PREGÃO ELETRÔNICO N.º 0017/2022 – EDITAL RETIFICADO

Processo nº 22/4000-0000309-9

O **BADESUL DESENVOLVIMENTO S.A. - AGÊNCIA DE FOMENTO/RS** torna público que realizará licitação por meio da utilização de recursos de tecnologia da informática – INTERNET, na modalidade PREGÃO ELETRÔNICO, do tipo **MENOR PREÇO GLOBAL,** que se regerá pelas disposições da Lei Federal nº 13.303, de 30 de junho de 2016, Lei Federal nº 123/2006, de 26 de dezembro de 2006 e suas alterações, Lei Estadual nº. 11.389 de 25 de novembro de 1999, pelo Decreto Estadual nº. 42.434, de 09 de setembro de 2003, Lei Estadual nº. 13.191, de 30 de junho de 2009, e pelo Regulamento Interno de Licitações, pelo estabelecido no presente Edital e seus anexos, mediante as seguintes condições:

DATA DA PUBLICAÇÃO: 08 de novembro de 2022

RECEBIMENTO DAS PROPOSTAS: até às 14h00min do dia 01 de dezembro de 2022

ABERTURA DAS PROPOSTAS: às 14h01min do dia 01 de dezembro de 2022

INÍCIO DA SESSÃO DE DISPUTA DE PREÇOS: às 14h10min do dia 01 de dezembro de 2022

LOCAL: www.pregaobanrisul.com.br ou através do "link" no site www.banrisul.com.br

FORMALIZAÇÃO DE CONSULTAS: licita@badesul.com.br

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

PREGÃO ELETRÔNICO N.º 0017/2022

Processo nº 22/4000-0000309-9

1 DO OBJETO

1.1 Contratação, pelo **menor preço global**, de serviço de solução de Firewall de Próxima Geração (Next-Generation Firewall (NGFW) e demais especificações.

1.2 A Contratação obedecerá aos critérios especificados no Termo de Referência deste Edital (Anexo I do Edital).

2 DO EDITAL

2.1 O Edital poderá ser obtido no site www.pregaobanrisul.com.br ou no site www.badesul.com.br.

2.2 A licitação será realizada na forma eletrônica, por meio do endereço www.pregaobanrisul.com.br ou através do "link" no site www.banrisul.com.br, mediante condições de segurança, criptografia e autenticação.

3 DAS CONDIÇÕES GERAIS DE PARTICIPAÇÃO

3.1 Poderá participar desta licitação empresa cujo objeto social seja compatível com o objeto da licitação e que atenda a todas as exigências estabelecidas neste Edital e seus Anexos.

3.2 Não poderá participar desta licitação, empresa enquadrada em qualquer das seguintes hipóteses:

3.2.1 cujo administrador ou sócio detentor de mais de 5% (cinco por cento) do capital social seja diretor ou empregado do Badesul;

3.2.2 suspensa pelo Badesul;

3.2.3 declarada inidônea pela União, por Estado, pelo Distrito Federal ou pelo Estado do Rio Grande do Sul, enquanto perdurarem os efeitos da sanção;

3.2.4 constituída por sócio de empresa que estiver suspensa, impedida ou declarada inidônea;

3.2.5 cujo administrador seja sócio de empresa suspensa, impedida ou declarada inidônea;

3.2.6 constituída por sócio que tenha sido sócio ou administrador de empresa suspensa, impedida ou declarada inidônea, no período dos fatos que deram ensejo à sanção;

3.2.7 cujo administrador tenha sido sócio ou administrador de empresa suspensa, impedida ou declarada inidônea, no período dos fatos que deram ensejo à sanção;

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

3.3 Que se enquadre em impedimentos contidos em normativos internos do Badesul.

3.4 Aplica-se a vedação prevista no item anterior, também:

3.4.1 à contratação do próprio empregado ou dirigente, como pessoa física, bem como à participação dele em procedimentos licitatórios, na condição de licitante;

3.4.2 a quem tenha relação de parentesco, até o terceiro grau civil, com:

3.4.3 dirigente do Badesul;

3.4.4 empregado do Badesul cujas atribuições envolvam a atuação na área responsável pela licitação ou contratação;

3.4.5 autoridade do Estado do Rio Grande do Sul.

3.4.6 cujo proprietário, mesmo na condição de sócio, tenha terminado seu prazo de gestão ou rompido seu vínculo com o Badesul há menos de 12 (doze) meses.

3.5 É vedada a participação sob forma de consórcio;

3.6 É vedada a subcontratação.

3.7 O licitante para participar do certame deverá declarar em campo eletrônico o pleno conhecimento e atendimento às exigências de habilitação;

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

3.9 A participação dos interessados, no dia e hora fixados no preâmbulo deste Edital, dar-se-á por meio da digitação da senha privativa da licitante, nos termos do item do credenciamento, e subsequente encaminhamento da proposta de preços exclusivamente por meio eletrônico;

3.10 A informação de dados para acesso à sessão do pregão deve ser feita na página inicial do site www.pregaobanrisul.com.br ou através do “link” no site www.banrisul.com.br;

3.11 A simples participação neste Pregão implica na aceitação de todos os seus termos, condições, normas, especificações e detalhes.

4 DO CREDENCIAMENTO

4.1 O credenciamento dos licitantes dar-se-á pelas atribuições de chave de identificação e de senha pessoal e intransferível para acesso ao sistema, obtidos junto à Seção de Cadastro da Central de Licitações do Estado – CELIC;

4.2 O credenciamento e a sua manutenção no respectivo cadastro dependerão de registro cadastral na CELIC;

4.3 O credenciamento junto ao provedor do sistema implica na responsabilidade legal do licitante ou de seu representante legal e na presunção de sua capacidade técnica para realização das transações inerentes ao pregão eletrônico;

4.4 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 BADESUL, responsabilidade por eventuais danos decorrentes do uso indevido da senha, ainda que por terceiros;

4.5 A perda da senha ou quebra do sigilo deverão ser comunicadas imediatamente à Seção de Cadastro da CELIC, para imediato bloqueio de acesso;

4.6 No caso de perda da senha, poderá ser solicitada nova senha na Seção de Cadastro da CELIC, até às 17 horas do último dia útil anterior à data de abertura da sessão do pregão.

5 DA PARTICIPAÇÃO DE MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE

5.1 Os licitantes que declararem, eletronicamente, em campo próprio, quando do envio da proposta inicial, o enquadramento social de que trata este item, devidamente comprovado conforme estabelece o presente Edital, terão tratamento diferenciado e favorecido nos termos da Lei Complementar federal nº 123/2006.

5.2 A ausência dessa declaração, no momento do envio da proposta, significará a desistência da microempresa e/ou de empresa de pequeno porte de utilizar-se das prerrogativas a elas concedidas pela Lei Complementar federal nº 123/2006.

5.3 Consideram-se empatadas as propostas apresentadas pelas microempresas e empresas de pequeno porte que estiverem no limite de até 5% (cinco por cento) superiores à proposta mais bem classificada, desde que esta não seja microempresa ou empresa de pequeno porte.

5.4 Ocorrendo o empate, nos termos da Lei Complementar federal nº 123/2006, a microempresa e empresa de pequeno porte melhor classificada poderá apresentar proposta inferior à proposta de menor preço apurada no certame, no prazo máximo de 5 (cinco) minutos após o encerramento dos lances, sob pena de preclusão.

5.5 No caso de não contratação da microempresa ou da empresa de pequeno porte serão convocadas as empresas remanescentes, de mesmo enquadramento social, na ordem classificatória, para o exercício de mesmo direito, que se encontrem na situação de empate.

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

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

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

5.9 A não regularização da documentação implicará decadência do direito à contratação, sem prejuízo da aplicação da multa de 2% (dois por cento) sobre o valor total da proposta inicial, sendo facultado à Administração convocar as licitantes remanescentes, na ordem de classificação para assinatura da Ata de Registros de preços.

6 DOS PEDIDOS DE ESCLARECIMENTOS, IMPUGNAÇÕES E RECURSOS

6.1 **Os esclarecimentos quanto ao Edital poderão ser solicitados ao pregoeiro em até 3 (três) dias úteis anteriores à data fixada para a abertura da licitação, exclusivamente para o *e-mail*: licita@badesul.com.br.**

6.2 As impugnações ao Edital deverão ser dirigidas ao pregoeiro e enviadas **exclusivamente para o *e-mail*: licita@badesul.com.br**, devendo as impugnações estar assinadas pelo representante legal da empresa.

6.3 Decairá do direito de impugnação ao Edital o licitante que não se manifestar em até 2 (dois) dias úteis antes da data fixada para a abertura da licitação, apontando as falhas ou irregularidades que o viciaram, hipótese em

que tal comunicação não terá efeito de recurso.

6.4 O licitante que apresentar impugnação deverá enviar suas razões fundamentadas ao pregoeiro exclusivamente pelo e-mail **licita@badesul.com.br,** que responderá e submeterá à aprovação da Autoridade Competente.

6.5 Caberá ao pregoeiro, auxiliado pelo setor responsável pela elaboração do Edital, decidir sobre a impugnação no prazo de até vinte e quatro horas.

6.6 A impugnação feita tempestivamente não impedirá o licitante de participar do processo licitatório até o trânsito em julgado da decisão a ela pertinente.

6.7 Acolhida a impugnação do licitante contra o instrumento convocatório, será definida e publicada nova data para realização do certame.

7 DA REFERÊNCIA DE TEMPO

7.1 Todas as referências de tempo citadas no aviso da licitação, neste Edital, e durante a sessão pública, observarão obrigatoriamente o horário de Brasília/DF e serão registradas no sistema eletrônico e na documentação relativa ao certame.

8 DA PROPOSTA

8.1 A proposta de preços prevista no edital deverá ser encaminhada em formulário eletrônico específico, devendo constar os seguintes itens:

8.1.1 Descrição detalhada do objeto da licitação;

8.1.2 Indicação do valor em real, discriminando os valores unitários dos itens, devendo o preço incluir 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 ele, exceto aqueles que este edital indicar como ressarcível.

8.2 A proposta deverá considerar a entrega dos produtos no local indicado pelo Edital;

8.3 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;

8.4 Caberá à licitante acompanhar as operações no sistema eletrônico durante a sessão pública do pregão, sendo responsável pelo ônus decorrente

da perda de negócios diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão;

8.5 As ofertas serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração nas mesmas, sob alegação de erro, omissão ou qualquer outro pretexto;

8.6 As propostas apresentadas nesta licitação terão prazo de validade mínima de 60 (sessenta) dias a contar da data da sessão pública do pregão;

8.7 O licitante poderá apresentar proposta, somente para o(s) Lote(s) que efetivamente demonstrar interesse;

8.8 Os licitantes arcarão com todos os custos decorrentes da elaboração e apresentação de suas propostas;

8.9 Até a abertura da sessão os licitantes poderão retirar ou substituir a proposta anteriormente apresentada;

8.10 Após a abertura da sessão não caberá a desistência da proposta, salvo por motivo justo decorrente de fato superveniente e aceito pelo pregoeiro;

8.11 O descumprimento dos requisitos de habilitação e proposta sujeitará o licitante às sanções previstas neste Edital e a Lei 13.303/2016;

8.12 Nos casos de emissão de declaração falsa, a licitante estará sujeita à tipificação no crime de falsidade ideológica, previsto no art. 299 do Código Penal Brasileiro, nos crimes previstos nos arts. 90 e 93 da Lei Federal nº. 8.666/1993, e no art. 5º da Lei federal 12.846/2013, sem prejuízo da aplicação das sanções administrativas previstas no presente Edital.

8.13 Efetuado o julgamento dos lances ou propostas, será promovida a verificação de sua efetividade, promovendo-se a desclassificação daqueles que:

8.13.1 Contenham vícios insanáveis;

8.13.2 Descumpram especificações técnicas constantes do instrumento convocatório;

8.13.3 Apresentem preços manifestamente inexequíveis;

8.13.4 Se encontrem acima do orçamento estimado para a contratação;

8.13.5 Não tenham sua exequibilidade demonstrada, quando exigido pelo BADESUL;

8.13.6 Apresentem desconformidade com outras exigências do instrumento convocatório, salvo se for possível a acomodação a seus termos antes da adjudicação do objeto e sem que se prejudique a atribuição de tratamento isonômico entre os licitantes.

8.14 A verificação da efetividade dos lances ou propostas poderá ser feita exclusivamente em relação aos lances e propostas mais bem classificados.

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

9 DA ABERTURA DA PROPOSTA E DA ETAPA COMPETITIVA

9.1 A abertura da sessão pública ocorrerá na data e na hora indicadas no Edital.

9.2 **Durante a sessão pública, a comunicação entre o pregoeiro e os licitantes ocorrerá exclusivamente pelo sistema eletrônico.**

9.3 O pregoeiro verificará as propostas apresentadas e desclassificará, motivadamente, aquelas que não estejam em conformidade com os requisitos estabelecidos neste Edital.

9.4 A desclassificação da proposta será sempre fundamentada e registrada no sistema, com acompanhamento em tempo real pelos licitantes, anexando-se cópia das propostas desclassificadas aos autos do processo licitatório.

9.5 O sistema ordenará, automaticamente, as propostas classificadas pelo pregoeiro.

9.6 Somente os licitantes com propostas classificadas participarão da fase de lances.

9.7 Os licitantes classificados poderão encaminhar lances sucessivos, exclusivamente por meio do sistema eletrônico, sendo imediatamente informados do horário e do valor consignados no registro de cada lance.

9.8 Os licitantes somente poderão oferecer lances inferiores ao último por eles ofertado e registrado pelo sistema eletrônico.

9.9 No caso de dois ou mais lances iguais, prevalecerá aquele que for recebido e registrado primeiro.

9.10 Durante o transcurso da sessão, os licitantes terão informações, em tempo real, do valor do menor lance registrado, mantendo-se em sigilo a identificação da ofertante.

9.11 Será permitida aos licitantes a apresentação de lances intermediários durante a disputa.

9.12 A apresentação de lances respeitará o intervalo mínimo de 1% (um por cento).

9.13 Não poderá haver desistência dos lances ofertados após a abertura da sessão, sujeitando-se os licitantes desistentes às sanções previstas neste Edital.

9.14 Caso o licitante não apresente lances, concorrerá com o valor de sua proposta.

9.15 Durante a fase de lances, o pregoeiro poderá excluir, justificadamente, lance cujo valor seja manifestamente inexequível.

9.16 O sistema eletrônico encaminhará aviso de fechamento iminente dos lances, após o que transcorrerá período de até trinta minutos, aleatoriamente determinado também pelo sistema eletrônico, findo o qual será automaticamente encerrada a recepção de lances.

9.17 Definida a proposta vencedora, para fins de empate ficto, aplica-se o disposto neste Edital, se for o caso.

10 DA NEGOCIAÇÃO

10.1 Após o encerramento da etapa de lances e da aplicação do empate ficto, se for o caso, o pregoeiro poderá encaminhar, pelo sistema eletrônico, contraproposta ao licitante que tenha apresentado lance mais vantajoso, visando a que seja obtida melhor proposta, observado o critério de julgamento estabelecido, não se admitindo negociar condições diferentes daquelas previstas no Edital.

10.2 A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

11 DA ACEITABILIDADE E JULGAMENTO DAS PROPOSTAS

11.1 O licitante classificado em primeiro lugar, por convocação e no prazo definido pelo pregoeiro, deverá encaminhar a proposta de preço adequada ao valor proposto, por meio eletrônico – www.pregaobanrisul.com.br.

11.2 O licitante que abandonar o certame, deixando de enviar a documentação solicitada, será desclassificado e estará sujeito às sanções previstas neste Edital.

11.3 O pregoeiro poderá solicitar parecer de técnicos pertencentes ao quadro de pessoal do órgão ou entidade contratante ou de terceiros, para orientar sua decisão.

11.4 Não se considerará qualquer oferta de vantagem não prevista neste Edital, inclusive financiamentos subsidiados ou a fundo perdido.

11.5 Não se admitirá proposta que apresente valores simbólicos, irrisórios ou de valor zero, incompatíveis com os preços de mercado, exceto quando se referirem a materiais e instalações de propriedade do licitante, para os quais ele renuncie expressamente à parcela ou à totalidade de

remuneração.

11.6 Na verificação da conformidade da melhor proposta apresentada com os requisitos deste Edital, será desclassificada aquela que:

11.6.1 Contenham vícios insanáveis;

11.6.2 Se encontrem acima do orçamento estimado para a contratação mesmo após a negociação com o licitante na forma do § 1º do art. 57 da Lei nº. 13.303, de 30 de junho de 2016, salvo se adotado o orçamento sigiloso, situação na qual será revogada a licitação;

11.6.3 Não tenham sua exequibilidade demonstrada, quando exigido pelo Pregoeiro;

11.6.4 Não atenda às exigências do ato convocatório da licitação;

11.6.5 Apresentem desconformidade com outras exigências do instrumento convocatório, salvo se for possível a acomodação a seus termos antes da adjudicação do objeto e sem que se prejudique a atribuição de tratamento isonômico entre os licitantes.

11.6.6 Apresentar preços manifestamente inexequíveis não comprovando sua exequibilidade.

11.7 A verificação da efetividade dos lances ou propostas será feita exclusivamente em relação aos lances e propostas mais bem classificados, obedecendo-se a ordem de classificação.

11.8 Em caso de divergência entre valores grafados em algarismos e por extenso, prevalecerá o valor por extenso.

11.9 A Administração concederá ao licitante a oportunidade de demonstrar a exequibilidade de sua proposta.

11.10 O pregoeiro poderá realizar diligências para aferir a exequibilidade da proposta ou exigir do licitante a sua demonstração.

11.11 Se houver indícios de inexequibilidade da proposta de preço, o pregoeiro poderá efetuar diligência, podendo-se adotar, dentre outros, os seguintes procedimentos:

11.11.1 Questionamentos junto ao licitante para a apresentação de justificativas e comprovações em relação aos custos com indícios de inexequibilidade;

11.11.2 Pesquisas em órgãos públicos ou empresas privadas;

11.11.3 Verificação de outros contratos que o licitante mantenha com a Administração Pública ou com a iniciativa privada;

11.11.4 Pesquisa de preço com fornecedores dos insumos utilizados, tais como: atacadistas, lojas de suprimentos, supermercados e fabricantes;

11.11.5 Verificação de notas fiscais dos produtos adquiridos pelo licitante;

11.11.6 Levantamento de indicadores salariais ou trabalhistas publicados por órgãos de pesquisa;

11.11.7 Estudos setoriais;

11.11.8 Consultas às Secretarias de Fazenda Federal, Distrital, Estadual ou Municipal;

11.11.9 Análise de soluções técnicas escolhidas e/ou condições excepcionalmente favoráveis que o licitante disponha para atendimento do objeto da licitação;

11.11.10 Demais verificações que porventura se fizerem necessárias.

11.12 Será considerada inexequível a proposta que não venha a ter demonstrada sua viabilidade por meio de documentação que comprove que os custos envolvidos na contratação são coerentes com os de mercado do objeto deste Pregão.

11.13 Será vencedor o licitante que atender a íntegra do Edital e ofertar o menor preço, considerando previsto no **Anexo I – Termo de Referência**.

11.14 A classificação dos lances apresentados, a indicação da proposta vencedora e demais informações relativas à sessão pública constarão de ata divulgada no sistema eletrônico, sem prejuízo das demais formas de publicidade previstas na legislação pertinente.

11.15 Erros no preenchimento da Planilha de Custos e Formação de Preços não constituem motivo para desclassificação da proposta, podendo ser ajustada pelo licitante, no prazo indicado pelo pregoeiro, desde que não haja majoração do preço proposto.

12 DA CLASSIFICAÇÃO DAS PROPOSTAS

12.1 Encerrada a etapa de lances, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à compatibilidade do preço em relação ao estimado para a contratação e verificará a habilitação do licitante;

12.2 Se a proposta não for aceitável ou se o licitante não atender às exigências habilitatórias ou recusar-se a assinar o contrato, o pregoeiro examinará a proposta subsequente e, assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao edital. Nesta etapa, o Pregoeiro poderá negociar com o licitante para que seja obtida melhor proposta;

12.3 As concorrentes remanescentes convocadas ficam obrigadas a atender a convocação e a assinar o contrato respectivo, no prazo fixado pelo

BADESUL, ressalvados os casos de vencimento das respectivas propostas, sujeitando-se às sanções cabíveis no caso de recusa ou de não atendimento das condições de habilitação;

12.4 Será declarado vencedor, o licitante que atender as exigências deste Instrumento e que for detentor do lance de melhor preço, ofertado eletronicamente.

13 DA HABILITAÇÃO DA PROPOSTA DA LICITANTE VENCEDORA

13.1 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 1(uma) hora, depois de encerrada a disputa, os documentos abaixo elencados, caso não seja possível verificar pela internet a autenticidade de algum dos documentos de habilitação, poderá ser requerida documentação complementar por meio do encaminhamento de documento original ou cópia autenticada no prazo máximo de 03 (três) dias úteis a contar da sessão do pregão, conforme item 13.2.

13.1.1 **Documentos Relativos à Habilitação Jurídica**

13.1.1.1 Cópia da Cédula de Identidade, caso o licitante seja pessoa física;

13.1.1.2 No caso de empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

13.1.1.3 No caso de sociedade empresária ou empresa individual de responsabilidade limitada - EIRELI: ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial da respectiva sede, acompanhado de documento comprobatório de seus administradores;

13.1.1.4 Em se tratando de Microempreendedor Individual – MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, na forma da Resolução CGSIM nº 16, de 2009, cuja aceitação ficará condicionada à verificação da autenticidade no sítio www.portaldoempreendedor.gov.br;

13.1.1.5 No caso de sociedade simples: inscrição do ato constitutivo no Registro Civil das Pessoas Jurídicas do local de sua sede, acompanhada de prova da indicação dos seus administradores;

13.1.1.6 Decreto de autorização, no caso 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.

13.1.2 **Documentos Relativos à Regularidade Fiscal**

13.1.2.1 Prova de inscrição no Cadastro de Pessoas Físicas (CPF), em se tratando de pessoa física;

13.1.2.2 Prova de inscrição no Cadastro Nacional da Pessoa Jurídica (CNPJ) do estabelecimento, sede ou filial, conforme o caso, se pessoa jurídica;

13.1.2.3 Prova de regularidade com a Fazenda Federal, mediante a apresentação de Certidão Conjunta Negativa de Débito relativa a Tributos e Contribuições Federais e à Dívida Ativa da União, emitidas respectivamente pela Secretaria da Receita Federal e Procuradoria-Geral da Fazenda Nacional (PGFN).

13.1.2.4 **Prova de regularidade com a Fazenda Estadual do Estado do Rio Grande do Sul independentemente da localização da sede ou da filial da licitante.**

13.1.2.5 Prova de Regularidade com a Fazenda Municipal da Sede do Licitante;

13.1.2.6 Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943.

13.1.2.7 Prova de regularidade perante o Fundo de Garantia do Tempo de Serviço/FGTS, mediante apresentação do Certificado de Regularidade do FGTS/CRF, expedido pela Caixa Econômica Federal, emitido na jurisdição fiscal da sede da contratada.

13.1.3 **Documentos Relativos à Qualificação Econômico-Financeira**

13.1.3.1 **Certificado de Capacidade Financeira de Licitantes emitido pela Contadoria e Auditoria-Geral do Estado – CAGE, disponível no site www.sisacf.sefaz.rs.gov.br.** ou a sua substituição pelo Balanço patrimonial e demonstrações contábeis, inclusive notas explicativas, do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, acompanhado do Anexo II do Decreto nº 36.601/1996 – Análise Contábil da Capacidade Financeira de Licitante (Anexo V deste Edital),

13.1.3.2 É dispensada a exigência do item 13.1.3.1 para o Microempreendedor Individual – MEI, que está prescindido da elaboração do Balanço Patrimonial e demais Demonstrações Contábeis na forma do §2º do art. 1.179 do Código civil – Lei n° 10.406/02;

13.1.3.3 O licitante enquadrado como microempresa e empresa de pequeno porte estará dispensado da apresentação do balanço patrimonial e das

demonstrações contábeis do último exercício, na forma do art. 3º da Lei estadual n° 13.706/2011.

13.1.3.4 Certidão negativa de insolvência, falência, recuperação judicial ou extrajudicial, apresentação de plano especial (microempresas e empresas de pequeno porte) e concordatas deferidas antes da vigência da Lei Federal nº 11.101/2005, expedida pelo distribuidor da sede da pessoa jurídica ou, de execução patrimonial, expedida no domicílio da pessoa física, com data de emissão não superior a 180 (cento e oitenta) dias anteriores à data prevista para o recebimento da documentação da habilitação e da proposta.

13.1.4 **Documentos Relativos à Qualificação Técnica**

13.1.5 Atestado de Capacidade Técnica fornecido por pessoa jurídica de direito público ou privado, que comprove que a licitante executou ou executa, atividades pertinentes e compatíveis em características técnicas com o objeto do presente Termo de Referência.

13.1.5.1 O atestado apresentado deverá conter comprovação de experiência da Licitante no fornecimento de solução e prestação de suporte técnico de Next-Generation Firewall, por período não inferior a 01 (um) ano.

13.1.6 **Demais Documentos**

13.1.6.1 Declaração do licitante de 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 o Anexo III, assinada sob pena de inabilitação;

13.1.6.2 Prova de enquadramento em Microempresa – ME ou Empresa de Pequeno Porte – EPP, registrada pela Junta Comercial ou Cartório de Registros Especiais, caso se tratar dessas espécies.

13.1.6.2.1 As Microempresas e Empresas de Pequeno Porte deverão apresentar os documentos, mesmo que estes apresentem alguma restrição. (Lei Complementar nº 123/06).

13.1.7 Os itens 13.1.1(Documentos Relativos à Habilitação Jurídica); 13.1.2(Documentos Relativos à Regularidade Fiscal) e 13.1.3(Documentos Relativos à Qualificação Econômico-Financeira) podem ser substituídos pelo Certificado de Fornecedor do Estado – CFE, comprovando registro(s) na(s) família(s) correspondente(s), com prazo de validade vigente, inclusive para a documentação nele contida.

13.1.7.1 Se o certificado estiver válido, mas uma das certidões estiver vencida, ele não será aceito em substituição das referidas documentações e não deverá ser anexado ao sistema.

13.2 Caso não seja possível verificar a autenticidade de algum dos

documentos de habilitação, poderá ser requerida documentação complementar pelo chat, a qual deverá ser enviada para o protocolo do BADESUL, situado na Rua Andrade Neves, 175 – Térreo – Centro Histórico – Porto Alegre (RS), no prazo máximo de 3 (três) dias úteis, contados a partir da data que for divulgado o resultado da habilitação em sessão eletrônica, em envelope opaco e lacrado, contendo as seguintes indicações no seu anverso:

ENVELOPE DOCUMENTOS PARA HABILITAÇÃO/PROPOSTA
PREGÃO ELETRÔNICO Nº 0008/2021
RAZÃO SOCIAL DO LICITANTE
CNPJ OU EQUIVALENTE

13.3 Na falta de consignação do prazo de validade dos documentos arrolados no subitem 13.1.2 (Documentos Relativos à Regularidade Fiscal), exceto subitens 13.1.2.1 e 13.1.2.2, serão considerados válidos pelo prazo de 90 (noventa) dias contados da data de sua emissão.

13.4 Os documentos referentes à habilitação do licitante deverão estar válidos no dia de abertura da sessão pública.

13.5 Caso o julgamento da habilitação não coincidir com a data da abertura da sessão, ocorrendo a perda de validade dos documentos no transcuro da licitação e não for possível ao pregoeiro verificar a sua renovação por meio de consulta a *site*s oficiais, o licitante será convocado a encaminhar no prazo de no mínimo 2 (duas) horas, documento válido que comprove o atendimento das exigências deste Edital, sob pena de inabilitação, ressalvado o disposto quanto à comprovação de regularidade fiscal das microempresas e empresas de pequeno porte, conforme estatui o art. 43, §1º, da Lei Complementar nº 123/2006.

13.6 Quando da apreciação dos documentos para habilitação, o pregoeiro procederá ao que segue:

13.6.1 Se os documentos para habilitação não estiverem completos e corretos, ou contrariarem qualquer dispositivo deste Edital, o pregoeiro considerará o licitante inabilitado;

13.6.2 No caso de inabilitação do primeiro classificado, serão requeridos, os documentos para habilitação do licitante subsequente, na ordem de classificação, e assim sucessivamente, até que sejam atendidas as condições do Edital.

13.7 Os licitantes remanescentes ficam obrigados a atender à convocação

e a assinar o contrato no prazo fixado pela Administração, ressalvados os casos de vencimento das respectivas propostas, sujeitando-se às sanções cabíveis no caso de recusa.

13.8 Os documentos deverão ser apresentados no idioma oficial do Brasil, ou para ele vertidos por Tradutor Público e Intérprete Comercial, sendo que a tradução não dispensa a apresentação dos documentos em língua estrangeira a que se refere.

14 DO CRITÉRIO DE JULGAMENTO

14.1 As propostas apresentadas de acordo com as especificações e exigências deste edital serão classificadas pela ordem crescente dos preços propostos, considerando-se vencedor, dentre os qualificados, o licitante que apresentar o **MENOR PREÇO GLOBAL** respeitado o critério de aceitabilidade dos preços.

15 DOS RECURSOS

15.1 Dos atos do pregão caberá recurso que dependerá de manifestação do licitante ao final da sessão pública, em formulário eletrônico específico, manifestando sua intenção com registro da síntese das suas razões, sendo-lhe concedido o prazo de 05 (cinco) dias úteis para apresentação das razões do recurso, ficando os demais licitantes desde logo intimados para apresentar contrarrazões em igual número de dias, que começarão a contar do término daquele prazo;

15.2 O recurso contra decisão do Pregoeiro não terá efeito suspensivo e o seu acolhimento importará na invalidação apenas dos atos insuscetíveis de aproveitamento;

15.3 A falta de manifestação imediata e motivada do licitante importará na decadência do direto de recurso e na adjudicação do objeto da licitação pelo pregoeiro ao vencedor;

15.4 A petição de recurso dirigida à Autoridade Administrativa deverá ser fundamentada e enviada eletronicamente;

15.5 Não serão aceitos recursos encaminhados fora do sistema eletrônico;

15.6 Não serão aceitos como recursos as alegações e memoriais que não se relacionem às razões indicadas pelo licitante na sessão pública;

15.7 Decididos os recursos e constatada a regularidade dos atos procedimentais, a Autoridade Administrativa homologará o resultado da licitação;

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

16 DA ADJUDICAÇÃO E HOMOLOGAÇÃO

16.1 Inexistindo manifestação recursal, o pregoeiro adjudicará o objeto da licitação ao licitante vencedor, com a posterior homologação do resultado pela autoridade superior;

16.2 Havendo a interposição de recurso, após o julgamento e seu trânsito em julgado, a autoridade superior adjudicará e homologará o procedimento licitatório ao licitante vencedor.

17 DO TERMO DE CONTRATO

17.1 O adjudicatário terá o prazo de 5 dias para a assinatura do contrato.

17.2 Alternativamente à convocação para comparecer perante o órgão ou entidade para a assinatura do contrato, a Administração poderá encaminhá-lo para assinatura, mediante correspondência postal com aviso de recebimento (AR) ou meio eletrônico, para que seja assinado no prazo de 5 (cinco) dias, a contar da data de seu recebimento.

17.3 O prazo previsto poderá ser prorrogado, por igual período, por solicitação justificada do adjudicatário e aceita pela Administração.

17.4 O prazo de vigência do contrato será o previsto no contrato, e quando este for dispensado no **Anexo I – Termo de Referência** do Edital.

17.5 O local de entrega será previsto no **Anexo I – Termo de Referência** do Edital.

17.6 Previamente à contratação, será realizada consulta ao Cadastro de Fornecedores Impedidos de Licitar e Contratar com a Administração Pública Estadual - CFIL/RS e ao Cadastro Informativo - CADIN/RS, pelo contratante, para identificar possível impedimento relativo ao licitante vencedor, cujo comprovante será anexado ao processo.

17.7 Se o adjudicatário, no ato da assinatura do contrato, não comprovar que mantém as condições de habilitação, ou quando, injustificadamente, recusar-se à assinatura, poderá ser convocado outro licitante, desde que respeitada a ordem de classificação, para, após a verificação da aceitabilidade da proposta, negociação e comprovados os requisitos de habilitação, celebrar a contratação, sem prejuízo das sanções previstas neste Edital e das demais cominações legais.

17.8 É facultado à Administração, quando o convocado não assinar o

contrato, revogar a licitação, sem prejuízo da aplicação das cominações previstas na Lei Federal 13.303/2016, no Regulamento Interno de Licitações e Contratos desta empresa e neste Edital.

18 DAS SANÇÕES ADMINISTRATIVAS

18.1 Sem prejuízo da faculdade de rescisão contratual, o Badesul poderá aplicar sanções de natureza moratória e punitiva ao licitante, diante do não cumprimento das cláusulas do edital.

18.1.1 advertência por escrito, sempre que ocorrerem pequenas irregularidades, assim entendidas aquelas que não acarretem prejuízos significativos para o Badesul

18.1.2 multa:

18.1.3 até 0,5% sobre o valor da sua proposta, ao licitante que se comportar de modo inidôneo ou agir de má-fé;

18.1.4 até 1% sobre o valor da sua proposta, ao licitante que não mantiver a proposta, salvo se em decorrência de fato superveniente devidamente justificado; deixar de entregar a documentação de habilitação exigida para o certame; apresentar documento falso; ou fizer declaração falsa;

18.1.5 até 5% sobre o valor da sua proposta, nos casos do licitante vencedor que, chamado para assinar, aceitar ou retirar o contrato, a Ata de Registro de Preços ou instrumentos equivalentes, no prazo de validade da sua proposta, não comparecer ou recusar-se injustificadamente, sem prejuízos de ser promovida contra o licitante faltoso a competente ação civil para ressarcir a BADESUL dos prejuízos causados;

18.1.6 até 10% sobre o valor da sua proposta, ao licitante que fraudar a licitação.

18.2 suspensão temporária de participação em licitação e impedimento de contratar com o Badesul**, pelo prazo de até 2 (dois) anos**, em consonância com as situações e os prazos abaixo indicados:

18.2.1 por até **3 (três) meses**, o licitante que se comportar de modo inidôneo ou agir de má-fé;

18.2.2 por até **6 (seis) meses**, o licitante que, por dolo ou má-fé, não mantiver a proposta, salvo se em decorrência de fato superveniente devidamente justificado; por dolo ou má-fé, deixar de entregar a documentação de habilitação exigida para o certame, prejudicando o Badesul apresentar documento falso; ou fizer declaração falsa;

18.2.3 Por até **1 (um) ano**, o licitante vencedor que, chamado para assinar,

aceitar ou retirar o contrato, a Ata de Registro de Preço ou instrumentos equivalentes, no prazo de validade da sua proposta, não comparecer ou recusar-se injustificadamente;

18.2.4 Por até **2 (dois) anos**, o licitante que fraudar a licitação.

18.3 As penalidades previstas nos incisos 18.1.1 e 18.1.3 do caput poderão ser aplicadas juntamente com a do inciso II.

18.4 A sanção de suspensão leva à inclusão do licitante no Cadastro de Fornecedores Impedidos de Licitar e Contratar – CFIL/RS.

18.5 A sanção de suspensão poderá também ser aplicada às empresas ou aos profissionais que:

18.5.1 Tenham sofrido condenação definitiva por praticarem, por meios dolosos, fraude fiscal no recolhimento de quaisquer tributos;

18.5.2 Tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

18.5.3 Demonstrem não possuir idoneidade para contratar com a empresa pública ou a sociedade de economia mista em virtude de atos ilícitos praticados.

18.6 A aplicação de penalidades não exime o licitante da obrigação de reparar os danos, perdas ou prejuízos que sua conduta venha a causar à BADESUL.

19 DAS DISPOSIÇÕES GERAIS

19.1 Caso o licitante vencedor não apresente situação regular no ato da assinatura do contrato, ou venha recusar-se a celebrá-lo, injustamente, dentro do prazo estabelecido e na vigência de sua proposta, sujeitar-se-á às sanções cabíveis, reservando-se o BADESUL, o direito de independentemente de qualquer aviso ou notificação, renovar a licitação ou convocar os remanescentes;

19.2 Na convocação dos remanescentes, será observada a classificação final da sessão originária do pregão, devendo o(s) convocado(s) apresentar os documentos de habilitação cuja validade tenha se expirado no prazo transcorrido da data da primeira sessão;

19.3 Somente será considerado habilitado o licitante que houver preenchido os requisitos de habilitação na data da primeira sessão e que apresentar, na segunda sessão, os documentos que porventura estiverem vencidos;

19.4 Os concorrentes remanescentes convocados se obrigam a atender a

convocação e a assinar o contrato respectivo, no prazo fixado pelo BADESUL, ressalvados os casos de vencimento das respectivas propostas, sujeitando-se às sanções cabíveis, no caso de recusa ou de não atendimento das condições de habilitação;

19.5 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;

19.6 É facultado ao Pregoeiro ou à Autoridade Superior, em qualquer fase da licitação, a promoção de diligência destinada a esclarecer ou complementar a instrução do processo, vedada a inclusão posterior de documento ou informação que deveria constar do ato da sessão pública;

19.7 O BADESUL, na pessoa do Pregoeiro ou da Autoridade superior, reserva-se o direito de proceder ao exame das informações e comprovantes, por visitas "in loco" ou por outras medidas adequadas;

19.8 Caso seja necessária a diligência do Pregoeiro para verificação da habilitação do licitante, a sessão poderá ser interrompida ou suspensa por ordem do Pregoeiro, que determinará o reinício dos trabalhos em momento oportuno, após a realização das diligências necessárias;

19.9 É facultado ao Pregoeiro 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;

19.10 É facultado ainda ao Pregoeiro convocar os licitantes para quaisquer esclarecimentos porventura necessários ao entendimento de suas propostas; que uma vez intimados, deverão fazê-lo no prazo determinado pelo Pregoeiro, sob pena de desclassificação/inabilitação;

19.11 A Microempresa ou Empresa de Pequeno Porte que apresentar documentos com restrições tem assegurado o prazo de 2 (dois) dias úteis, a partir da publicação da adjudicação da licitação, para apresentar as respectivas certidões negativas ou positivas com efeito de negativas;

19.12 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 contrato, ou revogar a licitação;

19.13 A Administração do BADESUL poderá anular ou revogar, parcialmente ou na sua totalidade este Pregão, observadas as disposições legais pertinentes;

19.14 Os casos omissos serão resolvidos pelo Pregoeiro, que a eles aplicará

as disposições da Lei Federal 13.303/2016, no Regulamento Interno de Licitações e Contratos desta empresa e disposições supletivas, se couberem, desde que não venham a conflitar com a referida legislação;

19.15 Fica desde logo esclarecido, que todos os participantes deste Pregão, pelo simples fato de nele licitarem, sujeitam-se a todos os seus termos, condições, normas, especificações e detalhes, comprometendo-se a cumpri-lo fielmente, independentemente de qualquer manifestação escrita ou expressa;

19.16 O desatendimento de exigências formais não essenciais não importará no afastamento da licitante, desde que seja possível a aferição da sua qualificação e a exata compreensão da sua proposta, durante a realização da sessão pública de Pregão, e desde que não comprometa o interesse do BADESUL, bem como a finalidade e a segurança da futura contratação;

19.17 As normas que disciplinam este Pregão serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse do BADESUL e a segurança da contratação;

19.18 A proponente que vier a ser contratada ficará obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, dentro do limite legalmente admitido na Lei 13.303/2016, sobre o valor inicial do contrato;

19.19 Quaisquer informações e esclarecimentos relativos a esta licitação serão prestados pelo Pregoeiro, por escrito, através do e-mail: badesul.licita@badesul.com.br;

19.20 Vista ao processo será fornecida ao representante legal devidamente identificado e mediante solicitação pelo e-mail: licita@badesul.com.br;

19.21 Os resultados dos julgamentos e demais procedimentos relativos ao certame, serão divulgados de acordo com a legislação pertinente, bem como no “site” www.pregaobanrisul.com.br.

19.22 **Nos termos do acórdão 1.211/2021, o prazo para inserção de proposta ou outros documentos de habilitação exigíveis poderá ser prorrogado uma única vez pelo prazo de 30 minutos.**

19.23 **A hipótese do parágrafo anterior refere-se à complementação de documento ausente ou a substituição de documento incorreto.**

19.24 **Na ausência da totalidade da documentação no sistema, o prazo não será prorrogado, estando o licitante sujeito a desclassificação e/ou inabilitação.**

20 DOS ANEXOS

20.1 Fazem parte integrante e complementar deste Edital:

ANEXO I - TERMO DE REFERÊNCIA - DETALHAMENTO DO OBJETO

ANEXO II - PROPOSTA DE PREÇOS

ANEXO III - PLANILHA DE CUSTOS E FORMAÇÃO DE PREÇOS

ANEXO IV - MODELO DE COMPROVAÇÃO DE ATENDIMENTO ÀS ESPECIFICAÇÕES TÉCNICAS (DEVERÁ SER INSERIDO NO SISTEMA JUNTAMENTE COM A PROPOSTA DE PREÇOS)

ANEXO V - ANÁLISE CONTÁBIL DA CAPACIDADE FINANCEIRA DA LICITANTE

ANEXO VI - CARTA DE FIANÇA BANCÁRIA PARA GARANTIA DE EXECUÇÃO CONTRATUAL

ANEXO VII - DECLARAÇÃO DO LICITANTE DE QUE NÃO EMPREGA MENOR DE 18 ANOS

ANEXO VIII - MINUTA DO CONTRATO

21 DO FORO

21.1 Fica eleito o Foro da Comarca de Porto Alegre para dirimir quaisquer dúvidas oriundas deste Pregão.

Porto Alegre, 08 de novembro de 2022.

Kalil Sehbe Neto,
Diretor-Financeiro.

Visto Jurídico

PREGÃO ELETRÔNICO N.º 0017/2022

Processo nº 22/4000-0000309-9

ANEXO I

TERMO DE REFERÊNCIA

1. DO OBJETO

1.1. Serviço de solução de Firewall de Próxima Geração (Next-Generation Firewall (NGFW) e demais especificações.

2. DA JUSTIFICATIVA DA AQUISIÇÃO

2.1. A implantação de segurança de Tecnologia da Informação visa atender as crescentes demandas de proteção ao ambiente de TI proporcionada pelas intensas ameaças externas ou internas à privacidade e confidencialidade dos dados gerados no trabalho diário dos funcionários na nossa empresa.

2.2. Para implementar e prover adequadamente a segurança de Tecnologia da Informação no BADESUL se faz necessária e urgente a atualização/instalação de equipamento destinado à proteção/preservação do acesso às informações no ambiente de TI;

2.3. O Firewall é uma solução de segurança que controla o acesso entre servidores e estações locais de uma rede local e as conexões oriundas ou destinadas à Internet.

2.4. É composto por Hardware e Software que permitem a aplicação de políticas de acesso, que visam:

2.4.1. obter maior segurança e prevenção às ameaças de invasão;

2.4.2. impedir que a rede, servidores e ativos de informação sejam acessados sem autorização;

2.4.3. evitar que informações sejam capturadas;

2.4.4. bloquear programas indesejados na rede como compartilhamento de dados e de mensagens instantâneas;

2.4.5. reduzir o tráfego indesejado e utilização otimizada da banda disponível;

2.4.6. permitir a auditoria nos acessos a recursos da rede;

2.4.7. agilidade e rapidez na monitoração e gerenciamento da segurança;

2.4.8. monitorar e gerenciar as permissões e bloquear os acessos indevidos às informações confidenciais e contribuir para a melhoria da

segurança ao acesso externo do ambiente, entre outras ações pertinentes à política de segurança do BADESUL;

2.5. Trata-se, portanto, de serviços indispensáveis, de natureza continuada, à proteção dos dados da Entidade, exercida por meio de controle de acesso aos recursos, de monitoramento do fluxo de rede e salvaguarda contra-ataques externos;

2.6. O atual contrato de software e hardware Firewall Appliance foi firmado em 21/03/2016 através do Pregão Eletrônico nº 003/2016 com a empresa Aker Consultoria e Informática S/A, atualmente denominada OGASEC CYBER SECURITY;

2.7. O Firewall Appliance atualmente em operação conta com uma solução de firewall baseada em software livre, denominada PFSense que oferece um nível básico de proteção diante da dimensão e grande fluxo de informações trafegadas na nossa rede.

2.8. A proteção da rede implementada no PFSense é baseada na filtragem de pacotes, aplicando regras de bloqueios nas camadas de rede e transporte do modelo OSI.

2.9. Dessa forma, ele atua apenas com base nos cabeçalhos dos pacotes da camada de rede (Ipv4, Ipv6 e ICMP) e da camada de transporte (UDP e TCP). Assim, é possível criar regras apenas com base nos endereços IP (origem e/ou destino), portas (origem e/ou destino) e protocolos citados anteriormente;

2.10. A atual solução não possui mecanismos que permitam o monitoramento detalhado do tráfego a nível das aplicações que estão trafegando dados, qual o nível de risco do tráfego e se ele pode trazer ameaças para a rede.

2.11. Esse tipo de informação é muito importante para prover uma rápida análise caso ocorra algum incidente e para a geração de relatórios sobre uso da banda, o que auxilia a diagnosticar de forma rápida e eficiente as causas de possíveis ataques cibernéticos ou lentidão na rede;

2.12. Com a vigência da Lei Geral de Proteção de Dados, que amplia as exigências do Marco Civil da Internet e reforça a utilização de melhores práticas de mercado no que tange aspectos da Segurança da Informação, a utilização de um Firewall de Próxima Geração auxilia na proteção das informações através do monitoramento e da restrição de Ips maliciosos que estejam tentando se comunicar com a rede ou impedindo que usuários internos tenham acesso a endereços maliciosos na internet;

2.13. Nos últimos tempos, uma forma comum de invasão nos servidores é através de acessos remotos mal protegidos que atraem a atenção de grupos de ransomware.

2.14. Uma forma de barrar esse acesso é adicionando um fator à autenticação, como, por exemplo, utilizando o "múltiplo fator de autenticação" de senhas. Os Firewall de Próxima Geração possuem ferramentas capazes de implementar esta camada de segurança nos acessos via VPN;

2.15. Após a realização de pesquisas dos padrões atuais de mercado para o objeto por meio de acesso a catálogos, sites dos fabricantes, análise de processos semelhantes e às boas práticas do processo licitatório, na busca por qualidade dos produtos a serem contratados que apoiarão de forma contínua e permanente todas as atividades administrativas e estratégicas do Badesul e objetivando alcançar o maior retorno ao investimento, entendemos que os fabricantes da solução de Firewall de Próxima Geração (Next-Generation Firewall (NGFW) devam estar classificados como líderes de mercado no Quadrante Mágico de Firewall (Magic Quadrant for Network Firewall) pelo menos uma vez nos mais recentes relatórios produzidos pela consultoria norte-americana Gartner Inc.

2.16. Estar entre os líderes de mercado, segundo o Quadrante Mágico do GARTNER significa dizer que que os fabricantes atendem aos requisitos de segurança, qualidade e preservação de recursos públicos investidos, visto que os equipamentos desenvolvidos pelos fabricantes enquadrados nesta categoria são nativamente possuidores das características técnicas mais avançadas do mercado;

2.16.1. *Gartner Inc.* é considerada a organização líder internacional em pesquisa e aconselhamento tecnológico, respeitada como fonte independente e não tendenciosa de opiniões consultivas acerca da área de tecnologia da informação.

2.17. A contratação se dará em lote único em razão de a solução de firewall permear todas as comunicações da Rede de Computadores do BADESUL, constituindo um elemento crítico para a disponibilidade, confiabilidade, segurança e desempenho de todos os serviços acessíveis pela rede.

2.18. Devido a essa criticidade, a solução foi concebida com características de redundância para que seja tolerante a eventuais falhas de seus componentes elementares.

2.19. Além disso, contratar empresas distintas para o fornecimento de equipamentos, licenças, serviços de instalação e serviço de suporte técnico poderia gerar conflito de responsabilidade entre as empresas envolvidas. Sendo assim, por uma questão de ganho de escala e simplificação dos processos administrativos, o não parcelamento é mais vantajoso.

2.19.1. Os softwares que compõem a solução estão em permanente evolução, como também estão em constante desenvolvimento as ameaças que

colocam em risco os sistemas de informação: novas ferramentas de ataque surgem todos os dias, e novas vulnerabilidades são descobertas e alardeadas com a mesma frequência.

2.19.2. Por tais motivos, o software de uma solução de segurança necessita estar permanentemente atualizado, com as mais recentes versões dos mecanismos de defesa e as ferramentas mais atuais para proteção e gerenciamento de segurança das comunicações de rede.

2.19.3. A experiência do BADESUL no uso da solução de firewall registra inúmeras situações em que o suporte técnico especializado se mostrou imprescindível para manter os serviços no ar:

2.19.3.1. Problemas com novas características implementadas nas novas versões do software, bem como sua instalação e configuração, sempre demandam conhecimento especializado para resolução de eventuais problemas.

2.19.3.2. A implementação de novas regras de segurança e tratamento de incidentes de segurança também motivaram, no passado, abertura de chamados técnicos junto ao suporte técnico especializado.

2.19.4. Em suma, além dos argumentos supracitados, por ser de responsabilidade da contratada da solução de Next-Generation Firewall a prestação de garantia de funcionamento do hardware e software, suas licenças de uso, serviços de implantação, configuração, atualizações contínuas, repasse de conhecimento e treinamento, necessitamos que a mesma empresa vencedora do certame preste o serviço de suporte técnico pelo período de 60 (sessenta) meses, pois, como não sabemos qual será o produto homologado, a prestadora do referido suporte deverá possuir certificação comprovada pelo fabricante da solução de Next-Generation Firewall ofertada, garantindo assim que as falhas, interrupções ou outros problemas de funcionamento sejam resolvidos com a maior brevidade possível.

3. DA ESPECIFICAÇÃO DO OBJETO E DA EXECUÇÃO DO SERVIÇO

3.1. O fabricante da solução de Firewall de Próxima Geração (Next-Generation Firewall (NGFW) deve estar classificado como líder de mercado no Quadrante Mágico de Firewall (Magic Quadrant for Network Firewall) pelo menos uma vez nos mais recentes relatórios produzidos pela consultoria norte-americana Gartner Inc. disponível em https://www.gartner.com/document/4007809;

3.2. A solução deve consistir em uma plataforma de proteção de rede baseada em *appliance* físico com funcionalidades de *Next-Generation Firewall*

(NGFW) e console de gerência e monitoramento, com capacidade para operar em alta disponibilidade em modo ativo-ativo para controle de tráfego de dados por identificação de usuários e por camada 7, com controle de aplicação, administração de largura de banda (QoS), VPN Ipsec e SSL, IPS, prevenção contra ameaças de vírus, spywares e malwares "Zero Day", Filtro de URL, inspeção de tráfego criptografado (SSL inspection), proteção de firewall de aplicação Web (WAF), bem como controle de transmissão de dados e acesso à internet compondo uma plataforma de segurança integrada. A solução deverá ter a capacidade de operar com pelo menos 200 (duzentos) usuários simultâneos quando todos os recursos de proteção especificados estiverem ativos ao mesmo tempo. Modelo de referência: Fortinet Fortigate FG-100F;

3.3. Aquisição de licenças de Next-Generation Endpoint (NGE) com conexão remota segura Zero Trust Agent para proteção de equipamentos de 200 (duzentos) usuários finais, monitorados através de uma central única de monitoração, para proteção anti-malware, live protection, análise de comportamento, reputação de downloads, controle de aplicativos, dispositivos e filtro de URL, detecção de tráfego malicioso, sincronização com AD, políticas por usuários e grupos de usuários, console de gerenciamento em nuvem e suporte a Windows pelo período de 60 meses. Modelo de referência: Fortinet FortiClient ZTNA;

3.4. Aquisição de licença de sistema de análise e geração de relatórios dos registros de acesso e atividades realizadas (logs) na administração e operação da solução, bem como de todo o tráfego controlado e monitorado pela mesma. Modelo de referência: Fortinet FortiAnalyzer;

3.5. Para os itens que representem bens materiais, a CONTRATADA deverá dispor, para prestação dos serviços, produtos novos (*appliance*), sem uso anterior;

3.6. Por cada *appliance* físico que compõe a plataforma de segurança, entende-se o hardware, software e as licenças necessárias para o seu funcionamento;

3.6.1. Por plataforma de segurança entende-se hardware e software integrados do tipo *appliances*;

3.7. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos *appliances* desde que sejam do mesmo fabricante e obedeçam a todos os requisitos mínimos desta especificação;

3.8. A comunicação entre os *appliances* de segurança e o módulo de gerência deve ser através de meio criptografado;

3.9. Os *appliances* de segurança devem suportar operar em cluster ativo-ativo sem a necessidade de licenças adicionais;

3.10. Por alta disponibilidade (HA) entende-se que a solução deverá ser composta ao menos por dois appliances, licenciados para funcionamento em redundância no modo ativo-ativo;

3.11. Cada appliance deverá ser capaz de executar a totalidade das capacidades exigidas para cada função, não sendo aceitos somatórias para atingir os limites mínimos;

3.12. O hardware e o software (componentes da solução) fornecidos não podem constar, no momento da apresentação da proposta, em listas de end-of-sale, end-of-support, end-of-engineering-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante. O proponente deverá apresentar uma carta de compromisso certificando que os componentes da solução estão de acordo com essa exigência;

3.13. **As ferramentas de gerenciamento da solução de firewall e do Next-Generation Endpoint deverão possuir padrão Web seguro e hospedagem em nuvem;**

3.14. A solução deverá consistir em *appliance* físico de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração;

3.15. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;

3.16. O hardware e software que executem a funcionalidade de proteção de rede deverá ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

3.17. O hardware e software que executem as funcionalidades console de gerência e monitoração, deverão ser do tipo appliance físico ou virtual;

3.18. Todos os equipamentos fornecidos deverão ser próprios para montagem em rack 19 polegadas, incluindo kit tipo trilho para adaptação se necessário e todos os acessórios (como cabo de energia, conectores, etc.) necessários para sua instalação;

3.19. O software do appliance deverá ser fornecido em sua versão mais atualizada;

3.20. O *appliance* não deve sofrer degradação de performance quando as funcionalidades de Firewall, Controle de aplicação WEB e IPS tiverem habilitadas de forma simultânea, sendo que o tráfego deverá ser inspecionado

de modo bidirecional e a inspeção deve ser feita para toda a sessão do pacote, sem qualquer utilização de feature de bypass do pacote/sessão;

3.21. Visando modernizar o ambiente do BADESUL com uma tecnologia atual e com o olhar voltado para um cenário de longo prazo, consideramos que as soluções e os fornecedores deverão possuir algumas características desejáveis, como:

3.21.1. Devem garantir os requisitos de serviço e suporte remoto;

3.21.2. Devem possuir uma forte estratégia de produto de segurança em nuvem e com hospedagem no Brasil;

3.21.3. A solução deverá possuir um sistema de gerenciamento em painel de controle único e ser nativo do mesmo fabricante do equipamento;

3.21.4. Oferecer licenciamento empacotado com boa relação custo-benefício e suporte técnico para reduzir o TCO do firewall;

3.21.5. Todas as especificações dos equipamentos devem ser nativas do fabricante e não podem depender de parceria com terceiros.

3.22. **Especificações gerais**:

Item		**Produto**
Equipamentos e licenças	1	Firewall de Próxima Geração (Next Generation Firewall – NGFW) do tipo *appliance* com sistema de gestão integrado em formato GUI (gráfico) do próprio fabricante, suporte técnico e garantia de 60 meses Modelo de referência: Fortinet Fortigate FG-100F
	2	Ferramenta de visibilidade, análise e segurança de Endpoints para conexão remota e segura Zero Trust Network Agent, padrão web, autenticação multifator (MFA), integração com Active Directory (AD) e hospedagem em nuvem Modelo de referência: Fortinet FortiClient ZTNA
	3	Sistema de Gerenciamento de logs, análise e plataforma de relatórios Modelo de referência: Fortinet FortiAnalyzer
Serviço de instalação	4	Serviço de instalação, configuração, atualização e treinamento de pessoal
Suporte técnico	5	Suporte técnico durante a vigência contratual (60 meses)

3.22.1. **Item 1: Firewall de Próxima Geração (Next Generation Firewall – NGFW)**;

3.22.1.1. **Características do Equipamento:**

3.22.1.1.1. Deve suportar, no mínimo, 20 Gbps com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6;

3.22.1.1.2. Deve suportar, no mínimo, 2.6 Gbps de throughput IPS;

3.22.1.1.3. Deve suportar, no mínimo, 11.5 Gbps de throughput de VPN IPSec;
3.22.1.1.4. Deve suportar, no mínimo, 1 Gbps de throughput de VPN SSL;
3.22.1.1.5. Deve suportar, no mínimo, 1 Gbps de throughput de Inspeção SSL;
3.22.1.1.6. Deve suportar, no mínimo, 2.2 Gbps de throughput de Controle de Aplicação;
3.22.1.1.7. Deve suportar, no mínimo, 1 Gbps de throughput com as seguintes funcionalidades habilitadas simultaneamente, para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: firewall, controle de aplicação, IPS e antimalware;
3.22.1.1.8. Suporte a, no mínimo, 1.5 Milhões de conexões simultâneas;
3.22.1.1.9. Suporte a, no mínimo, 56.000 novas conexões por segundo;
3.22.1.1.10. Estar licenciado para, ou suportar sem o uso de licença, 2.000 túneis de VPN IPSEC Site-to-Site simultâneos;
3.22.1.1.11. Estar licenciado para, ou suportar sem o uso de licença, 16.000 túneis de clientes VPN IPSEC simultâneos;
3.22.1.1.12. Estar licenciado para, ou suportar sem o uso de licença, 500 clientes de VPN SSL simultâneos;
3.22.1.1.13. Possuir ao menos 12 interfaces 1Gbps RJ45;
3.22.1.1.14. Possuir ao menos 4 interfaces 1Gbps SFP;
3.22.1.1.15. Possuir ao menos 1 interface 1Gbps RJ45 dedicada à gerenciamento;
3.22.1.1.16. Possuir ao menos 1 interface serial de console;
3.22.1.1.17. Possuir ao menos 2 interfaces 1Gbps RJ45 dedicadas à HA (Alta Disponibilidade);
3.22.1.1.18. Possuir ao menos 1 interface 1Gbps RJ45 dedicada à DMZ;
3.22.1.1.19. Possuir ao menos 2 interfaces 10Gbps SFP+;
3.22.1.1.20. Estar licenciado e ter incluso sem custo adicional, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance;
3.22.1.1.21. Possuir fonte de alimentação 100-240V AC redundante interna;
3.22.1.1.22. Possuir no máximo 1 RU de altura;
3.22.1.1.23. Deve possuir suporte a 4094 VLAN Tags 802.1q;
3.22.1.1.24. Deve possuir suporte a agregação de links 802.3ad e LACP;
3.22.1.1.25. Deve possuir suporte a Policy based routing ou policy based forwarding;
3.22.1.1.26. Deve possuir suporte a roteamento multicast (PIM-SM e PIM-DM);

3.22.1.1.27. Deve possuir suporte a DHCP Relay;
3.22.1.1.28. Deve possuir suporte a DHCP Server;
3.22.1.1.29. Deve suportar sFlow;
3.22.1.1.30. Deve possuir suporte a Jumbo Frames;
3.22.1.1.31. Deve suportar sub-interfaces ethernet logicas;
3.22.1.1.32. Deve suportar NAT dinâmico e estático;
3.22.1.1.33. Deve suportar Tradução de porta (PAT);
3.22.1.1.34. Deve suportar NAT de Origem, NAT de Destino e NAT de forma simultânea;
3.22.1.1.35. Deve poder combinar NAT de origem e NAT de destino na mesma politica
3.22.1.1.36. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
3.22.1.1.37. Deve suportar NAT64 e NAT46;
3.22.1.1.38. Deve implementar o protocolo ECMP;
3.22.1.1.39. Deve permitir monitorar via SNMP falhas de hardware, uso de recursos por número elevado de sessões, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;
3.22.1.1.40. Enviar log para sistemas de monitoração externos, simultaneamente;
3.22.1.1.41. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;
3.22.1.1.42. Deve possuir suporte ao protocolo de criptografia TLS (Transport Layer Security) na versão 1.3;
3.22.1.1.43. Proteção anti-spoofing;
3.22.1.1.44. Suportar otimização do tráfego entre dois equipamentos;
3.22.1.1.45. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
3.22.1.1.46. Para IPv6, deve suportar roteamento estático e dinâmico (RIPng, OSPFv3, BGP4+);
3.22.1.1.47. Suportar OSPF graceful restart;
3.22.1.1.48. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
3.22.1.1.49. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;
3.22.1.1.50. Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;

3.22.1.1.51. Deve suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
3.22.1.1.52. Suporte a configuração de alta disponibilidade Ativo/Ativo: Em modo transparente;
3.22.1.1.53. Suporte a configuração de alta disponibilidade Ativo/Ativo: Em layer 3;
3.22.1.1.54. Suporte a configuração de alta disponibilidade Ativo/Ativo: Em layer 3 e com no mínimo 2 equipamentos no cluster;
3.22.1.1.55. A configuração em alta disponibilidade deve sincronizar: Sessões;
3.22.1.1.56. A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede;
3.22.1.1.57. A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs;
3.22.1.1.58. A configuração em alta disponibilidade deve sincronizar:Tabelas FIB;
3.22.1.1.59. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;
3.22.1.1.60. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance;
3.22.1.1.61. Em alta disponibilidade, deve ser possível o uso de clusters virtuais, seja ativo-ativo permitindo a distribuição de carga entre diferentes contextos;
3.22.1.1.62. O módulo de gerência deve ser capaz de gerenciar e administrar a solução descrita neste termo;
3.22.1.1.63. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança;
3.22.1.1.64. Centralizar a administração de regras e políticas dos equipamentos de proteção de rede, uxando uma única interface de gerenciamento;
3.22.1.1.65. Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas;
3.22.1.1.66. O gerenciamento da solução deve suportar acesso via SSH e interface WEB (HTTPS), incluindo, mas não limitado à, exportar configuração dos sistemas virtuais (contextos) por ambas interfaces;

3.22.1.1.67. O gerenciamento deve permitir/possuir monitoração de logs, ferramentas de investigação de logs e acesso concorrente de administradores;
3.22.1.1.68. Deve possuir um mecanismo de busca por comandos ou auto-complete no gerenciamento via SSH, de forma a facilitar a configuração pelo administrador;
3.22.1.1.69. Deve suportar a criação de regras que fiquem ativas em horário definido e suportar criação de regras com data de expiração;
3.22.1.1.70. Deve suportar backup das configurações e rollback de configuração para a última configuração salva;
3.22.1.1.71. Deve suportar a validação das políticas, avisando quando houver regras que ofusquem ou confitem com outras (shadowing);
3.22.1.1.72. Deve permitir a viaualisação dos logs de uma regra especial em tempo real;
3.22.1.1.73. Deve possibilitar a integração com outras soluções de SIEM de mercado;
3.22.1.1.74. Deve suportar geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;
3.22.1.1.75. Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-Malware), etc;
3.22.1.1.76. Deve prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus, Anti-Malware), e URLs que passam pela solução;
3.22.1.1.77. Deve ser possível exportar os logs em CSV ou outro formato de texto estruturado;
3.22.1.1.78. Deve possibilitar a geração ou exportação de relatórios de eventos no formato PDF;
3.22.1.1.79. Deve possibilitar rotação do log;
3.22.1.1.80. Deve ter capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura;
3.22.1.1.81. Deve permitir a criação de filtros com base em qualquer característica do evento, tais como a origem e o IP destino, serviço, tipo de evento, severidade do evento, nome do ataque, o país de origem e destino, etc;
3.22.1.1.82. Deve permitir a integração com servidores de autenticação LDAP Microsoft Active Directory e Radius;
3.22.1.1.83. Deve permitir a visualização de gráficos e mapa de ameaças;

3.22.1.1.84. Deve possuir mecanismo para que logs antigos sejam removidos automaticamente;
3.22.1.1.85. Deve permitir a criação de dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino;
3.22.1.1.86. Deve possuir a capacidade de visualizar na interface gráfica da solução, informações do sistema como licenças, memória, disco e uso de CPU;
3.22.1.1.87. A solução deve possuir painéis de eventos em tempo real com possibilidade de configuração das atualizações e frequências;
3.22.1.1.88. Deve possuir controle, inspeção e descriptografia de SSL para tráfego de entrada (Inbound) e Saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);
3.22.1.1.89. A solução deve identificar potenciais vulnerabilidades e destacar as melhores práticas que poderiam ser usadas para melhorar a segurança e o desempenho geral de uma rede;
3.22.1.1.90. O console de administração deve suportar pelo menos inglês, espanhol e português.
3.22.1.1.91. O console deve suportar o gerenciamento de switches e pontos de acesso wireless para melhorar o nível de segurança
3.22.1.1.92. A solução deve oferecer suporte à integração nativa de equipamentos de proteção de email, firewall de aplicativos, proxy, cache e ameaças avançadas.
3.22.1.1.93. Deverá ser comprovado que a solução ofertada foi aprovada no conjunto de critérios de avaliação contido nos testes da NSS Labs, da ICSA Labs, ou por meio de certificação similar, que cumpra a mesma finalidade ou que ateste as mesmas funcionalidades.
3.22.1.2. **Controle por Politica de Firewall:**
3.22.1.2.1. Deverá suportar controles por zona de segurança;
3.22.1.2.2. Controles de políticas por porta e protocolo;
3.22.1.2.3. Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
3.22.1.2.4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

3.22.1.2.5. Firewall deve ser capaz de aplicar a inspeção UTM (Application Control e Webfiltering no mínimo) diretamente às políticas de segurança versus via perfis;
3.22.1.2.6. Além dos endereços e serviços de destino, objetos de serviços de Internet devem poder ser adicionados directamente às políticas de firewall;
3.22.1.2.7. Ele deve suportar a automação de situações como detecção de equipamentos comprometidos, status do sistema, alterações de configuração, eventos específicos e aplicar uma ação que pode ser notificação, bloqueio de um computador, execução de scripts ou funções em nuvem pública.
3.22.1.2.8. Deve suportar o padrão de indústria 'syslog' protocol para armanazemento usando o formato Common Event Format (CEF);
3.22.1.2.9. Deve haver uma maneira de assegurar que o armazenamento dos logs em tempo real não superam a velocidade de upload;
3.22.1.2.10. Deve suportar o protocolo padrão da indústria VXLAN;
3.22.1.2.11. Deve suportar objetos de endereço IPv4 e IPv6, consolidados na mesma regra/política de firewall
3.22.1.2.12. Deve possuir base com objetos de endereço IP, de serviços da internet como Google e Office 365, atualizados dinamicamente pela solução;
3.22.1.2.13. A solução deve oferecer suporte à integração nativa com a solução de sandbox, proteção de email, cache e firewall de aplicativos da Web;
3.22.1.3. **Controle de Aplicações:**
3.22.1.3.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
3.22.1.3.2. Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado a: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
3.22.1.3.3. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;
3.22.1.3.4. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;

3.22.1.3.5. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
3.22.1.3.6. Identificar o uso de táticas evasivas via comunicações criptografadas;
3.22.1.3.7. Atualizar a base de assinaturas de aplicações automaticamente;
3.22.1.3.8. Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos;
3.22.1.3.9. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;
3.22.1.3.10. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;
3.22.1.3.11. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
3.22.1.3.12. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;
3.22.1.3.13. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;
3.22.1.3.14. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo;
3.22.1.3.15. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;
3.22.1.3.16. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);
3.22.1.3.17. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação;
3.22.1.3.18. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;
3.22.1.3.19. Deve ser possível configurar Application Override permitindo selecionar aplicações individualmente;

3.22.1.4. **Prevenção de Ameaças:**

3.22.1.4.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;

3.22.1.4.2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

3.22.1.4.3. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;

3.22.1.4.4. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;

3.22.1.4.5. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes politicas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

3.22.1.4.6. Deve permitir o bloqueio de vulnerabilidades;

3.22.1.4.7. Deve incluir proteção contra ataques de negação de serviços;

3.22.1.4.8. Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise de decodificação de protocolo;

3.22.1.4.9. Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise para detecção de anomalias de protocolo;

3.22.1.4.10. Deverá possuir o seguinte mecanismos de inspeção de IPS: IP Defragmentation;

3.22.1.4.11. Deverá possuir o seguinte mecanismos de inspeção de IPS: Remontagem de pacotes de TCP;

3.22.1.4.12. Deverá possuir o seguinte mecanismos de inspeção de IPS: Bloqueio de pacotes malformados;

3.22.1.4.13. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;

3.22.1.4.14. Detectar e bloquear a origem de portscans;

3.22.1.4.15. Bloquear ataques efetuados por worms conhecidos;

3.22.1.4.16. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

3.22.1.4.17. Possuir assinaturas para bloqueio de ataques de buffer overflow;

3.22.1.4.18. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

3.22.1.4.19. Identificar e bloquear comunicação com botnets;

3.22.1.4.20. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
3.22.1.4.21. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;
3.22.1.4.22. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
3.22.1.4.23. Os eventos devem identificar o país de onde partiu a ameaça;
3.22.1.4.24. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
3.22.1.4.25. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;
3.22.1.4.26. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança;
3.22.1.4.27. Suportar e estar licenciado com proteção contra ataques de dia zero por meio de integração com solução de Sandbox em nuvem, do mesmo fabricante;
3.22.1.5. **Filtro de URL:**
3.22.1.5.1. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
3.22.1.5.2. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local, em modo de proxy transparente e explícito;
3.22.1.5.3. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
3.22.1.5.4. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;
3.22.1.5.5. Possuir pelo menos 60 categorias de URLs;

3.22.1.5.6. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;
3.22.1.5.7. Permitir a customização de página de bloqueio;
3.22.1.5.8. Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site);
3.22.1.5.9. Além do Explicit Web Proxy, suportar proxy Web transparente;
3.22.1.6. **Identificação de Usuários:**
3.22.1.6.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;
3.22.1.6.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;
3.22.1.6.3. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso como, mas não limitado à, utilização de sistemas virtuais, segmentos de rede, etc;
3.22.1.6.4. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;
3.22.1.6.5. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários;
3.22.1.6.6. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);
3.22.1.6.7. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
3.22.1.6.8. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

3.22.1.6.9. Permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso a internet e gerenciamento da solução;
3.22.1.6.10. Prover no mínimo um token nativamente, possibilitando autenticação de duplo fator;
3.22.1.7. **QoS e Traffic Shaping:**
3.22.1.7.1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube, Ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máxima largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;
3.22.1.7.2. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;
3.22.1.7.3. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;
3.22.1.7.4. Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo;
3.22.1.7.5. Suportar a criação de políticas de QoS e Traffic Shaping por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;
3.22.1.7.6. Suportar a criação de políticas de QoS e Traffic Shaping por porta;
3.22.1.7.7. O QoS deve possibilitar a definição de tráfego com banda garantida;
3.22.1.7.8. O QoS deve possibilitar a definição de tráfego com banda máxima;
3.22.1.7.9. O QoS deve possibilitar a definição de fila de prioridade;
3.22.1.7.10. Suportar marcação de pacotes Diffserv, inclusive por aplicação;
3.22.1.7.11. Suportar modificação de valores DSCP para o Diffserv;
3.22.1.7.12. Suportar priorização de tráfego usando informação de Type of Service;
3.22.1.7.13. Deve suportar QOS (traffic-shapping), em interface agregadas ou redundantes;
3.22.1.8. **Filtro de dados:**
3.22.1.8.1. Permitir a criação de filtros para arquivos e dados pré-definidos;
3.22.1.8.2. Os arquivos devem ser identificados por extensão e tipo;
3.22.1.8.3. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);

3.22.1.8.4. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
3.22.1.8.5. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
3.22.1.8.6. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;
3.22.1.9. **Geo localização:**
3.22.1.9.1. Suportar a criação de políticas por geo-localização, permitindo o trafego de determinado Pais/Países sejam bloqueados;
3.22.1.9.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
3.22.1.9.3. Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas;
3.22.1.10. **VPN:**
3.22.1.10.1. Suportar VPN Site-to-Site e Cliente-To-Site;
3.22.1.10.2. Suportar IPSec VPN;
3.22.1.10.3. Suportar SSL VPN;
3.22.1.10.4. A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;
3.22.1.10.5. A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
3.22.1.10.6. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
3.22.1.10.7. A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);
3.22.1.10.8. Suportar VPN em em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;
3.22.1.10.9. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de throubleshooting;
3.22.1.10.10. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
3.22.1.10.11. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
3.22.1.10.12. Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;

3.22.1.10.13. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
3.22.1.10.14. Deverá manter uma conexão segura com o portal durante a sessão;
3.22.1.10.15. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior);
3.22.1.10.16. Deve suportar Auto-Discovery Virtual Private Network (ADVPN)
3.22.1.10.17. Deve suportar agregação de túneis IPSec
3.22.1.10.18. Deve suportar algoritmo de balanceamento do tipo WRR (Weighted Round Robin) em agregação de túneis IPSec
3.22.1.10.19. A VPN IPSec deve suportar Forward Error Correction (FEC)
3.22.1.10.20. Deve suportar TLS 1.3 em VPN SSL;
3.22.1.11. **SD-WAN:**
3.22.1.11.1. Deve implementar balanceamento de link por hash do IP de origem;
3.22.1.11.2. Deve implementar balanceamento de link por hash do IP de origem e destino;
3.22.1.11.3. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links.
3.22.1.11.4. Deve implementar balanceamento de link por custo configurado do link.
3.22.1.11.5. Deve suportar o balanceamento de, no mínimo, 256 links;
3.22.1.11.6. Deve suportar o balanceamento de links de interfaces físicas, sub-interfaces lógicas de VLAN e túneis IPSec
3.22.1.11.7. Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;
3.22.1.11.8. Deve gerar log de eventos que registrem alterações no estado dos links do SDWAN, monitorados pela checagem de saúde
3.22.1.11.9. Deve suportar Zero-Touch Provisioning
3.22.1.11.10. Possuir checagem do estado de saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Perda de Pacotes
3.22.1.11.11. Deve ser possível configurar a porcentagem de perda de pacotes e o tempo de latência e jitter, na medição de estado de link. Estes valores serão utilizados pela solução para decidir qual link será utilizado
3.22.1.11.12. A solução deve permitir modificar o intervalo de tempo de checagem, em segundos, para cada um dos links.

3.22.1.11.13. A checagem de estado de saúde deve suportar teste com Ping, HTTP e DNS
3.22.1.11.14. Suportar UDP Hole Punching em arquitetura ADVPN
3.22.1.11.15. A checagem de estado de saúde deve suportar a marcação de pacotes com DSCP, para avaliação mais precisa de links que possuem QoE configurado
3.22.1.11.16. As regras de escolha do link SD-WAN devem suportar o reconhecimento de aplicações, grupos de usuários, endereço IP de destino e Protocolo.
3.22.1.11.17. Deve suportar a configuração de nível mínimo de qualidade (latência, jitter e perda de pacotes) para que determinado link seja escolhido pelo SD-WAN
3.22.1.11.18. Deve suportar envio de BGP route-map para BGP neighbors, caso a qualidade mínima de um link não seja detectada pela checagem de saúde do link.
3.22.2. **Item 2: Ferramenta de gerenciamento da solução de Next-Generation Endpoint**;
3.22.2.1. **Características da Ferramenta:**
3.22.2.1.1. Possuir gerenciamento centralizado do software cliente de segurança, a partir de um console central, do próprio fabricante;
3.22.2.1.2. O licenciamento deve se basear no número de clientes de segurança registrados no gerenciamento centralizado, do mesmo fabricante;
3.22.2.1.3. O software cliente de segurança deve ser compatível com pelos menos os seguintes sistemas operacionais:
3.22.2.1.3.1. Microsoft Windows: 7 (32 e 64 bits), 8 (32 e 64 bits), 8,1 (32 e 64 bits) e 10 (32 e 64 bits);
3.22.2.1.3.2. Microsoft Windows Server 2012 ou superior;
3.22.2.1.3.3. macOS 11+, 10.15, 10.14;
3.22.2.1.3.4. iOS 9.0 ou superior;
3.22.2.1.3.5. Android 5.0 ou superior;
3.22.2.1.3.6. Linux Ubuntu 16.04 ou superior;
3.22.2.1.3.7. Linux Red Hat 7.4 ou superior;
3.22.2.1.3.8. Linux CentOS 7.4 ou superior com KDE ou GNOME;
3.22.2.1.4. O software de gerenciamento centralizado deve suportar a instalação no Microsoft Windows Server 2012 ou superior;
3.22.2.1.5. Deve ter uma interface gráfica do usuário, pelo menos nos idiomas inglês, português e espanhol;
3.22.2.1.6. Deve permitir o backup do arquivo de configuração;

3.22.2.1.7. O cliente de segurança deverá enviar os logs para o servidor de gerenciamento central;
3.22.2.1.8. O cliente de segurança deve permitir a configuração local via XML (eXtensible Markup Language);
3.22.2.1.9. Deve controlar o acesso a dispositivos removíveis e ser capaz de monitorar, permitir e negar acesso a dispositivos USB, de acordo com as seguintes características do dispositivo:
3.22.2.1.9.1. Device Class;
3.22.2.1.9.2. Manufacturer;
3.22.2.1.9.3. Vendor ID;
3.22.2.1.9.4. Product ID;
3.22.2.1.9.5. Revision;
3.22.2.1.10. Deve poder definir o nível do log em: emergency, alert, critical, error, warning, notice, information, debug;
3.22.2.1.11. Deve ter a capacidade de desabilitar os serviços de proxy para fins de solução de problemas;
3.22.2.1.12. Deve ser capaz de ativar seletivamente logs, de acordo com as funcionalidades licenciadas para a plataforma: Antivírus, Firewall de Aplicação, Telemetria, Agente de Logon Único (Single Sign One), Proxy, IPSec VPN, AntiExploit, SSL VPN, Atualizações, Vulnerabilidades, Filtro Web e Sandbox;
3.22.2.1.13. Deve suportar exportar logs diretamente do cliente de segurança;
3.22.2.1.14. Deve ter interface gráfica de gerenciamento via web (HTTPS);
3.22.2.1.15. Deve permitir a criação de usuários de diferentes perfis administrativos;
3.22.2.1.16. Deve permitir importar informações do Microsoft Active Directory usando LDAP;
3.22.2.1.17. Deve permitir o registro manual da estação através do uso de uma senha;
3.22.2.1.18. Deve permitir a criação de grupos de clientes para facilitar o gerenciamento;
3.22.2.1.19. Deve ser capaz de enviar logs para uma plataforma de log do mesmo fabricante;
3.22.2.1.20. Dever permitir a instalação do certificado digital no cliente;
3.22.2.1.21. Deve conter informações sobre o sistema operacional no qual o cliente está instalado;
3.22.2.1.22. Deve informar o perfil de segurança criado e/ou aplicado;

3.22.2.1.23. Deve permitir a implantação automática de clientes de terminal de acordo com a OU do MS AD;
3.22.2.1.24. Deve permitir a manutenção de várias instâncias de instaladores com recursos diferentes (AV, VPN, WF, etc.) e arquiteturas (x86, x64, etc.);
3.22.2.1.25. Deve permitir a implantação de equipamentos que NÃO pertencem ao active directory (AD);
3.22.2.1.26. Deve ter um painel em que possa verificar rapidamente o status de integridade dos clientes;
3.22.2.1.27. Os usuários administradores devem poder sincronizar com o AD, para permitir o login com as mesmas credenciais;
3.22.2.1.28. Deve ser capaz de definir funções administrativas;
3.22.2.1.29. Deve suportar fazer backup / restaurar configurações do console, configuração do servidor, políticas de terminal etc.;
3.22.2.1.30. O fabricante deve fornecer um portal para baixar o instalador do cliente de segurança e permitir a instalação local;
3.22.2.1.31. O console de gerenciamento central deve poder instalar o cliente de segurança nos computadores Windows associados a um domínio da Microsoft;
3.22.2.1.32. Deve fornecer informações da estação de trabalho, no mínimo e não se limitando a: Nome completo, Telefone, E-mail, Informações pessoais obtidas minimamente de (entrada manual, linkedin, google, Sistema operacional e/ou Salesforce), status do cliente, Nome do host, etiqueta de host;
3.22.2.1.33. Deve suportar upload de uma foto ou avatar para identificação rápida do usuário;
3.22.2.1.34. Deve relatar rapidamente o nível de vulnerabilidade da estação de trabalho;
3.22.2.1.35. Deve ter um sistema de notificação pop-up;
3.22.2.1.36. Deve ter uma lista de notificações atuais e anteriores;
3.22.2.1.37. Deve fornecer informações sobre a vulnerabilidade, patches, versões afetadas etc., bem como o CVE correspondente;
3.22.2.2. **Funcionalidades de VPN**
3.22.2.2.1. Deve permitir split-tunnel para VPN IPSec e SSL
3.22.2.2.2. Na VPN split-tunneling, deve permitir configurar exceções baseadas no reconhecimento de aplicações locais, podendo especificar o nome do processo, caminho completo e diretório onde está instalado localmente, para não serem direcionadas ao túnel VPN.

3.22.2.2.3. Na VPN split-tunneling, deve permitir configurar exceções baseadas em domínio, para não serem direcionadas ao túnel VPN
3.22.2.2.4. Deve permitir selecionar de forma automática o gateway remoto mais próximo para conexão VPN, baseado em:
3.22.2.2.4.1. Tempo de resposta de ping
3.22.2.2.4.2. TCP Round Trip Time (TCP Three-Way Handshare SYN, SYN-ACK, ACK)
3.22.2.2.5. Deve permitir conectar automaticamente à um túnel SSL VPN backup quando um túnel IPSec VPN falhar.
3.22.2.2.6. Deve permitir associar tags à um usuário remoto de VPN, de acordo com as regras de conformidade
3.22.2.2.7. Deve permitir bloquear acesso à determinadas VPN's de usuário, baseado nas tags associadas ao usuário.
3.22.2.2.8. Deve permitir criar regras para associação de tags, de acordo com os seguintes parâmetros:
3.22.2.2.8.1. Grupo Active Directory
3.22.2.2.8.2. Existência de Antivírus instalado
3.22.2.2.8.3. Existência de Antivírus atualizado
3.22.2.2.8.4. Certificado
3.22.2.2.8.5. Cliente de Segurança Gerenciado Centralmente
3.22.2.2.8.6. Existência de Arquivo em determinado diretório do cliente
3.22.2.2.8.7. Domínio logado
3.22.2.2.8.8. Versão de Sistema Operacional
3.22.2.2.8.9. Chave de Registro do Windows
3.22.2.2.8.10. Processo em execução
3.22.2.2.8.11. Malware detectado pelo Sandbox nos últimos 7 dias
3.22.2.2.8.12. Nível de Vulnerabilidade do dispositivo
3.22.2.2.8.13. Windows Security, sendo a checagem das seguintes aplicações, se estão habilitadas:
3.22.2.2.8.13.1. Windows Defender
3.22.2.2.8.13.2. Bitlocker Disk Encryption
3.22.2.2.8.13.3. Exploit Guard
3.22.2.2.8.13.4. Application Guard
3.22.2.2.8.13.5. Windows Firewall
3.22.2.2.9. Deve permitir que o usuário configure VPNs localmente
3.22.2.2.10. Deve permitir que o usuário desconecte uma VPN
3.22.2.2.11. Deve permitir a conexão VPN antes do login
3.22.2.2.12. Deve permitir conexão VPN automática

3.22.2.2.13. Deve suportar a configuração de senha para o usuário acessar a configuração do cliente
3.22.2.2.14. Deve permitir a autenticação de dois fatores fornecida pelo mesmo fabricante
3.22.2.2.15. IPSEC:
3.22.2.2.15.1. Deve permitir que o usuário crie novas VPNs IPSEC
3.22.2.2.15.2. Deve permitir que várias VPNs IPSEC sejam definidas simultaneamente
3.22.2.2.15.3. Deve permitir a autenticação usando nome de usuário e senha
3.22.2.2.15.4. Deve permitir a autenticação usando certificados digitais
3.22.2.2.15.5. Deve permitir a seleção dos modos Principal e Agressivo;
3.22.2.2.15.6. Deve permitir a configuração do DHCP por IPSec;
3.22.2.2.15.7. Deve permitir o uso do NAT Traversal;
3.22.2.2.15.8. Deve permitir a escolha de grupos Diffie-Hellman (1,2,5 e 14);
3.22.2.2.15.9. Deve permitir configurações de expiração de chave IKE;
3.22.2.2.15.10. Deve suportar IKEv1 e IKEv2
3.22.2.2.15.11. Deve permitir o uso do Perfect Forward Secrecy;
3.22.2.2.15.12. Deve suportar o uso de certificados para autenticação na VPN IPSec
3.22.2.2.15.13. Deve suportar usuário e senha para autenticação VPN IPSec
3.22.2.2.15.14. Deve suportar o uso de certificados em cartão inteligente para autenticação na VPN IPSec
3.22.2.2.15.15. Deve suportar o bloqueio de tráfego IPv6 na VPN IPsec
3.22.2.2.16. SSL:
3.22.2.2.16.1. Deve permitir que o usuário crie novas VPNs SSL
3.22.2.2.16.2. Deve permitir que várias VPNs SSL sejam definidas simultaneamente
3.22.2.2.16.3. Deve permitir a personalização da porta TCP na qual a VPN SSL funciona
3.22.2.2.16.4. Deve permitir a autenticação usando nome de usuário e senha
3.22.2.2.16.5. Deve permitir a autenticação usando certificados digitais
3.22.2.2.16.6. Para uso específico de VPN SSL (pelo menos):
3.22.2.2.16.6.1. Especificação IP do concentrador
3.22.2.2.16.6.2. Especificação da porta do hub
3.22.2.2.16.7. Deve permitir autenticação SAML SSO para VPN SSL

3.22.2.2.16.8. Deve permitir enviar tráfego IPV4 e IPV6 simultaneamente pelo mesmo túnel VPN SSL

3.22.2.3. **Funcionalidades de VPN:**

3.22.2.3.1. Deve permitir split-tunnel para VPN IPSec e SSL;

3.22.2.3.2. Na VPN split-tunneling, deve permitir configurar exceções baseadas no reconhecimento de aplicações locais, podendo especificar o nome do processo, caminho completo e diretório onde está instalado localmente, para não serem direcionadas ao túnel VPN;

3.22.2.3.3. Na VPN split-tunneling, deve permitir configurar exceções baseadas em domínio, para não serem direcionadas ao túnel VPN;

3.22.2.3.4. Deve permitir selecionar de forma automática o gateway remoto mais próximo para conexão VPN, baseado em:

3.22.2.3.4.1. Tempo de resposta de ping;

3.22.2.3.4.2. TCP Round Trip Time (TCP Three-Way Handshare SYN, SYN-ACK, ACK);

3.22.2.3.5. Deve permitir conectar automaticamente à um túnel SSL VPN backup quando um túnel IPSec VPN falhar;

3.22.2.3.6. Deve permitir associar tags à um usuário remoto de VPN, de acordo com as regras de conformidade;

3.22.2.3.7. Deve permitir bloquear acesso à determinadas VPN's de usuário, baseado nas tags associadas ao usuário;

3.22.2.3.8. Deve permitir criar regras para associação de tags, de acordo com os seguintes parâmetros:

3.22.2.3.8.1. Grupo Active Directory;

3.22.2.3.8.2. Existência de Antivírus instalado;

3.22.2.3.8.3. Existência de Antivírus atualizado;

3.22.2.3.8.4. Certificado;

3.22.2.3.8.5. Cliente de Segurança Gerenciado Centralmente;

3.22.2.3.8.6. Existência de Arquivo em determinado diretório do cliente;

3.22.2.3.8.7. Domínio logado;

3.22.2.3.8.8. Versão de Sistema Operacional;

3.22.2.3.8.9. Chave de Registro do Windows;

3.22.2.3.8.10. Processo em execução;

3.22.2.3.8.11. Malware detectado pelo Sandbox nos últimos 7 dias;

3.22.2.3.8.12. Nível de Vulnerabilidade do dispositivo;

3.22.2.3.8.13. Windows Security, sendo a checagem das seguintes aplicações, se estão habilitadas:

3.22.2.3.8.13.1. Windows Defender;

3.22.2.3.8.13.2. Bitlocker Disk Encryption;

3.22.2.3.8.13.3. Exploit Guard;
3.22.2.3.8.13.4. Application Guard;
3.22.2.3.8.13.5. Windows Firewall.
3.22.2.3.9. Deve permitir que o usuário configure VPNs localmente;
3.22.2.3.10. Deve permitir que o usuário desconecte uma VPN;
3.22.2.3.11. Deve permitir a conexão VPN antes do login;
3.22.2.3.12. Deve permitir conexão VPN automática;
3.22.2.3.13. Deve suportar a configuração de senha para o usuário acessar a configuração do cliente;
3.22.2.3.14. Deve permitir a autenticação de dois fatores fornecida pelo mesmo fabricante;
3.22.2.3.15. IPSEC:
3.22.2.3.15.1. Deve permitir que o usuário crie novas VPNs IPSEC;
3.22.2.3.15.2. Deve permitir que várias VPNs IPSEC sejam definidas simultaneamente;
3.22.2.3.15.3. Deve permitir a autenticação usando nome de usuário e senha;
3.22.2.3.15.4. Deve permitir a autenticação usando certificados digitais
3.22.2.3.15.5. Deve permitir a seleção dos modos Principal e Agressivo;
3.22.2.3.15.6. Deve permitir a configuração do DHCP por IPSec;
3.22.2.3.15.7. Deve permitir o uso do NAT Traversal;
3.22.2.3.15.8. Deve permitir a escolha de grupos Diffie-Hellman (1,2,5 e 14);
3.22.2.3.15.9. Deve permitir configurações de expiração de chave IKE;
3.22.2.3.15.10. Deve suportar IKEv1 e IKEv2;
3.22.2.3.15.11. Deve permitir o uso do Perfect Forward Secrecy;
3.22.2.3.15.12. Deve suportar o uso de certificados para autenticação na VPN IPSec;
3.22.2.3.15.13. Deve suportar usuário e senha para autenticação VPN IPSec;
3.22.2.3.15.14. Deve suportar o uso de certificados em cartão inteligente para autenticação na VPN IPSec;
3.22.2.3.15.15. Deve suportar o bloqueio de tráfego IPv6 na VPN IPsec
3.22.2.3.16. SSL:
3.22.2.3.16.1. Deve permitir que o usuário crie novas VPNs SSL;
3.22.2.3.16.2. Deve permitir que várias VPNs SSL sejam definidas simultaneamente;
3.22.2.3.16.3. Deve permitir a personalização da porta TCP na qual a VPN SSL funciona;
3.22.2.3.16.4. Deve permitir a autenticação usando nome de usuário e senha;
3.22.2.3.16.5. Deve permitir a autenticação usando certificados digitais;

3.22.2.3.16.6. Para uso específico de VPN SSL (pelo menos):
3.22.2.3.16.6.1. Especificação IP do concentrador;
3.22.2.3.16.6.2. Especificação da porta do hub;
3.22.2.3.16.7. Deve permitir autenticação SAML SSO para VPN SSL;
3.22.2.3.16.8. Deve permitir enviar tráfego IPV4 e IPV6 simultaneamente pelo mesmo túnel VPN SSL;
3.22.2.4. **Análise de Vulnerabilidade:**
3.22.2.4.1. O cliente de segurança deve ter um módulo de pesquisa de vulnerabilidades integrado e permitir o gerenciamento central no console do mesmo fabricante;
3.22.2.4.2. Deve permitir que o usuário inicie uma análise de vulnerabilidade sob demanda;
3.22.2.4.3. As vulnerabilidades encontradas devem ser exibidas localmente com um link para visualizar informações de um banco de dados na Internet. Deve ter pelo menos: nome, gravidade e detalhes;
3.22.2.4.4. Os resultados da verificação de vulnerabilidades devem incluir pelo menos: lista de vulnerabilidades, número de vulnerabilidades classificadas como críticas, altas, médias e baixas;
3.22.2.4.5. Deve permitir a aplicação automática de patches;
3.22.2.4.6. Deve detalhar quais correções requerem instalação manual;
3.22.2.4.7. A verificação de vulnerabilidades deve ser permitida de maneira ordenada e autônoma a partir do console central;
3.22.2.5. **Funcionalidades de Filtro de Conteúdo WEB:**
3.22.2.5.1. Deve permitir a configuração do perfil de filtro da web a partir do console central do mesmo fabricante;
3.22.2.5.2. O fabricante deve fazer consultas on-line com o cliente de segurança sobre a categoria de um determinado site (por exemplo, interesse geral, tecnologia, hackers, pornografia etc.) para aplicar a política de controle de acesso à Internet;
3.22.2.5.3. O cliente de segurança deve suportar regras estáticas de acesso à Internet com base em expressões regulares;
3.22.2.5.4. Para um determinada URL, os acessos devem ser: permitir, bloquear, alertar ou monitorar;
3.22.2.5.5. Deve configurar o filtro de URL com base em caracteres simples, curinga e expressões regulares (regex);
3.22.2.5.6. Deve permitir que as configurações de filtro URL sejam importadas do firewall do mesmo fabricante;
3.22.2.5.7. Deve implementar mecanismo Safe Search, para limitar acesso à conteúdo em buscadores Google e Bing;

3.22.2.5.8. Possuir pelo menos 80 categorias de filtro URL.

3.22.3. **Item 3: Sistema de Gerenciamento de logs, análise e plataforma de relatório**

3.22.3.1. Características:

3.22.3.1.1. Deve ser do tipo appliance virtual (VM);

3.22.3.1.2. Possuir capacidade de recebimento de logs de pelo menos 1 mil dispositivos;

3.22.3.1.3. Possuir a capacidade de receber pelo menos 6 GBytes de logs diários;

3.22.3.1.4. Possuir pelo menos 3 TB de espaço em disco;

3.22.3.1.5. Deverá ser compatível com ambiente VMware ESXi 5.5, 6.0, 6.5, 6.7 e 7.0;

3.22.3.1.6. Deverá ser compatível com ambiente Microsoft Hyper-V 2008 R2/2012/2012 R2/2016;

3.22.3.1.7. Deverá ser compatível com ambiente Citrix XenServer 6.0+ e Open Source Xen 4.1+;

3.22.3.1.8. Deverá ser compatível com ambiente KVM;

3.22.3.1.9. Deverá ser compatível com ambiente Nutanix AHV;

3.22.3.1.10. Deverá ser compatível com ambiente Amazon Web Services (AWS);

3.22.3.1.11. Deverá ser compatível com ambiente Microsoft Azure;

3.22.3.1.12. Deverá ser compatível com o ambiente Google Cloud (GPC);

3.22.3.1.13. Deverá ser compatível com o ambiente Oracle Cloud Infrastructure (OCI);

3.22.3.1.14. Deverá ser compatível com o ambiente Alibaba Cloud (AliCloud);

3.22.3.1.15. Não deve possuir limite na quantidade de múltiplas vCPU;

3.22.3.1.16. Não deve possuir limite para suporte a expansão de memória RAM;

3.22.3.2. Requisitos Mínimos de Funcionalidade

3.22.3.2.1. Suportar o acesso via SSH e WEB (HTTPS) para gerenciamento de soluções;

3.22.3.2.2. Possuir comunicação e autenticação criptografada com usuário e senha para obter relatórios, na interface gráfica (GUI) e via linha de comando no console de gerenciamento;

3.22.3.2.3. Permitir o acesso simultâneo à administração, bem como permitir que pelo menos 2 (dois) perfis sejam criados para administração e monitoramento;

3.22.3.2.4. Suportar SNMP versão 2 e 3;

3.22.3.2.5. Permitir a virtualização do gerenciamento e administração dos dispositivos, nos quais cada administrador só tem acesso aos computadores autorizados;
3.22.3.2.6. Permitir a criação de um administrador geral, que tenha acesso geral a todas as instâncias de virtualização da solução;
3.22.3.2.7. Permitir ativar e desativar para cada interface da plataforma, as permissões de acesso HTTP, HTTPS, SSH;
3.22.3.2.8. Possuir autenticação de usuários para acesso à plataforma via LDAP;
3.22.3.2.9. Possuir autenticação de usuários para acesso à plataforma via Radius;
3.22.3.2.10. Possuir autenticação de usuários para acesso à plataforma via TACACS +;
3.22.3.2.11. Possuir geração de relatórios de tráfego em tempo real, em formato de mapa geográfico;
3.22.3.2.12. Possuir geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas;
3.22.3.2.13. Possuir geração de relatórios de tráfego em tempo real, em formato de gráfico;
3.22.3.2.14. Possuir definição de perfis de acesso ao console com permissão granular, como: acesso de gravação, acesso de leitura, criação de novos usuários e alterações nas configurações gerais;
3.22.3.2.15. Possuir um assistente gráfico para adicionar novos dispositivos, usando seu endereço IP, usuário e senha;
3.22.3.2.16. Possuir visualização da quantidade de logs enviados de cada dispositivo monitorado;
3.22.3.2.17. Possuir mecanismos de apagamento automático para logs antigos;
3.22.3.2.18. Permitir importação e exportação de relatórios;
3.22.3.2.19. Deve ter a capacidade de criar relatórios no formato HTML;
3.22.3.2.20. Deve ter a capacidade de criar relatórios em formato PDF;
3.22.3.2.21. Deve ter a capacidade de criar relatórios no formato XML;
3.22.3.2.22. Deve ter a capacidade de criar relatórios no formato CSV;
3.22.3.2.23. Deve permitir exportar os logs no formato CSV;
3.22.3.2.24. Deve gerar logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário;
3.22.3.2.25. Os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar;

3.22.3.2.26. A solução deve ter relatórios predefinidos;
3.22.3.2.27. Deve poder enviar automaticamente os logs para um servidor FTP externo para a solução;
3.22.3.2.28. A duplicação de relatórios existentes deve ser possível para edição posterior;
3.22.3.2.29. Ter a capacidade de personalizar a capa dos relatórios obtidos;
3.22.3.2.30. Permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos mesmos logs;
3.22.3.2.31. Os logs de auditoria das regras e alterações na configuração do objeto devem ser exibidos em uma lista diferente dos logs relacionados ao tráfego de dados;
3.22.3.2.32. Ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas;
3.22.3.2.33. Deve ter um mecanismo de "pesquisa detalhada" para navegar pelos relatórios em tempo real;
3.22.3.2.34. Deve permitir que os arquivos de log sejam baixados da plataforma para uso externo;
3.22.3.2.35. Ter a capacidade de gerar e enviar relatórios periódicos automaticamente;
3.22.3.2.36. Permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades;
3.22.3.2.37. Permitir o envio por e-mail relatórios automaticamente;
3.22.3.2.38. Deve permitir que o relatório seja enviado por email ao destinatário específico;
3.22.3.2.39. Permitir a programação da geração de relatórios, conforme calendário definido pelo administrador;
3.22.3.2.40. É necessário exibir graficamente em tempo real a taxa de geração de logs para cada dispositivo gerenciado;
3.22.3.2.41. Deve permitir o uso de filtros nos relatórios;
3.22.3.2.42. Deve permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros;
3.22.3.2.43. Permitir especificar o idioma dos relatórios criados;
3.22.3.2.44. Gerar alertas automáticos por email, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros;
3.22.3.2.45. Deve permitir o envio automático de relatórios para um servidor SFTP ou FTP externo;

3.22.3.2.46. Deve ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios;
3.22.3.2.47. Possibilitar visualizar nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros;
3.22.3.2.48. Deve ter uma ferramenta que permita analisar o desempenho na geração de relatórios, a fim de detectar e corrigir problemas na geração deles;
3.22.3.2.49. Importar arquivos com logs de dispositivos compatíveis conhecidos e não conhecidos pela plataforma, para geração posterior de relatórios;
3.22.3.2.50. Deve ser possível definir o espaço que cada instância de virtualização pode usar para armazenamento de log;
3.22.3.2.51. Deve fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado;
3.22.3.2.52. Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos
3.22.3.2.53. Deve permitir visualizar em tempo real os logs recebidos;
3.22.3.2.54. Deve permitir o encaminhamento de log no formato syslog;
3.22.3.2.55. Deve permitir o encaminhamento de log no formato CEF (Common Event Format);
3.22.3.2.56. Deve incluir um painel para operações SOC que monitore as principais ameaças à segurança da sua rede;
3.22.3.2.57. Deve incluir o painel para operações do SOC que monitora o envolvimento do usuário e o uso suspeito da web em sua rede;
3.22.3.2.58. Deve incluir o painel para operações SOC que monitora o tráfego na sua rede;
3.22.3.2.59. Deve incluir o painel para operações SOC que monitoram o tráfego de aplicativos e sites na sua rede;
3.22.3.2.60. Deve incluir o painel para operações SOC que monitoram detecções de ameaças de dia zero em sua rede (sandboxing);
3.22.3.2.61. Deve incluir o painel para operações SOC que monitora a atividade do terminal na sua rede;
3.22.3.2.62. Deve incluir o painel para operações SOC que monitoram a atividade da VPN na sua rede;
3.22.3.2.63. Deve incluir um painel para operações SOC que monitora pontos de acesso Wi-Fi e SSIDs;

3.22.3.2.64. Deve incluir o painel para operações SOC que monitoram o desempenho dos recursos locais da solução (CPU, Memória);
3.22.3.2.65. Deve permitir a criação de painéis personalizados para monitorar operações SOC;
3.22.3.2.66. Gerar alertas de eventos a partir de logs recebidos;
3.22.3.2.67. Permitir a criação de incidentes a partir de alertas de eventos para o terminal;
3.22.3.2.68. Deve permitir o suporte a logs nas nuvens públicas do AWS, Azure ou Google;
3.22.3.2.69. Suportar o padrão SAML para autenticação do usuário administrador;
3.22.3.2.70. Possuir relatório de avaliação de risco para e-mail;
3.22.3.2.71. Possuir relatório de conformidade com o PCI sem fio;
3.22.3.2.72. Possuir relatório de APs e SSIDs autorizados, bem como clientes WIFi;
3.22.3.2.73. Possuir relatório de vulnerabilidades da solução de segurança gerenciada do equipamento terminal;
3.22.3.2.74. Possuir relatório de aplicativo da web, se tiver uma plataforma de segurança da web;
3.22.3.3. Relatórios de Firewall
3.22.3.3.1. Deve ter um relatório de conformidade com o PCI DSS;
3.22.3.3.2. Possuir um relatório de uso do aplicativo SaaS;
3.22.3.3.3. Possuir um relatório de prevenção de perda de dados (DLP);
3.22.3.3.4. Possuir um relatório de VPN;
3.22.3.3.5. Possuir um relatório IPS (Intruder Prevention System);
3.22.3.3.6. Possuir um relatório de reputação do cliente;
3.22.3.3.7. Possuir um relatório de análise de segurança do usuário;
3.22.3.3.8. Possuir um relatório de análise de ameaças cibernéticas;
3.22.3.3.9. Possuir um breve relatório resumido diário de eventos e incidentes de segurança;
3.22.3.3.10. Possuir um relatório de tráfego DNS;
3.22.3.3.11. Possuir um relatório de tráfego de e-mail;
3.22.3.3.12. Possuir um relatório dos 10 principais aplicativos usados na rede;
3.22.3.3.13. Possuir um relatório dos 10 principais sites usados na rede;
3.22.3.3.14. Possuir um relatório de uso de mídia social;
3.22.4. **Item 4: Serviço de instalação, configuração, atualização e treinamento de pessoal**;

3.22.4.1. O Serviço de Instalação e Configuração dos equipamentos e licenciamentos fornecidos neste Termo de Referência, é definida conforme segue:
3.22.4.1.1. O serviço de instalação deverá ser prestado localmente nas dependências do Badesul, na Rua General Andrade Neves, 175, 15º andar, Centro Histórico, Porto Alegre/RS;
3.22.4.1.2. O serviço de instalação dos equipamentos deverá ser iniciado imediatamente após a sua entrega;
3.22.4.1.3. O serviço de instalação deverá ser realizado por técnico certificado para a linha de equipamentos fornecidos;
3.22.4.1.4. Instalação física de todos os equipamentos e elementos, como conectorização de cabos e fibras óticas, provisionamento de posição e fixação em rack, fontes de energia e adaptadores diversos;
3.22.4.1.5. Conexão elétrica e lógica;
3.22.4.1.6. Configuração de todos os equipamentos e licenças fornecidos;
3.22.4.1.7. Atualização de todos os produtos de software e firmware para as versões mais recentes e recomendadas pelo fabricante da solução, incluindo os Appliances Virtuais;
3.22.4.1.8. Migração e ajuste de todas as regras, perfis e demais configurações dos equipamentos fornecidos a partir do equipamento atualmente em uso no Badesul;
3.22.4.1.9. Adequações de topologia e configurações dos produtos utilizados pela CONTRATANTE para o devido funcionamento dessas soluções;
3.22.4.2. Como premissa os serviços deverão ser executados de maneira não disruptiva, sem ocasionar ou incorrer em indisponibilidade não programada em janelas predefinidas junto da equipe da CONTRATANTE;
3.22.4.3. Ações disruptivas deverão ser executadas fora dos horários operacionais da CONTRATANTE, incluindo finais de semanas e feriados, e com a devida comunicação antecipada, planejamento conjunto e participação da CONTRATANTE;
3.22.4.4. Todo o serviço de instalação e configuração será realizado com o acompanhamento de técnicos da CONTRATANTE, aos quais deverá ser repassado todo o conhecimento necessário para operação e manutenção dos equipamentos fornecidos pela Contratada, na modalidade hands-on;
3.22.4.5. A CONTRATADA deverá entregar documentação contendo, minimanente:
3.22.4.5.1. Documentação As Built das instalações e de todos produtos utilizados pela CONTRATANTE, de maneira a documentar essa arquitetura de serviços e produtos, com a topologia contendo esses elementos. Juntamente

com acessos administrativos ao portal de gerência do fabricante, e os documentos dos serviços e contratação de licenciamentos, vigências de assinaturas, de suporte e de garantias;
3.22.4.5.2. Descrição da arquitetura da solução instalada, com diagrama(s) que ilustre(m) a topologia das ligações entre todos os equipamentos;
3.22.4.5.3. Descrição do procedimento de instalação e configuração dos equipamentos;
3.22.4.5.4. Listagem de correções (patches) e atualizações (updates) aplicadas nos softwares e firmwares que integram os equipamentos.
3.22.4.5.5. Após o fornecimento da documentação a CONTRATADA deverá promover a passagem de conhecimento em reunião com hands-on para a equipe da CONTRATANTE, revisando a documentação e apresentando entrega do Serviço de Instalação e Configuração;
3.22.4.6. Após a conclusão do serviço de instalação, os equipamentos deverão estar totalmente operacionais, em perfeitas condições de funcionamento e integrados à rede, bem como configurados de tal forma que atendam a todos os requisitos especificados neste edital;
3.22.4.7. Caso seja satisfeita a condição estabelecida no subitem 3.22.4.6, o BADESUL emitirá, em até 5 (cinco) dias úteis, Termo de Recebimento Definitivo do objeto deste Termo de Referência. Caso contrário, o BADESUL emitirá, em igual prazo, Termo de Recusa, no qual constarão os itens em desconformidade;
3.22.4.8. Em caso de recusa da entrega, o BADESUL concederá novo prazo à Contratada para ajuste das desconformidades apontadas no Termo de Recusa;
3.22.4.9. Caso as desconformidades não sejam sanadas no prazo estabelecido no subitem 3.22.4.8, serão aplicados os ajustes de pagamento na respectiva fatura da Contratada, nos termos estabelecidos no subitem 3.22.4.10;
3.22.4.10. Serão aplicados ajustes de pagamento em caso de atraso na entrega dos equipamentos nas dependências do BADESUL e em caso de atraso na execução do serviço de instalação dos equipamentos, conforme estabelecido abaixo:
3.22.4.10.1. Quando o atraso, na entrega ou na instalação, for de até 30 (trinta) dias, serão descontados 0,3% (três décimos por cento) por dia sobre o valor do fornecimento não realizado;
3.22.4.10.2. Quando o atraso, na entrega ou na instalação, for superior a 30 (trinta) dias, será descontado 20% (vinte por cento) sobre o valor do fornecimento não realizado.

3.22.4.11. Mesmo com a concessão do prazo para ajustes, referido no subitem 3.22.4.8, a Contratada estará sujeita à instauração de Processo Administrativo Punitivo para eventual aplicação de penalidades, nos termos estabelecidos no contrato.
3.22.4.12. A CONTRATADA deverá treinar a equipe técnica do Badesul na implantação da solução descrita no objeto deste Termo de Referência;
3.22.4.13. O treinamento consiste na transferência de tecnologia (de no mínimo 24 horas de treinamento, em curso(s) ministrado(s) por profissional(ais) certificado(s) do fabricante da solução Firewall de Próxima Geração ou UTM, ferramentas de gerenciamento, software de endpoint e software, entre outros, ou seja, de todos os elementos que comporão a solução da CONTRATADA;
3.22.4.14. A equipe técnica do Badesul que deverá ser treinada consiste de 02 (dois) técnicos de Administração de Rede devendo ser entregue a cada participante seu respectivo certificado de participação;
3.22.4.15. A CONTRATADA, obrigatoriamente, deverá entregar, em até 60 dias da data de assinatura do contrato, uma documentação AS-BUILT da solução, contendo todos os componentes listados, com os firmware utilizados, parâmetros adotados, senhas de administrador, diagramas, catálogos dos produtos, regras adotadas, com a topologia contendo estes elementos. Juntamente com acessos administrativos ao portal de gerência do fabricante, e os documentos dos serviços e contratação de licenciamentos, vigências de assinaturas, de suporte e de garantias. Esta documentação deverá ser entregue em mídia digital em arquivos abertos e editáveis;
3.22.5. **Item 5: Serviço de suporte técnico;**
3.22.5.1. A Contratada deverá prestar o serviço de suporte técnico para o firewall, licenças e instalações, durante toda a vigência contratual;
3.22.5.2. O serviço de suporte técnico consiste no acionamento da Contratada, por parte do BADESUL, para atendimento das seguintes demandas relacionadas ao firewall:
3.22.5.2.1. Identificação e resolução de problemas;
3.22.5.2.2. Instalação de pacotes de correção e novas versões do firewall;
3.22.5.2.3. Configuração de novas funcionalidades;
3.22.5.2.4. Alteração de configurações em uso;
3.22.5.2.5. Análise de impacto de mudanças nas configurações e na instalação de pacotes de correção e novas versões do firewall;
3.22.5.2.6. Avaliação da base instalada, bem como apresentação de recomendações e melhores práticas para operação e utilização do firewall;

3.22.5.2.7. Abertura e acompanhamento de chamados com o fabricante do firewall, nos casos em que for necessário;
3.22.5.2.8. Treinar a equipe técnica do Badesul quando houver atualização tecnológica da solução;
3.22.5.2.9. Esclarecimento de dúvidas.
3.22.5.3. **O serviço de suporte técnico deverá estar disponível para abertura, atendimento e acompanhamento de chamados em regime 24x7x365, ou seja, 24 horas por dia, 7 dias por semana, durante todos os dias do ano, sem pausa;**
3.22.5.4. Para este serviço o Badesul estão previstas a utilização de cinco (05) horas/mês, correspondendo a sessenta (60) horas ano e limitadas a trezentas (300) horas técnicas destinadas ao serviço de suporte técnico válidas para o período de sessenta (60) meses de contrato;
3.22.5.5. A previsão de cinco (05) horas/mês trata-se apenas de uma estimativa para a totalização das trezentas (300) horas do contrato e, portanto, não havendo obrigatoriedade para o BADESUL quanto à sua utilização;
3.22.5.6. As horas terão a seguinte fração de consumo:
3.22.5.6.1. Durante horário comercial, que abrange início as 8h00min até 18h00min, em dias de semana, uma fração de quinze (15) minutos;
3.22.5.6.2. Fora do horário comercial, que abrande início as 18h01min até as 7h59min, finais de semana e feriados, uma fração de sessenta (60) minutos;
3.22.5.7. A Contratada deverá prestar o serviço de suporte técnico sempre que demandado pelo Badesul;
3.22.5.8. Não há previsão quanto à distribuição da demanda pelo serviço de suporte técnico ao longo da vigência contratual, sendo responsabilidade da Contratada ajustar-se com os atendimentos dos serviços solicitados pelo BADESUL, de acordo com os prazos estabelecidos nos subitens 3.22.5.14.1 a 3.22.5.14.4;
3.22.5.9. Não será facultado à Contratada recusar a demanda do BADESUL pelo serviço de suporte técnico, desde que esteja em conformidade com o disposto no subitem 3.22.5.2;
3.22.5.10. A Contratada deverá prestar o serviço de suporte técnico de forma remota;
3.22.5.11. A Contratada deverá prestar o serviço de suporte técnico em idioma português do Brasil, em ambas as modalidades acima descritas;
3.22.5.11.1. O serviço de suporte técnico na modalidade remota compreende os equipamentos alocados na unidade do Badesul localizada na Rua General Andrade Neves, 175, 15º andar, Centro Histórico, Porto Alegre/RS bem como também aos sistemas objeto deste Termo de Referência;

3.22.5.12. Para a abertura e acompanhamento de chamados, a Contratada deverá fornecer interface web com as seguintes funcionalidades:

3.22.5.12.1. Abertura de chamado;

3.22.5.12.2. Listagem de chamados abertos;

3.22.5.12.3. Descrição do tipo de chamado e da sua solução;

3.22.5.12.4. Horário de abertura e fechamento dos chamados;

3.22.5.12.5. Quantidade de horas alocadas e consumidas no atendimento;

3.22.5.12.6. Nome dos responsáveis pelo chamado (cliente e fornecedor);

3.22.5.12.7. Histórico de todos atendimentos realizados (dia / semana / mês / ano);

3.22.5.12.8. Saldo de horas disponíveis no contrato.

3.22.5.13. Além do sistema de chamados descrito no item 3.22.5.12, a Contratada deverá fornecer também ao Badesul um endereço de e-mail e número de telefone que possibilite a realização de ligações para sua central de atendimento técnico de maneira auxiliar a fins de abertura e acompanhamento de chamados;

3.22.5.14. Ao abrir um chamado de suporte técnico, o Badesul irá classificá-lo nos seguintes níveis de severidade, conforme descrito abaixo:

3.22.5.14.1. Severidade 1: Solicitação para resolução de problema crítico no firewall, que esteja colocando em risco ou gerando indisponibilidade em serviços de TI críticos do Badesul, não havendo solução de contorno.	Prazo para início do atendimento: até 4 (quatro) horas úteis
3.22.5.14.2. Severidade 2: Solicitação para resolução de problema crítico no firewall, que esteja colocando em risco ou gerando indisponibilidade em serviços de TI críticos do Badesul, havendo solução de contorno	Prazo para início do atendimento: até 8 (oito) horas úteis
3.22.5.14.3. Severidade 3: Solicitação para realização de procedimento técnico, dentre os descritos no subitem 3.22.5.2, não havendo situação que envolva quaisquer indisponibilidades nos serviços de TI do Badesul	Prazo para início do atendimento: até 5 (cinco) dias úteis
3.22.5.14.4. Severidade 4: Solicitação para esclarecimento de dúvidas quanto às soluções fornecidas, não havendo situação que envolva	Prazo para início do atendimento: até 2 (dois) dias úteis

quaisquer indisponibilidades de serviços de TI do Badesul	

3.22.5.15. Em caso de descumprimento dos prazos estabelecidos nos subitens 3.22.5.14.1 a 3.22.5.14.4, será descontado do valor do chamado de suporte técnico solucionado o correspondente a 0,1% (um décimo por cento) por hora ou dia de atraso no início do atendimento de cada chamado de suporte técnico, limitado a 20% (vinte por cento) do total da fatura mensal do serviço de suporte técnico;

3.22.5.16. Adicionalmente aos ajustes de pagamento estabelecidos no subitem 3.22.5.15, em caso de descumprimento dos prazos estabelecidos nos subitens 3.22.5.14.1 a 3.22.5.14.4, a Contratada estará sujeita à instauração de Processo Administrativo Punitivo para eventual aplicação de penalidades, nos termos estabelecidos no Contrato;

3.22.5.17. A Contratada deverá manter o Badesul informado acerca do andamento dos chamados abertos;

3.22.5.18. A finalização de cada atendimento somente poderá ser efetuada com anuência formal do responsável técnico do Badesul;

3.22.5.19. Até o 5° dia útil de cada mês, iniciando a partir do mês subsequente ao início da prestação do serviço de suporte técnico, a Contratada deverá fornecer ao Badesul Relatório Mensal de Atendimentos contendo minimamente as seguintes informações;

3.22.5.19.1. Relação dos chamados em atendimento e solucionados no período de apuração, contendo para cada chamado:

3.22.5.19.1.1. Identificação do chamado;

3.22.5.19.1.2. Descrição do chamado;

3.22.5.19.1.3. Data e horário da abertura do chamado;

3.22.5.19.1.4. Data e horário do início do atendimento do chamado;

3.22.5.19.1.5. Data e horário da resolução do chamado;

3.22.5.19.1.6. Severidade do chamado, conforme estabelecido no subitem 3.22.5.14;

3.22.5.19.1.7. Modalidade de atendimento (remoto ou presencial);

3.22.5.19.1.8. Descrição do chamado;

3.22.5.19.1.9. Indicação se o atendimento ao chamado ocorreu nos prazos máximos estabelecidos nos subitens 3.22.5.14.1 a 3.22.5.14.4;

3.22.5.19.1.10. Horas de suporte técnico prestados para o chamado;

3.22.5.19.1.11. Horas ou dias de descumprimento dos prazos máximos estabelecidos nos subitens 3.22.5.14.1 a 3.22.5.14.4 para o chamado;

3.22.5.19.2. Percentual de desconto total na fatura mensal, calculado conforme o disposto no subitem 3.22.5.15;

4. DAS ESPECFICAÇÕES TÉCNICAS EXIGIDAS NA PROPOSTA DE PREÇOS

4.1. A fim de complementar as informações dispostas em sua proposta de preços, o licitante deverá apresentar comprovação ponto a ponto, por meio de documentação oficial do fabricante, do atendimento às especificações mínimas dos produtos dos itens 3.22.1, 3.22.2 e 3.22.3 e ser apresentada conforme modelo do **"ANEXO – MODELO DE COMPROVAÇÃO DE ATENDIMENTO ÀS ESPECIFICAÇÕES TÉCNICAS" (deverá ser inserido no sistema juntamente com a proposta de preços)**, indicando a documentação técnica oficial do fabricante que embase tal cumprimento e, inclusive, com a indicação da evidência de cada item na documentação técnica conforme exemplo ilustrado a seguir:

Item	Descrição do item	Documento técnico	Referência na documentação técnica
x.xx.x	Descrição do item	Manual, folder, link do site do fabricante etc.	Indicação da evidência na documentação técnica

4.2. Em caso de não comprovação do "ANEXO IV – MODELO DE COMPROVAÇÃO DE ATENDIMENTO ÀS ESPECIFICAÇÕES TÉCNICAS" ou não comprovação dos itens, a empresa será desclassificada.

4.3. Poderão ser realizadas diligências perante as pessoas jurídicas indicadas nos Atestados de Capacidade Técnica e juntamente ao fabricante dos equipamentos ofertados, visando à confirmação das informações prestadas.

5. DAS QUANTIDADES

5.1. Os itens que compõem o lote único bem como suas quantidades são os seguintes:

Item		Produto	Quantidades
Equipamentos e licenças	1	Firewall de Próxima Geração (Next Generation Firewall – NGFW) do tipo *appliance* com sistema de gestão integrado em formato GUI (gráfico) do próprio fabricante, suporte técnico e garantia de 60 meses	2

	2	Ferramenta de visibilidade, análise e segurança de Endpoints para conexão remota e segura Zero Trust Network Agent, padrão web, autenticação multifator (MFA), integração com Active Directory (AD) e hospedagem em nuvem	200 usuários
	3	Sistema de Gerenciamento de logs, análise e plataforma de relatórios	1
Serviço de instalação	4	Serviço de instalação, configuração, atualização e treinamento de pessoal	1
Suporte técnico	5	Suporte técnico mensal durante a vigência contratual (60 meses)	1

6. DO LOCAL DE ENTREGA DOS EQUIPAMENTOS E PRESTAÇÃO DO SERVIÇO

6.1. Os produtos serão entregues no estabelecimento do Badesul, na Rua Gen. Andrade Neves Nº 175 – Centro - Porto Alegre/RS. CEP 90.010-210.

6.2. O serviço será prestado de forma remota, ressalvados os casos em que for necessária a presença eventual da contratada na sede do Badesul, o que ocorrerá de forma excepcional e mediante prévia justificativa da área técnica.

7. DO PREÇO

7.1. O preço referente à execução dos serviços contratados, serão os seguintes:

Item		Produto	Valor Unitário
Equipamentos e licenças	1	Firewall de Próxima Geração (Next Generation Firewall – NGFW) do tipo *appliance* com sistema de gestão integrado em formato GUI (gráfico) do próprio fabricante, suporte técnico e garantia de 60 meses	
	2	Ferramenta de visibilidade, análise e segurança de Endpoints para conexão remota e segura Zero Trust Network Agent, padrão web, autenticação multifator (MFA), integração com Active Directory (AD) e hospedagem em nuvem	
	3	Sistema de Gerenciamento de logs, análise e plataforma de relatórios	

Serviço de instalação	4	Serviço de instalação, configuração, atualização e treinamento de pessoal	
Suporte técnico	5	Suporte técnico mensal, durante a vigência contratual (60 meses)	

7.2. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação. Não será admitido aditivo contratual em função de variação cambial.

8. DO VALOR MÁXIMO ACEITÁVEL

8.1. Após a sessão de lances serão desclassificadas as propostas que apresentarem valor global superiora a R$ 425.366,10 (quatrocentos e vinte e cinco mil trezentos e sessenta e seis reais e dez centavos), composto por:

item	Tipo de Serviço	Tipo de Formato da Contração	Quantidade Estimada	Valor unitário	Valor total
1	Aquisição de equipamento	UNIDADE	2	R$ 112.125,00	R$ 224.250,00
2	Aquisição de licença	UNIDADE	200 usuários	R$ 332,00	R$ 66.400,00
3	Aquisição de licença	UNIDADE	1	R$ 46.216,10	R$ 46.216,10
4	Serviço de instalação	UNIDADE	1	R$ 30.000,00	R$ 30.000,00
5	Serviço de Suporte Técnico	MENSALIDADE	60	R$ 975,00	R$ 58.500,00
TOTAL					**R$ 425.366,10**

8.2. O valor para o Item 1 deverá perfazer em torno de 52,72% do total, admitindo-se o ajuste tanto dos percentuais como do valor unitário para fins de cálculo do valor global.

8.3. O valor para o Item 2 deverá perfazer em torno de 15,61% do total, admitindo o ajuste tanto dos percentuais como do valor unitário para fins de cálculo do valor global.

8.4. O valor para o Item 3 deverá perfazer em torno de 10,87% do total, admitindo o ajuste tanto dos percentuais como do valor unitário para fins de cálculo do valor global.

8.5. O valor para o serviço do Item 4 deverá perfazer em torno de 7,05%

do total, admitindo o ajuste tanto dos percentuais como do valor unitário para fins de cálculo do valor global.

8.6. O valor para o serviço do Item 5 deverá perfazer em torno de 13,75% do total, admitindo o ajuste tanto dos percentuais como do valor unitário para fins de cálculo do valor global.

8.7. Para fins de contratação, depois de apurado o valor global, serão calculados os valores individuais dos itens, os quais deverão corresponder às proporções acima definidas, sobre o valor total global, dividindo-se pelas quantidades para se obter o valor unitário.

9. DA VALIDADE DA PROPOSTA:

9.1. O prazo de validade da proposta será de no mínimo 60 dias, a contar da data de abertura das propostas.

PREGÃO ELETRÔNICO N.º 0017/2022

Processo nº 22/4000-0000309-9

ANEXO II

PROPOSTA DE PREÇOS

Senhores:

Apresentamos nossa proposta para fornecimento do objeto do presente Pregão, acatando todas as características e exigências constantes no edital e conforme abaixo.

Empresa:				
CNPJ/MF:				
Endereço:				
Contato:			**Telefones:**	
E-mail:			**Fax:**	
Nome de quem assina o contrato:				
RG:	**Órgão Expedidor:**		**Cargo na Empresa:**	
Estado Civil			**Profissão**	

ITEM	QUANTIDADE	MODELO	VALOR UNITÁRIO	VALOR TOTAL
1				
2				
3				
4				
5				
Valor Global			**R$**	

Proposta válida até: _____

..... de ..... de 2022.

_____

Assinatura do dirigente da empresa

Nome do dirigente da empresa

PREGÃO ELETRÔNICO N.º 0017/2022

Processo nº 22/4000-0000309-9

ANEXO III

PLANILHA[1] DE CUSTOS

QUADRO RESUMO DO CONTRATO			
Item	**Valor unitário do item**	**Quantidade**	**Valor total**
1			R$
2			
3			
4			
5			
Valor Global do Contrato	R$		

.	**Nº Processo**	
	Licitação Nº	

- Dia_ /_ /_ às_ :_ horas

I	Mobilização (4)[4]	%	Valor (R$)
A			
B			

- **Custo por Unidade de medida – tipos e quantidades**

I	Tributos (especificar)	%	Valor Mensal
A			
B			
C			

[1] *Nota (1): Esta planilha poderá ser adaptada às características do serviço contratado, a serem estabelecidas no Termo de Referência.*

PREGÃO ELETRÔNICO N.º 0017/2022

Processo nº 22/4000-0000309-9

ANEXO IV

MODELO DE COMPROVAÇÃO DE ATENDIMENTO ÀS ESPECIFICAÇÕES TÉCNICAS
(deverá ser inserido no sistema juntamente com a proposta de preços)

ANEXO IV - MODELO DE COMPROVAÇÃO DE ATENDIMENTO ÀS ESPECIFICAÇÕES TÉCNICAS			
Item	**Descrição do item**	**Documento técnico**	**Referência na documentação técnica**
3.22.1.1.	Características do Equipamento:		
3.22.1.1.1.	Deve suportar, no mínimo, 20 Gbps com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6;		
3.22.1.1.2.	Deve suportar, no mínimo, 2.6 Gbps de throughput IPS;		
3.22.1.1.3.	Deve suportar, no mínimo, 11.5 Gbps de throughput de VPN IPSec;		
3.22.1.1.4.	Deve suportar, no mínimo, 1 Gbps de throughput de VPN SSL;		
3.22.1.1.5.	Deve suportar, no mínimo, 1 Gbps de throughput de Inspeção SSL;		
3.22.1.1.6.	Deve suportar, no mínimo, 2.2 Gbps de throughput de Controle de Aplicação;		
3.22.1.1.7.	Deve suportar, no mínimo, 1 Gbps de throughput com as seguintes funcionalidades habilitadas simultaneamente, para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: firewall, controle de aplicação, IPS e antimalware;		
3.22.1.1.8.	Suporte a, no mínimo, 1.5 Milhões de conexões simultâneas;		
3.22.1.1.9.	Suporte a, no mínimo, 56.000 novas conexões por segundo;		
3.22.1.1.10.	Estar licenciado para, ou suportar sem o uso de licença, 2.000 túneis de VPN IPSEC Site-to-Site simultâneos;		

3.22.1.1.11.	Estar licenciado para, ou suportar sem o uso de licença, 16.000 túneis de clientes VPN IPSEC simultâneos;		
3.22.1.1.12.	Estar licenciado para, ou suportar sem o uso de licença, 500 clientes de VPN SSL simultâneos;		
3.22.1.1.13.	Possuir ao menos 12 interfaces 1Gbps RJ45;		
3.22.1.1.14.	Possuir ao menos 4 interfaces 1Gbps SFP;		
3.22.1.1.15.	Possuir ao menos 1 interface 1Gbps RJ45 dedicada à gerenciamento;		
3.22.1.1.16.	Possuir ao menos 1 interface serial de console;		
3.22.1.1.17.	Possuir ao menos 2 interfaces 1Gbps RJ45 dedicadas à HA (Alta Disponibilidade);		
3.22.1.1.18.	Possuir ao menos 1 interface 1Gbps RJ45 dedicada à DMZ;		
3.22.1.1.19.	Possuir ao menos 2 interfaces 10Gbps SFP+;		
3.22.1.1.20.	Estar licenciado e ter incluso sem custo adicional, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance;		
3.22.1.1.21.	Possuir fonte de alimentação 100-240V AC redundante interna;		
3.22.1.1.22.	Possuir no máximo 1 RU de altura;		
3.22.1.1.23.	Deve possuir suporte a 4094 VLAN Tags 802.1q;		
3.22.1.1.24.	Deve possuir suporte a agregação de links 802.3ad e LACP;		
3.22.1.1.25.	Deve possuir suporte a Policy based routing ou policy based forwarding;		
3.22.1.1.26.	Deve possuir suporte a roteamento multicast (PIM-SM e PIM-DM);		
3.22.1.1.27.	Deve possuir suporte a DHCP Relay;		
3.22.1.1.28.	Deve possuir suporte a DHCP Server;		
3.22.1.1.29.	Deve suportar sFlow;		
3.22.1.1.30.	Deve possuir suporte a Jumbo Frames;		
3.22.1.1.31.	Deve suportar sub-interfaces ethernet logicas;		
3.22.1.1.32.	Deve suportar NAT dinâmico e estático;		
3.22.1.1.33.	Deve suportar Tradução de porta (PAT);		
3.22.1.1.34.	Deve suportar NAT de Origem, NAT de Destino e NAT de forma simultânea;		
3.22.1.1.35.	Deve poder combinar NAT de origem e NAT de destino na mesma politica		
3.22.1.1.36.	Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;		
3.22.1.1.37.	Deve suportar NAT64 e NAT46;		
3.22.1.1.38.	Deve implementar o protocolo ECMP;		

3.22.1.1.39.	Deve permitir monitorar via SNMP falhas de hardware, uso de recursos por número elevado de sessões, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;		
3.22.1.1.40.	Enviar log para sistemas de monitoração externos, simultaneamente;		
3.22.1.1.41.	Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;		
3.22.1.1.42.	Deve possuir suporte ao protocolo de criptografia TLS (Transport Layer Security) na versão 1.3		
3.22.1.1.43.	Proteção anti-spoofing;		
3.22.1.1.44.	Suportar otimização do tráfego entre dois equipamentos;		
3.22.1.1.45.	Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);		
3.22.1.1.46.	Para IPv6, deve suportar roteamento estático e dinâmico (RIPng, OSPFv3, BGP4+);		
3.22.1.1.47.	Suportar OSPF graceful restart;		
3.22.1.1.48.	Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;		
3.22.1.1.49.	Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;		
3.22.1.1.50.	Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;		
3.22.1.1.51.	Deve suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;		
3.22.1.1.52.	Suporte a configuração de alta disponibilidade Ativo/Ativo: Em modo transparente;		
3.22.1.1.53.	Suporte a configuração de alta disponibilidade Ativo/Ativo: Em layer 3;		
3.22.1.1.54.	Suporte a configuração de alta disponibilidade Ativo/Ativo: Em layer 3 e com no mínimo 2 equipamentos no cluster;		
3.22.1.1.55.	A configuração em alta disponibilidade deve sincronizar: Sessões;		
3.22.1.1.56.	A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede;		
3.22.1.1.57.	A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs;		
3.22.1.1.58.	A configuração em alta disponibilidade deve sincronizar Tabelas FIB;		
3.22.1.1.59.	O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;		

3.22.1.1.60.	Deve possuir suporte a criação de sistemas virtuais no mesmo appliance;		
3.22.1.1.61.	Em alta disponibilidade, deve ser possível o uso de clusters virtuais, seja ativo-ativo permitindo a distribuição de carga entre diferentes contextos;		
3.22.1.1.62.	O módulo de gerência deve ser capaz de gerenciar e administrar a solução descrita neste termo;		
3.22.1.1.63.	O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança;		
3.22.1.1.64.	Centralizar a administração de regras e políticas dos equipamentos de proteção de rede, usando uma única interface de gerenciamento;		
3.22.1.1.65.	Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas;		
3.22.1.1.66.	O gerenciamento da solução deve suportar acesso via SSH e interface WEB (HTTPS), incluindo, mas não limitado à exportar configuração dos sistemas virtuais (contextos) por ambas interfaces;		
3.22.1.1.67.	O gerenciamento deve permitir/possuir monitoração de logs, ferramentas de investigação de logs e acesso concorrente de administradores;		
3.22.1.1.68.	Deve possuir um mecanismo de busca por comandos ou auto-complete no gerenciamento via SSH, de forma a facilitar a configuração pelo administrador;		
3.22.1.1.69.	Deve suportar a criação de regras que fiquem ativas em horário definido e suportar criação de regras com data de expiração;		
3.22.1.1.70.	Deve suportar backup das configurações e rollback de configuração para a última configuração salva;		
3.22.1.1.71.	Deve suportar a validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras (shadowing);		
3.22.1.1.72.	Deve permitir a visualização dos logs de uma regra especial em tempo real;		
3.22.1.1.73.	Deve possibilitar a integração com outras soluções de SIEM de mercado;		
3.22.1.1.74.	Deve suportar geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;		
3.22.1.1.75.	Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-Malware), etc;		

3.22.1.1.76.	Deve prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus, Anti-Malware), e URLs que passam pela solução;		
3.22.1.1.77.	Deve ser possível exportar os logs em CSV ou outro formato de texto estruturado;		
3.22.1.1.78.	Deve possibilitar a geração ou exportação de relatórios de eventos no formato PDF;		
3.22.1.1.79.	Deve possibilitar rotação do log;		
3.22.1.1.80.	Deve ter capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura;		
3.22.1.1.81.	Deve permitir a criação de filtros com base em qualquer característica do evento, tais como a origem e o IP destino, serviço, tipo de evento, severidade do evento, nome do ataque, o país de origem e destino, etc;		
3.22.1.1.82.	Deve permitir a integração com servidores de autenticação LDAP Microsoft Active Directory e Radius;		
3.22.1.1.83.	Deve permitir a visualização de gráficos e mapa de ameaças;		
3.22.1.1.84.	Deve possuir mecanismo para que logs antigos sejam removidos automaticamente;		
3.22.1.1.85.	Deve permitir a criação de dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino;		
3.22.1.1.86.	Deve possuir a capacidade de visualizar na interface gráfica da solução, informações do sistema como licenças, memória, disco e uso de CPU;		
3.22.1.1.87.	A solução deve possuir painéis de eventos em tempo real com possibilidade de configuração das atualizações e frequências;		
3.22.1.1.88.	Deve possuir controle, inspeção e descriptografia de SSL para tráfego de entrada (Inbound) e Saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);		
3.22.1.1.89.	A solução deve identificar potenciais vulnerabilidades e destacar as melhores práticas que poderiam ser usadas para melhorar a segurança e o desempenho geral de uma rede;		
3.22.1.1.90.	O console de administração deve suportar pelo menos inglês, espanhol e português.		
3.22.1.1.91.	O console deve suportar o gerenciamento de switches e pontos de acesso wireless para melhorar o nível de segurança		

3.22.1.1.92.	A solução deve oferecer suporte à integração nativa de equipamentos de proteção de email, firewall de aplicativos, proxy, cache e ameaças avançadas.		
3.22.1.1.93.	Deverá ser comprovado que a solução ofertada foi aprovada no conjunto de critérios de avaliação contido nos testes da NSS Labs, da ICSA Labs, ou por meio de certificação similar, que cumpra a mesma finalidade ou que ateste as mesmas funcionalidades.		
3.22.1.2.	Controle por Política de Firewall:		
3.22.1.2.1.	Deverá suportar controles por zona de segurança;		
3.22.1.2.2.	Controles de políticas por porta e protocolo;		
3.22.1.2.3.	Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;		
3.22.1.2.4.	Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;		
3.22.1.2.5.	Firewall deve ser capaz de aplicar a inspeção UTM (Application Control e Webfiltering no mínimo) diretamente às políticas de segurança versus via perfis;		
3.22.1.2.6.	Além dos endereços e serviços de destino, objetos de serviços de Internet devem poder ser adicionados diretamente às políticas de firewall;		
3.22.1.2.7.	Ele deve suportar a automação de situações como detecção de equipamentos comprometidos, status do sistema, alterações de configuração, eventos específicos e aplicar uma ação que pode ser notificação, bloqueio de um computador, execução de scripts ou funções em nuvem pública.		
3.22.1.2.8.	Deve suportar o padrão de indústria 'syslog' protocol para armazenamento usando o formato Common Event Format (CEF);		
3.22.1.2.9.	Deve haver uma maneira de assegurar que o armazenamento dos logs em tempo real não superam a velocidade de upload;		
3.22.1.2.10.	Deve suportar o protocolo padrão da indústria VXLAN;		
3.22.1.2.11.	Deve suportar objetos de endereço IPv4 e IPv6, consolidados na mesma regra/política de firewall		
3.22.1.2.12.	Deve possuir base com objetos de endereço IP, de serviços da internet como Google e Office 365, atualizados dinamicamente pela solução;		

3.22.1.2.13.	**A solução deve oferecer suporte à integração nativa com a solução de sandbox, proteção de e-mail, cache e firewall de aplicativos da Web;**		
3.22.1.3.	Controle de Aplicações:		
3.22.1.3.1.	Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;		
3.22.1.3.2.	Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado a: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;		
3.22.1.3.3.	Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;		
3.22.1.3.4.	Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;		
3.22.1.3.5.	Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;		
3.22.1.3.6.	Identificar o uso de táticas evasivas via comunicações criptografadas;		
3.22.1.3.7.	Atualizar a base de assinaturas de aplicações automaticamente;		
3.22.1.3.8.	Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos;		
3.22.1.3.9.	Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;		
3.22.1.3.10.	Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;		
3.22.1.3.11.	O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;		

3.22.1.3.12.	Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;		
3.22.1.3.13.	Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;		
3.22.1.3.14.	Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo;		
3.22.1.3.15.	Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;		
3.22.1.3.16.	Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);		
3.22.1.3.17.	Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação;		
3.22.1.3.18.	Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;		
3.22.1.3.19.	Deve ser possível configurar Application Override permitindo selecionar aplicações individualmente;		
3.22.1.4.	Prevenção de Ameaças:		
3.22.1.4.1.	Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;		
3.22.1.4.2.	Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);		
3.22.1.4.3.	As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;		
3.22.1.4.4.	Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;		
3.22.1.4.5.	Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes politicas por zona de segurança, endereço		

	de origem, endereço de destino, serviço e a combinação de todos esses itens;		
3.22.1.4.6.	Deve permitir o bloqueio de vulnerabilidades;		
3.22.1.4.7.	Deve incluir proteção contra ataques de negação de serviços;		
3.22.1.4.8.	Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise de decodificação de protocolo;		
3.22.1.4.9.	Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise para detecção de anomalias de protocolo;		
3.22.1.4.10.	Deverá possuir o seguinte mecanismos de inspeção de IPS: IP Defragmentation;		
3.22.1.4.11.	Deverá possuir o seguinte mecanismos de inspeção de IPS: Remontagem de pacotes de TCP;		
3.22.1.4.12.	Deverá possuir o seguinte mecanismos de inspeção de IPS: Bloqueio de pacotes malformados;		
3.22.1.4.13.	Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;		
3.22.1.4.14.	Detectar e bloquear a origem de portscans;		
3.22.1.4.15.	Bloquear ataques efetuados por worms conhecidos;		
3.22.1.4.16.	Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;		
3.22.1.4.17.	Possuir assinaturas para bloqueio de ataques de buffer overflow;		
3.22.1.4.18.	Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;		
3.22.1.4.19.	Identificar e bloquear comunicação com botnets;		
3.22.1.4.20.	Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;		
3.22.1.4.21.	Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;		
3.22.1.4.22.	Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;		
3.22.1.4.23.	Os eventos devem identificar o país de onde partiu a ameaça;		
3.22.1.4.24.	Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;		

3.22.1.4.25.	Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;		
3.22.1.4.26.	Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança;		
3.22.1.4.27.	Suportar e estar licenciado com proteção contra ataques de dia zero por meio de integração com solução de Sandbox em nuvem, do mesmo fabricante;		
3.22.1.5.	Filtro de URL:		
3.22.1.5.1.	Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);		
3.22.1.5.2.	Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local, em modo de proxy transparente e explícito;		
3.22.1.5.3.	Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;		
3.22.1.5.4.	Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;		
3.22.1.5.5.	Possuir pelo menos 60 categorias de URLs;		
3.22.1.5.6.	Deve possuir a função de exclusão de URLs do bloqueio, por categoria;		
3.22.1.5.7.	Permitir a customização de página de bloqueio;		
3.22.1.5.8.	Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site);		
3.22.1.5.9.	Além do Explicit Web Proxy, suportar proxy Web transparente;		
3.22.1.6.	Identificação de Usuários:		
3.22.1.6.1.	Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;		

3.22.1.6.3.	Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso como, mas não limitado à utilização de sistemas virtuais, segmentos de rede, etc;		
3.22.1.6.4.	Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;		
3.22.1.6.5.	Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;		
3.22.1.6.6.	Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);		
3.22.1.6.7.	Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;		
3.22.1.6.8.	Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;		
3.22.1.6.9.	Permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso a internet e gerenciamento da solução;		
3.22.1.6.10.	Prover no mínimo um token nativamente, possibilitando autenticação de duplo fator;		
3.22.1.7.	QoS e Traffic Shaping:		
3.22.1.7.1.	Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube, Ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máxima largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;		
3.22.1.7.2.	Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;		

3.22.1.7.3.	Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;		
3.22.1.7.4.	Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo;		
3.22.1.7.5.	Suportar a criação de políticas de QoS e Traffic Shaping por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;		
3.22.1.7.6.	Suportar a criação de políticas de QoS e Traffic Shaping por porta;		
3.22.1.7.7.	O QoS deve possibilitar a definição de tráfego com banda garantida;		
3.22.1.7.8.	O QoS deve possibilitar a definição de tráfego com banda máxima;		
3.22.1.7.9.	O QoS deve possibilitar a definição de fila de prioridade;		
3.22.1.7.10.	Suportar marcação de pacotes Diffserv, inclusive por aplicação;		
3.22.1.7.11.	Suportar modificação de valores DSCP para o Diffserv;		
3.22.1.7.12.	Suportar priorização de tráfego usando informação de Type of Service;		
3.22.1.7.13.	Deve suportar QOS (traffic-shapping), em interface agregadas ou redundantes;		
3.22.1.8.	Filtro de dados:		
3.22.1.8.1.	Permitir a criação de filtros para arquivos e dados pré-definidos;		
3.22.1.8.2.	Os arquivos devem ser identificados por extensão e tipo;		
3.22.1.8.3.	Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);		
3.22.1.8.4.	Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;		
3.22.1.8.5.	Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;		
3.22.1.8.6.	Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;		
3.22.1.9.	Geo localização:		
3.22.1.9.1.	Suportar a criação de políticas por geo-localização, permitindo o tráfego de determinado Pais/Países sejam bloqueados;		
3.22.1.9.2.	Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;		

3.22.1.9.3.	Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas;		
3.22.1.10.	VPN:		
3.22.1.10.1.	Suportar VPN Site-to-Site e Cliente-To-Site;		
3.22.1.10.2.	Suportar IPSec VPN;		
3.22.1.10.3.	Suportar SSL VPN;		
3.22.1.10.4.	A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;		
3.22.1.10.5.	A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;		
3.22.1.10.6.	A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);		
3.22.1.10.7.	A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);		
3.22.1.10.9.	Suportar VPN em em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;		
3.22.1.10.10.	Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting;		
3.22.1.10.11.	Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;		
3.22.1.10.12.	Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;		
3.22.1.10.13.	Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;		
3.22.1.10.14.	Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;		
3.22.1.10.15.	Deverá manter uma conexão segura com o portal durante a sessão;		
3.22.1.10.16.	O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior);		
3.22.1.10.17.	Deve suportar Auto-Discovery Virtual Private Network (ADVPN)		
3.22.1.10.18.	Deve suportar agregação de túneis IPSec		
3.22.1.10.19.	Deve suportar algoritmo de balanceamento do tipo WRR (Weighted Round Robin) em agregação de túneis IPSec		
3.22.1.10.20.	A VPN IPSec deve suportar Forward Error Correction (FEC)		
3.22.1.10.21.	Deve suportar TLS 1.3 em VPN SSL;		
3.22.1.11.	SD-WAN:		

3.22.1.11.1.	Deve implementar balanceamento de link por hash do IP de origem;		
3.22.1.11.2.	Deve implementar balanceamento de link por hash do IP de origem e destino;		
3.22.1.11.3.	Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links.		
3.22.1.11.4.	Deve implementar balanceamento de link por custo configurado do link.		
3.22.1.11.5.	Deve suportar o balanceamento de, no mínimo, 256 links;		
3.22.1.11.6.	Deve suportar o balanceamento de links de interfaces físicas, sub-interfaces lógicas de VLAN e túneis IPSec		
3.22.1.11.7.	Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;		
3.22.1.11.8.	Deve gerar log de eventos que registrem alterações no estado dos links do SDWAN, monitorados pela checagem de saúde		
3.22.1.11.9.	Deve suportar Zero-Touch Provisioning		
3.22.1.11.10.	Possuir checagem do estado de saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Perda de Pacotes		
3.22.1.11.11.	Deve ser possível configurar a porcentagem de perda de pacotes e o tempo de latência e jitter, na medição de estado de link. Estes valores serão utilizados pela solução para decidir qual link será utilizado		
3.22.1.11.12.	A solução deve permitir modificar o intervalo de tempo de checagem, em segundos, para cada um dos links.		
3.22.1.11.13.	A checagem de estado de saúde deve suportar teste com Ping, HTTP e DNS		
3.22.1.11.14.	Suportar UDP Hole Punching em arquitetura ADVPN		
3.22.1.11.15.	A checagem de estado de saúde deve suportar a marcação de pacotes com DSCP, para avaliação mais precisa de links que possuem QoE configurado		
3.22.1.11.16.	As regras de escolha do link SD-WAN devem suportar o reconhecimento de aplicações, grupos de usuários, endereço IP de destino e Protocolo.		
3.22.1.11.17.	Deve suportar a configuração de nível mínimo de qualidade (latência, jitter e perda de pacotes) para que determinado link seja escolhido pelo SD-WAN		
3.22.1.11.18.	Deve suportar envio de BGP route-map para BGP neighbors, caso a qualidade mínima de um link não seja detectada pela checagem de saúde do link.		
3.22.2.	Item 2: Ferramenta de gerenciamento da solução de Next-Generation Endpoint;		

3.22.2.1.	Características da Ferramenta:		
3.22.2.1.1.	Possuir gerenciamento centralizado do software cliente de segurança, a partir de um console central, do próprio fabricante;		
3.22.2.1.2.	O licenciamento deve se basear no número de clientes de segurança registrados no gerenciamento centralizado, do mesmo fabricante;		
3.22.2.1.3.	O software cliente de segurança deve ser compatível com pelos menos os seguintes sistemas operacionais:		
3.22.2.1.3.1.	Microsoft Windows: 7 (32 e 64 bits), 8 (32 e 64 bits), 8,1 (32 e 64 bits) e 10 (32 e 64 bits);		
3.22.2.1.3.2.	Microsoft Windows Server 2012 ou superior;		
3.22.2.1.3.3.	macOS 11+, 10.15, 10.14;		
3.22.2.1.3.4.	iOS 9.0 ou superior;		
3.22.2.1.3.5.	Android 5.0 ou superior;		
3.22.2.1.3.6.	Linux Ubuntu 16.04 ou superior;		
3.22.2.1.3.7.	Linux Red Hat 7.4 ou superior;		
3.22.2.1.3.8.	Linux CentOS 7.4 ou superior com KDE ou GNOME;		
3.22.2.1.4.	O software de gerenciamento centralizado deve suportar a instalação no Microsoft Windows Server 2012 ou superior;		
3.22.2.1.5.	Deve ter uma interface gráfica do usuário, pelo menos nos idiomas inglês, português e espanhol;		
3.22.2.1.6.	Deve permitir o backup do arquivo de configuração;		
3.22.2.1.7.	O cliente de segurança deverá enviar os logs para o servidor de gerenciamento central;		
3.22.2.1.8.	O cliente de segurança deve permitir a configuração local via XML (eXtensible Markup Language);		
3.22.2.1.9.	Deve controlar o acesso a dispositivos removíveis e ser capaz de monitorar, permitir e negar acesso a dispositivos USB, de acordo com as seguintes características do dispositivo:		
3.22.2.1.9.1.	Device Class;		
3.22.2.1.9.2.	Manufacturer;		
3.22.2.1.9.3.	Vendor ID;		
3.22.2.1.9.4.	Product ID;		
3.22.2.1.9.5.	Revision;		
3.22.2.1.10.	Deve poder definir o nível do log em: emergency, alert, critical, error, warning, notice, information, debug;		
3.22.2.1.11.	Deve ter a capacidade de desabilitar os serviços de proxy para fins de solução de problemas;		

3.22.2.1.12.	Deve ser capaz de ativar seletivamente logs, de acordo com as funcionalidades licenciadas para a plataforma: Antivírus, Firewall de Aplicação, Telemetria, Agente de Logon Único (Single Sign One), Proxy, IPSec VPN, AntiExploit, SSL VPN, Atualizações, Vulnerabilidades, Filtro Web e Sandbox;		
3.22.2.1.13.	Deve suportar exportar logs diretamente do cliente de segurança;		
3.22.2.1.14.	Deve ter interface gráfica de gerenciamento via web (HTTPS);		
3.22.2.1.15.	Deve permitir a criação de usuários de diferentes perfis administrativos;		
3.22.2.1.16.	Deve permitir importar informações do Microsoft Active Directory usando LDAP;		
3.22.2.1.17.	Deve permitir o registro manual da estação através do uso de uma senha;		
3.22.2.1.18.	Deve permitir a criação de grupos de clientes para facilitar o gerenciamento;		
3.22.2.1.19.	Deve ser capaz de enviar logs para uma plataforma de log do mesmo fabricante;		
3.22.2.1.20.	Dever permitir a instalação do certificado digital no cliente;		
3.22.2.1.21.	Deve conter informações sobre o sistema operacional no qual o cliente está instalado;		
3.22.2.1.22.	Deve informar o perfil de segurança criado e/ou aplicado;		
3.22.2.1.23.	Deve permitir a implantação automática de clientes de terminal de acordo com a OU do MS AD;		
3.22.2.1.24.	Deve permitir a manutenção de várias instâncias de instaladores com recursos diferentes (AV, VPN, WF, etc.) e arquiteturas (x86, x64, etc.);		
3.22.2.1.25.	Deve permitir a implantação de equipamentos que NÃO pertencem ao active directory (AD);		
3.22.2.1.26.	Deve ter um painel em que possa verificar rapidamente o status de integridade dos clientes;		
3.22.2.1.27.	Os usuários administradores devem poder sincronizar com o AD, para permitir o login com as mesmas credenciais;		
3.22.2.1.28.	Deve ser capaz de definir funções administrativas;		
3.22.2.1.29.	Deve suportar fazer backup / restaurar configurações do console, configuração do servidor, políticas de terminal etc.;		
3.22.2.1.30.	O fabricante deve fornecer um portal para baixar o instalador do cliente de segurança e permitir a instalação local;		
3.22.2.1.31.	O console de gerenciamento central deve poder instalar o cliente de segurança nos computadores Windows associados a um domínio da Microsoft;		

3.22.2.1.32.	Deve fornecer informações da estação de trabalho, no mínimo e não se limitando a: Nome completo, Telefone, E-mail, Informações pessoais obtidas minimamente de (entrada manual, linkedin, google, Sistema operacional e/ou Salesforce), status do cliente, Nome do host, etiqueta de host;		
3.22.2.1.33.	Deve suportar upload de uma foto ou avatar para identificação rápida do usuário;		
3.22.2.1.34.	Deve relatar rapidamente o nível de vulnerabilidade da estação de trabalho;		
3.22.2.1.35.	Deve ter um sistema de notificação pop-up;		
3.22.2.1.36.	Deve ter uma lista de notificações atuais e anteriores;		
3.22.2.1.37.	Deve fornecer informações sobre a vulnerabilidade, patches, versões afetadas etc., bem como o CVE correspondente;		
3.22.2.2.	Funcionalidades de VPN		
3.22.2.2.1.	Deve permitir split-tunnel para VPN IPSec e SSL		
3.22.2.2.2.	Na VPN split-tunneling, deve permitir configurar exceções baseadas no reconhecimento de aplicações locais, podendo especificar o nome do processo, caminho completo e diretório onde está instalado localmente, para não serem direcionadas ao túnel VPN.		
3.22.2.2.3.	Na VPN split-tunneling, deve permitir configurar exceções baseadas em domínio, para não serem direcionadas ao túnel VPN		
3.22.2.2.4.	Deve permitir selecionar de forma automática o gateway remoto mais próximo para conexão VPN, baseado em:		
3.22.2.2.4.1.	Tempo de resposta de ping		
3.22.2.2.4.2.	TCP Round Trip Time (TCP Three-Way Handshare SYN, SYN-ACK, ACK)		
3.22.2.2.5.	Deve permitir conectar automaticamente à um túnel SSL VPN backup quando um túnel IPSec VPN falhar.		
3.22.2.2.6.	Deve permitir associar tags à um usuário remoto de VPN, de acordo com as regras de conformidade		
3.22.2.2.7.	Deve permitir bloquear acesso à determinadas VPN's de usuário, baseado nas tags associadas ao usuário.		
3.22.2.2.8.	Deve permitir criar regras para associação de tags, de acordo com os seguintes parâmetros:		
3.22.2.2.8.1.	Grupo Active Directory		
3.22.2.2.8.2.	Existência de Antivírus instalado		
3.22.2.2.8.3.	Existência de Antivírus atualizado		
3.22.2.2.8.4.	Certificado		
3.22.2.2.8.5.	Cliente de Segurança Gerenciado Centralmente		

3.22.2.2.8.6.	Existência de Arquivo em determinado diretório do cliente		
3.22.2.2.8.7.	Domínio logado		
3.22.2.2.8.8.	Versão de Sistema Operacional		
3.22.2.2.8.9.	Chave de Registro do Windows		
3.22.2.2.8.10.	Processo em execução		
3.22.2.2.8.11.	Malware detectado pelo Sandbox nos últimos 7 dias		
3.22.2.2.8.12.	Nível de Vulnerabilidade do dispositivo		
3.22.2.2.8.13.	Windows Security, sendo a checagem das seguintes aplicações, se estão habilitadas:		
3.22.2.2.8.13.1.	Windows Defender		
3.22.2.2.8.13.2.	Bitlocker Disk Encryption		
3.22.2.2.8.13.3.	Exploit Guard		
3.22.2.2.8.13.4.	Application Guard		
3.22.2.2.8.13.5.	Windows Firewall		
3.22.2.2.9.	Deve permitir que o usuário configure VPNs localmente		
3.22.2.2.10.	Deve permitir que o usuário desconecte uma VPN		
3.22.2.2.11.	Deve permitir a conexão VPN antes do login		
3.22.2.2.12.	Deve permitir conexão VPN automática		
3.22.2.2.13.	Deve suportar a configuração de senha para o usuário acessar a configuração do cliente		
3.22.2.2.14.	Deve permitir a autenticação de dois fatores fornecida pelo mesmo fabricante		
3.22.2.2.15.	IPSEC:		
3.22.2.2.15.1.	Deve permitir que o usuário crie novas VPNs IPSEC		
3.22.2.2.15.2.	Deve permitir que várias VPNs IPSEC sejam definidas simultaneamente		
3.22.2.2.15.3.	Deve permitir a autenticação usando nome de usuário e senha		
3.22.2.2.15.4.	Deve permitir a autenticação usando certificados digitais		
3.22.2.2.15.5.	Deve permitir a seleção dos modos Principal e Agressivo;		
3.22.2.2.15.6.	Deve permitir a configuração do DHCP por IPSec;		
3.22.2.2.15.7.	Deve permitir o uso do NAT Traversal;		
3.22.2.2.15.8.	Deve permitir a escolha de grupos Diffie-Hellman (1,2,5 e 14);		
3.22.2.2.15.9.	Deve permitir configurações de expiração de chave IKE;		
3.22.2.2.15.10.	Deve suportar IKEv1 e IKEv2		
3.22.2.2.15.11.	Deve permitir o uso do Perfect Forward Secrecy;		
3.22.2.2.15.12.	Deve suportar o uso de certificados para autenticação na VPN IPSec		
3.22.2.2.15.13.	Deve suportar usuário e senha para autenticação VPN IPSec		

3.22.2.2.15.14.	Deve suportar o uso de certificados em cartão inteligente para autenticação na VPN IPSec		
3.22.2.2.15.15.	Deve suportar o bloqueio de tráfego IPv6 na VPN IPsec		
3.22.2.2.16.	SSL:		
3.22.2.2.16.1.	Deve permitir que o usuário crie novas VPNs SSL		
3.22.2.2.16.2.	Deve permitir que várias VPNs SSL sejam definidas simultaneamente		
3.22.2.2.16.3.	Deve permitir a personalização da porta TCP na qual a VPN SSL funciona		
3.22.2.2.16.4.	Deve permitir a autenticação usando nome de usuário e senha		
3.22.2.2.16.5.	Deve permitir a autenticação usando certificados digitais		
3.22.2.2.16.6.	Para uso específico de VPN SSL (pelo menos):		
3.22.2.2.16.6.1.	Especificação IP do concentrador		
3.22.2.2.16.6.2.	Especificação da porta do hub		
3.22.2.2.16.7.	Deve permitir autenticação SAML SSO para VPN SSL		
3.22.2.2.16.8.	Deve permitir enviar tráfego IPV4 e IPV6 simultaneamente pelo mesmo túnel VPN SSL		
3.22.2.3.	Funcionalidades de VPN:		
3.22.2.3.1.	Deve permitir split-tunnel para VPN IPSec e SSL;		
3.22.2.3.2.	Na VPN split-tunneling, deve permitir configurar exceções baseadas no reconhecimento de aplicações locais, podendo especificar o nome do processo, caminho completo e diretório onde está instalado localmente, para não serem direcionadas ao túnel VPN;		
3.22.2.3.3.	Na VPN split-tunneling, deve permitir configurar exceções baseadas em domínio, para não serem direcionadas ao túnel VPN;		
3.22.2.3.4.	Deve permitir selecionar de forma automática o gateway remoto mais próximo para conexão VPN, baseado em:		
3.22.2.3.4.1.	Tempo de resposta de ping;		
3.22.2.3.4.2.	TCP Round Trip Time (TCP Three-Way Handshare SYN, SYN-ACK, ACK);		
3.22.2.3.5.	Deve permitir conectar automaticamente à um túnel SSL VPN backup quando um túnel IPSec VPN falhar;		
3.22.2.3.6.	Deve permitir associar tags à um usuário remoto de VPN, de acordo com as regras de conformidade;		
3.22.2.3.7.	Deve permitir bloquear acesso à determinadas VPN's de usuário, baseado nas tags associadas ao usuário;		

3.22.2.3.8.	Deve permitir criar regras para associação de tags, de acordo com os seguintes parâmetros:		
3.22.2.3.8.1.	Grupo Active Directory;		
3.22.2.3.8.2.	Existência de Antivírus instalado;		
3.22.2.3.8.3.	Existência de Antivírus atualizado;		
3.22.2.3.8.4.	Certificado;		
3.22.2.3.8.5.	Cliente de Segurança Gerenciado Centralmente;		
3.22.2.3.8.6.	Existência de Arquivo em determinado diretório do cliente;		
3.22.2.3.8.7.	Domínio logado;		
3.22.2.3.8.8.	Versão de Sistema Operacional;		
3.22.2.3.8.9.	Chave de Registro do Windows;		
3.22.2.3.8.10.	Processo em execução;		
3.22.2.3.8.11.	Malware detectado pelo Sandbox nos últimos 7 dias;		
3.22.2.3.8.12.	Nível de Vulnerabilidade do dispositivo;		
3.22.2.3.8.13.	Windows Security, sendo a checagem das seguintes aplicações, se estão habilitadas:		
3.22.2.3.8.13.1.	Windows Defender;		
3.22.2.3.8.13.2.	Bitlocker Disk Encryption;		
3.22.2.3.8.13.3.	Exploit Guard;		
3.22.2.3.8.13.4.	Application Guard;		
3.22.2.3.8.13.5.	Windows Firewall.		
3.22.2.3.9.	Deve permitir que o usuário configure VPNs localmente;		
3.22.2.3.10.	Deve permitir que o usuário desconecte uma VPN;		
3.22.2.3.11.	Deve permitir a conexão VPN antes do login;		
3.22.2.3.12.	Deve permitir conexão VPN automática;		
3.22.2.3.13.	Deve suportar a configuração de senha para o usuário acessar a configuração do cliente;		
3.22.2.3.14.	Deve permitir a autenticação de dois fatores fornecida pelo mesmo fabricante;		
3.22.2.3.15.	IPSEC:		
3.22.2.3.15.1.	Deve permitir que o usuário crie novas VPNs IPSEC;		
3.22.2.3.15.2.	Deve permitir que várias VPNs IPSEC sejam definidas simultaneamente;		
3.22.2.3.15.3.	Deve permitir a autenticação usando nome de usuário e senha;		
3.22.2.3.15.4.	Deve permitir a autenticação usando certificados digitais		
3.22.2.3.15.5.	Deve permitir a seleção dos modos Principal e Agressivo;		
3.22.2.3.15.6.	Deve permitir a configuração do DHCP por IPSec;		
3.22.2.3.15.7.	Deve permitir o uso do NAT Traversal;		

3.22.2.3.15.8.	Deve permitir a escolha de grupos Diffie-Hellman (1,2,5 e 14);		
3.22.2.3.15.9.	Deve permitir configurações de expiração de chave IKE;		
3.22.2.3.15.10.	Deve suportar IKEv1 e IKEv2;		
3.22.2.3.15.11.	Deve permitir o uso do Perfect Forward Secrecy;		
3.22.2.3.15.12.	Deve suportar o uso de certificados para autenticação na VPN IPSec;		
3.22.2.3.15.13.	Deve suportar usuário e senha para autenticação VPN IPSec;		
3.22.2.3.15.14.	Deve suportar o uso de certificados em cartão inteligente para autenticação na VPN IPSec;		
3.22.2.3.15.15.	Deve suportar o bloqueio de tráfego IPv6 na VPN IPsec		
3.22.2.3.16.	SSL:		
3.22.2.3.16.1.	Deve permitir que o usuário crie novas VPNs SSL;		
3.22.2.3.16.2.	Deve permitir que várias VPNs SSL sejam definidas simultaneamente;		
3.22.2.3.16.3.	Deve permitir a personalização da porta TCP na qual a VPN SSL funciona;		
3.22.2.3.16.4.	Deve permitir a autenticação usando nome de usuário e senha;		
3.22.2.3.16.5.	Deve permitir a autenticação usando certificados digitais;		
3.22.2.3.16.6.	Para uso específico de VPN SSL (pelo menos):		
3.22.2.3.16.6.1.	Especificação IP do concentrador;		
3.22.2.3.16.6.2.	Especificação da porta do hub;		
3.22.2.3.16.7.	Deve permitir autenticação SAML SSO para VPN SSL;		
3.22.2.3.16.8.	Deve permitir enviar tráfego IPV4 e IPV6 simultaneamente pelo mesmo túnel VPN SSL;		
3.22.2.4.	Análise de Vulnerabilidade:		
3.22.2.4.1.	O cliente de segurança deve ter um módulo de pesquisa de vulnerabilidades integrado e permitir o gerenciamento central no console do mesmo fabricante;		
3.22.2.4.2.	Deve permitir que o usuário inicie uma análise de vulnerabilidade sob demanda;		
3.22.2.4.3.	As vulnerabilidades encontradas devem ser exibidas localmente com um link para visualizar informações de um banco de dados na Internet. Deve ter pelo menos: nome, gravidade e detalhes;		
3.22.2.4.4.	Os resultados da verificação de vulnerabilidades devem incluir pelo menos: lista de vulnerabilidades, número de vulnerabilidades classificadas como críticas, altas, médias e baixas;		
3.22.2.4.5.	Deve permitir a aplicação automática de patches;		

3.22.2.4.6.	Deve detalhar quais correções requerem instalação manual;		
3.22.2.4.7.	A verificação de vulnerabilidades deve ser permitida de maneira ordenada e autônoma a partir do console central;		
3.22.2.5.	Funcionalidades de Filtro de Conteúdo WEB:		
3.22.2.5.1.	Deve permitir a configuração do perfil de filtro da web a partir do console central do mesmo fabricante;		
3.22.2.5.2.	O fabricante deve fazer consultas on-line com o cliente de segurança sobre a categoria de um determinado site (por exemplo, interesse geral, tecnologia, hackers, pornografia etc.) para aplicar a política de controle de acesso à Internet;		
3.22.2.5.3.	O cliente de segurança deve suportar regras estáticas de acesso à Internet com base em expressões regulares;		
3.22.2.5.4.	Para um determinada URL, os acessos devem ser: permitir, bloquear, alertar ou monitorar;		
3.22.2.5.5.	Deve configurar o filtro de URL com base em caracteres simples, curinga e expressões regulares (regex);		
3.22.2.5.6.	Deve permitir que as configurações de filtro URL sejam importadas do firewall do mesmo fabricante;		
3.22.2.5.7.	Deve implementar mecanismo Safe Search, para limitar acesso à conteúdo em buscadores Google e Bing;		
3.22.2.5.8.	Possuir pelo menos 80 categorias de filtro URL.		
3.22.3.	Item 3: Sistema de Gerenciamento de logs, análise e plataforma de relatório		
3.22.3.1.	Características:		
3.22.3.1.1.	Deve ser do tipo appliance virtual (VM);		
3.22.3.1.2.	Possuir capacidade de recebimento de logs de pelo menos 1 mil dispositivos;		
3.22.3.1.3.	Possuir a capacidade de receber pelo menos 6 GBytes de logs diários;		
3.22.3.1.4.	Possuir pelo menos 3 TB de espaço em disco;		
3.22.3.1.5.	Deverá ser compatível com ambiente VMware ESXi 5.5, 6.0, 6.5, 6.7 e 7.0;		
3.22.3.1.6.	Deverá ser compatível com ambiente Microsoft Hyper-V 2008 R2/2012/2012 R2/2016;		
3.22.3.1.7.	Deverá ser compatível com ambiente Citrix XenServer 6.0+ e Open Source Xen 4.1+;		
3.22.3.1.8.	Deverá ser compatível com ambiente KVM;		
3.22.3.1.9.	Deverá ser compatível com ambiente Nutanix AHV;		
3.22.3.1.10.	Deverá ser compatível com ambiente Amazon Web Services (AWS);		

3.22.3.1.11.	Deverá ser compatível com ambiente Microsoft Azure;		
3.22.3.1.12.	Deverá ser compatível com o ambiente Google Cloud (GPC);		
3.22.3.1.13.	Deverá ser compatível com o ambiente Oracle Cloud Infrastructure (OCI);		
3.22.3.1.14.	Deverá ser compatível com o ambiente Alibaba Cloud (AliCloud);		
3.22.3.1.15.	Não deve possuir limite na quantidade de múltiplas vCPU;		
3.22.3.1.16.	Não deve possuir limite para suporte a expansão de memória RAM;		
3.22.3.2.	Requisitos Mínimos de Funcionalidade		
3.22.3.2.1.	Suportar o acesso via SSH e WEB (HTTPS) para gerenciamento de soluções;		
3.22.3.2.2.	Possuir comunicação e autenticação criptografada com usuário e senha para obter relatórios, na interface gráfica (GUI) e via linha de comando no console de gerenciamento;		
3.22.3.2.3.	Permitir o acesso simultâneo à administração, bem como permitir que pelo menos 2 (dois) perfis sejam criados para administração e monitoramento;		
3.22.3.2.4.	Suportar SNMP versão 2 e 3;		
3.22.3.2.5.	Permitir a virtualização do gerenciamento e administração dos dispositivos, nos quais cada administrador só tem acesso aos computadores autorizados;		
3.22.3.2.6.	Permitir a criação de um administrador geral, que tenha acesso geral a todas as instâncias de virtualização da solução;		
3.22.3.2.7.	Permitir ativar e desativar para cada interface da plataforma, as permissões de acesso HTTP, HTTPS, SSH;		
3.22.3.2.8.	Possuir autenticação de usuários para acesso à plataforma via LDAP;		
3.22.3.2.9.	Possuir autenticação de usuários para acesso à plataforma via Radius;		
3.22.3.2.10.	Possuir autenticação de usuários para acesso à plataforma via TACACS +;		
3.22.3.2.11.	Possuir geração de relatórios de tráfego em tempo real, em formato de mapa geográfico;		
3.22.3.2.12.	Possuir geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas;		
3.22.3.2.13.	Possuir geração de relatórios de tráfego em tempo real, em formato de gráfico;		
3.22.3.2.14.	Possuir definição de perfis de acesso ao console com permissão granular, como: acesso de gravação, acesso de leitura, criação de novos usuários e alterações nas configurações gerais;		

3.22.3.2.15.	Possuir um assistente gráfico para adicionar novos dispositivos, usando seu endereço IP, usuário e senha;		
3.22.3.2.16.	Possuir visualização da quantidade de logs enviados de cada dispositivo monitorado;		
3.22.3.2.17.	Possuir mecanismos de apagamento automático para logs antigos;		
3.22.3.2.18.	Permitir importação e exportação de relatórios;		
3.22.3.2.19.	Deve ter a capacidade de criar relatórios no formato HTML;		
3.22.3.2.20.	Deve ter a capacidade de criar relatórios em formato PDF;		
3.22.3.2.21.	Deve ter a capacidade de criar relatórios no formato XML;		
3.22.3.2.22.	Deve ter a capacidade de criar relatórios no formato CSV;		
3.22.3.2.23.	Deve permitir exportar os logs no formato CSV;		
3.22.3.2.24.	Deve gerar logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário;		
3.22.3.2.25.	Os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar;		
3.22.3.2.26.	A solução deve ter relatórios predefinidos;		
3.22.3.2.27.	Deve poder enviar automaticamente os logs para um servidor FTP externo para a solução;		
3.22.3.2.28.	A duplicação de relatórios existentes deve ser possível para edição posterior;		
3.22.3.2.29.	Ter a capacidade de personalizar a capa dos relatórios obtidos;		
3.22.3.2.30.	Permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos mesmos logs;		
3.22.3.2.31.	Os logs de auditoria das regras e alterações na configuração do objeto devem ser exibidos em uma lista diferente dos logs relacionados ao tráfego de dados;		
3.22.3.2.32.	Ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas;		
3.22.3.2.33.	Deve ter um mecanismo de "pesquisa detalhada" para navegar pelos relatórios em tempo real;		
3.22.3.2.34.	Deve permitir que os arquivos de log sejam baixados da plataforma para uso externo;		
3.22.3.2.35.	Ter a capacidade de gerar e enviar relatórios periódicos automaticamente;		

3.22.3.2.36.	Permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades;		
3.22.3.2.37.	Permitir o envio por e-mail relatórios automaticamente;		
3.22.3.2.38.	Deve permitir que o relatório seja enviado por email ao destinatário específico;		
3.22.3.2.39.	Permitir a programação da geração de relatórios, conforme calendário definido pelo administrador;		
3.22.3.2.40.	É necessário exibir graficamente em tempo real a taxa de geração de logs para cada dispositivo gerenciado;		
3.22.3.2.41.	Deve permitir o uso de filtros nos relatórios;		
3.22.3.2.42.	Deve permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros;		
3.22.3.2.43.	Permitir especificar o idioma dos relatórios criados;		
3.22.3.2.44.	Gerar alertas automáticos por email, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros;		
3.22.3.2.45.	Deve permitir o envio automático de relatórios para um servidor SFTP ou FTP externo;		
3.22.3.2.46.	Deve ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios;		
3.22.3.2.47.	Possibilitar visualizar nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros;		
3.22.3.2.48.	Deve ter uma ferramenta que permita analisar o desempenho na geração de relatórios, a fim de detectar e corrigir problemas na geração deles;		
3.22.3.2.49.	Importar arquivos com logs de dispositivos compatíveis conhecidos e não conhecidos pela plataforma, para geração posterior de relatórios;		
3.22.3.2.50.	Deve ser possível definir o espaço que cada instância de virtualização pode usar para armazenamento de log;		
3.22.3.2.51.	Deve fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado;		
3.22.3.2.52.	Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos		

3.22.3.2.53.	Deve permitir visualizar em tempo real os logs recebidos;		
3.22.3.2.54.	Deve permitir o encaminhamento de log no formato syslog;		
3.22.3.2.55.	Deve permitir o encaminhamento de log no formato CEF (Common Event Format);		
3.22.3.2.56.	Deve incluir um painel para operações SOC que monitore as principais ameaças à segurança da sua rede;		
3.22.3.2.57.	Deve incluir o painel para operações do SOC que monitora o envolvimento do usuário e o uso suspeito da web em sua rede;		
3.22.3.2.58.	Deve incluir o painel para operações SOC que monitora o tráfego na sua rede;		
3.22.3.2.59.	Deve incluir o painel para operações SOC que monitoram o tráfego de aplicativos e sites na sua rede;		
3.22.3.2.60.	Deve incluir o painel para operações SOC que monitoram detecções de ameaças de dia zero em sua rede (sandboxing);		
3.22.3.2.61.	Deve incluir o painel para operações SOC que monitora a atividade do terminal na sua rede;		
3.22.3.2.62.	Deve incluir o painel para operações SOC que monitoram a atividade da VPN na sua rede;		
3.22.3.2.63.	Deve incluir um painel para operações SOC que monitora pontos de acesso Wi-Fi e SSIDs;		
3.22.3.2.64.	Deve incluir o painel para operações SOC que monitoram o desempenho dos recursos locais da solução (CPU, Memória);		
3.22.3.2.65.	Deve permitir a criação de painéis personalizados para monitorar operações SOC;		
3.22.3.2.66.	Gerar alertas de eventos a partir de logs recebidos;		
3.22.3.2.67.	Permitir a criação de incidentes a partir de alertas de eventos para o terminal;		
3.22.3.2.68.	Deve permitir o suporte a logs nas nuvens públicas do AWS, Azure ou Google;		
3.22.3.2.69.	Suportar o padrão SAML para autenticação do usuário administrador;		
3.22.3.2.70.	Possuir relatório de avaliação de risco para e-mail;		
3.22.3.2.71.	Possuir relatório de conformidade com o PCI sem fio;		
3.22.3.2.72.	Possuir relatório de APs e SSIDs autorizados, bem como clientes WIFi;		
3.22.3.2.73.	Possuir relatório de vulnerabilidades da solução de segurança gerenciada do equipamento terminal;		
3.22.3.2.74.	Possuir relatório de aplicativo da web, se tiver uma plataforma de segurança da web;		
3.22.3.3.	Relatórios de Firewall		

3.22.3.3.1.	Deve ter um relatório de conformidade com o PCI DSS;		
3.22.3.3.2.	Possuir um relatório de uso do aplicativo SaaS;		
3.22.3.3.3.	Possuir um relatório de prevenção de perda de dados (DLP);		
3.22.3.3.4.	Possuir um relatório de VPN;		
3.22.3.3.5.	Possuir um relatório IPS (Intruder Prevention System);		
3.22.3.3.6.	Possuir um relatório de reputação do cliente;		
3.22.3.3.7.	Possuir um relatório de análise de segurança do usuário;		
3.22.3.3.8.	Possuir um relatório de análise de ameaças cibernéticas;		
3.22.3.3.9.	Possuir um breve relatório resumido diário de eventos e incidentes de segurança;		
3.22.3.3.10.	Possuir um relatório de tráfego DNS;		
3.22.3.3.11.	Possuir um relatório de tráfego de e-mail;		
3.22.3.3.12.	Possuir um relatório dos 10 principais aplicativos usados na rede;		
3.22.3.3.13.	Possuir um relatório dos 10 principais sites usados na rede;		
3.22.3.3.14.	Possuir um relatório de uso de mídia social;		

PREGÃO ELETRÔNICO N.º 0017/2022

Processo nº 22/4000-0000309-9

ANEXO V

ANÁLISE CONTÁBIL DA CAPACIDADE FINACEIRA

GOVERNO DO ESTADO DO RIO GRANDE DO SUL ANEXO II AO DECRETO Nº 36.601, de 10-04-96.			J	**IDENTIFICAÇÃO DO PROCESSO**				
			NÚMERO				FOLHA	
ANÁLISE CONTÁBIL DA CAPACIDADE FINANCEIRA DE LICITANTE – ACF								
A	IDENTIFICAÇÃO DO EDITAL OU CARTA-CONVITE							
CÓDIGO	NOME DO LICITADOR				NÚMERO	MODALID.	DATA	
B	IDENTIFICAÇÃO DO LICITANTE							
CGC/MF:					ATIVIDADE PRINCIPAL	CNAE	SE	
FIRMA/RAZÃO SOCIAL:				CNJ			CGC/TE	
ENDEREÇO (rua, avenida, praça, etc.)					NÚMERO	CONJ.	CEP	
NOME DO REPRESENTANTE LEGAL						TELEFONE		
BALANÇO APRESENTADO PERÍODO:		DATA DO BALANÇO ANUAL			Nº LIVRO DIÁRIO	Nº DO RJC		
C	IDENTIFICAÇÃO DO CONTADOR OU TÉCNICO EM CONTABILIDADE							
NOME:			CP	Nº DO REGISTRO NO CRC			TELEFONE	
ENDEREÇO (rua, avenida, praça etc.)					NÚMERO	CONJ.	CEP	
D	IDENTIFICAÇÃO DA AUDITORIA							
NOME:						Nº DO REGISTRO NO CRC		

E	BALANÇO PATRIMONIAL REESTRUTURADO		**F**	DEMONSTRAÇÃO DA ANÁLISE FINANCEIRA DO LICITANTE				
	CONTAS	Em R$ Mil		ÍNDICE	VALOR	NOTA	PESO	NP
1	ATIVO CIRCULANTE AJUSTADO (ACA)		1	LIQUIDEZ CORRENTE				
2	PASSIVO CIRCULANTE (PC)							
3	ACA + REALIZÁVEL A LONGO PRAZO		2	LIQUIDEZ GERAL				
4	PC + PASSIVO A LONGO PRAZO							
5	ATIVO PERMANENTE		3	GRAU DE IMOBILIZAÇÃO				
6	PATRIMÔNIO LÍQUIDO AJUSTADO							
7	PASSIVO CIRCULANTE		4	ENDIVIDAMENTO DE CURTO PRAZO				
8	PATRIMÔNIO LÍQUIDO AJUSTADO							
9	PC + PASSIVO A LONGO PRAZO		5	ENDIVIDAMENTO GERAL				
10	PATRIMÔNIO LÍQUIDO AJUSTADO							
11	DESPESA ANTECIPADA		NF	NOTA FINAL DA CAPACIDADE FINANCEIRA RELATIVA = å NP				

			R		
12	RESULTADOS DE EXERCÍCIOS FUTUROS				
13	CAPITAL SOCIAL INTEGRALIZADO		**G**	RESULTADO DA ANÁLISE	
14	PATRIMÔNIO LÍQUIDO				
15	CONSISTÊNCIA (vide instruções no verso)				

H	IDENTIFICAÇÃO DO SERVIDOR PÚBLICO

NOME:	MATRÍCULA

I	DECLARAÇÃO E ASSINATURAS

O representante legal da empresa licitante e o contador ou técnico em contabilidade declaram, sob as penas da Lei, que as informações prestadas neste formulário são a expressão da verdade, bem como autorizam o licitador, por si ou por outrem e a qualquer tempo, examinar os livros e os documentos relativos à escrituração contábil, para confrontação dos dados aqui demonstrados.

LICITANTE	CONTADOR OU TÉCNICO EM CONTABILIDADE	LICITADOR
DATA:	DATA:	DATA:

PREGÃO ELETRÔNICO N.º 0017/2022

Processo nº 22/4000-0000309-9

ANEXO VI

CARTA DE FIANÇA BANCÁRIA PARA GARANTIA DE EXECUÇÃO CONTRATUAL (Modelo)

1. Pela presente, o (a) [nome da instituição fiadora] com sede em [endereço completo], por seus representantes legais infra-assinados, declara que se responsabiliza como fiador e principal pagador, com expressa renúncia dos benefícios estatuídos no Artigo 827, do Código Civil Brasileiro, da empresa (nome da empresa), com sede em [endereço completo], até o limite de R$ [valor da garantia] (valor por extenso) para efeito de garantia à execução do contrato nº [número do contrato, formato xx/ano], decorrente do processo licitatório [modalidade e número do instrumento convocatório da licitação – ex.: PE nº xx/ano], firmado entre a afiançada e o(a)[órgão/entidade]para [objeto da licitação].

2. A fiança ora concedida visa garantir o cumprimento, por parte de nossa afiançada, de todas as obrigações estipuladas no contrato retromencionado, abrangendo o pagamento de:

a) prejuízos advindos do não cumprimento do contrato;

b) multas moratórias e punitivas aplicadas pela Administração ao contratado;

c) prejuízos causados ao contratante ou a terceiros decorrentes de culpa ou dolo durante a execução do contrato; e

d) obrigações previdenciárias e/ou trabalhistas não adimplidas pelo contratado.

3. Esta fiança é válida por (prazo, contado em dias, correspondente à vigência do contrato) (valor por escrito) dias, contados a partir de (data de início da vigência do contrato), vencendo-se, portanto, em (data).

4. Na hipótese de inadimplemento de qualquer das obrigações assumidas pela afiançada, o (a) (nome da instituição fiadora) efetuará o pagamento das importâncias que forem devidas, no âmbito e por efeito da presente fiança, até o limite acima estipulado, no prazo de 48 (quarenta e oito) horas, contado do recebimento de comunicação escrita do [órgão/entidade].

5. A comunicação de inadimplemento deverá ocorrer até o prazo máximo de 3 (três) meses após o vencimento desta fiança.

6. Nenhuma objeção ou oposição da nossa afiançada será admitida ou

invocada por este fiador com o fim de escusar-se do cumprimento da obrigação assumida neste ato e por este instrumento perante o [órgão/entidade].

7. Obriga-se este fiador, outrossim, pelo pagamento de quaisquer despesas judiciais e/ou extrajudiciais, bem assim por honorários advocatícios, na hipótese de o [órgão/entidade] se ver compelido a ingressar em juízo para demandar o cumprimento da obrigação a que se refere a presente fiança.

8. Se, no prazo máximo de 3 (três) meses após a data de vencimento desta Carta de Fiança, o (a) (nome da instituição fiadora) não tiver recebido do(a)[órgão/entidade] qualquer comunicação relativa a inadimplemento da afiançada, ou termo circunstanciado de que a afiançada cumpriu todas as cláusulas do contrato, acompanhado do original desta Carta de Fiança, esta fiança será automaticamente extinta, independentemente de qualquer formalidade, aviso, notificação judicial ou extrajudicial, deixando, em consequência, de produzir qualquer efeito e ficando o fiador exonerado da obrigação assumida por força deste documento.

9. Declara, ainda, este fiador, que a presente fiança está devidamente contabilizada e que satisfaz às determinações do Banco Central do Brasil e aos preceitos da legislação bancária aplicáveis e, que, os signatários deste Instrumento estão autorizados a prestar a presente fiança.

10. Declara, finalmente, que está autorizado pelo Banco Central do Brasil a expedir Carta de Fiança Bancária e que o valor da presente se contém dentro dos limites que lhe são autorizados pela referida entidade federal.

(Local e data)
(Instituição garantidora)
(Assinaturas autorizadas)

PREGÃO ELETRÔNICO N.º 0017/2022

Processo nº 22/4000-0000309-9

ANEXO VII

MODELO

DECLARAÇÃO DE QUE NÃO EMPREGA MENOR DE 18 ANOS

Ref.: (identificação da licitação)

....., inscrito no CNPJ nº....., por intermédio de seu representante legal o (a) Senhor (a) ....., portador(a) da Carteira de Identidade nº..... e do CPF nº. ..... DECLARA, para fins do disposto no inciso V do art. 27 da Lei nº. 8.666, de 21 de junho de 1993, acrescido pela Lei nº. 9.854, de 27 de outubro de 1999, que não emprega menor de dezoito anos em trabalho noturno, perigoso ou insalubre e não emprega menor de dezesseis anos.

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

.....

(data)

.....

(representante legal)

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

PREGÃO ELETRÔNICO N.º 0017/2022

Processo nº 22/4000-0000309-9

ANEXO VIII

MINUTA DE CONTRATO DE SERVIÇOS SEM DEDICAÇÃO EXCLUSIVA DE MÃO DE OBRA

CONTRATANTE:

BADESUL DESENVOLVIMENTO S.A. - AGÊNCIA DE FOMENTO/RS, instituição financeira de economia mista, inscrita no CNPJ/MF sob o nº. 02.885.855/0001-72, com sede na Rua Gen. Andrade Neves Nº 175 - 18º andar, representada neste ato pelo seu _____, Senhor _____, (nacionalidade), (estado civil), (profissão), portador da Carteira de Identidade SSP/RS n.º _____, inscrito no CPF/MF sob n.º _____, residente e domiciliado na (endereço e cidade), doravante denominada simplesmente BADESUL;

CONTRATADO:

_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ __, inscrita no CNPJ/MF sob o n.º _ __ _ _ _ _ _ _ _ _ _ _, com sede na rua _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _, (cidade/estado)_ _ _ _ _ _ _ _ _ _ _ _, representada neste ato pelo seu _ _ _ _ _ _ _ _ _ _ _ _ _ , Senhor _ _ _ _ _ _ _ _ _ _ _ _, (nacionalidade), (estado civil), (profissão), portador da Carteira de Identidade SSP/RS n.º _ _ _ _ _ _ _ _ , inscrito no CPF/MF sob n.º _ _ _ _ _ _ _ _ _ _ _, residente e domiciliado na (endereço e cidade), doravante denominada simplesmente CONTRATADA.

As partes acima qualificadas, em consonância com o processo de licitação, PE 0017/2022, com base na Lei Federal n°. 13.303, de 30 de junho de 2016, regendo-se pela mesma lei, pela Lei n°. 12.846, de 1º de agosto de 2013, pela Lei Complementar Federal nº. 123, de 14 de dezembro de 2006, pela Lei Estadual nº. 52.823, de 21 de dezembro de 2015, pela Lei Estadual nº. 13.706, de 06 de abril de 2011, pela Lei Estadual nº. 11.389, de 25 de novembro de 1999, pelo Decreto Estadual nº. 42.250, de 19 de maio de 2003, pelo Decreto Estadual nº. 48.160, de 14 de julho de 2011, e suas alterações posteriores, assim como pelo Projeto Básico/Termo de Referência e demais documentos constantes no processo e pelas cláusulas a seguir expressas, definidoras dos

direitos e responsabilidades das partes.

CLÁUSULA 1ª. DO OBJETO

1.1. Serviço de solução de Firewall de Próxima Geração (Next-Generation Firewall (NGFW) e demais especificações.

1.2. Os serviços serão prestados nas condições estabelecidas no Termo de Referência anexo I do Edital, independentemente de transcrição.

CLÁUSULA 2ª. DO REGIME DE EXECUÇÃO

2.1. A execução do presente contrato far-se-á pelo regime de **empreitada por preço unitário.**

CLÁUSULA 3ª. DA ESPECIFICAÇÃO DO OBJETO

3.1. Conforme item 3 do termo de referência, anexo I.

CLÁUSULA 4ª. DA QUANTIDADE ESTIMADA

4.1. Os itens que compõem o lote único bem como suas quantidades são os seguintes:

Item		Produto	Quantidades
Equipamentos e licenças	1	Firewall de Próxima Geração (Next Generation Firewall – NGFW) do tipo *appliance* com sistema de gestão integrado em formato GUI (gráfico) do próprio fabricante, suporte técnico e garantia de 60 meses	2
	2	Ferramenta de visibilidade, análise e segurança de Endpoints para conexão remota e segura Zero Trust Network Agent, padrão web, autenticação multifator (MFA), integração com Active Directory (AD) e hospedagem em nuvem	200 usuários
	3	Sistema de Gerenciamento de logs, análise e plataforma de relatórios	1
Serviço de instalação	4	Serviço de instalação, configuração, atualização e treinamento de pessoal	1
Suporte técnico	5	Suporte técnico mensal durante a vigência contratual (60 meses)	1

CLÁUSULA 5ª. DO PREÇO

5.1. O preço referente à execução dos serviços contratados, serão os seguintes:

Item		Produto	Valor Unitário
Equipamentos e licenças	1	Firewall de Próxima Geração (Next Generation Firewall – NGFW) do tipo *appliance* com sistema de gestão integrado em formato GUI (gráfico) do próprio fabricante, suporte técnico e garantia de 60 meses	
	2	Ferramenta de visibilidade, análise e segurança de Endpoints para conexão remota e segura Zero Trust Network Agent, padrão web, autenticação multifator (MFA), integração com Active Directory (AD) e hospedagem em nuvem	
	3	Sistema de Gerenciamento de logs, análise e plataforma de relatórios	
Serviço de instalação	4	Serviço de instalação, configuração, atualização e treinamento de pessoal	
Suporte técnico	5	Suporte técnico mensal, durante a vigência contratual (60 meses)	

5.2. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação. Não será admitido aditivo contratual em função de variação cambial.

CLÁUSULA 6ª. DO PAGAMENTO

6.1. O pagamento deverá ser efetuado no prazo de até 10 (dez) dias mediante a apresentação de Nota Fiscal ou da Fatura pela CONTRATADA, que deverá conter o detalhamento dos serviços executados;

6.2. O pagamento deverá ser efetuado mediante a apresentação de Nota Fiscal ou da Fatura pelo contratado, considerando os valores discriminados na Planilha de Custos e Formação de Preços anexa;

6.3. O documento fiscal deverá ser do estabelecimento que apresentou a proposta e, nos casos em que a emissão for de outro estabelecimento da empresa, o documento deverá vir acompanhado das certidões negativas relativas à regularidade fiscal;

6.4. Quando o documento for de outro estabelecimento localizado fora

do Estado, será exigida também certidão negativa relativa à Regularidade Fiscal junto à Fazenda Estadual do Rio Grande do Sul independentemente da localização da sede ou filial da CONTRATADA;

6.5. A protocolização somente poderá ser feita após a prestação dos serviços por parte da CONTRATADA;

6.6. A protocolização somente poderá ser feita após o cumprimento do objeto por parte da CONTRATADA;

6.7. A liberação das faturas de pagamento por parte do BADESUL fica condicionada à apresentação, pela CONTRATADA, de documentação fiscal correspondente à aquisição de bens e serviços relativos à execução do contrato, cujo prazo para dita exibição não deverá exceder a 30 (trinta) dias contados da data de suas emissões, conforme o preconizado pelo Decreto nº 36.117, de 03 de agosto de 1995;

6.8. Caso a Fatura contenha divergência com relação ao estabelecido no instrumento contratual, a Contratante ficará obrigada a comunicar a empresa Contratada o motivo da não aprovação. A devolução da Fatura, devidamente regularizada pela Contratada, deverá ser efetuada em até 02 (dois) dias úteis da data da comunicação;

6.9. Caso o valor pago a título de volume mensal total seja diferente do valor devido pela produção efetiva de serviços prestados, durante 03 (três) meses consecutivos ou 06 (seis) meses alternados, o órgão Contratante poderá, em comum acordo com a Contratada, redefinir o volume mensal total, de forma a ajustá-la a real demanda de serviços;

6.10. A Contratante se reserva o direito de descontar do pagamento os eventuais débitos da Contratada, inclusive os relacionados com multas, danos e prejuízos contra terceiros.

6.11. As Notas Fiscais deverão ser emitidas e encaminhadas ao órgão Contratante, até o 5° dia útil do mês subsequente à prestação dos serviços. Após aprovação pela Contratante, os pagamentos serão efetuados em 20 (vinte) dias corridos.

6.12. Após o recebimento da Nota Fiscal, a Contratante disporá de até 10 (dez) dias corridos, para aceite, aprovando os serviços realizados.

6.13. Haverá a retenção de todos os tributos nos quais o BADESUL seja responsável tributário.

6.14. O BADESUL poderá reter do valor da fatura da CONTRATADA a importância devida, até a regularização de suas obrigações sociais, trabalhistas ou contratuais.

6.15. O pagamento será efetuado por fornecimento efetivamente

realizado e aceito.

6.15.1. A glosa do pagamento durante a execução contratual, sem prejuízo das sanções cabíveis, só deverá ocorrer quando a CONTRATADA:

6.15.1.1. não produzir os resultados, deixar de executar, ou não executar as atividades com a qualidade mínima exigida no contrato; ou

6.15.1.2. deixar de utilizar materiais e recursos humanos exigidos para a execução do objeto, ou utilizá-los com qualidade ou quantidade inferior à demandada.

6.16. Caso o objeto não seja fornecido fielmente e/ou apresente alguma incorreção será considerado como não aceito e o prazo de pagamento será contado a partir da data de regularização.

6.17. Na fase da liquidação da despesa, deverá ser efetuada consulta ao CADIN/RS para fins de comprovação do cumprimento da relação contratual estabelecida nos termos do disposto no artigo 69, inciso IX, da Lei nº. 13.303, de 30 de junho de 2016;

6.17.1. Constatando-se situação de irregularidade da CONTRATADA junto ao CADIN/RS, será providenciada sua advertência, por escrito, para que, no prazo de 15 (quinze) dias, regularize sua situação ou, no mesmo prazo, apresente sua defesa.

6.18. Persistindo a irregularidade, o BADESUL poderá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à CONTRATADA a ampla defesa.

6.18.1. Os pagamentos a serem efetuados em favor do contratado, quando couber, estarão sujeitos à retenção, na fonte, dos seguintes tributos:

6.18.1.1. Imposto de Renda das Pessoas Jurídicas - IRPJ, Contribuição Social sobre o Lucro Líquido - CSLL, Contribuição para o Financiamento da Seguridade Social - COFINS, e Contribuição para os Programas de Integração social e de Formação do Patrimônio do Servidor Público - PIS/PASEP, na forma da Instrução Normativa RFB nº 1.234/2012, conforme determina o art. 64 da Lei federal nº 9.430/1996;

6.18.1.2. Contribuição Previdenciária, correspondente a onze por cento, na forma da Instrução Normativa RFB nº 971, de 13 de novembro de 2009, conforme determina a Lei federal nº 8.212/1991;

6.18.1.3. Imposto sobre Serviços de Qualquer Natureza - ISSQN, na forma da Lei Complementar federal nº 116/2003, combinada com a legislação municipal e/ou distrital sobre o tema.

6.19. As empresas dispensadas de retenções deverão entregar declaração, anexa ao documento de cobrança, em duas vias, assinadas pelo

representante legal, além de informar sua condição no documento fiscal, inclusive o enquadramento legal.

6.20. O contratante poderá reter do valor da fatura do contratado a importância devida, até a regularização de suas obrigações contratuais;

6.21. A Contratante se reserva o direito de descontar do pagamento os eventuais débitos da Contratada, inclusive os relacionados com multas, danos e prejuízos contra terceiros.

6.22. A nota fiscal deverá ser encaminhada através do e-mail badesul.fornecedores@badesul.com.br. Não será considerada recebida a nota fiscal encaminhada por qualquer outro meio.

CLÁUSULA 7ª. DO RECURSO FINANCEIRO

7.1. As despesas decorrentes do presente contrato correrão à conta de recursos próprios do BADESUL.

CLÁUSULA 8ª. DA ATUALIZAÇÃO MONETÁRIA

8.1. Os valores do presente contrato não pagos na data prevista serão corrigidos até a data do efetivo pagamento, *pro rata die*, pelo Índice de Preços ao Consumidor Amplo - IPCA, do Sistema Nacional de Índices de Preços ao Consumidor – SNIPC, ou outro que venha a substituí-lo.

CLÁUSULA 9ª. DA ANTECIPAÇÃO DE PAGAMENTO

9.1. As antecipações de pagamento em relação a data de vencimento, respeitada a ordem cronológica para cada fonte de recurso, terão um desconto equivalente à de 0,033% por dia de antecipação sobre o valor do pagamento.

CLÁUSULA 10ª. DOS PRAZOS

10.1. O prazo de duração do contrato é de 60 (sessenta) meses, contados da sua celebração.

CLÁUSULA 11ª. DO REAJUSTE

11.1. O contrato será reajustado somente referente ao **item "Suporte técnico durante a vigência contratual"**, observado o interregno mínimo de um ano, a contar da data limite para apresentação da proposta.

11.2. Nos reajustes subsequentes ao primeiro, o interregno mínimo de

um ano será contado a partir dos efeitos financeiros do último reajuste.

11.3. O valor do contrato será reajustado, em consequência da variação do IPCA (Índice de Preços ao Consumidor Amplo) do Sistema Nacional de Índices de Preços ao Consumidor – SNIPC, de acordo com a fórmula abaixo:

$$R = P0 \times [(IPCAn / IPCA0) - 1]$$

Onde:

R = parcela de reajuste;

P0 = Preço inicial do contrato no mês de referência dos preços ou preço do contrato no mês de aplicação do último reajuste;

IPCAn = número do índice IPCA referente ao mês do reajuste;

IPCA0 = número do índice IPCA referente ao mês da data da proposta, último reajuste.

11.4. A aplicação de índices de reajustamento pela fórmula acima deverá ocorrer independentemente dos mesmos serem positivos ou negativos.

11.5. O reajuste do valor contratual somente será admitido se o prazo de duração do contrato for superior a um ano em razão do próprio cronograma inicial ou por força de vicissitudes supervenientes não decorrentes de culpa da CONTRATADA, conforme estatuído na Lei nº 10.192, de 2001.

11.6. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

CLÁUSULA 12ª. DA FISCALIZAÇÃO

12.1. O titular e o substituto da fiscalização serão designados, mediante termo formal a ser emitido pelo Gestor do Contrato, por meio do Documento denominado Ato de Designação de Fiscal Técnico, anexo ao Processo, sendo estes encarregados de conferir o andamento das atividades e de corrigir desvios ou apontar eventuais irregularidades.

12.2. Sempre que solicitados pela fiscalização e de forma a dirimir dúvidas devidamente fundamentadas, serão realizados pela CONTRATADA, sem ônus adicionais, relatórios, documentos, laudos para esclarecer ou informar sobre problemas e soluções na execução dos serviços.

12.3. A fiscalização, sempre que possível, comunicará à contratada as providências necessárias para sanar eventuais problemas detectados na execução dos serviços. Porém, a ausência de manifestação escrita da fiscalização quando da ocorrência de falhas, não exime a contratada, em nenhuma hipótese, da responsabilidade de corrigi-las.

12.4. Qualquer fiscalização exercida pelo BADESUL será feita em seu exclusivo interesse e não implicará corresponsabilidade pela prestação dos

serviços contratados, sem que assista direito à CONTRATADA, eximir-se de suas obrigações pela fiscalização e perfeita execução dos serviços;

12.5. A fiscalização do BADESUL verificará a qualidade da prestação dos serviços, podendo exigir substituições ou reelaboração das atividades, quando não atenderem aos termos do objeto contratado, sem qualquer indenização pelos custos daí decorrentes.

CLÁUSULA 13ª. DO GESTOR DIRETO DO CONTRATO

13.1. O Gestor do contrato pelo Badesul, a quem caberão os controles sobre as normas, cumprimento das cláusulas contratuais e gerenciamento das dúvidas ou de questões técnicas surgidas no decorrer da prestação dos serviços do Contrato, será o Superintendente de Tecnologia da Informação.

CLÁUSULA 14ª. DA PERMISSÃO AO BANCO CENTRAL

14.1. O Contratado, nos termos do art. 33, §1º, da Resolução nº 4557, de 23 de fevereiro de 2017, permite acesso ao Banco Central do Brasil a:

14.1.1. termos firmados;

14.1.2. documentação e informações referentes aos serviços prestados; e

14.1.3. a suas dependências.

CLÁUSULA 15ª. DA GARANTIA DA EXECUÇÃO DO CONTRATO

15.1. A garantia poderá ser apresentada em uma das seguintes modalidades:

15.1.1. Caução em dinheiro ou Título da Dívida Pública, devendo este ter sido emitido sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Fazenda;

15.1.2. Seguro-garantia;

15.1.3. Fiança bancária, conforme modelo em anexo.

15.2. No caso de Apólice de Seguro Garantia a mesma deverá incluir, obrigatoriamente, a cobertura para a execução do contrato, bem como de todas as obrigações contratuais assumidas, inclusive, obrigações trabalhistas,

previdenciárias e fiscais e ainda possíveis penalidades, tais como multas de caráter punitivo.

15.3. O Contratado, no prazo de até 10 (dez) dias a contar da assinatura do contrato, prestará garantia no valor correspondente a 5% (cinco por cento) do valor total contratado, que será liberada após a execução do objeto da avença.

15.3.1. O prazo para apresentação da garantia poderá ser prorrogado por igual período a critério do BADESUL.

15.4. A inobservância do prazo fixado para apresentação da garantia, inclusive dos previstos nos itens 15.10 e 15.16, acarretará a aplicação de multa de 0,07% (sete centésimos por cento) do valor total do contrato por dia de atraso, até o máximo de 2% (dois por cento).

15.5. O atraso na apresentação da garantia autoriza a Administração a promover a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas.

15.6. O número do contrato deverá constar dos instrumentos de garantia a serem apresentados pelo garantidor.

15.7. Quando da abertura de processos para eventual aplicação de penalidade, a fiscalização do contrato deverá comunicar o fato à entidade garantidora paralelamente às comunicações de solicitação de defesa prévia ao contratado, bem como as decisões finais da instância administrativa.

15.8. A entidade garantidora não é parte interessada para figurar em processo administrativo instaurado pelo BADESUL com o objetivo de apurar prejuízos e/ou aplicar sanções ao contratado.

15.9. A validade da garantia, qualquer que seja a modalidade escolhida, deverá abranger um período de mais 3 (três) meses após o término da vigência contratual.

15.10. A garantia deverá ser integralizada no prazo máximo de 10 (dez) dias, sempre que dela forem deduzidos quaisquer valores ou quando houver alteração para acréscimo de objeto.

15.11. Qualquer que seja a modalidade escolhida, a garantia assegurará o pagamento de:

15.11.1. Prejuízo advindo do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

15.11.2. Prejuízos causados ao BADESUL ou a terceiro, decorrentes de culpa ou dolo durante a execução do contrato;

15.11.3. As multas moratórias e punitivas aplicadas pelo BADESUL ao contratado;

15.12. A garantia em dinheiro poderá ser efetuada em favor do BADESUL, em conta bancária específica com atualização monetária.

15.13. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada à nova situação ou renovada, no prazo máximo de 10 (dez) dias, seguindo os mesmos parâmetros utilizados quando da contratação.

15.14. O BADESUL fica autorizado a utilizar a garantia para corrigir quaisquer imperfeições na execução do objeto do contrato ou para reparar danos decorrentes da ação ou omissão do contratado, de seu preposto ou de quem em seu nome agir.

15.14.1. A autorização contida neste subitem é extensiva aos casos de multas aplicadas depois de esgotado o prazo recursal.

15.15. A garantia prestada será retida definitivamente, integralmente ou pelo saldo que apresentar, no caso de rescisão por culpa do contratado, sem prejuízo das sanções cabíveis.

15.16. Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, o contratado obriga-se a fazer a respectiva reposição no prazo máximo de 10 (dez) dias, contados da data em que for notificado.

15.17. O BADESUL não executará a garantia na ocorrência de uma ou mais das seguintes hipóteses:

15.17.1. Caso fortuito ou força maior;

15.17.2. Alteração, sem prévia anuência da entidade garantidora, das obrigações contratuais;

15.17.3. Descumprimento das obrigações pelo contratado decorrentes de atos ou fatos praticados pela Administração;

15.17.4. Atos ilícitos dolosos praticados por servidores da Administração.

15.18. Caberá à própria Administração apurar a isenção da responsabilidade prevista nos itens 15.17.3 e 15.17.4 do item anterior, não sendo a entidade garantidora parte no processo instaurado pela Administração.

15.19. Para efeitos da execução da garantia, os inadimplementos contratuais deverão ser comunicados pelo BADESUL ao contratado e/ou à entidade garantidora, no prazo de até 3 (três) meses após o término de vigência do contrato.

15.20. Não serão aceitas garantias que incluam outras isenções de responsabilidade que não as previstas neste Edital.

15.21. Será considerada extinta a garantia:

15.21.1. Com a devolução da apólice, título da dívida pública, carta de fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração do BADESUL, mediante

termo circunstanciado, de que o contratado cumpriu todas as cláusulas do contrato;

15.21.2. No prazo de 03 (três) meses após o término da vigência do contrato, exceto quando ocorrer comunicação de sinistros, por parte da Administração, devendo o prazo ser ampliado de acordo com os termos da comunicação.

15.22. A CONTRATADA é responsável pelos danos causados diretamente à BADESUL ou a terceiros, na forma do art. 76 da Lei nº. 13.303/2016.

CLÁUSULA 16ª. DAS OBRIGAÇÕES

16.1. As partes devem cumprir fielmente as cláusulas avençadas neste contrato, respondendo pelas consequências de sua inexecução parcial ou total.

CLÁUSULA 17ª. DAS OBRIGAÇÕES DA CONTRATADA

17.1. Executar os serviços conforme especificações contidas no ANEXO I- Termo de Referência e de sua proposta, com a alocação dos empregados necessários ao perfeito cumprimento das cláusulas contratuais, além de fornecer os materiais e equipamentos, ferramentas e utensílios necessários previstos.

17.2. Controlar a abertura de chamados técnicos assim como acompanhar seu andamento, visando cumprir o Acordo de Níveis de Serviços, expresso no item 3.22.5.14 do Anexo I - Termo de Referência.

17.3. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação, devendo comunicar ao BADESUL a superveniência de fato impeditivo da manutenção dessas condições.

17.4. Utilizar empregados habilitados e com conhecimentos básicos dos serviços a serem executados, em conformidade com as normas e determinações em vigor.

17.5. Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços efetuados em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados.

17.6. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, ficando o BADESUL autorizado a descontar da garantia, caso exigida no edital, ou dos pagamentos devidos ao contratado, o valor correspondente aos danos sofridos.

17.7. Apresentar os empregados devidamente uniformizados e identificados por meio de crachá, além de provê-los com os Equipamentos de Proteção Individual - EPI, quando for o caso.

17.8. Apresentar ao BADESUL, quando for o caso, a relação nominal dos empregados que adentrarão o órgão para a execução do serviço.

17.9. Atender às solicitações do BADESUL quanto à substituição dos empregados alocados, no prazo fixado pela administração, nos casos em que ficar constatado descumprimento das obrigações relativas à execução do serviço.

17.10. Orientar seus empregados quanto à necessidade de acatar as normas internas da Administração.

17.11. Orientar seus empregados a respeito das atividades a serem desempenhadas, alertando-os a não executar atividades não abrangidas pelo contrato.

17.12. Manter preposto nos locais de prestação de serviço, aceito pela Administração, para representá-lo na execução do contrato, quando couber;

17.13. Responder nos prazos legais, em relação aos seus empregados, por todas as despesas decorrentes da execução do serviço e por outras correlatas, tais como salários, seguros de acidentes, indenizações, tributos, vale-refeição, vale-transporte, uniformes, crachás e outras que venham a ser criadas e exigidas pelo Poder Público.

17.14. Fiscalizar regularmente os seus empregados designados para a prestação do serviço, a fim de verificar as condições de execução.

17.15. Comunicar ao BADESUL qualquer anormalidade constatada e prestar os esclarecimentos solicitados.

17.16. Arcar com as despesas decorrentes de qualquer infração cometida por seus empregados quando da execução do serviço objeto deste contrato.

17.17. Realizar os treinamentos que se fizerem necessários para o bom desempenho das atribuições de seus empregados.

17.18. Treinar seus empregados quanto aos princípios básicos de postura no ambiente de trabalho, tratamento de informações recebidas e manutenção de sigilo, comportamento perante situações de risco e atitudes para evitar atritos com servidores, colaboradores e visitantes do órgão.

17.19. Coordenar e supervisionar a execução dos serviços contratados.

17.20. Administrar todo e qualquer assunto relativo aos seus empregados.

17.21. Assumir todas as responsabilidades e tomar as medidas

necessárias ao atendimento dos seus empregados acidentados ou acometidos de mal súbito, por meio do preposto.

17.22. Instruir seus empregados quanto à prevenção de acidentes e de incêndios.

17.23. Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias, comerciais e as demais previstas na legislação específica, cuja inadimplência não transfere responsabilidade ao BADESUL.

17.24. Relatar ao BADESUL toda e qualquer irregularidade verificada no decorrer da prestação dos serviços.

17.25. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de 14 anos; nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre.

17.26. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento ao objeto da licitação, exceto quando ocorrer algum dos eventos arrolados no art. 81 da Lei 13.303/16.

17.27. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato.

17.28. O Contratado deverá, se for o caso, apresentar Programa de Integridade, nos termos da Lei Estadual nº 15.228, de 25 de setembro de 2018 e do seu Regulamento.

17.29. Formalizar a indicação de Preposto da empresa, e substituto eventual, como seu representante legal incluindo nome, cargo, números de telefone, endereços eletrônicos para, em tempo integral durante o período de vigência do contrato, sem ônus adicional, administrar, acompanhar, supervisionar e controlar todo e qualquer assunto relativo aos serviços contratados, respondendo por todos os atos e fatos gerados ou provocados pelos seus funcionários;

17.30. Participar de reuniões com o Gestor do Contrato para alinhamento de expectativas contratuais e entrega de documentos relativos aos serviços contratados;

17.31. Agendar a entrega dos equipamentos ou materiais no ambiente da Contratante, a fim de que seja designado pessoal para acompanhar a entrega;

17.32. Entregar os bens, objeto da contratação, devidamente protegidos e embalados contra danos de transporte e manuseio, contendo manuais e

guias de instalação (impressos e/ou por meio eletrônico), itens, acessórios de hardware e software necessários ao perfeito funcionamento dos equipamentos;

17.33. Desembalar, instalar, configurar e realizar todos os testes necessários à verificação do perfeito funcionamento da solução ofertada;

17.34. Executar fielmente o objeto de acordo com as normas legais e recomendações técnicas;

17.35. Garantir o objeto contratado nos prazos estabelecidos, nas condições e preços consignados em sua proposta comercial devendo estar inclusos todos os custos, impostos, taxas e demais encargos pertinentes à formação do preço;

17.36. Ter pleno conhecimento de todas as condições e peculiaridades inerentes aos serviços a serem executados não podendo invocar posteriormente desconhecimento para cobrança de serviços extras;

17.37. Obter todo e qualquer tipo de licença junto aos órgãos fiscalizadores para o perfeito e efetivo fornecimento da solução ofertada, sem ônus adicional para o contrato;

CLÁUSULA 18ª. DAS OBRIGAÇÕES DO BADESUL

18.1. Exercer o acompanhamento e a fiscalização do objeto, por servidores designados para esse fim, anotando em registro próprio as falhas detectadas, indicando dia, mês e ano, bem como o nome dos empregados eventualmente envolvidos, e encaminhando os apontamentos à Autoridade Administrativa para as providências cabíveis;

18.2. Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com as cláusulas contratuais;

18.3. Notificar a CONTRATADA por escrito da ocorrência de eventuais imperfeições no curso da execução do objeto, fixando prazo para a sua correção;

18.4. Pagar à CONTRATADA o valor resultante da prestação do objeto, no prazo e condições estabelecidas neste contrato;

18.5. Efetuar as retenções tributárias devidas sobre o valor da fatura de serviços da CONTRATADA, nos termos da legislação vigente.

18.6. Vetar o emprego de qualquer produto que considerar incompatível com as especificações apresentadas na proposta da empresa contratada, e que seja inadequado, nocivo ou possa danificar seus bens patrimoniais;

18.7. Permitir o acesso do pessoal da contratada ao local da prestação

do serviço e aos equipamentos de TI, obedecidas as regras e normas de segurança da Contratante e do BADESUL;

18.8. Prestar as informações e os esclarecimentos pertinentes ao serviço que venham a ser solicitados pelos profissionais da empresa contratada ou a seu Preposto;

18.9. Aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis;

18.10. Receber os objetos entregues pela empresa contratada, que estejam em conformidade com a proposta aceita, conforme inspeções a serem realizadas e emitir Termo de Recebimento Definitivo;

18.11. Rejeitar, com a devida justificativa, qualquer material entregue ou serviço executado em desacordo com as especificações e obrigações assumidas pela empresa contratada;

18.12. Indicar os servidores e técnicos que deverão participar da transferência de conhecimento operacional da solução;

18.13. Conferir toda a documentação técnica gerada e apresentada durante a execução dos serviços, efetuando o seu atesto quando ela estiver em conformidade com os padrões de informação e qualidade exigidos;

18.14. Informar à empresa contratada, durante a vigência do contrato, os novos locais para prestação da assistência técnica caso seja necessário o remanejamento de equipamentos para outras localidades;

18.15. Notificar à empresa Contratada, formal, circunstanciada e tempestivamente, as ocorrências ou anormalidades verificadas durante a execução do contrato, para que sejam adotadas as medidas necessárias;

18.16. Decidir e adotar as medidas julgadas cabíveis, em tempo hábil, que ultrapassem a competência do Gestor do Contrato;

18.17. Criar todas as condições físicas, estruturais, elétricas para a instalação e configuração dos equipamentos, sem que isto implique em custos para a Contratada.

CLÁUSULA 19ª. DO RECEBIMENTO DO OBJETO

19.1. Os serviços, caso estejam de acordo com as especificações do Edital e seus Anexos, serão recebidos:

19.1.1. Provisoriamente, por efeito de posterior verificação da conformidade do serviço com as especificações; e

19.1.2. Definitivamente, após verificação da qualidade e quantidade dos serviços e material, quando for o caso, e consequente aceitação.

19.2. A aceitação do objeto não exclui a responsabilidade civil, por vícios

de forma, quantidade, qualidade ou técnicos ou por desacordo com as correspondentes especificações, verificadas posteriormente.

19.3. O serviço e/ou material recusado será considerado como não prestado ou entregue.

19.4. Os custos de retirada e devolução dos materiais recusados, quando inclusos no objeto, bem como quaisquer outras despesas decorrentes, correrão por conta da CONTRATADA.

19.5. O serviço deverá ser prestado nos locais indicados no Termo de Referência.

CLÁUSULA 20ª. DA CONDUTA ÉTICA DO CONTRATADO E DO BADESUL

20.1. O CONTRATADO e o BADESUL comprometem-se a manter a integridade nas relações público-privadas, agindo de boa-fé e de acordo com os princípios da moralidade administrativa e da impessoalidade, além de pautar sua conduta por preceitos éticos e, em especial, por sua responsabilidade socioambiental.

20.2. Em atendimento ao disposto no caput desta Cláusula, a CONTRATADA obriga-se, inclusive, a:

20.2.1. não oferecer, prometer, dar, autorizar, solicitar ou aceitar, direta ou indiretamente, qualquer vantagem indevida, seja pecuniária ou de outra natureza, consistente em fraude, ato de corrupção ou qualquer outra violação de dever legal, relacionada com este Contrato, bem como a tomar todas as medidas ao seu alcance para impedir administradores, empregados, agentes, representantes, fornecedores, contratados ou subcontratados, seus ou de suas controladas, de fazê-lo;

20.2.2. impedir o favorecimento ou a participação de empregado ou dirigente do Badesul na execução do objeto do presente Contrato;

20.2.3. providenciar para que não sejam alocados, na execução do objeto do contrato, familiares de dirigente ou empregado do Badesul, considerando-se familiar o cônjuge, o companheiro ou o parente em linha reta ou colateral, por consanguinidade ou afinidade, até o terceiro grau;

20.2.4. observar o Código de Ética do Badesul vigente ao tempo da contratação, bem como a Política de Conduta e de Integridade das Licitações e Contratos Administrativos do Badesul e a Política Corporativa Anticorrupção do Badesul, assegurando-se de que seus representantes, administradores e todos os profissionais envolvidos na execução do objeto pautem seu comportamento e sua atuação pelos princípios neles constantes; e

20.2.5. adotar, na execução do objeto do contrato, boas práticas de sustentabilidade ambiental, de otimização de recursos, de redução de desperdícios e de redução da poluição.

20.3. O BADESUL recomenda, ao CONTRATADO, considerar em suas práticas de gestão a implantação de programa de integridade estruturado, voltado à prevenção, detecção e remediação da ocorrência de fraudes e atos de corrupção.

20.4. Verificada uma das situações mencionadas nos 20.2.1 e 20.2.2 desta Cláusula, compete ao CONTRATADO afastar imediatamente da execução do Contrato os agentes que impliquem a ocorrência dos impedimentos e favorecimentos aludidos, além de comunicar tal fato ao BADESUL, sem prejuízo de apuração de sua responsabilidade, caso tenha agido de má-fé.

20.5. O CONTRATADO declara ter conhecimento do Código de Ética do Badesul, bem como da Política de Conduta e de Integridade das Licitações e Contratos Administrativos do Badesul e da Política Corporativa Anticorrupção do Badesul, que poderão ser consultados por intermédio do sítio eletrônico www.badesul.com.br ou requisitados ao Gestor do Contrato.

20.6. Eventuais irregularidades ou descumprimentos das normas internas do BADESUL ou da legislação vigente podem ser denunciados à Ouvidoria por qualquer cidadão através dos seguintes canais: e-mail:ouvidoria@badesul.com.br; e telefone (08006425800).

CLÁUSULA 21ª. DAS SANÇÕES

21.1. Sem prejuízo da faculdade de rescisão contratual, o BADESUL poderá aplicar sanções de natureza moratória e punitiva ao contratado, diante do não cumprimento das cláusulas contratuais.

21.2. Com fundamento na Lei 13.303/2016 e Regulamento Interno de Licitações ficará impedida de licitar e contratar com o Badesul, pelo prazo de até 2 (dois) anos, garantida a ampla defesa, sem prejuízo da rescisão unilateral do contrato e da aplicação de multa, o contratado que:

21.2.1. apresentar documentação falsa;

21.2.2. ensejar o retardamento da execução de seu objeto;

21.2.3. falhar na execução do contrato;

21.2.4. fraudar a execução do contrato;

21.2.5. comportar-se de modo inidôneo;

21.2.6. cometer fraude fiscal.

21.3. Configurar-se-á o retardamento da execução quando o contratado:

21.3.1. deixar de iniciar, sem causa justificada, a execução do contrato após 7 (sete) dias contados da data da ordem de serviço ou assinatura do contrato;
21.3.2. deixar de realizar, sem causa justificada, os serviços definidos no contrato por 3 (três) dias seguidos ou por 10 (dez) dias intercalados.
21.4. 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 item 21.13.
21.5. Para os fins do item 21.2.5 reputar-se-ão inidôneos atos tais como os descritos nos arts. 337-F, 337-I, 337-J, 337-K, 337-L e no art. 337-M, §§ 1º e 2º, do Capítulo II-B, do Título XI da Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal).
21.6. O contratado que cometer qualquer das infrações discriminadas no item 21.2 ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:
21.6.1. multa:
21.6.1.1. compensatória de até 10% sobre o valor total atualizado do contrato nos casos de inexecução, execução imperfeita ou em desacordo com as especificações e negligência na execução do objeto contratado, e nos casos de descumprimento de cláusula contratual ou norma de legislação pertinente;
21.6.1.2. moratória de até 0,5% por dia de atraso injustificado sobre o valor da contratação, até o limite de 30 dias.
21.6.2. impedimento de licitar e de contratar com o BADESUL, pelo prazo de até dois anos.
21.7. As multas compensatórias e moratória poderão ser aplicadas cumulativamente, sem prejuízo da aplicação da sanção de impedimento de licitar e de contratar com o BADESUL.
21.8. As sanções decorrentes de fatos diversos serão consideradas independentes entre si, podendo ser aplicadas isoladamente ou, no caso das multas, cumulativamente, sem prejuízo da cobrança de perdas e danos que venham a ser causados ao interesse público e da possibilidade da rescisão contratual.
21.9. A multa dobrará a cada caso de reincidência, não podendo ultrapassar a 30% (trinta por cento) do valor do contrato.
21.10. 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 13.303/2016 e Regulamentos Interno de Licitações do Badesul.
21.11. O valor da multa poderá ser descontado das faturas devidas ao

contratado.

21.12. Se o valor a ser pago ao contratado não for suficiente para cobrir o valor da multa, a diferença será descontada da garantia contratual, se houver.

21.12.1. Se os valores das faturas e da garantia forem insuficientes, fica a contratado obrigada a recolher a importância devida no prazo de 15 (quinze) dias, contados da comunicação oficial.

21.12.2. Esgotados os meios administrativos para cobrança do valor devido pelo contratado ao contratante, o débito será encaminhado para cobrança judicial.

21.12.3. Caso o valor da garantia seja utilizado no todo ou em parte para o pagamento da multa, essa deve ser complementada no prazo de até 10 (dez) dias úteis, contado da solicitação do contratante.

21.13. 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.

21.14. A aplicação de sanções não exime a contratada da obrigação de reparar os danos, perdas ou prejuízos que venha a causar ao ente público.

21.15. As sanções previstas neste item não elidem a aplicação das penalidades estabelecidas na Lei federal nº 12.846/2013, conforme o disposto no seu art. 30 ou nos arts. 337-E a 337-P, Capítulo II-B, do Título XI da Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal).

CLÁUSULA 22ª. DA PROPRIEDADE INTELECTUAL E DIREITO AUTORAL

22.1. Todos os produtos gerados na vigência do contrato serão de propriedade do BADESUL. Isso inclui todos os dados, documentos e elementos de informação pertinentes à tecnologia de concepção, desenvolvimento, fixação em suporte físico de qualquer natureza e aplicação, tais como produtos de software, programas-fonte, classes e componentes, relatórios, diagramas, fluxogramas, modelos e arquivos.

22.2. É vedada a comercialização, a qualquer título, destes por parte da CONTRATADA.

22.3. A utilização de soluções ou componentes proprietários da CONTRATADA ou de terceiros na construção dos programas ou quaisquer artefatos relacionados ao presente contrato, que possam afetar a propriedade do produto, deve ser formal e previamente autorizada pelo BADESUL.

CLÁUSULA 23ª. DO SIGILO DAS INFORMAÇÕES

23.1. Caso a CONTRATADA venha a ter acesso a dados, materiais, documentos e informações de natureza sigilosa, direta ou indiretamente, em decorrência da execução do objeto contratual, deverá manter o sigilo deles, bem como orientar os profissionais envolvidos a cumprir esta obrigação, respeitando-se as diretrizes e normas da Política Corporativa de Segurança da Informação BADESUL.

23.2. Cabe à CONTRATADA cumprir as seguintes regras de sigilo e assegurar a aceitação e adesão às mesmas por profissionais que integrem ou venham a integrar a sua equipe na prestação do objeto deste Contrato, as quais perdurarão, inclusive, após a cessação do vínculo contratual e da prestação dos serviços:

23.2.1. cumprir as diretrizes e normas da Política de Segurança da Informação do BADESUL, necessárias para assegurar a integridade e o sigilo das informações;

23.2.2. não acessar informações sigilosas do BADESUL, salvo quando previamente autorizado por escrito;

23.3. sempre que tiver acesso às informações mencionadas no inciso anterior:

23.3.1. manter sigilo dessas informações, não podendo copiá-las, reproduzi-las, retê-las ou praticar qualquer outra forma de uso que não seja imprescindível para a adequada prestação do objeto deste Contrato;

23.3.2. limitar o acesso às informações aos profissionais envolvidos na prestação dos serviços objeto deste Contrato, os quais deverão estar cientes da natureza sigilosa das informações e das obrigações e responsabilidades decorrentes do uso dessas informações; e

23.3.3. informar imediatamente ao BADESUL qualquer violação das regras de sigilo ora estabelecidas que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo, bem como dos profissionais envolvidos, adotando todas as orientações do BADESUL para remediar a violação;

23.3.4. entregar ao BADESUL, ao término da vigência deste Contrato, todo e qualquer material de propriedade deste, inclusive notas pessoais envolvendo matéria sigilosa e registro de documentos de qualquer natureza que tenham sido criados, usados ou mantidos sob seu controle ou posse, assumindo o compromisso de não utilizar qualquer informação sigilosa a que teve acesso no âmbito deste Contrato;

23.3.5. quando e se assim o Badesul entender necessário, assinar Termos de Confidencialidade a ser disponibilizado pelo BADESUL, devendo nesse caso

ser firmado pelo representante legal da CONTRATADA e pelos profissionais que acessarão informações sigilosas; quando necessária a assinatura de Termo de Confidenciabilidade, esse deverá ser assinado pelos profissionais substitutos.

CLÁUSULA 24ª. DO PROGRAMA DE INTEGRIDADE

24.1. Fica estabelecida a exigência do Programa de Integridade à CONTRATADA de acordo com a Lei nº 15.228/2018, de 25 de setembro de 2018, Capítulo VIII.

24.2. O Programa de Integridade consiste, no âmbito da CONTRATADA, no conjunto de mecanismos e procedimentos internos de integridade, auditoria e incentivo à denúncia de irregularidades e na aplicação efetiva de códigos de ética e de conduta, políticas e diretrizes com o objetivo de detectar e sanar desvios, fraudes, irregularidades e atos ilícitos praticados contra a Administração Pública Estadual.

24.3. O Programa de Integridade deve ser estruturado, aplicado e atualizado de acordo com as características e riscos atuais das atividades da CONTRATADA, a qual, por sua vez, deve garantir o constante aprimoramento e adaptação do referido programa, visando a garantir a sua efetividade.

24.4. A implantação do Programa de Integridade, no âmbito da pessoa jurídica, correrá às suas expensas e dar-se-á no prazo de 180 (cento e oitenta) dias corridos, a partir da data de celebração do contrato.

24.5. Pelo descumprimento da exigência prevista no art. 37 da Lei 15.228/2018, a Administração Pública Estadual aplicará à empresa contratada multa de 0,02% (dois centésimos por cento), por dia, incidente sobre o valor do contrato.

24.6. O montante correspondente à soma dos valores básicos das multas moratórias será limitado a 10% (dez por cento) do valor do contrato.

24.7. O cumprimento da exigência da implantação fará cessar a aplicação da multa.

24.8. O cumprimento da exigência da implantação não implicará ressarcimento das multas aplicadas.

24.9. O não cumprimento da exigência prevista no art. 37 da Lei 15.228/2018, durante o período contratual, acarretará a impossibilidade de nova contratação da empresa com o Estado do Rio Grande do Sul até a sua regular situação, bem como a sua inscrição junto ao Cadastro Informativo das pendências perante órgãos e entidades da Administração Pública Estadual - CADIN/RS, de que trata a Lei nº 10.697, de 12 de janeiro de 1996.

CLÁUSULA 25ª. DA RESCISÃO

25.1. Sem prejuízo das hipóteses e condições de extinção dos contratos previstas no direito privado, a contratação poderá ser rescindida unilateralmente nas seguintes hipóteses:

25.1.1. pelo descumprimento de cláusulas contratuais, especificações, projetos ou prazos;

25.1.2. pelo cumprimento irregular de cláusulas contratuais, especificações, projetos e prazos;

25.1.3. pela lentidão do seu cumprimento, caso comprovada a impossibilidade da conclusão da obra, do serviço ou do fornecimento, nos prazos estipulados;

25.1.4. pelo atraso injustificado no início da obra, serviço ou fornecimento;

25.1.5. pela paralisação da obra, do serviço ou do fornecimento, sem justa causa e prévia comunicação;

25.1.6. pela subcontratação total ou parcial do seu objeto, não admitidas neste contrato;

25.1.7. pela cessão ou transferência, total ou parcial, das obrigações da CONTRATADA à outrem;

25.1.8. pela associação da CONTRATADA com outrem, a fusão, cisão, incorporação, a alteração social ou a modificação da finalidade ou da estrutura da empresa, salvo se não houver prejuízo à execução do contrato e aos princípios da administração pública, se forem mantidas as mesmas condições estabelecidas no contrato original e se forem mantidos os requisitos de habilitação;

25.1.9. pelo desatendimento das determinações regulares do fiscal e do gestor do contrato, assim como as de seus delegados e superiores;

25.1.10. pelo cometimento reiterado de faltas na sua execução, anotadas em registro próprio pela fiscalização;

25.1.11. pela decretação de falência ou a instauração de insolvência civil;

25.1.12. pela dissolução da sociedade ou o falecimento do contratado;

25.1.13. por razões de interesse público, de alta relevância e amplo conhecimento, justificadas e determinadas pelo Diretor da área gestora do contrato, ratificada pelo Diretor Presidente, e exaradas no processo administrativo a que se refere o contrato;

25.1.14. salvo nas hipóteses em que decorrer de ato ou fato do qual tenha praticado, participado ou contribuído a CONTRATADA, assim como em caso de calamidade pública, grave perturbação da ordem interna ou guerra, a suspensão da execução do contrato, por ordem escrita do Badesul, por prazo superior a 120 (cento e vinte) dias, ou ainda por repetidas suspensões que

totalizem o mesmo prazo, independentemente do pagamento obrigatório de indenizações pelas sucessivas e contratualmente imprevistas desmobilizações e mobilizações e outras previstas, assegurado à CONTRATADA, nesses casos, o direito de optar pela suspensão do cumprimento das obrigações assumidas pela CONTRATADA até que seja normalizada a situação;

25.1.15. salvo nas hipóteses indicadas na alínea 25.1.14, o atraso superior a 90 (noventa) dias dos pagamentos devidos pelo Badesul decorrentes de obras, serviços ou fornecimento, ou parcelas destes, já recebidos ou executados, ou a interrupção por mora do Badesul em cumprir obrigação de fazer a ela atribuída pelo contrato pelo mesmo prazo, assegurado à CONTRATADA o direito de optar pela suspensão do cumprimento de suas obrigações até que seja normalizada a situação;

25.1.16. pela não liberação, por parte do Badesul, de área, local ou objeto para execução de obra, serviço ou fornecimento, nos prazos contratuais, bem como das fontes de materiais naturais especificadas no projeto;

25.1.17. pela ocorrência de caso fortuito ou de força maior, regularmente comprovada, impeditiva da execução do contrato;

25.1.18. pelo descumprimento do disposto no inciso XXXIII do art. 7º da Constituição Federal, sem prejuízo das sanções penais cabíveis.

25.2. O termo de rescisão será precedido de Relatório indicativo dos seguintes aspectos, conforme o caso:

25.2.1. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

25.2.2. Relação dos pagamentos já efetuados e ainda devidos;

25.2.3. Indenizações e multas.

CLÁUSULA 26ª. DA CESSÃO DE DIREITO

26.1. A cessão de direitos ou a transferência do presente contrato, no todo ou em parte, é proibida sob pena de rescisão imediata.

CLÁUSULA 27ª. DAS VEDAÇÕES

27.1. É vedado ao contratado:

27.1.1. Caucionar ou utilizar este Contrato para qualquer operação financeira;

27.1.2. Interromper a execução dos serviços sob alegação de inadimplemento por parte do contratante, salvo nos casos previstos em lei.

CLÁUSULA 28ª. DA ANTICORRUPÇÃO

28.1. As Partes, por si e por seus administradores, diretores, empregados e agentes, obrigam-se a:

28.1.1. conduzir suas práticas comerciais de forma ética e em conformidade com os preceitos legais aplicáveis;

28.1.2. repudiar e não permitir qualquer ação que possa constituir ato lesivo nos termos da Lei nº 12.846, de 1º de agosto de 2013, e legislação correlata;

28.1.3. dispor ou comprometer-se a implementar, durante a vigência do Contrato quem mantêm, programa de conformidade e treinamento voltado à prevenção e detecção de violações das regras anticorrupção e dos requisitos estabelecidos no Contrato; notificar imediatamente a outra Parte se tiver conhecimento ou suspeita de qualquer conduta que constitua ou possa constituir prática de suborno ou corrupção referente à negociação, conclusão ou execução do Contrato, e declaram, neste ato, que não realizaram e nem realizarão qualquer pagamento, nem forneceram ou fornecerão benefícios ou vantagens a quaisquer autoridades governamentais, ou a consultores, representantes, parceiros ou terceiros a elas ligados, com a finalidade de influenciar qualquer ato ou decisão da administração pública ou assegurar qualquer vantagem indevida, obter ou impedir negócios ou auferir qualquer benefício indevido.

CLÁUSULA 29ª. DAS OBRIGAÇÕES SOCIOAMBIENTAIS

29.1. As Partes reconhecem a importância e se comprometem por si e por seus colaboradores a respeitar e a contribuir com o cumprimento dos Princípios Constitucionais, dos Direitos e Garantias Fundamentais e dos Direitos Sociais previstos na Constituição Federal, tais como, mas não limitadamente:

29.1.1. evitar qualquer forma de discriminação;

29.1.2. respeitar o meio ambiente;

29.1.3. repudiar o trabalho escravo e infantil;

29.1.4. garantir a liberdade de seus colaboradores em se associarem a sindicatos e negociarem coletivamente direitos trabalhistas;

29.1.5. colaborar para um ambiente de trabalho seguro e saudável;

29.1.6. evitar o assédio moral e sexual;

29.1.7. compartilhar este compromisso de Responsabilidade Social na cadeia de fornecedores;

29.1.8. trabalhar contra a corrupção em todas as suas formas, incluída a

extorsão e o suborno.

CLÁUSULA 30ª. DA PREVENÇÃO À LAVAGEM DE DINHEIRO

30.1. As Partes estão cientes que as pessoas jurídicas se sujeitam à lei brasileira e aos acordos internacionais de prevenção à lavagem de dinheiro e riscos operacionais, mas também às regras e normas de conduta definidas pela Lei nº 12.846, de 1º de agosto de 2013.

30.2. Neste sentido, havendo suspeita de eventual prática ilícita ou em desconformidade com o Contrato, ficará a critério exclusivo da Parte que suspeitar encerrar a relação contratual nos termos da Cláusula de extinção do Contrato firmado, independentemente de justificativa.

CLÁUSULA 31ª. DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

31.1. O CONTRATADO está ciente do inteiro teor da Política de Privacidade e Proteção de Dados Pessoais publicada no sítio do Badesul;

31.2. O CONTRATADO deve manter público e acessível o contato do Encarregado de Dados da empresa.

31.3. A partir da vigência da Lei 13.709/2018 (Lei Geral de Proteção de Dados – LGPD) o CONTRATADO adotará todas as providências necessárias ao adequado tratamento de dados pessoais, observando, dentre outros, os seguintes fundamentos previstos nesta legislação: o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

31.4. Consideram-se dados pessoais qualquer informação relacionada à pessoa natural identificada ou identificável.

31.5. Uma informação que identifica uma pessoa pode ser um dado simples, como um nome, números ou outros identificadores. Em sendo possível identificar um indivíduo diretamente das informações processadas, essas informações podem ser dados pessoais.

31.6. Se não for possível identificar diretamente um indivíduo a partir dessas informações, deverá ser ponderado se ele ainda é identificável, levando-se em consideração outras informações que poderão ser processadas em

conjunto, através de meios razoáveis, para identificar esse indivíduo

31.7. É assegurado ao contratante a realização de diligências para verificar o cumprimento do tratamento de dados pessoais decorrente do presente contrato.

31.8. É assegurado ao contratante o direito de regresso em face da contratada em eventual ação judicial em decorrência do inadequado tratamento dos dados pessoais.

CLÁUSULA 32ª. DA SEGURANÇA DA INFORMAÇÃO

32.1. O CONTRATADO está ciente do inteiro teor da Política de Segurança da Informação e de Segurança Cibernética publicada no sítio do Badesul.

CLÁUSULA 33ª. DAS ALTERAÇÕES

33.1. Eventuais alterações contratuais reger-se-ão pela disciplina do art. 81 da Lei Federal nº. 13.303/2016.

CLÁUSULA 34ª. DOS CASOS OMISSOS

34.1. Os casos omissos serão decididos segundo as disposições contidas na Lei nº. 13.303/2016, nas demais normas de licitações e contratos administrativos e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 - Código de Defesa do Consumidor - e normas e princípios gerais dos contratos.

CLÁUSULA 35ª. DA SUBCONTRATAÇÃO

35.1.1. Para execução do objeto deste Edital não será admitida a subcontratação, sob qualquer pretexto ou alegação.

CLÁUSULA 36ª. DO VALOR FISCAL DO CONTRATO

36.1. O valor estimativo do presente contrato, para fins fiscais, será de até **R$ 00,00 (xxx reais).**

CLÁUSULA 37ª. DAS DISPOSIÇÕES ESPECIAIS

37.1. Se qualquer das partes relevar eventual falta relacionada com a execução deste contrato, tal fato não significa liberação ou desoneração a

qualquer delas.

37.2. As partes considerarão cumprido o contrato quando todas as obrigações aqui estipuladas estiverem efetivamente satisfeitas, nos termos de direito e aceitas pela CONTRATADA.

37.3. Quando for o caso, os direitos patrimoniais e autorais de projetos ou serviços técnicos especializados desenvolvidos pela CONTRATADA ou por seus profissionais passam a ser propriedade do Badesul, sem prejuízo da preservação da identificação dos respectivos autores e da responsabilidade técnica a eles atribuída.

37.4. Haverá consulta prévia ao CADIN/RS, pelo órgão ou entidade competente, nos termos da Lei nº 10.697/1996, regulamentada pelo Decreto nº 36.888/1996.

37.5. O presente contrato somente terá eficácia após publicada a respectiva súmula.

CLÁUSULA 38ª. DAS DISPOSIÇÕES GERAIS

38.1. O Foro para solucionar os litígios que decorrerem da execução deste Termo de Contrato será o da Comarca de Porto Alegre/RS – Justiça Estadual.

38.2. E, assim, por estarem as partes ajustadas e acordadas, lavram e assinam este contrato, em 02 (duas) vias de iguais teor e forma, na presença de 02 (duas)testemunhas, para que produza seus jurídicos efeitos.

Porto Alegre/RS, ... de.....de 20.....

P/ CONTRATANTE:

P/ CONTRATADA:

TESTEMUNHAS