Bridge Mode*);
1.3.2.1.166. Suportar qualquer combinação de instâncias em modos diferentes de operação dentro do limite de instâncias solicitado.
1.3.2.1.167. Implementar roteamento estático e dinâmico (OSPF) em IPv4 e IPv6;
1.3.2.1.168. Suportar o tratamento de tráfego assimétrico de modo a não rejeitar tráfego válido para o Data Center de produção;
1.3.2.1.169. Suportar PBR – *Policy Based Routing;*
1.3.2.1.170. Implementar inspeção Stateful de tráfego IPv4 e IPv6;
1.3.2.1.171. Implementar simultaneamente a criação de regras de filtragem IPv4 e IPv6;
1.3.2.1.172. Implementar anti-spoofing (sem uso de ACLs) para endereços IPv4 e IPv6;
1.3.2.1.173. Implementar randomização do número de sequência TCP para conexões TCP que trafegam sobre IPv4 e/ou IPv6;
1.3.2.1.174. Implementar agrupamento lógico de objetos IPv4 e IPv6 (redes, hosts, serviços,etc), estáticos e dinâmicos, e a criação de regras (ACLs) usando tais objetos;
1.3.2.1.175. Permitir a visualização em tempo real de todas as conexões TCP e UDP ativas bem como a remoção de qualquer uma destas a qualquer momento;
1.3.2.1.176. Possuir mecanismo interno de captura de pacotes;
1.3.2.1.177. Permitir o armazenamento de pacotes capturados em formato tcpdump/pcap;
1.3.2.1.178. Suportar alta disponibilidade em modo ativo-standby com todas as funcionalidades habilitadas;
1.3.2.1.179. Suportar alta disponibilidade em modo ativo-ativo, com todas as unidades ativas simultaneamente;
1.3.2.1.180. Possibilitar o registro de toda a comunicação realizada através do firewall e de todas as tentativas de abertura de sessões e conexões que por ele forem recusadas;
1.3.2.1.181. Ser fornecida com seus softwares e licenças irrestritos, à exceção dos itens de subscrição que não possuam licença perpétua, em sua versão mais atual e completa. O fornecimento deve incluir todas as licenças de software necessárias para a implementação de todas as funcionalidades da solução, incluindo as licenças de subscrição, de modo a contemplar todo o período contratual;
1.3.2.1.182. Implementar o registro (l*ogging*) de toda a comunicação realizada através da solução de todas as tentativas de abertura de conexões ou sessões quem forem recusadas por esta;
1.3.2.1.183. Implementar, por interface, as funções de DHCP Server, Client e Relay;
1.3.2.1.184. Possibilitar a exportação de fluxos de dados em Netflow/Sflow/IPFix ou equivalente;
1.3.2.1.185. Possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como *Denial of Service (DoS)* do tipo *Flood, Scan, Session e Sweep*, permitindo filtragem de anomalias de Flooding, Scan, Source e Destination Session Limit, bem como filtragem de anomalias de protocolos;
1.3.2.1.186. Suportar reconhecimento de *ataques de DoS, reconnaissance, exploits e evasion;*
1.3.2.1.187. Possuir mecanismos de detecção/proteção de ataques (Reconhecimento de padrões, Análise de protocolos; Detecção de anomalias);
1.3.2.1.188. Implementar verificação de ataques na camada de aplicação;

1.3.2.1.189. Suportar a verificação de tráfego em tempo real utilizando aceleração de hardware ou software;
1.3.2.1.190. Identificar o uso de táticas evasivas comuns (*CET - Common Evasion Techniques* – tais como túneis, criptografia, fragmentação, inserção de tráfego, exaustão de recursos) seja por comunicações criptografadas ou em claro;
1.3.2.1.191. Permitir a criação de regras de controle de acesso baseadas em informação de reputação dos sites. A base de dados de reputação usada para consulta deve ser atualizada dinamicamente pelo fabricante;
1.3.2.1.192. Permitir criar políticas de acesso baseadas em filtro de categorias de URL, além de possuir categorias dinâmicas pré-configuradas;
1.3.2.1.193. Possuir módulo de filtro de URL integrado na própria ferramenta de Firewall;
1.3.2.1.194. Permitir a criação de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
1.3.2.1.195. Possuir integração com AD, LDAP, NAC, IAM para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
1.3.2.1.196. Incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via LDAP, MS Active Directory ou similares;
1.3.2.1.197. Incluir a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
1.3.2.1.198. Permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet antes de iniciar a navegação;
1.3.2.1.199. Possibilitar base de URLs local no *appliance*, evitando delay de comunicação/validação da URLs;
1.3.2.1.200. Possibilitar a criação de no mínimo 100 (cem) categorias de URLs customizadas;
1.3.2.1.201. Possibilitar a exclusão de URLs do bloqueio por categoria;
1.3.2.1.202. Possibilitar a customização de página de bloqueio;
1.3.2.1.203. Possibilitar o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando tal evento na tela de bloqueio e possibilitando a opção de continuar a navegação, seguindo acessando o site por um tempo);
1.3.2.1.204. Permitir que a atualização da base de dados de URLs seja automática com a opção de ser feita também manualmente;
1.3.2.1.205. Permitir a configuração de regras de exceção de inspeção de tráfego por endereço IP origem/destino e por VLAN ou ambiente, realizando apenas a comutação do tráfego sem executar inspeção;
1.3.2.1.206. Possuir capacidade de atualização manual e automática das assinaturas, por nodo;
1.3.2.1.207. Realizar a monitoração de ambientes de rede em modo transparente sem endereço IP associado às interfaces de monitoração;
1.3.2.1.208. Monitorar VLANs padrão 802.1Q;
1.3.2.1.209. Manter os logs de ataques e de alarmes enviados pelos subsistemas;
1.3.2.1.210. Ser capaz de realizar auditoria das atividades de cada usuário com perfil administrativo e permissão de acesso à solução;
1.3.2.1.211. Ser capaz de visualizar no mínimo as seguintes informações:
1.3.2.1.211.1. Incidentes de Intrusão;
1.3.2.1.211.2. Políticas aplicadas;
1.3.2.1.211.3. Atualizações instaladas;
1.3.2.1.211.4. *Login* e *Logout* na interface web de gerência;

1.3.2.1.211.5. Inclusões e remoções de regras;
1.3.2.1.211.6. Configurações relacionadas ao envio de informações detectada pelos sensores de prevenção contra invasão, para dispositivo de armazenamento externo a solução de gerenciamento.
1.3.2.1.212. Permitir enviar os logs de auditoria das atividades de cada usuário, para um servidor de Syslog/SIEM;
1.3.2.1.213. Permitir temporariamente o armazenamento dos dados coletados e inspecionados em banco de dados local;
1.3.2.1.214. Permitir inspeção em IPv6 incluindo tunelamento IPv4 em IPv6 e IPv6 em IPv6;
1.3.2.1.215. Permitir identificar/restringir o acesso de *hosts* externos ao perímetro monitorado baseando-se em informações de reputação, ranges IP e listas de domínios;
1.3.2.1.216. Possuir capacidade de criar regras independentes para cada instância de inspeção;
1.3.2.1.217. Ser capaz de reconstruir e inspecionar fluxos de dados na camada de aplicação;
1.3.2.1.218. Possuir capacidade de remontagem de fluxo TCP e IP *defragmentation*;
1.3.2.1.219. Possuir capacidade de resistência à ferramentas de evasão;
1.3.2.1.220. Possuir a capacidade de identificação de protocolos que utilizam portas aleatórias;
1.3.2.1.221. Detectar e bloquear ataques independente do sistema operacional alvo;
1.3.2.1.222. Permitir monitoração de sessões de pacotes na rede, atuando em modo "*Stateful Inspection*" (análise pacote a pacote e todo o seu estado), sendo capaz de bloquear ataques e tráfego não autorizado ou suspeito;
1.3.2.1.223. Possuir filtros de "*PortScan*", protegendo a rede contra-ataques do tipo "*Scan*";
1.3.2.1.224. Possuir filtros de proteção a equipamentos de rede, protegendo contra ataques a vulnerabilidades de equipamentos de rede (ex.: roteadores, switches, etc);
1.3.2.1.225. Realizar análise e decodificação de fluxos de pacotes nas camadas 2 à 7 com no mínimo suporte aos seguintes protocolos e aplicações: IP, DNS, H.323, TCP, RPC, SIP, ICMP, HTTP, HTTPS, QUIC, FTP, ARP, Telnet, SMTP, UDP, IMAP e SMB (quando aplicado);
1.3.2.1.226. Possuir filtros de vulnerabilidades específicos dos protocolos de VoIP que bloqueiem: anomalias de protocolos, ataques de negação de serviço, vulnerabilidades específicas conhecidas, ferramentas de ataque e geradores de tráfego que causem degradação ou indisponibilidade de serviços;
1.3.2.1.227. Detectar e bloquear as seguintes categorias de ataques e ameaças:
1.3.2.1.227.1. Malwares (assinatura de IPS que trata malware);
1.3.2.1.227.2. *Port Scans*;
1.3.2.1.227.3. Ataques VoIP;
1.3.2.1.227.4. Ataques IPv6;
1.3.2.1.227.5. Ataques DoS;
1.3.2.1.227.6. Buffer Overflows;
1.3.2.1.227.7. Ataques P2P;
1.3.2.1.227.8. Anomalias em protocolos e aplicações;
1.3.2.1.227.9. Ameaças *Zero-Day*;
1.3.2.1.227.10. Pacotes malformados;
1.3.2.1.227.11. Segmentação TCP e fragmentação IP;
1.3.2.1.228. Possuir no mínimo as seguintes proteções contra-ataques a aplicações Web:
1.3.2.1.228.1. *Authentication;*
1.3.2.1.228.2. *Brute Force;*
1.3.2.1.228.3. *Buffer Overflow;*
1.3.2.1.228.4. *Cache Poisoning;*
1.3.2.1.228.5. *Client-side attacks;*
1.3.2.1.228.6. *Cross-Site Scripting;*

1.3.2.1.228.7. *Cross-Site Scripting (XSS);*
1.3.2.1.228.8. *CSRF (Cross-Site Request Forgery);*
1.3.2.1.228.9. *CSRF (Cross-Site Request Forgery);*
1.3.2.1.228.10. *Directory Indexing;*
1.3.2.1.228.11. *Information Disclosure;*
1.3.2.1.228.12. *Injection Attacks;*
1.3.2.1.228.13. *Malicious Files Execution;*
1.3.2.1.228.14. *Malware;*
1.3.2.1.228.15. *Path Traversal;*
1.3.2.1.228.16. *Phishing;*
1.3.2.1.228.17. *Ransomware;*
1.3.2.1.228.18. *SQL Injection;*
1.3.2.1.228.19. *Web Protection;*
1.3.2.1.228.20. *Zero-Day Exploit;*
1.3.2.1.229. Permitir criar regras para filtro (ACLs) com base em:
1.3.2.1.229.1. Endereços de origem/destino;
1.3.2.1.229.2. Protocolos;
1.3.2.1.229.3. Serviços;
1.3.2.1.229.4. Domínios, Subdomínios;
1.3.2.1.229.5. Uso de caractere coringa para referenciar complementos de URL;
1.3.2.1.229.6. Listas de IP;
1.3.2.1.229.7. Objetos Dinâmicos;
1.3.2.1.230. Permitir a seleção de nós de objetos dinâmicos do tipo árvore importados de entidades externas diretamente nas ACLs;
1.3.2.1.231. Permitir a criação de ACLs por agendamento para que possam entrar e sair em vigor com dia e hora pré-agendados;
1.3.2.1.232. Implementar protocolo DTLS (TLS over UDP);
1.3.2.1.233. Suportar o encaminhamento e análise de tráfego em jumbo frame (9100 bytes);
1.3.2.1.234. Implementar proteção contra-ataques DDoS através dos seguintes métodos:
1.3.2.1.235. Controle (limite de quantidade) de conexões por origem;
1.3.2.1.236. Controle (limite de quantidade) de conexões por destino;
1.3.2.1.237. Possibilitar que os pacotes sejam capturados para análise;
1.3.2.1.238. Ser capaz de identificar e bloquear ataques baseados em análises de anomalias de tráfego, anomalias de protocolo, assinaturas e vulnerabilidades;
1.3.2.1.239. Ser fornecida com uma configuração de filtros recomendados pré-configurados;
1.3.2.1.240. Permitir o retorno de uma configuração aplicada erroneamente (perda de acesso ao modo configuração) de maneira automática (*rollback* automático);
1.3.2.1.241. Permitir a identificação de anomalia de rede observando o tráfego ou informações do fluxo de ativos da rede de forma nativa;
1.3.2.1.242. Permitir a análise do comportamento da rede, com o intuito de detectar ameaças com origem/destino a ambientes monitorados pela funcionalidade de NGIPS;
1.3.2.1.243. Permitir a análise do comportamento da rede fornecendo visibilidade do uso do ambiente monitorado para auxiliar na solução de falhas de rede ou degradação de desempenho, disponibilizando, no mínimo, as seguintes informações:
1.3.2.1.243.1. Fluxos de sessão dos hosts;
1.3.2.1.243.2. Hora de início/fim;
1.3.2.1.243.3. Quantidade de dados trafegados;

1.3.2.1.244. Ser gerenciável via porta de console, SSH e HTTPS;
1.3.2.1.245. Suportar diferentes métodos de autenticação como MFA, SSO, entre outros;
1.3.2.1.246. Suportar políticas de acesso por identidade, grupo, perfil, aplicação e dispositivo;
1.3.2.1.247. Permitir o uso com restrições de funcionalidades de uma ou mais aplicações para um determinado grupo de usuários, negando totalmente o uso para os demais usuários. Todos esses usuários devem ser autenticados através de um serviço de autenticação definido pelo administrador da solução;
1.3.2.1.248. Negar totalmente o uso de uma ou mais aplicações, independente do usuário;
1.3.2.1.249. Permitir segregação de acesso por perfis e por grupos de usuário baseado em aplicação (ex: perfil do usuário_1 pode acessar somente um conjunto de aplicações “A” e o grupo do usuário_2 pode acessar somente um conjunto de aplicações “B”;
1.3.2.1.250. Ser capaz de identificar as aplicações por heurística a fim de detectá-las através de análise comportamental do tráfego observado;
1.3.2.1.251. Permitir a criação de filtros de controle de acesso baseados em geolocalização;
1.3.2.1.252. Possuir capacidade de criar assinaturas definidas pelo usuário com uso de expressões regulares;
1.3.2.1.253. Ter a capacidade de identificar o tipo de arquivo trafegado e permitir a criação de políticas de detecção e bloqueio de eventos baseados no tipo de arquivo;
1.3.2.1.254. Efetuar análise de conteúdo de aplicações em camada 7;
1.3.2.1.255. Possuir regras que blindem equipamentos de rede contra ataques que explorem vulnerabilidades, detectem tunelamento de protocolos, e cabeçalhos IP incompletos, além de filtros que permitam e detecção e controle de aplicações, tais como Youtube, MS Teams, TOR, Instagram, etc;
1.3.2.1.256. Prover filtros de detecção de aplicações e suas categorias permitindo a ativação de controles de banda;
1.3.2.1.257. Suportar a identificação e controle de aplicações através de inspeção profunda de pacotes (*Deep Packet Inspection*), independentemente das portas/protocolo, técnicas de evasão usadas pela aplicação;
1.3.2.1.258. Implementar múltiplos métodos de identificação e classificação das aplicações, incluindo categoria, subcategoria, tipo e nível de risco;
1.3.2.1.259. Suportar o controle sobre aplicações desconhecidas (e não somente sobre aplicações conhecidas);
1.3.2.1.260. Contar com ferramentas de visibilidade que permitam administrar o tráfego de aplicações;
1.3.2.1.261. Possibilitar que o controle de portas seja aplicado para todas as aplicações;
1.3.2.1.262. Permitir criar regras para monitoramento e controle das aplicações e serviços nos ambientes monitorados, sendo capaz de executar, no mínimo, as seguintes ações:
1.3.2.1.263. Permitir o uso irrestrito de uma ou mais aplicações;
1.3.2.1.264. Permitir o uso irrestrito de uma ou mais aplicações para um determinado grupo de usuários, negando totalmente o uso para os demais usuários. Todos esses usuários devem ser autenticados através de um serviço de autenticação definido pelo administrador da solução;
1.3.2.1.265. Possibilitar a diferenciação e controle de partes das funcionalidades das aplicações como, por exemplo, permitir o chat e bloquear a transferência de arquivos;
1.3.2.1.266. Suportar o controle de aplicações Web 3.0 e padrões anteriores, definindo quais são as operações permitidas para cada uma destas aplicações;
1.3.2.1.267. Incluir a capacidade de atualização da base de assinaturas de aplicação de forma automática com a opção de ser feita manualmente;
1.3.2.1.268. Permitir a customização de regras de detecção de aplicações proprietárias;
1.3.2.1.269. Reconhecer e inspecionar aplicações IPv6;

1.3.2.1.270. Ser capaz de identificar tráfego de aplicações mesmo que estas estejam usando portas fora do padrão (identificação pela aplicação e não pela porta/protocolo);
1.3.2.1.271. Permitir a classificação das aplicações de acordo com a categoria, tipo e nível de risco.
1.3.2.1.272. Suportar descriptografia de SSL para identificação de aplicações;
1.3.2.1.273. Possibilitar o uso da mesma base de políticas de segurança tanto para o ambiente on-premise como para o ambiente em nuvem;
1.3.2.1.274. Suportar cache, filtragem de conteúdo e controle de acesso por usuário, grupo e aplicação;
1.3.2.1.275. Suportar integração com diretórios corporativos (ex;: Active Directory, LDAP, Radius) para autenticação e aplicação de políticas;
1.3.2.1.276. Gerar relatórios detalhados de navegação, incluindo acessos permitidos, bloqueados e tentativas de *bypass*;
1.3.2.1.277. Prover controle e visibilidade do uso de aplicações SaaS (ex.: Microsoft 365, Google Workspace, Salesforce, Dropbox etc;);
1.3.2.1.278. Permitir inspeção e bloqueio de Shadow IT, identificando e restringindo uso de aplicações não autorizadas;
1.3.2.1.279. Oferecer proteção contra *malware, phishing* e vazamento de dados (DLP) em acessos externos, inclusive de usuários móveis e remotos;
1.3.2.1.280. Permitir definição de políticas únicas e centralizadas, aplicáveis de forma consistente a ambientes locais e em nuvem;
1.3.2.1.281. Prover monitoramento e relatórios unificados, com correlação de eventos entre as funcionalidades de segurança;
1.3.2.1.282. Permitir alertas automáticos e execução de ações preventivas (ex.: bloqueio de IPs/domínios, quarentena de usuários, ativação de políticas de DLP, entre outros);
1.3.2.1.283. Suportar funcionalidade nativa de CASB, com visibilidade e controle de uso de aplicações SaaS;
1.3.2.1.284. Suportar o controle granular de atividades em SaaS (ex: upload, download, visualização);
1.3.2.1.285. Suportar integração com serviços de diretório (ex: Active Directory, LDAP, SAML, Azure AD);
1.3.2.1.286. Implementar proteção contra ameaças avançadas (malware, phishing, ransomware);
1.3.2.1.287. Oferecer relatórios e dashboards gerenciais e operacionais;
1.3.2.1.288. Possibilitar que a solução gere relatórios de conformidade;
1.3.2.1.289. Disponibilizar APIs abertas para integração com plataformas de SIEM, SOAR e demais sistemas de segurança;
1.3.2.1.290. Suportar a operação da funcionalidade de PROXY;
1.3.2.1.290.1. Implementar, para a funcionalidade de PROXY, licenciamento para pelo menos 500 (quinhentos) usuários simultâneos;
1.3.2.1.290.2. Possibilitar que o tráfego de usuários remotos e dispositivos móveis seja automaticamente redirecionado para o proxy em nuvem, garantindo inspeção e aplicação de políticas corporativas;
1.3.2.1.290.3. O proxy em nuvem deve ser fornecido em arquitetura multi-região, assegurando baixa latência e disponibilidade global;
1.3.2.1.291. Suportar a operação da funcionalidade de SWG de forma nativa e integrada ao fabricante da solução ofertada;
1.3.2.1.291.1. Implementar, para a funcionalidade de SWG, licenciamento para pelo menos 500 (quinhentos) usuários simultâneos;
1.3.2.1.291.2. Estar disponível também em modelo SaaS nativo do fabricante, para uso em cenários de acesso remoto, filiais e mobilidade;
1.3.2.1.291.3. Implementar, pelo menos, as seguintes funcionalidades:

1.3.2.1.291.4. Filtragem de URL com categorização por base de dados global, atualizada em tempo real;
1.3.2.1.291.5. Inspeção de tráfego HTTPS/SSL/TLS, com capacidade de decriptografia seletiva e controle granular;
1.3.2.1.291.6. Proteção contra ameaças web (*malware, phishing, ransomware, C&C*) com uso de *Threat Intelligence* nativa do fabricante da solução ofertada;
1.3.2.1.291.7. Controle de aplicações Web e SaaS (Shadow IT);
1.3.2.1.291.8. Análise de sandbox em nuvem para arquivos e conteúdos suspeitos acessados via web;
1.3.2.1.291.9. Oferecer relatórios unificados de tráfego, ameaças, usuários e uso de aplicações SaaS;
1.3.2.1.291.10. Disponibilizar APIs nativas para integração com soluções de SIEM, SOAR entre outras;
1.3.2.1.291.11. Disponibilizar registros e auditorias para suporte a LGPD/GDPR e políticas de compliance;
1.3.2.1.291.12. Permitir definição de políticas baseadas em usuário, grupo, dispositivo, geolocalização e contexto de acesso;
1.3.2.1.291.13. Oferecer recursos de *data protection* em acessos web (controle de upload/download, DLP web);
1.3.2.1.292. Implementar a funcionalidade de gateway VPN, suportando no mínimo, túneis na modalidade IPSec VPN LAN-to-LAN e túneis do tipo VPN Client;
1.3.2.1.292.1. Implementar a migração de configurações VPN existentes no ambiente existente de VPN IPSec LAN-to-LAN, mantendo todas a políticas de criptografia, políticas de NAT e filtros de acesso para o ambiente da nova solução apresentada sem a necessidade de alterações nas configurações da VPN do parceiro, com exceção do endereço *"peer"* ou de parâmetros obsoletos, se for pertinente;
1.3.2.1.292.2. Permitir a negociação de túneis IPSec VPN LAN-to-LAN com suporte a, no mínimo:
1.3.2.1.292.2.1. Protocolo IKEv2 para a autenticação de pares IPSec e definição de parâmetros de VPN;
1.3.2.1.292.2.2. Algoritmos de criptografia AES-128 e AES-256;
1.3.2.1.292.2.3. Algoritmos de integridade: SHA-256, SHA-384 e SHA-512;
1.3.2.1.292.2.4. Métodos de autenticação: PSK e RSA;
1.3.2.1.292.2.5. Grupos DH (Diffie-Hellman) para troca de chaves de 2048 bits;
1.3.2.1.292.2.6. Suportar "Perfect Forward Secrecy" e ECDHE-RSA;
1.3.2.1.292.2.7. Suportar a realização de testes de leitura e verificação de CRL (Certificate Revocation List), validando certificado não confiável e certificado revogado;
1.3.2.1.292.3. Suportar a terminação de pelo menos 1.000 (mil) túneis IPSec VPN LAN-to-LAN (Site-to-Site) simultaneamente para cada nodo de hardware. Caso sejam necessárias licenças, estas devem ser fornecidas;
1.3.2.1.292.4. Suportar e prover a terminação simultânea de túneis TLS/SSL ou IPSec, através de *Software Client*, de modo que suporte um total de pelo menos 2.000 (dois mil) usuários VPN, independentemente do tipo de sessão. Caso sejam necessárias licenças, estas devem ser fornecidas;
1.3.2.1.292.5. Suportar configuração de autenticação de usuário de *VPN Client* utilizando senha do dominio do AD, validando o campo "Name".
1.3.2.1.292.6. Suportar configuração e testes de autenticação de usuário de *VPN Client* utilizando o cartão Banrisul Identidade Digital, validando o campo "User Principal Name" (UPN, OID 1.3.6.1.4.1.311.20.2.3) do domínio servidor de gestão de identidades;
1.3.2.1.292.7. Suportar versões do Software *VPN Client* para, no mínimo, os seguintes sistemas operacionais: Windows – 10 e 11, Linux e MacOS;

1.3.2.1.292.8. Permitir o controle de expiração da senha do usuário de *VPN Client* através da definição da quantidade de dias que faltam para a expiração, interagindo com o AD (Microsoft Active Directory) garantindo que o usuário seja avisado, solicitando a troca de senha e atualizando-a no domínio do AD.
1.3.2.1.292.9. Permitir visualizar no software *VPN Client* o endereço privado adquirido durante a negociação da conexão VPN com o concentrador;
1.3.2.1.292.10. Permitir *authentication, authorization and accounting* (AAA) de usuário através de servidor RADIUS;
1.3.2.1.292.11. Implementar o registro (logging) dos comandos executados por usuário e eventuais tentativas não autorizadas de execução de comandos (“accounting”);
1.3.2.1.292.12. Implementar a utilização de certificados digitais para o próprio nodo, suportando integração com certificados digitais (X.509 v3) de terceiros para não repúdio de transações por VPN, e oferecer capacidade de integração com pelo menos 4 Autoridades Certificadoras diferentes;
1.3.2.1.292.13. Suportar leitura e verificação de CRL (Certificate Revocation List) através de, no mínimo, conexões HTTP e LDAP;
1.3.2.1.292.14. Suportar leitura e verificação de OCSP (Online Certificate Status Protocol);
1.3.2.1.292.15. Permitir a terminação de conexões no modo IPSEC over TCP e IPSEC over UDP;
1.3.2.1.292.16. Permitir a configuração de uma lista de acesso “Split Tunneling” nos túneis VPN, de modo a explicitar quais as redes que podem continuar sendo acessíveis de forma direta (sem IPSec) durante uma conexão VPN;
1.3.2.1.292.17. Implementar alta disponibilidade das conexões IPSEC VPN Lan-to-Lan, permitindo a utilização de um segundo nodo em modo “*stand by*”. Em caso de falha de um dos nodos, não deve haver perda das conexões ativas (*Stateful Failover*) e a transição destas conexões entre o nodo que falhou e o nodo que assumiu o tráfego deve ser completamente transparente para o usuário final conectado;
1.3.2.1.292.18. Permitir a criação de “banners” personalizados para indicar se houve sucesso ou falha na requisição de acesso VPN e, em caso de sucesso, mensagens de natureza administrativa;
1.3.2.1.292.19. Permitir a utilização de AD, LDAP, LDAP/SSL, LDAP/TLS, RADIUS, hardware tokens (SecurID ou equivalente), certificados X509 (gravados em disco e/ou em tokens criptográficos/SmartCards); No caso de uso de Software Client, este deve suportar e ter compatibilidade com os métodos de autenticação referidos.
1.3.2.1.292.20. Permitir autenticação através de SmartCard para a qual a infraestrutura deve atender aos seguintes requisitos:
1.3.2.1.292.21. Permitir a utilização de PKI própria com cadeia de dois níveis;
1.3.2.1.292.22. Permitir a utilização de certificados digitais com, no mínimo, par de chaves RSA de 4096 bits e algoritmo de hash SHA-512 para as Autoridades Certificadoras Raiz e Intermediária;
1.3.2.1.292.23. Permitir a utilização de certificados digitais com, no mínimo, par de chaves RSA de 2048 bits e algoritmo de hash SHA-256 para os certificados de entidades finais (Leaf);
1.3.2.1.292.24. Utilizar o valor do campo "User Principal Name" (UPN, OID 1.3.6.1.4.1.311.20.2.3), presente na extensão "Subject Alternative Name" do certificado X.509, para identificar a conta do usuário.
1.3.2.1.292.25. Permitir a utilização, em plataforma Microsoft Windows, de um *Cryptographic Service Provider (CSP)* desenvolvido pelo CONTRATANTE para acesso ao certificado e chave privada utilizados na autenticação do usuário;
1.3.2.1.292.26. Criar diferentes grupos de usuários, com definição por grupo e do tipo de serviço permitido sobre as conexões SSL para o concentrador SSL VPN (web, e-mail, sistemas de arquivos, etc.);
1.3.2.1.292.27. Suportar NAT (Network Address Translation) bi-directional (overlapping) em VPN LAN-to-LAN na qual o mesmo endereçamento IP existe nos dois “peers”;

1.3.2.1.292.28. Suportar operação no modo transparente a NAT (“NAT-transparent mode”), permitindo a utilização dos clientes VPN em ambientes em que já se efetue PAT (Port Address Translation);
1.3.2.1.292.29. Possibilitar a visualização no concentrador o número de conexões VPN estabelecidas em um dado instante e os respectivos parceiros/usuários que estão fazendo uso destas;
1.3.2.1.292.30. Operar em alta disponibilidade com manutenção e compartilhamento do estado de sessão TCP entre os mesmos elementos de um cluster;
1.3.2.1.292.31. Em caso de falha de uma das unidades, não poderá haver perda de nenhuma das conexões VPN ativas (*stateful failover*) e a transição destas conexões entre as duas unidades deve ser completamente transparente para o usuário final, inclusive para alta disponibilidade com dois nós ativos e para redes de roteamento / tráfego assimétrico;
1.3.2.1.292.32. Permitir que os endereços IP de VPN (endereços privados) sejam obtidos a partir de um servidor DHCP especificado pelo administrador do sistema;
1.3.2.1.292.33. Possibilitar a associação de diferentes pools de endereços IP aos diferentes grupos de usuários que solicitarem conexão ao concentrador VPN;
1.3.2.1.292.34. Permitir a definição dos horários do dia e dos dias da semana em que um dado perfil de usuário ou grupo pode requisitar uma conexão VPN;
1.3.2.1.292.35. Permitir o mapeamento de atributos LDAP e RADIUS para parâmetros existentes na configuração local de grupos do concentrador;
1.3.2.1.292.36. Possibilitar escolher, para cada grupo, se os parâmetros usados serão os definidos localmente ou os mapeados de um grupo externo LDAP/RADIUS.
1.3.2.1.292.37. As conexões VPN efetuadas através do *Software Client* devem possuir as seguintes funcionalidades:
1.3.2.1.292.38. Permitir a realização de verificação de parâmetros na máquina do usuário antes da apresentação das credenciais de identificação (pré-Login);
1.3.2.1.292.39. Permitir verificar pelo menos os seguintes atributos: chaves de registro, arquivos, endereços IP e versão do sistema operacional;
1.3.2.1.292.40. Permitir a criação de políticas baseadas pelo menos nos seguintes parâmetros: Sistema operacional; Antivírus; Chave de registro (existência e valor específico a ela atribuído); Arquivos do sistema; Existência de Personal Stateful firewall habilitado;
1.3.2.1.292.41. Permitir a criação de pools de endereços IP de VPN (endereços privados) internamente ao equipamento;
1.3.2.1.292.42. Suportar a integração com servidores RADIUS para que estes façam a atribuição dos endereços IP de VPN (endereços privados) aos clientes;
1.3.2.1.293. Suportar a operação da funcionalidade de SD-WAN, devendo:
1.3.2.1.293.1. Ser disponibilizada de forma nativa e integrada ao fabricante;
1.3.2.1.293.2. Permitir que as políticas de segurança configuradas no NGFW sejam aplicadas de maneira consistente ao tráfego roteado pela funcionalidade de SD-WAN, sem necessidade de appliances adicionais de terceiros;
1.3.2.1.293.3. Suportar múltiplos links WAN simultâneos (MPLS, Internet, 4G/5G, satélite, entre outros), com balanceamento dinâmico de carga;
1.3.2.1.293.4. Suportar seleção dinâmica de caminhos baseada em métricas de latência, jitter, perda de pacotes e disponibilidade;
1.3.2.1.293.5. Possuir mecanismo de failover automático em caso de degradação ou indisponibilidade de link, com tempo de convergência reduzido;
1.3.2.1.293.6. Suportar priorização de aplicações críticas e suporte a QoS de forma integrada;

1.3.2.1.293.7. Implementar mecanismo de roteamento application-aware, permitindo criação de políticas de roteamento baseadas no mínimo, em aplicações, usuários e grupos;
1.3.2.1.293.8. Realizar identificação de aplicações pelo mesmo sistema de detecção do NGFW, garantindo consistência entre políticas de segurança e de conectividade;
1.3.2.1.293.9. Inspecionar todo tráfego roteado pela SD-WAN nativamente pelo NGFW, com suporte a, no mínimo: NGIPS, Antivírus, Antimalware, Anti-bot, Filtragem de URL e DNS e Controle de aplicações;
1.3.2.1.293.10. Permitir integração com demais componentes do fabricante da solução ofertada;
1.3.2.1.293.11. Suportar gateways virtuais de SD-WAN em nuvens públicas (AWS, Azure, GCP, OCI), disponibilizados como appliances oficiais do fabricante da solução ofertada;
1.3.2.1.293.12. Possuir administração unificada das instâncias em nuvem e on-premise pelo mesmo painel de gerenciamento;
1.3.2.1.293.13. Suportar a otimização de conectividade para aplicações SaaS (ex.: Microsoft 365, Salesforce, Zoom), com priorização de rotas e inspeção segura;
1.3.2.1.293.14. Suportar a topologias hub-and-spoke, full-mesh e híbridas, com orquestração centralizada;
1.3.2.1.293.15. Disponibilizar console de administração unificado com visibilidade em tempo real de, pelo menos: Performance dos links WAN, SLA de aplicações, Relatórios de tráfego e de segurança;
1.3.2.1.293.16. Permitir definição de políticas únicas de segurança e conectividade de forma centralizada;
1.3.2.1.293.17. Suporte a APIs abertas para integração com soluções de SIEM e SOAR, entre outras;
1.3.2.1.294. Implementar o uso de INTELIGÊNCIA ARTIFICIAL / MACHINE LEARNING para apoio às atividades de Configuração, Operação, Relatórios, *Analytics*, Auditoria e Compliance, devendo:
1.3.2.1.294.1. Identificar regras redundantes, conflitantes ou obsoletas e recomendar ajustes automáticos para otimização da política de segurança;
1.3.2.1.294.2. Dispor de assistente virtual ou recurso equivalente que utilize IA para simplificar a criação e ajuste de políticas de segurança;
1.3.2.1.294.3. Fornecer resumos ou relatórios gerados com apoio de IA/Machine Learning;
1.3.2.1.294.4. Consolidar automaticamente eventos de segurança em relatórios executivos e técnicos, em linguagem clara, nos idiomas português brasileiro ou inglês (preferencialmente nessa ordem);
1.3.2.1.294.5. Detectar anomalias no tráfego e priorização inteligente de eventos relevantes;
1.3.2.1.294.6. Implementar o fornecimento de informações dinâmicas que utilizem IA para correlacionar eventos de rede, aplicações, usuários e ameaças, entre outros;
1.3.2.1.294.7. Classificar eventos em níveis de criticidade;
1.3.2.1.294.8. Auxiliar no cumprimento de normas e frameworks de segurança, tais como LGPD, GDPR, PCI-DSS, HIPAA, ISO 27001, NIST, entre outros;
1.3.2.1.294.9. Gerar trilhas de auditoria detalhadas, com correlação entre acessos, políticas aplicadas e decisões de bloqueio/permissão, etc;
1.3.2.1.295. Implementar mecanismos de *compliance*, com recomendações de ajustes em políticas de firewall;
1.3.2.1.295.1. Exibir alertas em caso de configuração em desacordo com padrões de melhoras práticas;

1.3.2.2. CENÁRIO B - FIREWALL EM NUVEM e ADMINISTRAÇÃO COMPLEMENTAR

1.3.2.2.1. O cenário B engloba o ambiente de firewall em nuvem e a infraestrutura *on-premise* de administração complementar ao CENÁRIO A - Core de Segurança de Rede, devendo:
1.3.2.2.2. Implementar a funcionalidade de Firewall em Nuvem, devendo:

1.3.2.2.2.1. Ser parte integrante do ecossistema de segurança do fabricante da solução, com gerenciamento unificado de políticas, logs e relatórios entre as modalidades *on-premise* e virtualizado em nuvem;
1.3.2.2.2.2. Implementar modelo de licenciamento Bring Your Own License (BYOL);
1.3.2.2.2.3. Possuir minimamente duas licenças para *appliance* virtual bem como todos os recursos necessários para que um nodo seja implementado em nuvem pública (como por exemplo, AWS, Azure, GCP, etc), de modo que seja uma instância com as mesmas funcionalidades de inspeção e gerenciada no mesmo *dashboard* do restante da solução, possibilitando o uso de créditos do contrato do CONTRATANTE junto à nuvem pública para cobrir os custos de infraestrutura em nuvem da VM, da rede e de outros serviços relacionados à nuvem pública em questão;
1.3.2.2.2.4. Suportar sincronização de objetos de rede, usuários e grupos com o ambiente corporativo do CONTRATANTE;
1.3.2.2.2.5. Implementar Prevenção e Proteção contra Ameaças (Threat Prevention / Threat Protection) real, ou seja, realizando análise e inspeção completa de todo conteúdo dos pacotes, garantindo um *throughput* mínimo de 05 Gbps (cinco gigabits por segundo) para cada appliance virtual, com todas as funcionalidades de Threat Prevention habilitadas simultaneamente;
1.3.2.2.2.5.1. Caso sejam necessários outros itens de referência para determinar a capacidade de desempenho da funcionalidade de Firewall em Nuvem, devem ser tomados como referência os valores equivalentes a um terço da especificação dos requisitos de desempenho solicitados no CENÁRIO A - Core de Segurança de Rede;
1.3.2.2.2.6. Prover, de forma nativa:
1.3.2.2.2.6.1. Inspeção de tráfego L7 (Application Control e URL Filtering);
1.3.2.2.2.6.2. IPS/IDS integrado;
1.3.2.2.2.6.3. Inspeção SSL/TLS (inclusive TLS 1.3);
1.3.2.2.2.6.4. Controle de usuários e identidades;
1.3.2.2.2.6.5. Proteção contra malware e C2C (Command & Control);
1.3.2.2.2.6.6. Monitoramento centralizado e em tempo real;
1.3.2.2.2.6.7. Relatórios unificados (on-premise + nuvem);
1.3.2.2.2.6.8. Integração via APIs REST para automação e DevSecOps;
1.3.2.2.2.7. Consumir Threat Intelligence nativa do fabricante em tempo real;
1.3.2.2.2.8. Suportar VPN site-to-site e client-based, com protocolos padrão (IKEv2/IPSec);
1.3.2.2.2.9. Ser compatível com roteamento dinâmico em nuvens públicas;
1.3.2.2.2.10. Suportar conexão híbrida e multi-cloud, integrando ambientes on-premise, filiais e datacenters;
1.3.2.2.2.11. Suportar *auto scaling* e balanceamento de carga nativos em nuvem;
1.3.2.2.2.12. Oferecer mecanismos de alta disponibilidade (HA) com failover automático;
1.3.2.2.2.13. Suportar a IA e Machine Learning para análise de tráfego;
1.3.2.2.2.14. Suportar funcionalidades de microssegmentação em nuvem, possibilitando a divisão de rede de nuvem em zonas de segurança menores e isoladas, aplicando políticas de segurança individuais a cada carga de trabalho ou aplicativo;

1.3.2.2.3. Implementar infraestrutura on-premise de administração complementar ao CENÁRIO A - Core de Segurança de Rede, devendo:
1.3.2.2.4. Ser composta por um conjunto de dois equipamentos individuais (um nodo para cada Data Center – FIGURA 3), com as mesmas especificações de funcionalidades do CENÁRIO A, contudo, com porte muito menor, devendo ser usada como referência, para definição de porte desses equipamentos, as seguintes premissas:

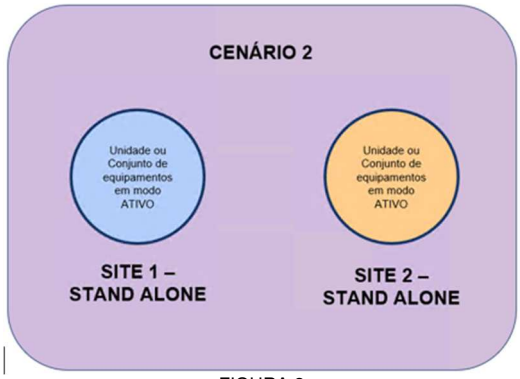


FIGURA 3

1.3.2.2.4.1. Ser fornecido com no mínimo 8 (oito) portas Gigabit Ethernet 1000BaseT para cada equipamento, prontas para uso, independente das interfaces de gerenciamento;
1.3.2.2.4.2. Possuir ao menos uma interface dedicada para gerenciamento out-of-band no padrão RJ45 Gigabit Ethernet para cada equipamento;
1.3.2.2.4.3. Suportar agregação de interfaces de rede de acordo com o padrão IEEE 802.3ad (LACP);
1.3.2.2.4.4. Suportar pelo menos 150.000 (cento e cinquenta mil) conexões simultâneas;
1.3.2.2.4.5. Suportar pelo menos 50.000 (cinquenta mil) sessões simultâneas;
1.3.2.2.4.6. Suportar pelo menos 10.000 (dez mil) sessões de decriptografia concorrentes;
1.3.2.2.4.7. Implementar pelo menos, 25.000 (vinte e cinco mil) novas conexões TCP por segundo;
1.3.2.2.4.8. Implementar pelo menos 500 (quinhentas) conexões SSL concorrentes;
1.3.2.2.4.9. Implementar Prevenção e Proteção contra Ameaças (Threat Prevention / Threat Protection) real, ou seja, realizando análise e inspeção completa de todo conteúdo dos pacotes, garantindo um *throughput* mínimo de 01 Gbps (um gigabit por segundo) para cada equipamento, com todas as funcionalidades e todas as assinaturas habilitadas simultaneamente, considerando pacotes TCP multiprotocolo em IPv4 e IPv6;
1.3.2.2.4.10. Implementar Inspeção TLS Completa, ou seja, atuar realizando abertura, análise e inspeção profunda completa de todo conteúdo dos pacotes criptografados e aplicando a esse tráfego as respectivas diretrizes de segurança, garantindo um throughput mínimo de 500 Mbps (quinhentos megabits por segundo) para cada equipamento, considerando chaves de criptografia de 2048 bits com hash SHA256 e pelo menos as seguintes funcionalidades habilitadas simultaneamente: NGIPS (Intrusion Prevention System), Anti-Malware, Anti-Virus em tráfego de Rede, Sandboxing, Advanced Malware Protection, DNS Filtering, Anti-Bot, Anti-C&C, URL/Web Filtering, Proteção contra Exploits e Zero-Day;
1.3.2.2.4.11. Suportar um throughput real de IPSec VPN para cada nodo de, no mínimo, 1 Gbps (um gigabit por segundo);
1.3.2.2.4.12. Suportar funcionalidades de SD-WAN do fabricante;
1.3.2.2.4.13. Suportar o uso do serviço de DDNS (Dynamic Domain Name System);
1.3.2.2.4.14. Suportar integração com Single Sign-on;
1.3.2.2.4.15. Suportar mecanismos de autenticação de usuários e autenticação multifator (MFA), que não dependam da infraestrutura interna do CONTRATANTE;
1.3.2.2.4.15.1. O sistema de autenticação deverá ser capaz de operar de forma autônoma e independente, mesmo em situações de indisponibilidade da rede corporativa do CONTRATANTE;
1.3.2.2.4.15.2. A solução deve suportar o uso desses mecanismos de autenticação para conexões VPN IPsec no modelo client-to-server, bem como para demais serviços que exijam autenticação de usuários;
1.3.2.2.4.16. Suportar gerenciamento descentralizado de usuários, permitindo que as mesmas credenciais de autenticação sejam válidas e reconhecidas em diferentes equipamentos de NGFW da solução, sem dependência de repositórios locais;

1.3.2.2.4.17. Suportar integração com o Microsoft Entra ID (Azure AD) para autenticação e controle de acesso baseados em identidade, suportando MFA e protocolos modernos de autenticação, como SAML, OAuth e OpenID Connect;
1.3.2.2.4.18. Suportar e prover a terminação simultânea de túneis TLS/SSL ou IPSec, através de Software Client, de modo que suporte um total de pelo menos 500 (quinhentos) usuários VPN, independentemente do tipo de sessão. Caso sejam necessárias licenças, estas devem ser fornecidas;
1.3.2.2.4.19. Possuir Homologação na Anatel sempre que sejam passíveis de homologação compulsória pela referida agência reguladora;
1.3.2.2.4.20. Ser compatíveis com o padrão de fixação em rack(s) de 19" (dezenove polegadas) ou fornecidos na forma de módulos de outros equipamentos com fixação em rack(s) de 19". Devem ser fornecidos kits de suporte específico para este fim. Eventuais ajustes na estrutura do rack (fixação de colunas, etc.) necessários para a instalação da solução deverão ser executados pela LICITANTE;
1.3.2.2.4.20.1. Possuir fontes de alimentação redundantes com tensão de entrada de 220 Volts CA 60 Hz;
1.3.2.2.4.21. Ser fornecidos juntamente com todos os cabos, tomadas, acessórios e softwares necessários à completa carga, instalação, configuração e operação dos equipamentos. Os cabos de energia deverão ter conectores no padrão IEC-320 C13-C14;

1.3.2.3. CENÁRIO C - FUNCIONALIDADES COMPLEMENTARES

1.3.2.3.1. O cenário C engloba funcionalidades complementares ao núcleo da Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida, devendo:
1.3.2.4. Implementar a funcionalidade Análise de tráfego de rede com capacidades de Detecção e Resposta Estendida com a finalidade de detectar e interromper possíveis atacantes ativos na rede, garantindo a proteção dos ativos do CONTRATANTE, devendo:
1.3.2.4.1. Ser capaz de detectar ataques direcionados, ameaças internas e malware utilizando análises avançadas baseadas em Inteligência Artificial (IA) e aprendizado de máquina (ML);
1.3.2.4.2. Monitorar tanto dispositivos gerenciados quanto não gerenciados;
1.3.2.4.3. Analisar dados de rede ricos com aprendizado de máquina para identificar com precisão ataques direcionados, insiders maliciosos e endpoints comprometidos;
1.3.2.4.4. Detectar atividades indicativas de táticas adversárias, incluindo comando e controle (C2), movimento lateral, exfiltração de dados e atividade de malware através do perfilamento de comportamento e da detecção de anomalias;
1.3.2.4.5. Detectar atividades pós-intrusão, reduzindo o Tempo Médio de Detecção (MTTD);
1.3.2.4.6. Fornecer detecção superior às ferramentas de segurança isoladas (siloed tools), aplicando análises a um conjunto integrado de dados, incluindo alertas de segurança, logs de rede, endpoints e nuvem;
1.3.2.4.7. Suportar a coleta de no mínimo 20GB (vinte gigabytes) por dia, incluindo logs de rede e logs de aplicações aprimorados;
1.3.2.4.8. Ser capaz de utilizar firewalls de próxima geração existentes (e/ou firewalls de terceiros) para a coleta de dados de tráfego de rede;
1.3.2.4.9. Possibilitar o agrupamento de alertas relacionados em incidentes;
1.3.2.4.9.1. Os alertas devem incluir informações detalhadas sobre o usuário, aplicação e dispositivo, bem como dados de processos coletados;
1.3.2.4.10. Possuir integração com um serviço de prevenção de malware para determinar se processos suspeitos são, de fato, malwares;
1.3.2.4.11. Possuir integração para orquestrar respostas em diferentes ferramentas de rede e segurança;
1.3.2.4.12. Realizar análise baseada em assinaturas, comportamento e inteligência artificial (IA / Machine Learning);

1.3.2.4.13. Permitir disparo automático de mensagens e ações corretivas para outros elementos de segurança (Ex: NGFW, NGIPS, EDR, XDR, NAC, etc);
1.3.2.4.14. Possibilitar regras temporárias de contenção (por IP, usuário, dispositivo ou aplicação);
1.3.2.4.15. Gerar alertas em tempo real via e-mail, syslog, SNMP, APIs REST ou conectores nativos para SIEM, SOAR, entre outras soluções;
1.3.2.4.16. Suportar playbooks automáticos ou integração com plataformas de orquestração de resposta a incidentes;
1.3.2.4.17. Possuir feeds de inteligência de ameaças globais atualizados regularmente;
1.3.2.4.18. Permitir ingestão de feeds externos via STIX/TAXII;
1.3.2.4.19. Disponibilizar dashboard unificado com visão de ameaças, incidentes e respostas aplicadas
1.3.2.4.20. Fornecer relatórios customizáveis para auditoria, conformidade e governança;
1.3.2.4.21. Correlacionar eventos de rede com outros domínios de segurança (endpoint, identidade, nuvem, etc);
1.3.2.5. Implementar a funcionalidade de Zero Trust Network Access (ZTNA), contemplando, no mínimo:
1.3.2.5.1. Licenciamento inicial para pelo menos 500 (quinhentas) conexões ZTNA simultâneas, suportando expansão;
1.3.2.5.2. Acesso baseado em identidade: integração com diretórios (AD, LDAP, Azure AD, Okta) e suporte a MFA;
1.3.2.5.3. Avaliação de contexto: análise de identidade, dispositivo, localização e postura de segurança;
1.3.2.5.4. Microssegmentação dinâmica: políticas de acesso restritas a aplicações e serviços específicos;
1.3.2.5.5. Integração com ferramentas de SIEM, SOAR, entre outras, permitindo exportação de logs e eventos via syslog, API ou outros protocolos padrão;
1.3.2.5.6. Inspeção de tráfego ZTNA com pelo menos os seguintes mecanismos: NGIPS (Intrusion Prevention System), Anti-Malware, Anti-Virus em tráfego de Rede, Sandboxing, Advanced Malware Protection, DNS Filtering, Anti-Bot, Anti-C&C, URL/Web Filtering, Proteção contra Exploits e Zero-Day;
1.3.2.5.7. Suporte a ZTNA client-based (com agente) e clientless (via navegador);
1.3.2.5.8. Integração com SD-WAN e VPN nativas da solução;
1.3.2.5.9. Implementação do bloqueio automático de usuários ou dispositivos suspeitos;
1.3.2.5.10. APIs ou playbooks de automação para integração com SOAR e orquestração de resposta a incidentes;

1.3.2.6. Implementar a funcionalidade de proteção de dispositivos de usuários devendo:
1.3.2.6.1. Implementar licenciamento inicial para pelo menos 500 (quinhentos) dispositivos, suportando expansão;
1.3.2.6.2. Ocorrer de forma integrada e nativa com o fabricante da solução, garantindo gestão unificada de políticas e eventos;
1.3.2.6.3. Suportar o gerenciamento centralizado de políticas de acesso, controle de aplicações, prevenção contra ameaças e quarentena de endpoints;
1.3.2.6.4. Ser capaz de correlacionar eventos de rede e de endpoint, de forma automatizada, para identificar atividades maliciosas;
1.3.2.6.5. Permitir isolamento, de forma automática ou manual, de endpoints comprometidos diretamente a partir do NGFW ou de console de gerenciamento especifica para esta funcionalidade;
1.3.2.6.6. Suportar resposta orquestrada a incidentes, incluindo bloqueio de tráfego, revogação de credenciais e aplicação de quarentena em endpoints;

1.3.2.6.7. Compartilhar a mesma base de inteligência de ameaças do fabricante do NGFW, atualizada em tempo real;
1.3.2.6.8. Permitir propagação automática de IoCs (Indicators of Compromise) entre endpoints e NGFW;
1.3.2.6.9. Realizar bloqueios e quarentenas coordenadas entre NGFW e endpoints, a partir de um único evento de ameaça identificado;
1.3.2.6.10. Suportar políticas de acesso baseadas em Zero Trust Network Access (ZTNA), aplicadas de forma contínua e dinâmica;
1.3.2.6.11. Consolidar dados de tráfego, incidentes de segurança, status de endpoints e ações de resposta aplicadas;
1.3.2.7. Implementar a funcionalidade de proteção de e-mails, devendo:
1.3.2.7.1. Implementar licenciamento inicial para pelo menos 500 (quinhentas) caixas de e-mail, suportando expansão;
1.3.2.7.2. Implementar proteção avançada de e-mails com detecção de malware, phishing, spam, ataques de spoofing, ransomware, links maliciosos, entre outros tipos de ameaça, atendendo minimamente as seguintes funcionalidades: Antivírus e AntiMalware, Anti-Phishing, Filtro de Spam e Categorias, Proteção contra links maliciosos, Inspeção avançada de anexos e suporte a DLP (Data Loss Prevention);
1.3.2.7.3. Permitir aplicação centralizada de políticas, visibilidade completa de eventos, relatórios detalhados e correlação automática com alertas de firewall e outros sistemas de segurança do ambiente do CONTRATANTE;
1.3.2.7.4. Compartilhar informações de inteligência de ameaças da solução (IP Reputation, URLs maliciosos, comportamento anômalo, etc);
1.3.2.7.5. Permitir aplicação de políticas consistentes de segurança no tráfego de e-mail;
1.3.2.7.6. Possibilitar alertas e correlações automáticas com outros elementos de segurança como por exemplo, NGFW, NGIPS, NAC, EDR, XDR, entre outros;
1.3.2.7.7. Realizar inspeção e proteção via API nativa para plataforma de e-mail Microsoft 365;
1.3.2.7.8. Implementar proteção contra phishing, spear-phishing, BEC (Business Email Compromise), malware e ransomware;
1.3.2.7.9. Aplicar sandboxing avançado para análise dinâmica de anexos suspeitos, com suporte a arquivos executáveis, documentos, scripts e arquivos compactados;
1.3.2.7.10. Permitir análise de links e URLs contidos em mensagens, incluindo reescrita de URLs, verificação em tempo real e bloqueio de links maliciosos;
1.3.2.7.11. Possuir recurso de retração de e-mails maliciosos após a entrega, com remoção automática da caixa do usuário, com ou sem interação do administrador;
1.3.2.7.12. Fornecer relatórios executivos e técnicos personalizáveis, com visão detalhada de incidentes, tendências e métricas de segurança;
1.3.2.7.13. Possuir console unificado de gerenciamento com suporte a múltiplos administradores;
1.3.2.7.14. Empregar tecnologias de proteção baseadas em Inteligência Artificial e Machine Learning para análise de comportamento e detecção de anomalias;
1.3.2.7.15. Oferecer proteção para caixas de e-mail ativas e retroativas (*retrospective scanning*) de mensagens anteriores ao início do serviço;
1.3.2.7.16. Suportar autenticação multifator (MFA) para administradores;
1.3.2.7.17. Permitir políticas de e-mail granulares com ações customizadas como por exemplo bloqueio, quarentena, aviso, etc;
1.3.2.8. Implementar Administração e Gerenciamento Centralizado da solução devendo:

1.3.2.8.1. Permitir a instalação, monitoramento, configuração e atualização de múltiplos equipamentos, simultaneamente, estejam estes instalados localmente ou remotamente.
1.3.2.8.2. Ser capaz de monitorar, configurar, diagnosticar problemas e gerar relatórios de múltiplos equipamentos e funcionalidades;
1.3.2.8.3. Permitir a criação e aplicação de respostas a eventos, proporcionando visibilidade sobre ameaças detectadas, gerando respostas automáticas em caso de incidentes;
1.3.2.8.4. Permitir aplicar um ou mais perfis de inspeção de tráfego a um ambiente ou a um grupo de ambientes;
1.3.2.8.5. Suportar a aplicação de diversos perfis de inspeção de tráfego, trabalhando de maneira simultânea em diferentes ambientes físicos ou lógicos;
1.3.2.8.6. Permitir que toda alteração de política e definições na console de gerenciamento seja registrada;
1.3.2.8.7. Categorizar os eventos de acordo com a severidade;
1.3.2.8.8. Permitir configurar diferentes perfis de usuários com níveis de privilégios hierárquicos;
1.3.2.8.9. Permitir monitorar o uso da CPU sendo possível definir nos dois tipos diferentes de alertas, para diferentes níveis de uso da CPU;
1.3.2.8.10. Permitir monitorar o uso de disco, sendo possível definir nos dois tipos diferentes de alertas, para diferentes níveis de uso do disco;
1.3.2.8.11. Permitir monitorar o uso da memória do appliance, sendo possível definir nos dois tipos diferentes de alertas, para diferentes níveis de uso de memória;
1.3.2.8.12. Permitir monitorar se as interfaces estão recebendo tráfego;
1.3.2.8.13. Gerar gráficos em tempo real das estatísticas do tráfego, ataques filtrados, elementos de rede e serviços;
1.3.2.8.14. Ser gerenciado através de interface WEB segura (HTTPS) ou console da aplicação (client);
1.3.2.8.15. Prover que toda a comunicação entre dispositivos e o gateway de gerenciamento de segurança seja criptografada;
1.3.2.8.16. Possuir recurso de geolocalização;
1.3.2.8.17. Permitir gerar relatórios gráficos, bem como a criação de relatórios periódicos de forma automática;
1.3.2.8.18. Permitir o envio automático dos relatórios para e-mail escolhido pelo administrador da solução;
1.3.2.8.19. Exportar relatórios para, no mínimo, o formato PDF;
1.3.2.8.20. Possuir banco de dados interno para armazenamento dos logs, permitindo ao administrador da solução que redirecione o armazenamento dessa base de dados em um volume de disco remoto;
1.3.2.8.21. Possuir ferramenta interna de manutenção do banco de dados, capaz de realizar no mínimo as seguintes funções:
1.3.2.8.21.1. Backup Manual dos dados e das configurações do sistema de gerenciamento;
1.3.2.8.21.2. Backup agendado dos dados e das configurações do sistema de gerenciamento;
1.3.2.8.21.3. Armazenar no disco local do sistema de gerenciamento o backup dos nodos e sistema de gerenciamento. Assim que o backup for concluído o sistema de gerenciamento deve ser capaz de copiar os dados para hosts diferentes.
1.3.2.8.22. Operar em modo alta disponibilidade, sendo que se o primeiro servidor falhar, o segundo deve continuar operando normalmente sem prejuízos ao gerenciamento do ambiente;
1.3.2.8.23. Permitir integração com ferramentas de monitoramento de rede e SIEM, além de permitir o envio de alertas por e-mail notificando incidentes de segurança;
1.3.2.8.24. Possuir um painel de monitoramento de eventos, contendo pelo menos as estatísticas dos principais filtros acionados, principais atacantes, principais alvos dos ataques, etc;

1.3.2.8.25. Possuir API que permita soluções externas, como o próprio SIEM, a interagir com a solução, devendo permitir pelo menos a adição e remoção de endereços IP suspeitos em listas de reputação, e também permitindo adicionar e remover endereços IP suspeitos da quarentena;
1.3.2.8.26. Possuir módulo de relatórios próprio, incluindo *templates* que indiquem os principais riscos de segurança detectados no ambiente, contando com modelos pré-estabelecidos;
1.3.2.8.27. Ser fornecida em formato virtualizado ou on-premise, com o dimensionamento adequado ao porte da solução, de forma que devem ser fornecidos todos os requisitos de software, hardware e licenciamento, conforme o caso, necessários para o pleno funcionamento da solução, operando em alta disponibilidade nos datacenters da CONTRATANTE, sendo que, no caso de indisponibilidade da console de gerenciamento principal, a secundária possa ser utilizada sem gerar prejuízos ao ambiente;
1.3.2.8.28. No caso de uso em formato virtualizado, a solução de gerenciamento centralizado deve ser compatível com o formato de servidores ou appliance virtuais em ambiente VMware versão 8.0U3 ou superior;
1.3.2.8.28.1. O número de servidores que compõe a solução não pode ser superior a 5. Este número pode, no entanto, chegar a 10 (dez) servidores, caso todos os componentes utilizem a modalidade ativo / ativo distribuídos entre dois datacenters. O número máximo de servidores virtuais não pode extrapolar a quantidade e tamanho definidos na tabela abaixo:

Quantidade Máxima	VM	vCPU	Memoria
8 (oito)	Pequena	2	4 GB
6 (seis)	Média	4	8 GB
4 (quatro)	Grande	8	16 GB
2 (duas)	Extra Grande	16	32 GB

1.3.2.8.29. Possuir *dashboard* que permita a adição ou remoção de painéis que serão utilizados no monitoramento do ambiente, customizáveis para cada usuário administrador;
1.3.2.8.30. Permitir a integração com serviços de diretório, tendo suporte aos métodos de autenticação RADIUS, e Active Directory, além de autenticação local (para uso enquanto solução não é integrada com restante da infraestrutura);
1.3.2.8.31. Atuar como ponto central para o gerenciamento de política, devendo possuir versionamento de políticas, capacidade de roll-back, além de capacidade de importação e exportação de configurações;
1.3.2.8.32. Apresentar, através de dashboards ou relatórios, a visualização:
1.3.2.8.32.1. dos aplicativos mais acessados na rede;
1.3.2.8.32.2. dos principais sistemas operacionais;
1.3.2.8.32.3. do risco estimado das aplicações;
1.3.2.8.32.4. do tráfego por categoria de aplicação;
1.3.2.8.32.5. dos top hosts que estão enviando arquivos na rede;
1.3.2.8.32.6. das conexões por reputação de URL;
1.3.2.8.32.7. dos usuários que estão enviando mais informações na rede;
1.3.2.8.32.8. dos eventos por protocolo de aplicação;
1.3.2.8.32.9. das estatísticas de protocolos;
1.3.2.8.32.10. das aplicações e sistemas operacionais que trafegam na rede;
1.3.2.8.32.11. das estatísticas de eventos por segundo por firewall;
1.3.2.8.32.12. das estatísticas de conexões por segundo por firewall;
1.3.2.8.32.13. das conexões por porta, por IP de origem, por IP de destino;

1.3.2.8.32.14. das conexões ao longo do tempo, das conexões por aplicações;
1.3.2.8.32.15. do tráfego por porta, por IP de origem, por IP de destino;d
1.3.2.8.32.16. do tráfego ao longo do tempo permitindo a customização do tempo da base de consulta;
1.3.2.8.32.17. do tráfego por aplicações;
1.3.2.8.32.18. das conexões por país de origem ou de destino;
1.3.2.8.32.19. do tráfego por pais de origem ou de destino;
1.3.2.8.32.20. das sessões criptografadas ao longo do tempo;
1.3.2.8.32.21. das sessões não criptografadas ao longo do tempo;
1.3.2.8.33. Mostrar como é feito o download de novas assinaturas (manual e automático);
1.3.2.8.34. Mostrar segregação de acesso por perfil de usuário baseado em aplicações;
1.3.2.8.35. Mostrar a visibilidade de aplicações rodando em uma porta *default*;
1.3.2.8.36. Mostrar a visibilidade de aplicações em qualquer condição de regra;
1.3.2.8.37. Mostrar a identificação de aplicações com base em app-id, porta ou app-id com portas;
1.3.2.8.38. Mostrar a ativação e desativação de uma política dentro da plataforma;
1.3.2.8.39. Mostrar as opções que a solução suporta para trazer a visibilidade em caso de troubleshooting;
1.3.2.8.40. Visualizar sessões SSL com erro ao longo do tempo;
1.3.2.8.41. Visualizar o status de Certificados SSL;
1.3.2.8.42. Visualizar os motivos de falha de descriptografia SSL;
1.3.2.8.43. Visualizar o tráfego por reputação URL;
1.3.2.8.44. Visualizar as conexões bloqueadas por reputação URL;
1.3.2.8.45. Visualizar as conexões bloqueadas por categoria URL;
1.3.2.8.46. Mostrar o tráfego bloqueado por categoria URL;
1.3.2.8.47. Mostrar as conexões permitidas por categoria URL;
1.3.2.8.48. Mostrar o tráfego permitido por reputação URL;
1.3.2.8.49. Visualizar as informações VPN Lan-toLan (site to site);
1.3.2.8.50. Visualizaras as informações VPN Client- to-site;
1.3.2.8.51. Mostrar os indicadores de compromisso de hosts;
1.3.2.8.52. Mostrar os indicadores de compromisso de usuários;
1.3.2.8.53. Visualizar as ameaças de malware, eventos de intrusão, principais atacantes e principais alvos;
1.3.2.8.54. Mostrar os eventos de intrusão descartados;
1.3.2.8.55. Mostrar os eventos de intrusão informação por pais de origem;
1.3.2.8.56. Mostrar os eventos de intrusão informação por pais de destino;
1.3.2.8.57. Mostrar acessos baseados em URL filtering (domínio, subdomínio com prefixos e sufixos);
1.3.2.8.58. Mostrar a identificação de chamadas HTTP sem nome (IPs explícitos);
1.3.2.8.59. Mostrar as informações de vulnerabilidades;
1.3.2.8.60. Visualizar a utilização de CPU, memória, taxa de transferência das interfaces, estatísticas de conexões, utilização de disco, conexões ativas, pico de conexões, NAT Translations, pico de NAT Translations, estatísticas de desempenho e total de conexões por segundo;
1.3.2.8.61. Mostrar todas as ações realizadas pelos usuários (logon/criação/alteração/adição/exclusão de conteúdo, configurações, parametrizações, etc.) e nos usuários (criação/alteração/deleção de usuários, inclusão/alteração, alterações de senhas, etc.);
1.3.2.8.62. Mostrar a exportação das trilhas de auditoria para consumo das soluções de armazenamento e correlacionamento de eventos do banco (ex.: SIEM, etc.) por meio de mecanismos de exposição seguros (API, Web Service, etc.);

1.3.2.8.63. Mostrar a rastreabilidade do tráfego gerado de modo que se compreenda o que ocorreu em determinado evento (ex.: Usuário/IP - Data/Hora - Origem/Destino - Ação efetuada - Regra/Política afetada);
1.3.2.8.64. Mostrar a visibilidade de atividades dos usuários por tipo de aplicação, URL acessada, nome do usuário, grupo de usuário a que ele pertence;

ESPECIFICAÇÃO DOS TESTES DE BANCADA

Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida

1. TESTES DE BANCADA

1.1. A PROPONENTE deve providenciar, localmente no ambiente do CONTRATANTE ou, em laboratório oficial do fabricante, a depender do requisito a ser validado, os ambientes de testes para validação dos seguintes requisitos:

1.1.1. CONECTIVIDADE e DESEMPENHO GERAL: Considerando a ausência de algumas informações e de parâmetros padronizados em todos os datasheets de fabricantes, torna-se necessária a verificação de alguns requisitos exigidos, devendo ser validados os seguintes itens para os equipamentos do CENÁRIO A – Core de Segurança de Rede (conforme definido na PLANILHA DE ESPECIFICAÇÕES TÉCNICAS):

1.1.1.1. Requisitos a validar:

1.1.1.1.1. Suportar pelo menos 3.000.000 (três milhões) de sessões simultâneas por nodo ou no mínimo 12.000.000 (doze milhões) de conexões simultâneas por nodo;
1.1.1.1.2. Implementar pelo menos, 250.000 (duzentas e cinquenta mil) novas conexões TCP por segundo por nodo;
1.1.1.1.3. Implementar pelo menos 300.000 (trezentos mil) conexões SSL concorrentes por nodo;
1.1.1.1.4. Gerar latência média igual ou inferior a 100 (cem) microssegundos considerando tráfego não criptografado e funcionalidades avançadas de inspeção desabilitadas (impacto da inserção do firewall na linha de comunicação);
1.1.1.1.5. Identificar diferenças de comportamento de inspeção para tráfego simétrico e assimétrico;

1.1.1.2. Condições para o teste:

1.1.1.2.1. O equipamento deve estar em configuração padrão, com firmware estável e todas as licenças para a realização do teste ativas;
1.1.1.2.2. O gerador de tráfego deve ser capaz de gerar e manter fluxos TCP e TLS em alta escala;
1.1.1.2.3. As medições devem ser feitas com ferramentas de precisão para latência (*timestamping* em hardware, quando aplicável);
1.1.1.2.4. As métricas devem ser coletadas via CLI, API, SNMP ou contadores do equipamento testado e do gerador de tráfego;
1.1.1.2.5. O gerador de tráfego deve estar configurado e calibrado;
1.1.1.2.6. As medições devem ser feitas após a estabilização da conectividade com o gerador de tráfego;
1.1.1.2.7. As licenças e recursos de inspeção devem estar ativados;
1.1.1.2.8. Os certificados TLS devem estar configurados;
1.1.1.2.9. Os contadores devem estar zerados antes do teste;
1.1.1.2.10. A coleta automatizada de métricas deve estar habilitada;
1.1.1.2.11. A sincronização de tempo deve estar corretamente configurada (NTP);
1.1.1.2.12. O ambiente de teste deve estar isolado e controlado;

1.1.1.3. Observações sobre a documentação:

1.1.1.3.1. Documentar firmware, versão de software e modelo e número de série dos equipamentos;
1.1.1.3.2. Executar cada teste individualmente, começando com as cargas menores;
1.1.1.3.3. Repetir as medições por três vezes, por no mínimo 02 (dois) minutos cada medição, para garantir consistência dos resultados, observando que esse tempo deve ser contado após estabilização da

conectividade com o gerador de tráfego;
1.1.1.3.4. Registrar capturas de tela e logs dos contadores de sessão e conexão;

1.1.1.4. Alinhamento das Definições:

1.1.1.4.1. Conexão simultânea: entidade definida por uma estrutura de dados que contém os atributos *src IP, src port, dst IP, dst port, protocol* que permanecem na tabela de conexões do firewall;
1.1.1.4.2. Sessão: objeto lógico do dispositivo (ex.: sessão de firewall/*NAT/inspection*), normalmente mapeado de forma associada a uma ou mais conexões (sessão de nível de aplicação/estado mantido pelo dispositivo);
1.1.1.4.3. Sessões de decriptografia concorrentes: sessões ativas onde o tráfego TLS é interceptado e decifrado pelo firewall (*TLS forward proxy / SSL inspection*) e re-encriptado para o destino;
1.1.1.4.4. Novas conexões TCP: taxa de estabelecimento de novas conexões TCP (SYNs completando handshake e encerramento com FIN e FIN-ACK) por segundo;
1.1.1.4.5. Conexões SSL concorrentes: sessões TLS ativas estabelecidas e mantidas;
1.1.1.4.6. Tráfego Simétrico: pacotes de ida/volta passam pelo mesmo dispositivo/caminho;
1.1.1.4.7. Tráfego Assimétrico: pacotes de ida e volta percorrem caminhos diferentes;
1.1.1.4.8. Latência: Tempo de ida e volta por salto de rede do firewall do modo *device forwarding+inspection;*

1.1.1.5. Requisitos de referência do laboratório *(hardware/software)*:

1.1.1.5.1. NOTA: Os requisitos de referência visam simular um ambiente o mais próximo possível da realidade do CONTRATANTE assim como sugerir critérios para a padronização dos testes. Apesar dos requisitos de referência serem apenas um referencial para a montagem do ambiente de testes, e, portanto, não serem estritamente obrigatórios, o cenário de testes apresentado deve ser capaz de gerar as situações descritas, senão da forma proposta, com similaridade técnica a ser justificada e avaliada pela equipe técnica do CONTRATANTE caso algum item não seja apresentado exatamente como descrito.

1.1.1.5.2. Gerador/Analisador de tráfego de alta escala (ex.: IXIA/Keysight, Spirent TestCenter, etc) capaz de:
1.1.1.5.2.1. Gerar milhões de conexões simultâneas e 250 mil novas conexões por segundo;
1.1.1.5.2.2. Criar 100 mil sessões com negociação TLS real (certificados);
1.1.1.5.2.3. Medir latência com precisão de microssegundos (*hardware timestamping*);
1.1.1.5.3. Máquinas de tráfego adicionais (para escala de *endpoints*) ou múltiplos chassis do gerador;
1.1.1.5.4. Clientes/Servidores virtuais (*containers/VMs*) ou estrutura similar para simular aplicações quando necessário;
1.1.1.5.5. Certificados e PKI local para *TLS Inspection* (incluindo CA root para cada cliente);
1.1.1.5.6. Ferramentas de medição e coleta: SNMP, APIs dos vendors, syslog, *counters CLI*;
1.1.1.5.7. Infraestrutura de sincronização de tempo / NTP;

1.1.1.6. Parâmetros de Referência de Medição:

1.1.1.6.1. Contadores: conexões ativas, sessões ativas, *SSL sessions, TLS-inspection sessions*, novas conexões, CPU, MEM, *hardware offload usage*, regras processadas;
1.1.1.6.2. Gerador: número de sockets abertas, conexões ativas, novas conexões, *throughput, per-flow latency/timestamps;*
1.1.1.6.3. Medição de latência: usar *hardware timestamping* no gerador de tráfego ou placa de rede, medir *one-way* ou *per-packet processing time*;
1.1.1.6.4. Log: Coletar syslog/alerts;

1.1.2. PERFORMANCE DE INSPEÇÃO:

1.1.2.1. Como referência para os testes de Performance de Inspeção, devem ser consideradas diferentes métricas de *Traffic Blend Mix* como critério para realização dos testes:

1.1.2.1.1. Amostra de Perfil de Tráfego (*Traffic Blend Mix*) de referência do fabricante: deve ser informado nos resultados dos testes qual o *blend de tráfego* o fabricante utiliza como parâmetro para atingir os números referenciados no seu *datasheet* oficial;

1.1.2.1.2. Amostra de Perfil de Tráfego SSL (Traffic Blend Mix SSL) do CONTRATANTE: Deve ser considerado como referência de tráfego para os testes específicos que fazem menção ao blend SSL do CONTRATANTE o seguinte mix de tráfego:

Aplicação / Tipo de Tráfego	Proporção (%)	Protocolo	Tamanho Médio	Descrição da Ação
HTTPS-64K-10-GET TLS 1.2	70%	HTTPS	64 KB	Requisições Web curtas
HTTPS-64K-10-GET TLS 1.3	30%	HTTPS	64 KB	Requisições Web curtas

1.1.2.1.3. Amostra de Perfil de Tráfego (*Traffic Blend Mix*) do CONTRATANTE: Deve ser considerado como referência de tráfego para os testes específicos que fazem menção ao *blend* do CONTRATANTE o seguinte mix de tráfego:

Aplicação / Tipo de Tráfego	Proporção (%)	Protocolo	Tamanho Médio	Descrição da Ação
HTTP GET – 676 KB	22%	HTTP	676 KB	Página Web de alta carga
HTTP Audio	9%	HTTP	128 Kbps	Streaming de áudio
BitTorrent File Download	2%	TCP	1 MB	Transferência P2P
DNS	5%	UDP/TCP	128 bytes	Consultas e respostas DNS
Exchange-Outlook Email	3%	TCP	17 KB	Mensagens MIME corporativas
Facebook Superflow	1%	HTTPS	250 KB	Tráfego social web
FTP GET 1 MB file	2%	FTP	1 MB	Transferência de arquivo
HTTP Post 100 K PDF File	4%	HTTP	100 KB	Upload de documentos
HTTPS 10 K GET of 10 K file	17%	HTTPS	10 KB	Requisições Web curtas
HTTPS 100 K GET of 100 K file	5%	HTTPS	100 KB	Requisições médias criptografadas
LinkedIn Manage Connections	6%	HTTPS	512 KB	Sessões de rede corporativa
Oracle Enterprise	5%	TCP	variável	Transações de banco de dados
POP3 Message 256–512 bytes	2%	TCP	512 bytes	Mensagens pequenas
Salesforce	5%	HTTPS	200 KB	Aplicativo SaaS corporativo
SMB Enterprise	4%	TCP	512 KB	Compartilhamento de arquivos
SMTP 100 K MIME Message with PDF	3%	TCP	100 KB	E-mails com anexos
SSH Login	1%	TCP	variável	Sessões interativas seguras

Twitter-Base-FB	2%	HTTPS	64 KB	Redes sociais e APIs
YouTube	2%	HTTPS	2 MB	Streaming de vídeo

1.1.2.2. Devem ser validados os seguintes requisitos nos testes de **performance de inspeção** para os equipamentos do CENÁRIO A – Core de Segurança de Rede (conforme definido na PLANILHA DE ESPECIFICAÇÕES TÉCNICAS):

1.1.2.2.1. Implementar Prevenção e Proteção contra Ameaças (*Threat Prevention / Threat Protection*) real, ou seja, realizando análise e inspeção completa de todo conteúdo dos pacotes, garantindo um *throughput* mínimo de **32 Gbps (trinta e dois gigabits por segundo)** para cada nodo, com todas as funcionalidades e todas as assinaturas habilitadas simultaneamente, considerando pacotes TCP multiprotocolo em IPv4 e IPv6, **tendo como referência o *Traffic Blend Mix* do fabricante;**

1.1.2.2.2. Implementar Prevenção e Proteção contra Ameaças (*Threat Prevention / Threat Protection*) real, ou seja, realizando análise e inspeção completa de todo conteúdo dos pacotes, garantindo um *throughput* mínimo de **7 Gbps (sete gigabits por segundo)** para cada nodo, com todas as funcionalidades e todas as assinaturas habilitadas simultaneamente, considerando pacotes TCP multiprotocolo em IPv4 e IPv6, **tendo como referência o *Traffic Blend Mix* do CONTRATANTE;**

1.1.2.2.3. Implementar Inspeção TLS Completa, ou seja, atuar realizando abertura, análise e inspeção profunda completa de todo conteúdo dos pacotes criptografados e aplicando a esse tráfego as respectivas diretrizes de segurança, garantindo um *throughput* mínimo de **19 Gbps (dezenove gigabits por segundo)** para cada nodo, considerando chaves de criptografia de 2048 bits com *hash* SHA256 e pelo menos as seguintes funcionalidades habilitadas simultaneamente: NGIPS (Intrusion Prevention System), Anti-Malware / Anti-Virus, Sandboxing / Advanced Malware Protection, DNS Filtering, Anti-Bot / Anti-C&C, URL Filtering, Web Filtering, Proteção contra Exploits e Zero-Day, **tendo como referência o *Traffic Blend Mix* do fabricante;**

1.1.2.2.4. Implementar Inspeção TLS Completa, ou seja, atuar realizando abertura, análise e inspeção profunda completa de todo conteúdo dos pacotes criptografados e aplicando a esse tráfego as respectivas diretrizes de segurança, garantindo um *throughput* mínimo de **11 Gbps (onze gigabits por segundo)** para cada nodo, considerando chaves de criptografia de 2048 bits com *hash* SHA256 e pelo menos as seguintes funcionalidades habilitadas simultaneamente: NGIPS (Intrusion Prevention System), Anti-Malware / Anti-Virus, Sandboxing / Advanced Malware Protection, DNS Filtering, Anti-Bot / Anti-C&C, URL Filtering, Web Filtering, Proteção contra Exploits e Zero-Day, **tendo como referência o *Traffic Blend Mix* SSL do CONTRATANTE;**

1.1.2.3. Testes de Threat Prevention:
1.1.2.3.1. Configurações obrigatórias:
1.1.2.3.1.1. *Threat Prevention / Threat Protection* ativado em todos os fluxos;
1.1.2.3.1.2. Inspeção de conteúdo habilitada (*Deep Packet Inspection*);
1.1.2.3.1.3. Todas as assinaturas de segurança, reputação, *malware* e *exploit* ativas;
1.1.2.3.1.4. Políticas de segurança aplicadas em modo prevenção (não apenas detecção);
1.1.2.3.1.5. Modo de encaminhamento *inline* (sem *bypass*);
1.1.2.3.1.6. Logs e relatórios ativados para coleta de métricas;
1.1.2.3.1.7. Apresentar valores de latência obtidos nos testes com as funcionalidades de Threat Prevention / Threat Protection ativadas;

1.1.2.4. Testes de *Threat Prevention* com *TLS Inspection*:
1.1.2.4.1. Configurações adicionais obrigatórias:
1.1.2.4.1.1. Abertura e inspeção completa de pacotes TLS 1.2 e TLS 1.3;
1.1.2.4.1.2. Chaves de criptografia RSA 2048 bits com hash SHA-256;
1.1.2.4.1.3. Validar as seguintes assinaturas e mecanismos ativos: NGIPS (Intrusion Prevention System),

Anti-Malware / Anti-Virus, Sandboxing / Advanced Malware Protection, DNS Filtering, Anti-Bot / Anti-C&C, URL Filtering, Web Filtering, Proteção contra Exploits e Zero-Day;
1.1.2.4.1.4. Apresentar valores de latência obtidos nos testes com as funcionalidades de Threat Prevention / Threat Protection com TLS Inspection ativadas;

1.1.2.4.1.5. Não serão permitidos resultados com erros de negociação TLS ou falhas de inspeção maiores que 1% nas amostras de tráfego testadas, observando que estas devem ser avaliadas após estabilização da conectividade com o gerador de tráfego;

1.1.3. AMBIENTE VPN: Devem ser validados os seguintes requisitos no teste para os equipamentos do CENÁRIO A – Core de Segurança de Rede (conforme definido na PLANILHA DE ESPECIFICAÇÕES TÉCNICAS):
1.1.3.1. Configurar, diagnosticar e operacionalizar VPNs (Site-to-Site e Remote Access), aplicando técnicas como: Diffie-Hellman, IPsec – ESP, IKEv2, Tunnel mode, Transport mode, Hairpinning, Split Tunneling, Always-on, NAT Traversal, SSL VPN Clientless;
1.1.3.2. Configurar duas conexões VPN L2L com redundância (redundância de peer, Dual VPN com SD-WAN ou similar) do equipamento da solução a ser ofertada para o gateway VPN existente no ambiente de produção do CONTRATANTE (Cisco Firepower ASA);
1.1.3.3. Testar para o modo VPN L2L a aplicação de regras de ACL, filtros, NAT e PAT;
1.1.3.4. Configurar duas conexões VPN Client em modo *Full Tunneling* e *Split Tunneling*;
1.1.3.5. Implementar *Stateful Failover*, ou seja, em caso de falha de uma das unidades, não poderá haver perda de nenhuma das conexões ativas e a transição destas conexões entre os dois nodos deve ser completamente transparente para o usuário final, inclusive para alta disponibilidade e para redes de roteamento.
1.1.3.6. Configurar e testar redundância de *failover*, de modo a não haver perda de conexões VPN estabelecidas durante a troca de equipamento ativo;

1.1.4. INTEGRAÇÕES: Devem ser validados os seguintes requisitos no teste para os equipamentos do CENÁRIO A – Core de Segurança de Rede (conforme definido na PLANILHA DE ESPECIFICAÇÕES TÉCNICAS):
1.1.4.1. Implementar a declaração dinâmica de objetos externos, via integração nativa ou API, possibilitando a consulta a objetos externos à solução de modo que estes possam ser utilizados como parâmetros das regras de filtragem *("Access Control Entry" / "Access Control List"*) e sejam atualizados automaticamente (sem a necessidade de recompilar as regras de filtragem existentes, nem adicionar ou excluir objetos manualmente na solução quando for alterado no ambiente externo que originou os objetos) para pelo menos as seguintes fontes de objetos: Cisco ACI, Aruba ClearPass e Vmware;
1.1.4.2. Realizar configuração da comunicação via API do gerenciamento da solução com os ambientes Cisco ACI, Aruba ClearPass e Vmware existentes no ambiente do CONTRATANTE e realizar testes de aplicação de objetos externos, obtidos da consulta via API a essas soluções, na população de parâmetros das regras de filtragem *("Access Control Entry" / "Access Control List")* para que sejam utilizados nas regras de permissão ou bloqueio de tráfego quando passarem pelo NGFW. Validar também se os objetos consultados são atualizados automaticamente (sem a necessidade de recompilar as regras de filtragem existentes, nem adicionar ou excluir objetos manualmente na solução de NGFW quando for alterado no ambiente externo que originou os objetos);

1.1.5. INTELIGÊNCIA ARTIFICIAL e MACHINE LEARNING: Devem ser validados os seguintes requisitos na solução ofertada:
1.1.5.1.1.1. Identificar regras redundantes, conflitantes ou obsoletas e recomendar ajustes automáticos para otimização da política de segurança;

1.1.5.1.1.2. Dispor de assistente virtual ou recurso equivalente que utilize IA para simplificar a criação e ajuste de políticas de segurança;
1.1.5.1.1.3. Fornecer resumos ou relatórios gerados com apoio de IA/Machine Learning;
1.1.5.1.1.4. Consolidar automaticamente eventos de segurança em relatórios executivos e técnicos, em linguagem clara, nos idiomas português brasileiro ou inglês (preferencialmente nessa ordem);
1.1.5.1.1.5. Detectar anomalias no tráfego e priorização inteligente de eventos relevantes;
1.1.5.1.1.6. Implementar o fornecimento de informações dinâmicas que utilizem IA para correlacionar eventos de rede, aplicações, usuários e ameaças, entre outros;
1.1.5.1.1.7. Classificar eventos em níveis de criticidade;
1.1.5.1.1.8. Auxiliar no cumprimento de normas e frameworks de segurança, tais como LGPD, GDPR, PCI-DSS, HIPAA, ISO 27001, NIST, entre outros;
1.1.5.1.1.9. Gerar trilhas de auditoria detalhadas, com correlação entre acessos, políticas aplicadas e decisões de bloqueio/permissão, etc;
1.1.5.1.2. Implementar mecanismos de *compliance*, com recomendações de ajustes em políticas de firewall;
1.1.5.1.2.1. Exibir alertas em caso de configuração em desacordo com padrões de melhoras práticas;

1.1.5.1.2.2. VALIDAÇÃO DE RECURSOS DE INTELIGÊNCIA ARTIFICIAL / MACHINE LEARNING: Os testes visam avaliar recursos nativos ou integrados de IA/ML, assistentes virtuais, motores de análise comportamental e mecanismos automatizados.
1.1.5.1.2.3. Os equipamentos deverão estar com todas as funcionalidades de segurança habilitadas e conectados a seus portais de inteligência e nuvem de gestão centralizada;
1.1.5.1.2.3.1. A validação dos testes seguirá os seguintes critérios:

Categoria	Objetivo do Teste	Evidência Esperada	Critério de Aceitação
Otimização de Políticas via IA	Avaliar se o sistema identifica regras redundantes, conflitantes ou obsoletas.	Relatório, resumo ou painel indicando sugestões automáticas de ajuste.	O sistema deve sugerir, de forma autônoma, pelo menos 75% das redundâncias detectadas por análise manual.
Assistente Virtual / IA de Configuração	Validar a existência e operação de assistente baseado em IA.	Interação por interface gráfica ou linha de comando com suporte contextual.	Deve compreender comandos em linguagem natural (PT-BR ou EN) e sugerir configurações corretas.
Anomalias e Priorização Inteligente	Validar se a IA detecta padrões anômalos de tráfego e prioriza eventos relevantes/críticos.	Exibição de alertas e ranking de eventos por criticidade.	O sistema deve evidenciar detecção automática de anomalias e priorização sem intervenção manual.
Compliance Assistido por IA	Verificar recursos que auxiliam na conformidade com LGPD, GDPR, PCI-DSS, etc.	Relatório, resumo ou painel indicando recomendações automáticas.	O sistema deve identificar lacunas e sugerir correções.
Alertas de Configuração Incorreta	Verificar se há alertas preventivos de má configuração.	Exibição de alertas ou notificações em caso de desacordo com padrões e melhores práticas de configuração.	A solução deve emitir ou relacionar alertas quando configurações infringirem melhores práticas.

1.1.5.1.2.3.1.1. Método de execução: Os testes serão realizados em ambiente de laboratório controlado, com a execução das etapas descritas a seguir:

1.1.5.1.2.3.1.1.1. Preparação do Ambiente – Instalar *appliances* físicos ou virtuais com todas as funcionalidades habilitadas;
1.1.5.1.2.3.1.1.2. Inserção de Políticas e Dados de Teste – Importar conjunto de regras simulando ambiente corporativo;
1.1.5.1.2.3.1.1.3. Execução de Análises de IA – Ativar módulos de IA e coletar sugestões e relatórios;
1.1.5.1.2.3.1.1.4. Avaliação de Conformidade – Acionar módulos de compliance assistido e revisar recomendações;

ANEXO XI - TERMO DE COMPROMISSO DE HOMOLOGAÇÃO

Banco do Estado do Rio Grande do Sul S.A., instituição financeira com sede na Rua Capitão Montanha, 177, em Porto Alegre, RS, inscrita no CNPJ sob o nº 92.702.067/0001-96, por seu representante legal no fim assinado, doravante denominado **BANRISUL**, e (razão social), com sede na (--Endereço da empresa --), nº..... , Bairro ....., em ..... -...., CEP .....-....., inscrita no CNPJ sob o n° ....., por seu representante legal no fim assinado, doravante denominada Licitante.

Por este **TERMO DE COMPROMISSO DE HOMOLOGAÇÃO**, as partes acima nomeadas e qualificadas resolvem firmar o presente, como providência anterior a assinatura do contrato e consoante previsto nos termos do edital.

CLÁUSULA PRIMEIRA - DO OBJETO

1.1. O presente TERMO DE COMPROMISSO DE HOMOLOGAÇÃO, define os direitos, obrigações e responsabilidades das partes em relação à fase de amostra e verificação da solução, anterior a assinatura do contrato, conforme previsto no Edital.

CLÁUSULA SEGUNDA – DA HOMOLOGAÇÃO

2.1. A contar da assinatura do presente Termo, a Licitante terá um prazo até 20 (vinte) dias úteis para disponibilizar o ambiente de testes para amostra e verificação, e, uma vez disponibilizado, deve realizar as validações por até 15 (quinze) dias úteis subsequentes, conforme previsto no edital.

2.2. Após a entrega do ambiente de testes, a equipe técnica do Banrisul iniciará os procedimentos relacionados com os testes de bancada da solução. Esta fase de homologação terá o objetivo de verificação e avaliação de atendimento aos requisitos técnicos exigidos no edital.

2.3. O prazo total para homologação da solução será de até 35 (trinta e cinco) dias úteis a contar da assinatura do presente termo.

2.5. Caso a equipe técnica do Banrisul entenda que solução ofertada em homologação não atenda a qualquer requisito técnico exigido em edital, a licitante será automaticamente desclassificada.

2.6. Em caso de desclassificação da licitante, esta terá 15 (quinze) dias corridos para retirar o equipamento instalado, sob pena desta atividade ser executada pela equipe técnica Banrisul, armazenando-o em local que a mais convenha.

2.7. O prazo total estipulado para homologação na presente cláusula, salvo autorização expressa e devidamente justificada do Banrisul, é improrrogável e, caso este não venha a ser cumprido por falhas ou erros de responsabilidade da licitante, esta será desclassificada.

2.8. Na fase de homologação não haverá pagamentos realizados pelo Banrisul, e caso ocorra a homologação, os pagamentos serão realizados na fase contratual, conforme cronograma previsto no Termo de Referência.

2.9. Caso a Licitante seja desclassificada, nada será devido à esta pelo Banrisul.

Porto Alegre, de de .

_____ _____

BANCO DO ESTADO DO RIO GRANDE DO SUL S.A. LICITANTE

TESTEMUNHAS:

_____ _____

Nome: Nome:

CPF: CPF:

ANEXO XII - TERMO DE RECEBIMENTO

Banco do Estado do Rio Grande do Sul S.A., instituição financeira com sede na Rua Capitão Montanha, 177, em Porto Alegre, RS, inscrita no CNPJ sob o nº 92.702.067/0001-96, por seu representante legal no fim assinado, doravante denominado **BANRISUL**, e (razão social), com sede na (--Endereço da empresa --), nº..... , Bairro ....., em ..... -...., CEP .....-....., inscrita no CNPJ sob o n° ....., por seu representante legal no fim assinado, doravante denominada Licitante.

Por este **TERMO DE RECEBIMENTO**, as partes acima nomeadas e qualificadas resolvem firmar o presente, como formalização de entrega definitiva da etapa/atividade referente a ..... .

1. IDENTIFICAÇÃO DA ETAPA

- **Contratada:** [Nome da Empresa / CNPJ]
- **Etapa Concluída:** [Ex: Etapa 01 - Levantamento de Dados / Etapa 02 - Projeto Executivo]
- **Período de Execução da Etapa:** [DD/MM/AAAA] a [DD/MM/AAAA]

2. DECLARAÇÃO DE RECEBIMENTO

Pelo presente instrumento, o **Banco do Estado do Rio Grande do Sul S.A** por intermédio do Gestor/Fiscal do Contrato abaixo assinado, declara o **RECEBIMENTO DEFINITIVO** da referida etapa/atividade. Após análise minuciosa, os serviços/produtos da etapa supracitada foram considerados **DE ACORDO** com o Termo de Referência, a Proposta da Contratada e as cláusulas contratuais, estando aptos para fins de faturamento e pagamento.

3. OBSERVAÇÕES E PENDÊNCIAS (Se houver):

.....
.....
.....
.....
.....
.....

4. CONCLUSÃO E ASSINATURAS

Fica a CONTRATADA autorizada a emitir a Nota Fiscal correspondente a esta etapa, observadas as retenções legais e contratuais aplicáveis.

Porto Alegre, de de .

_____ _____

BANCO DO ESTADO DO RIO GRANDE DO SUL S.A. LICITANTE

TESTEMUNHAS:

_____ _____

Nome: Nome:

CPF: CPF:

ANEXO XIII - TERMO DE ACEITAÇÃO DEFINITIVA

Banco do Estado do Rio Grande do Sul S.A., instituição financeira com sede na Rua Capitão Montanha, 177, em Porto Alegre, RS, inscrita no CNPJ sob o nº 92.702.067/0001-96, por seu representante legal no fim assinado, doravante denominado BANRISUL, e (razão social), com sede na (--Endereço da empresa --), nº..... , Bairro ....., em ..... -...., CEP .....-....., inscrita no CNPJ sob o n° ....., por seu representante legal no fim assinado, doravante denominada CONTRATADA.

Por este TERMO DE ACEITAÇÃO DEFINITIVA, as partes acima nomeadas e qualificadas resolvem firmar o presente como documento formal para a conclusão da etapa de Testes de Aceitação, para a qual o BANRISUL, através de sua equipe técnica, afirma ter efetuado todos os testes necessários para o pleno funcionamento do ambiente de produção em conjunto com a validação da CONTRATADA, e, para tanto, dá pleno aceite à solução implementada.

Também nesta data, estão sendo recebidas pelo BANRISUL, as versões finais dos documentos abaixo:

a) High Level Design (HLD);
b) Plano de Continuidade de Negócios (PCN);
c) Plano de Recuperação de Desastres (PRD);
d) Testes e Evidências da Validação do PRD;
e) Topologia Lógica;

Atendidas as condições de edital, declara-se encerrado o projeto de implementação da nova Solução de Estrutura de Segurança de Redes e Comunicações de Malha Híbrida – CORE DE SEGURANÇA DE REDE.

Porto Alegre, de de .

_____	_____
BANCO DO ESTADO DO RIO GRANDE DO SUL S.A.	LICITANTE
TESTEMUNHAS:	
_____	_____
Nome:	Nome:
CPF:	CPF:

TERMO DE RESPONSABILIDADE E DE MANUTENÇÃO DE SIGILO

Eu, _____, portador do documento de identidade nº _____, expedido pela _____, CPF nº _____, comprometo-me a manter sigilo sobre dados, processos, informações, documentos e matérias que eu venha a ter acesso ou conhecimentos no âmbito do CONTRATANTE, em razão das atividades profissionais a serem realizados e ciente do que preceituam a Lei Complementar 105/2001 que trata do sigilo bancário; o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), nos Artigos 153, 154, 314, 325 e 327 e suas alterações promovidas pela Lei 9.983/2000 e Lei 6.799/1980; o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código do Processo Penal), no Artigo 207; a Lei Federal nº 13.105, de 16 de março de 2015 (Código de Processo Civil); a Lei nº 8.159, de 8 de janeiro de 1991 (Lei de Arquivos), nos Artigos 4, 6 e 25; e o Decreto nº 7.845, de 14 de novembro de 2012 (Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo e dispõe sobre o Núcleo de Segurança e Credenciamento).

Tenho ciência de que o não cumprimento do aqui estabelecido estará a Licitante incidindo em falta gravíssima em conformidade com o estabelecido no Edital propriamente dito. E por estar de acordo com o presente Termo, assino-o na presença das testemunhas a seguir mencionadas.

Assinatura do Colaborador da CONTRATADA

Testemunhas:

_____ _____