Nível de Classificação	Grupo de acesso
Público	**PRODAM**

PREGÃO ELETRÔNICO SRP Nº 09/2024
(COMPRASNET 90.009/2024)

DOCUMENTO DE ORIGEM: SIGED 972/2024-72

SÍNTESE DO OBJETO E PROCEDIMENTOS

A PRODAM – Processamento de Dados Amazonas S.A, com base na Lei nº 13.303, de 30.06.2016, que regulamenta o Estatuto Jurídico das Empresas Públicas e Sociedades de Economia Mista, Decreto Estadual nº 39.032, de 24.05.2018, que institui o Estatuto Jurídico das Empresas Públicas e Sociedades de Economia Mista no âmbito do Estado do Amazonas, pelas normas de Direito, aplicando-se os princípios do direito administrativo e das normas de licitações e contratos da Administração Pública compatíveis, bem como as demais disposições legais aplicáveis à espécie e também pelo RILC- Regulamento Interno de Licitações e Contratos da PRODAM, pelas normas que o alteraram e pelas condições específicas desta licitação, torna pública a realização de processo licitatório, na modalidade de **PREGÃO ELETRÔNICO**, no critério de julgamento **MENOR PREÇO GLOBAL**, modo de disputa **ABERTO**, a ser realizada na forma abaixo:

1. DO OBJETO

1.1 Contratação de empresa especializada para eventual Aquisição de Serviços Gerenciados de Segurança da Informação destinado a proteção das redes computacionais dos clientes da PRODAM compreendendo a alocação de equipamentos Firewall de Próxima Geração (Next Generation Firewall-NGFW), operação e monitoramento remoto em regime 24x7, software para o gerenciamento centralizado e emissão de relatórios, prestação de serviços para instalação e configuração da solução, suporte técnico do fabricante para o hardware com garantia da solução e licenciamento do software para atualização pelo período de 36 meses, treinamento oficial do fabricante e transferência de conhecimento da solução para a equipe da PRODAM, conforme especificações detalhadas no Termo de Referência, constante do Anexo I, deste Instrumento convocatório.

2. DO LOCAL, DA DATA E HORÁRIO

2.1 O pregão eletrônico será realizado conforme local, data e horários a seguir:

2.1.1 Endereço Eletrônico: https://www.gov.br/compras;
UASG: 927131 – PROCESSAMENTO DE DADOS AMAZONAS – PRODAM – PREGÃO ELETRÔNICO SRP Nº 09/2024

2.1.2 Recebimento das propostas: de 21/08/2024 a 17/09/2024;

2.1.3 Início da sessão de disputa de preços: dia 17/09/2024 às 10h30, de Brasília;

2.2 Todas as referências de tempo no Instrumento convocatório, no Aviso e durante a Sessão pública do Pregão observarão obrigatoriamente o horário de **Brasília – DF** e, dessa forma, serão registradas no sistema eletrônico e na documentação relativa ao certame.

3. ORIGEM DE RECURSOS FINANCEIROS

3.1 A despesa com o pagamento do referido objeto será custeada com recursos próprios da

PRODAM – Processamento de Dados Amazonas S.A.

4. DOS PRAZOS DE PEDIDO DE ESCLARECIMENTO, IMPUGNAÇÃO E RECURSO.

4.1 Para os pedidos de Esclarecimento: Deverão ser encaminhados ao e-mail: licitacoes@prodam.am.gov.br até 03 (três) dias úteis antes da data fixada para a abertura das propostas, devendo a PRODAM responder aos pedidos de esclarecimentos no prazo de 3 (três) dias úteis;

4.2 Para a impugnação do Instrumento convocatório: Deverá ser encaminhada ao e-mail licitacoes@prodam.am.gov.br até 03 (três) dias úteis antes da data inicial fixada para abertura das propostas. A impugnação não possui efeito suspensivo e caberá ao pregoeiro, auxiliado pelos responsáveis pela elaboração do edital e dos anexos, decidir sobre a impugnação no prazo de 03 (três) dias úteis, contado da data de recebimento da impugnação. A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo pregoeiro, nos autos do processo de licitação.

4.3 Recurso:

4.3.1 Concluída a fase de habilitação, qualquer proponente poderá manifestar a intenção de recorrer, imediata e motivadamente, no prazo de 10 (dez) minutos. O proponente que desejar recorrer contra decisões do Pregoeiro poderá fazê-lo, manifestando a intenção de recurso com registro da síntese de suas razões no espaço previsto no próprio sistema eletrônico, sendo necessário juntar memoriais no prazo de 03 (três) dias úteis. Os interessados ficam, desde logo, intimados a apresentar contrarrazões em igual número de dias, que começarão a correr do término do prazo do recorrente.

4.3.2 A falta de manifestação, imediata e motivada, importará à preclusão do direito de recurso.

4.4 Os recursos e contrarrazões de recurso deverão ser preenchidos em campo específico no próprio sistema.

5. DO CREDENCIAMENTO

5.1 Os interessados em participar deste pregão deverão dispor de registro cadastral no SICAF – Sistema De Cadastro Unificado De Fornecedores

5.1.1 O cadastro no SICAF deverá ser feito no Portal de Compras do Governo Federal, no sítio https://www.gov.br/compras, por meio de certificado digital conferido pela Infraestrutura de Chaves Públicas Brasileira – ICP - Brasil.

5.2 O credenciamento junto ao provedor do sistema implica a responsabilidade do licitante ou de seu representante legal e a presunção de sua capacidade técnica para realização das transações inerentes a este Pregão.

5.3 O uso da senha de acesso pelo LICITANTE é de sua responsabilidade exclusiva, incluindo qualquer transação efetuada diretamente ou por seu representante, não cabendo ao provedor do sistema ou à PRODAM, responsabilidade por eventuais danos decorrentes do uso indevido da senha, ainda que por terceiros

5.4 O credenciamento junto ao provedor do sistema implica a responsabilidade legal da LICITANTE

e a presunção de sua capacidade técnica para realização das transações inerentes ao Pregão na forma eletrônica.

5.5 É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais no SICAF e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou desatualização dos dados cadastrais.

5.5.1 A não observância do disposto no subitem anterior poderá ensejar desclassificação no momento da habilitação

6. DAS CONDIÇÕES PARA PARTICIPAÇÃO

6.1. Poderão participar deste processo os interessados que atenderem a todas as exigências contidas neste Instrumento convocatório e seus Anexos.

6.2. Não poderão participar deste pregão os interessados que se enquadrarem em uma ou mais das situações relacionadas no art. 38 da Lei 13.303/16:

6.2.1. Cujo administrador ou sócio detentor de mais de 5% (cinco por cento) do capital social seja diretor ou empregado da empresa pública ou sociedade de economia mista contratante;

6.2.2. Suspensa pela empresa pública ou sociedade de economia mista;

6.2.3. Declarada inidônea pela União, por Estado, pelo Distrito Federal ou pela unidade federativa a que está vinculada a empresa pública ou sociedade de economia mista, enquanto perdurarem os efeitos da sanção;

6.2.4. Constituída por sócio de empresa que estiver suspensa, impedida ou declarada inidônea;

6.2.5. Cujo administrador seja sócio de empresa suspensa, impedida ou declarada inidônea;

6.2.6. 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;

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

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

6.3. É vedada também:

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

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

6.3.2.1 Dirigente de empresa pública ou sociedade de economia mista;

6.3.2.2 Empregado de empresa pública ou sociedade de economia mista cujas atribuições envolvam a atuação na área responsável pela licitação ou contratação;

6.3.2.3 Autoridade do ente público a que a empresa pública ou sociedade de economia mista esteja vinculada.

6.3.3 Cujo proprietário, mesmo na condição de sócio, tenha terminado seu prazo de gestão ou rompido seu vínculo com a respectiva empresa pública ou sociedade de economia mista promotora da licitação ou contratante há menos de 6 (seis) meses.

6.4. As condições de não participação e vedações serão consultadas na etapa de habilitação.

7. DA PARTICIPAÇÃO

7.1. A participação no certame se dará através de prévio credenciamento junto ao provedor do sistema, no site https://www.gov.br/compras, observando a data e os horários limites estabelecidos no **subitem 2.1** deste Instrumento convocatório.

7.2. Os licitantes deverão utilizar o certificado digital para acesso ao sistema.

7.3. Caberá ao licitante acompanhar as operações no sistema eletrônico durante a sessão pública do Pregão, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

7.4. No caso de desconexão com o Pregoeiro no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances, retornando o Pregoeiro, quando possível, sua atuação no certame, sem prejuízo dos atos realizados.

7.5. Quando a desconexão persistir por tempo superior a 10 (dez) minutos, a sessão do Pregão será suspensa e terá reinício somente após comunicação expressa aos participantes através do envio de mensagens pelo próprio sistema, marcando a sessão para continuidade do Pregão, havendo interstício de pelo menos 24 (vinte e quatro) horas entre os mesmos.

8. REGULAMENTO OPERACIONAL DO CERTAME

8.1. O certame será conduzido pelo Pregoeiro designado que terá, em especial, as seguintes atribuições:

I - conduzir a sessão pública;

II - receber, examinar e decidir as impugnações e os pedidos de esclarecimentos ao edital e aos anexos, além de poder requisitar subsídios formais aos responsáveis pela elaboração desses documentos;

III - verificar a conformidade da proposta em relação aos requisitos estabelecidos no edital;

IV - coordenar a sessão pública e o envio de lances;

V - verificar e julgar as condições de habilitação;

VI - sanar erros ou falhas que não alterem a substância das propostas, dos documentos de habilitação e sua validade jurídica;

VII - receber, examinar e decidir os recursos e encaminhá-los à autoridade competente quando mantiver sua decisão;

VIII - indicar o proponente habilitado no certame;

IX - conduzir os trabalhos da equipe de apoio; e

X - encaminhar o processo devidamente instruído à autoridade competente e propor a sua homologação.

Parágrafo único. O pregoeiro poderá solicitar manifestação técnica da assessoria jurídica ou de outros setores do órgão ou da entidade, a fim de subsidiar sua decisão.

9. DO ENVIO DAS PROPOSTAS DE PREÇOS

9.1 O encaminhamento de proposta pressupõe o pleno conhecimento e atendimento às exigências de habilitação previstas no Instrumento convocatório e seus Anexos. O fornecedor será responsável por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras suas propostas e lances.

9.2 As propostas de preços terão seus valores definidos conforme os itens no Anexo 01-A – Modelo de Proposta de Preços.

9.3 Ao apresentar sua proposta e ao formular lances, o licitante concorda especificamente com as seguintes condições:

9.3.1 O objeto ofertado deverá atender a todas as especificações constantes do Anexo I do Instrumento convocatório.

9.4 O prazo de validade da proposta não poderá ser inferior a **90 (noventa)** dias contados da data da Sessão Pública do Pregão.

9.5 Da entrega: Por se tratar de um Pregão pelo Sistema de Registro de Preços – SRP, a Prodam não se obriga a adquirir o objeto licitado, só o fazendo quando houver necessidade, ocasião em que serão formalizados o Contrato / Pedido de Compra / Autorização de Execução de Serviço para atendimento da demanda, conforme especificado no Anexo 1 – Termo de Referência deste instrumento convocatório.

9.5.1 Os preços deverão ser cotados em moeda corrente nacional, sendo neles inclusos todas e quaisquer despesas consideradas para composição dos preços, tais como, transportes, impostos, seguros, tributos diretos e indiretos incidentes sobre o fornecimento do objeto.

9.5.2 A proposta apresentada e levada em conta para efeito de julgamento será da exclusiva e total responsabilidade do licitante, não lhe cabendo o direito de pleitear quaisquer alterações, seja para mais ou para menos.

9.5.3 Local de faturamento: Indicar o Município e o Estado onde será efetuado o faturamento.

9.6 No caso de fornecimento de materiais:

9.6.1 **Diferencial de ICMS -** Para efeito de comprovação da incidência do Imposto Sobre Circulação de Mercadorias e Serviços (ICMS), a PRODAM está enquadrada como contribuinte do ICMS, nas operações interestaduais, com a alíquota de **18%. Para todo material adquirido fora do Estado será recolhido o diferencial de alíquota ao Estado do Amazonas.**

9.6.2 **Forma de apresentação dos preços**: Os licitantes de outros Estados deverão computar aos preços ofertados o percentual diferencial de alíquota de ICMS, **somente para efeito de julgamento**, correspondente a complementação de alíquota que será recolhida pela PRODAM ao Estado do Amazonas (Conforme Anexo 01-A – Modelo de Proposta de Preços). **Quando do envio de sua proposta final este percentual deverá ser expurgado.**

9.6.3 Os licitantes não abrangidos na área da Zona Franca de Manaus, não deverão incluir no seu preço o PIS e COFINS, em virtude da Lei Federal nº 10.996/2004, modificada pela Lei nº 11.945/2009, que estabelece que as vendas de mercadorias para as Zonas de Livre Comércio terão isenção tributária de PIS/COFINS. E ainda a isenção tributária

do Imposto sobre produtos Industrializados – IPI, em conformidade com o Decreto 7.212/2010.

10. ABERTURA DAS PROPOSTAS E DISPUTA

10.1 A partir do horário previsto no edital de licitação, a sessão pública será aberta automaticamente pelo sistema.

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

a. Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.

10.3 Durante o transcurso da sessão pública, os participantes serão informados, em tempo real, do valor do menor lance registrado. O sistema não divulgará o autor dos lances aos demais participantes. Os licitantes serão representados por seus códigos.

10.4 A etapa de lances da sessão pública terá duração de dez minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lances ofertados nos últimos dois minutos do período de duração da sessão pública.

10.5 O sistema informará a proposta de menor preço imediatamente após o encerramento da etapa de lances no período adicional de tempo.

10.6 Encerrada a etapa de lances da sessão pública, o Pregoeiro ratificará a proposta vencedora e solicitará da licitante os documentos descritos no **Anexo 2 – Documentos para habilitação**, para comprovar a regularidade de situação do autor da proposta, e solicitará a proposta comercial, contendo as especificações detalhadas do objeto licitado (preço unitário, preço total, e validade da proposta) atualizada em conformidade com o último lance, ambas no prazo máximo de 2h (duas horas) a contar da solicitação do pregoeiro; documentação essa avaliada conforme este instrumento convocatório. O Pregoeiro verificará, também, o cumprimento às demais exigências para habilitação contidas nos Anexos deste Instrumento convocatório.

10.7 É facultado ao pregoeiro prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante, antes de findo o prazo.

10.8 A critério do pregoeiro, de ofício, quando constatado que o prazo estabelecido no item 10.6 não é suficiente para o envio dos documentos exigidos poderá prorrogar o referido prazo.

11. JULGAMENTO DAS PROPOSTAS

11.1 O Pregoeiro efetuará o julgamento das propostas pelo critério de **MENOR PREÇO GLOBAL,** podendo encaminhar, pelo sistema eletrônico, contraproposta diretamente ao licitante que tenha apresentado o lance de menor valor, para que seja obtido preço melhor, bem como decidir sobre sua aceitação, observados os prazos para fornecimento, especificações técnicas e demais condições definidas neste Instrumento convocatório. O próprio sistema acusará quando houver empate técnico em se tratando de ME/EPP.

11.2 Após a sessão de lances, analisando a aceitabilidade ou não, o Pregoeiro analisará a documentação do arrematante.

11.3 Se a proposta ou lance de menor valor não atender as especificações técnicas e as condições mínimas de habilitação, o Pregoeiro examinará a proposta ou o lance subsequente, verificando a sua aceitabilidade e procedendo à sua habilitação, na ordem de classificação, e assim sucessivamente, até a apuração de uma proposta ou lance que atenda ao Instrumento convocatório.

11.3.1 Ocorrendo a situação a que se refere o subitem anterior, o Pregoeiro poderá negociar com o licitante para que seja obtido preço melhor para a PRODAM.

11.4 A proposta deverá ser apresentada em 01 (uma) via original, na língua portuguesa corrente no Brasil, salvo quanto às expressões técnicas impressas através de edição eletrônica de textos em papel timbrado do proponente, bem como ser redigida de forma clara, legível, sem rasuras, emendas ou entrelinhas.

11.5 Quando necessário, o Pregoeiro poderá solicitar ao proponente que demonstre a exequibilidade de seus preços através de planilha de custos e/ou formação de preços e/ou comprovação de contratos com preços semelhantes, entre outros, para análise e decisão do pregoeiro.

11.6 Constatado o atendimento das exigências fixadas no Instrumento convocatório, a licitante será declarada habilitada do certame pelo Pregoeiro, desde que não haja a manifestação da intenção de interposição de recurso pelas licitantes.

11.7 Caso seja declarada pelas licitantes a intenção de interpor recurso será aberto o prazo legal para recebimento do recurso.

12. DA ADJUDICAÇÃO E HOMOLOGAÇÃO

12.1 Não havendo a intenção de interposição de recurso pelas licitantes, caberá ao Diretor-Presidente da PRODAM deliberar sobre a adjudicação e homologação do objeto ao vencedor do Pregão.

12.2 Havendo recurso, o Diretor-Presidente da PRODAM, após deliberar sobre o mesmo, adjudicará o objeto ao licitante vencedor, homologando também o processo.

12.3 Por se tratar de um pregão para registro de preços, a homologação do resultado desta licitação não implicará em direito à contratação.

13. DA ATA DE REGISTRO DE PREÇOS

13.1 Homologado o resultado da licitação, a PRODAM, respeitadas as ordens de classificação, convocará os interessados para assinatura da **Ata de Registro de Preços** que, após cumpridos os requisitos de publicidade, terá efeito de compromisso de fornecimento nas condições estabelecidas.

13.2 As convocações de que tratam o subitem anterior deverão ser atendidas no prazo máximo de 5 (cinco) dias úteis, prorrogável apenas 1 (uma) única vez e por igual período, desde que a solicitação seja apresentada ainda durante o transcurso do interstício inicial, desde que ocorra motivo justificado e aceito pela PRODAM, sob pena de decair o direito à contratação, sem prejuízo das sanções cabíveis.

13.3 A Ata firmada com os licitantes fornecedores observará o modelo do Anexo 3 – Minuta da Ata de Registro de Preços

13.4 Sempre que o licitante vencedor não atender à convocação, nos termos definidos no subitem

13.2, é facultado à Administração, dentro do prazo e condições estabelecidos, convocar remanescentes, na ordem de classificação, para fazê-lo em igual prazo e nas mesmas condições, ou revogar o item específico, respectivo ou a licitação.

13.5 Ao assinar a Ata de Registro de Preços, a adjudicatária obriga-se a fornecer o objeto a ela adjudicado, quando solicitado, conforme especificações e condições contidas neste Instrumento convocatório, em seus anexos e também na proposta apresentada, prevalecendo, no caso de divergência, as especificações e condições deste Instrumento convocatório.

13.6 A empresa fornecedora ficará obrigada a atender a todas as demandas solicitadas pela PRODAM, durante a vigência da Ata de Registro de Preços, mesmo se a entrega deles decorrente for prevista para data posterior ao seu vencimento.

13.7 Para cada demanda de serviços deverá ser celebrado instrumento de contrato, conforme Anexo 9 – Minuta de Contrato.

13.8 Caso o objeto não corresponda no todo ou em parte ao especificado no instrumento convocatório e seus respectivos anexos, o fornecedor deverá corrigir ou entregar, sem ônus para a PRODAM, o objeto do contrato, sob pena de aplicação de sanções a critério da Administração

13.9 A Ata de Registro de Preços terá validade de 12 (doze) meses contada a partir da data de sua assinatura, podendo ser prorrogada uma única vez por igual período.

14. GARANTIA

14.1 O fornecedor deverá proceder conforme solicitado no termo de referência.

15. OBRIGAÇÕES DO FORNECEDOR

15.1 Assinar a Ata de Registro de Preços.

15.2 Entregar o objeto conforme solicitação documentada no **Pedido de Compra/ Autorização de Execução de Serviços,** obedecendo aos prazos, bem como as especificações, objeto deste Instrumento convocatório.

15.3 Prestar os esclarecimentos que forem solicitados pela PRODAM e atender prontamente a eventuais solicitações/reclamações.

15.4 Dispor-se a toda e qualquer fiscalização da PRODAM, no tocante ao produto, assim como ao cumprimento das obrigações previstas neste Instrumento convocatório

15.5 Prover todos os meios necessários à garantia da plena operacionalidade do objeto contratado, inclusive considerados os casos de greve ou paralisação de qualquer natureza.

15.6 Manter durante toda a execução da Ata de Registro de Preços, em compatibilidade com as obrigações por ela assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

15.7 O fornecedor que se beneficie de tratamento diferenciado na forma do disposto na Lei Complementar Federal nº 123/2006 deverá preencher a declaração exclusiva para Microempresa e/ou Empresa de Pequeno Porte **(Anexo 7)**, a qual **deverá ser apresentada no momento da assinatura de contrato**, com fim de assumir o compromisso de informar à Prodam quaisquer alterações dos limites estabelecidos nos incisos I e II, do artigo 3º da referida Lei.

15.8 O fornecedor que se enquadrar nos limites e valores estabelecidos na Lei Estadual nº 4.370/2018 deverá possuir o Programa de Integridade de Compliance para contratar com a Administração Pública:

15.8.1 Se a empresa possuir o Programa de Integridade implantado deverá apresentar, **no momento da assinatura do contrato**, declaração emitida por empresa legalmente habilitada, informando sua existência nos termos do Art. 9º da citada lei, e a apresentação do checklist **(Anexo 8)** devidamente preenchido.

15.8.2 Caso a empresa não possua o Programa, a implantação deverá ocorrer no prazo de 180 (cento e oitenta) dias corridos, conforme artigo 5º da Lei nº 4.370/2018, contados a partir da data de celebração do contrato, comprovando por meio de declaração, emitida por empresa legalmente habilitada sob pena de multa e rescisão contratual, conforme artigo 6º da lei supracitada.

16. OBRIGAÇÕES DA PRODAM

16.1 Efetuar o registro do fornecedor e firmar a correspondente Ata de Registro de Preços;
16.2 Conduzir os procedimentos relativos a eventuais renegociações dos preços registrados;
16.3 Aplicar as sanções por descumprimento do pactuado na Ata de Registro de Preços;
16.4 Efetuar os pagamentos devidos ao Fornecedor, nas condições estabelecidas neste Instrumento convocatório;
16.5 Promover, por intermédio de colaborador indicado, a fiscalização e o acompanhamento da execução do objeto contratado, para que, durante a vigência da Ata de Registro de Preços, sejam mantidas as condições de habilitação e qualificação exigidas nesta licitação.

17. DO FORNECIMENTO E DO RECEBIMENTO DO OBJETO

17.1 Quando tiver necessidade e disponibilidade financeira, a PRODAM demandará a execução do objeto contratado, nas especificações e quantidades a serem adquiridas, encaminhando ao fornecedor e-mail:
17.2 Observado o prazo de entrega previsto no Anexo 1 – Termo de Referência deste instrumento convocatório, a PRODAM emitirá ao fornecedor, documento de termo de recebimento definitivo com o respectivo atesto dos serviços homologados, quanto à qualidade e quantidade
17.3 A aprovação do objeto pela PRODAM não exclui a responsabilidade civil do fornecedor por vícios de quantidade ou qualidade do mesmo ou disparidades com as especificações estabelecidas no Anexo 1 – Termo de Referência deste instrumento convocatório

18. DO PAGAMENTO

18.1 O prazo de pagamento será conforme estabelecido no Termo de Referência – Anexo 1 deste instrumento, realizado após os atestos e autorizações das áreas competentes da PRODAM.
18.2 Os pagamentos devidos pela PRODAM serão liquidados através de cheque nominal ou, através de depósito em conta corrente indicada pelo fornecedor.

18.3 No ato do pagamento, se houver qualquer multa a descontar, será o valor correspondente deduzido da quantia devida.

18.4 Será exigido do fornecedor quando da apresentação da Nota Fiscal correspondente cópia da seguinte documentação: prova de inscrição regular junto ao Cadastro Nacional de Pessoas Jurídicas (CNPJ), prova de regularidade fiscal e previdenciária, apresentando Certidão Negativa de Débitos relativos a Créditos Tributários Federais e à Dívida Ativa da União (C.N.D.) (portaria conjunta PGFN/RFB nº 1751/2014), prova de regularidade para com o Fundo de Garantia por Tempo de Serviço, Certidão de Regularidade de Situação junto ao F.G.T.S., Prova de regularidade para com a Fazenda Estadual e Municipal do domicílio do fornecedor ou outra equivalente, em validade; Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão 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 (NR)

18.4.1 Conforme disposto na Cláusula 2ª, inciso I, do protocolo ICMS 42, publicado no Diário Oficial da União (DOU) de 15/07/2009 e do Decreto nº 30.775 de 1/12/2010, os fornecedores deverão emitir Nota Fiscal Eletrônica nas compras governamentais, logo o licitante vencedor deverá emitir nota fiscal eletrônica

19. SANÇÕES ADMINISTRATIVAS.

19.1 Aos licitantes que deixarem de entregar a documentação exigida do certame, não mantiverem a proposta, apresentarem declaração ou documentação falsa exigida para o certame, ensejarem o retardamento da execução do certame; não mantiverem a proposta; falharem ou fraudarem a execução da presente aquisição; comportarem-se de modo inidôneo; fizerem declaração falsa ou cometerem fraude fiscal; poderão ser aplicadas, conforme o caso, as seguintes sanções, sem prejuízo da reparação dos danos causados à PRODAM pelo infrator:

19.1.1 Advertência e anotação restritiva no Cadastro de Fornecedores da PRODAM;

19.1.2 Multa;

19.1.3 Suspensão temporária de participação em licitação e impedimento de contratar com a Prodam, não superior a 2 (dois) anos;

19.2 Não será aplicada multa se, comprovadamente, o atraso da entrega do objeto advir de caso fortuito ou motivo de força maior, ambos aceitos pela PRODAM.

19.2 A aplicação das penalidades ocorrerá após defesa prévia do interessado, no prazo de 10 (dez) dias úteis a contar da intimação do ato.

20. DISPOSIÇÕES FINAIS

20.1 A presente licitação não importa necessariamente em contratação, podendo a Administração da PRODAM revogá-la no todo ou em parte, por razões de interesse público, derivadas de fato superveniente comprovado ou anulá-la por ilegalidade, de ofício ou por provocação mediante ato escrito e fundamentado disponibilizado no sistema para o conhecimento dos participantes

da licitação – não gerando a obrigação de indenizar.

20.2 Os proponentes assumem todos os custos de preparação e apresentação de suas propostas e a PRODAM não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

20.3 O proponente é responsável pela fidelidade e legitimidade das informações prestadas e dos documentos apresentados em qualquer fase da licitação. A falsidade de qualquer documento apresentado ou a inverdade das informações nele contidas implicará imediata desclassificação do proponente que o tiver apresentado, ou, caso tenha sido o vencedor, a rescisão do contrato, sem prejuízo das demais sanções cabíveis.

20.4 Após apresentação da proposta, não caberá desistência, salvo por motivo justo decorrente de fato superveniente e aceito pelo Pregoeiro.

20.5 Na contagem dos prazos estabelecidos neste Instrumento convocatório, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expedientes na PRODAM.

20.6 É facultado ao Pregoeiro, ou à Autoridade Superior, em qualquer fase da licitação, promover diligências com vistas a esclarecer ou a complementar a instrução do processo, vedada a inclusão posterior de documento ou informação que deveria constar no ato da sessão pública.

20.7 Os proponentes intimados para prestar quaisquer esclarecimentos adicionais deverão fazê-lo no prazo determinado pelo Pregoeiro, sob pena de desclassificação/inabilitação.

20.8 O desatendimento de exigências formais não essenciais não importará no afastamento do proponente, desde que seja possível a aferição da sua qualificação e a exata compreensão da sua proposta.

20.9 As normas que disciplinam este Pregão serão sempre interpretadas em favor da ampliação da disputa entre os proponentes, desde que não comprometam o interesse da Administração, a finalidade e a segurança da contratação.

20.10 As decisões referentes a este processo licitatório poderão ser comunicadas aos proponentes por qualquer meio de comunicação que comprove o recebimento; ou através por meio do sistema eletrônico através do site https://www.gov.br/compras; ou através da publicação no portal de transparência da PRODAM; ou, ainda, mediante publicação no Diário Oficial do Estado do Amazonas

20.11 Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário e local anteriormente estabelecido, desde que não haja comunicação do Pregoeiro em contrário.

20.12 O Instrumento convocatório encontra-se disponível no site https://www.gov.br/compras, bem como na página da PRODAM na internet, no endereço www.prodam.am.gov.br.

20.13 O foro designado para julgamento de quaisquer questões judiciais resultantes deste instrumento convocatório será o local da realização do certame, considerado aquele a que está vinculado ao Pregoeiro.

20.14 São partes integrantes deste instrumento convocatório:

20.14.1 **Anexo 1** – Termo de Referência;

20.14.1.1 – **Anexo 01-A** – Modelo de Proposta de Preços:

20.14.2 **Anexo 2** – Documentos para Habilitação;

20.14.3 **Anexo 3** – Minuta da Ata de Registro de Preços;
20.14.4 **Anexo 4** – Modelo de Declaração de Fato Superveniente Impeditivo de Habilitação;
20.14.5 **Anexo 5** – Modelo de Declaração Quanto ao Cumprimento às Normas Relativas ao Trabalho do Menor;
20.14.6 **Anexo 6** – Tabela de Preço Máximo;
20.14.7 **Anexo 7** – Modelo de Declaração – Somente para micro e pequenas empresas;
20.14.7 **Anexo 8** – Checklist – Programa de Integridade;
20.14.7 **Anexo 9** – Minuta de Contrato

Manaus (AM), 15 de agosto de 2024.

GILSON DE SENA DA SILVA
Assinado de forma digital por GILSON DE SENA DA SILVA
Dados: 2024.08.19 16:21:11 -04'00'

GILSON DE SENA DA SILVA
Pregoeiro

Nível de Classificação	Grupo de acesso
Público	**PRODAM**

PREGÃO ELETRÔNICO SRP 09/2024

ANEXO 1 – TERMO DE REFERÊNCIA

1. OBJETO DA CONTRATAÇÃO

Contratação do de Serviços Gerenciados de Segurança da Informação destinado a proteção das redes computacionais dos clientes da PRODAM compreendendo a alocação de equipamentos Firewall de Próxima Geração (*Next Generation Firewall-NGFW*), operação e monitoramento remoto em regime 24x7, software para o gerenciamento centralizado e emissão de relatórios, prestação de serviços para instalação e configuração da solução, suporte técnico do fabricante para o hardware com garantia da solução e licenciamento do software para atualizações pelo período de 36 meses, treinamento OFICIAL do fabricante e transferência de conhecimento da solução para a equipe da PRODAM.

2. DEMANDANTE

Este serviço está sendo demandada pela Superintendência de Negócios;

3. JUSTIFICATIVA PARA CONTRATAÇÃO

A PRODAM tem como objetivo organizacional a prestação de serviços especializados em Tecnologia da Informação e Comunicação aos órgãos integrantes da Administração Pública Estadual, prioritariamente. No Art. 5º do seu estatuto, em parágrafo único, estabelece: “Os recursos financeiros obtidos pela PRODAM serão prioritariamente orientados para atualização do parque tecnológico e a capacitação técnica, objetivando a segurança dos dados...”. A PRODAM disponibiliza serviços públicos para o cidadão, presta serviço de tecnologia da informação e comunicação e segurança da informação para grande parte dos órgãos do poder executivo estadual, e necessita dispor de ferramentas para proteção da informação para evitar a exploração de vulnerabilidades no ambiente tecnológico como contaminação por malwares, vazamento de informações e roubo de dados, dentre outros que, se concretizados, podem acarretar prejuízos financeiros e danos à imagem institucional.

Os Appliances de NGFW (Next Generation Firewall) são o primeiro nível de proteção em segurança da informação para as redes de computadores com acesso à Internet. Em virtude do

forte crescimento rede estadual ao longo dos últimos anos, desde 2020 a PRODAM disponibiliza para seus clientes as tecnologias de Firewall do tipo UTM do fabricante SOPHOS, que foram adquiridas pelo processo de PREGÃO ELETRÔNICO SRP N0 06/2019 devidamente protocolado internamente através do SPROWEB N0 3519/2019.

Face ao término da disponibilidade de itens da ARP de NGFW (Next Generation Firewall) da SOPHOS em 28 de agosto de 2023, (ARP no 06-2019) e, em face ao aumento continuado na sofisticação e quantidade de ameaças cibernéticas nos últimos anos no Brasil e no mundo, é imprescindível garantir a continuidade da proteção da rede corporativa aos acessos indevidos oriundos da Internet na rede dos clientes. Portanto, devido as responsabilidades inerentes da empresa PRODAM (Processamento de Dados Amazonas S.A), busca-se disponibilizar equipamentos para prestação dos serviços de segurança da informação aos clientes com APPLIANCE DE NEXT GENERATION FIREWALL que possuam, no mínimo, suporte e administração de banda (QOS), IPS, prevenção contra ameaças de vírus, Spywares, proteção contra bots, Malwares Zero day, filtro de URL, VPN IPSEC e SSL, gerenciamento centralizado, relatoria e serviço de suporte técnico especializado.

Atualmente a solução de segurança adotada pela PRODAM para rede de computadores de seus clientes é composta por um único conjunto de hardware e software com gerenciamento centralizado de segurança capaz de proteger de ameaças externas e internas, bem como controlar o fluxo de dados entre essas redes e a Internet, vem atendendo satisfatoriamente, entretanto sem capacidade de atender novas demandas solicitadas por alguns clientes. Além disso, a ausência de uma solução de antivírus em alguns clientes (SSP, SES, DETRAN etc.) vem elevando a carga sobre os firewalls no que tange ao tráfego de informações ocasionando em parte lentidão na experiência do usuário, conforme registrado do DOD (Documento de Oficialização da Demanda) elaborado pela Superintendência de Negócios que motivou este ETP (Estudo Técnico Preliminar). Vale destacar também que os equipamentos já estão chegando no tempo de vida útil (end-of-life).

O objetivo desta contratação é garantir a continuidade, indispensável e essencial, dos serviços prestados pela PRODAM na camada de proteção de firewall à segurança cibernética da rede corporativa do Estado do Amazonas, já utilizada nos últimos anos e adicionar o Serviço Gerenciado de Segurança, que será imprescindível para garantir a disponibilidade, integridade,

confidencialidade e proteção da infraestrutura tecnológica, dos dados e dos serviços da organização, considerando o planejamento financeiro da organização para este recursos bem como a redução de pessoal no quadro técnico da empresa.

4. ORIGEM DOS RECURSOS

Recursos próprios.

5. TIPO DE LICITAÇÃO

Menor preço global.

6. ITENS DE SERVIÇOS

Item	Descrição	Qtde.
1	SERVIÇO DE PROTEÇÃO DE PERÍMETRO PEQUENO PORTE POR 36 MESES	30
2	SERVIÇO DE PROTEÇÃO DE PERÍMETRO MÉDIO PORTE POR 36 MESES	20
3	SERVIÇO DE PROTEÇÃO DE PERÍMETRO GRANDE PORTE POR 36 MESES	20
4	SERVIÇO DE PROTEÇÃO DE DATACENTER PEQUENO PORTE POR 36 MESES	25
5	SERVIÇO DE PROTEÇÃO DE DATACENTER MÉDIO PORTE POR 36 MESES	20
6	SERVIÇO DE PROTEÇÃO DE DATACENTER GRANDE PORTE POR 36 MESES	4

7. ESPECIFICAÇOES TÉCNICAS DOS SERVIÇOS

7.1. As especificações técnicas do Hardware e Software referente aos equipamentos de Firewall, estarão descritas no Anexo 1-A deste Termo de Referência;

7.2. Implantação das Soluções

7.2.1. Será de inteira responsabilidade da CONTRATADA a correta instalação, configuração e funcionamento dos equipamentos e componentes da solução ofertada. Os equipamentos e componentes serão implementados pela CONTRATADA de acordo com os termos deste TR. Não serão admitidos configurações e ajustes que impliquem no funcionamento do equipamento ou

componente de hardware fora das condições normais recomendadas pelo fabricante;

7.2.2. Todas as atividades envolvidas serão acompanhadas e coordenadas por analistas e técnicos da CONTRATANTE;

7.2.3. A implantação das soluções, quando realizadas no ambiente de produção, poderão ter as atividades realizadas após o expediente (horários noturnos ou em finais de semana e feriados);

7.2.4. A CONTRATADA será responsável por efetuar as atividades de integração da solução de monitoração remota com o ambiente operacional da CONTRATANTE, sem prejuízo aos serviços desta;

7.2.5. A CONTRATADA deverá realizar a implantação das soluções, com configuração, instalação, testes e fornecimento dos hardwares e softwares relacionados, em regime de comodato, para o seguinte escopo:

7.2.5.1. Fornecimento dos APPLIANCES FIREWALL DE PRÓXIMA GERAÇAO com suporte a administração de banda (QOS), licenciado para controle de aplicações;

7.2.5.2. Serviço de IPS (Sistema de Prevenção de Intrusos), para detecção e bloqueio de intrusão nos segmentos protegidos;

7.2.5.3. Serviço de prevenção contra ameaças de vírus, Spywares, proteção contra bots, Malwares Zero day e filtro de URL;

7.2.5.4. Serviço de virtualização de contextos, VPN IPSEC e SSL;

7.2.5.5. Serviço de Sandbox e CDR (Content Disarm & Reconstruction);

7.2.5.6. Serviço de gerenciamento centralizado e alta disponibilidade (HA – High Avaliability) para os clientes da CONTRATANTE com instalação ON SITE, migração, suporte técnico, monitoramento por 36 (trinta e seis) meses;

7.2.6. O processo de implantação deve ser composto das seguintes atividades:

7.2.6.1. Deverá ser realizada uma reunião de kick-off do projeto, nas

instalações do CONTRATANTE, para cada migração dos clientes da PRODAM já existentes ou instalação em futuros novos clientes com a participação do gerente técnico do projeto, dos responsáveis comercial, de design da solução, pelo técnico responsável pela implementação do projeto;

7.2.6.2. O planejamento dos serviços de migração e/ou instalação devem resultar num documento tipo SOW (Scope of Work, em tradução livre, escopo de trabalho). Neste documento devem conter, por cliente da CONTRATANTE, a relação, descrição e quantidades dos produtos fornecidos, descrição da infraestrutura atual e desejada, topologia do ambiente, detalhamento dos serviços que serão executados, premissas do projeto, locais e horários de execução dos serviços, condições de execução dos serviços, pontos de contato do CONTRATANTE e CONTRATADA, cronograma de execução do projeto em etapas, com responsáveis e data e início e fim (se aplicável), relação da documentação a ser entregue ao final da execução dos serviços, responsabilidade do CONTRATANTE e CONTRATADA, plano de gerenciamento de mudanças, itens excluídos no projeto e termo de aceite;

7.2.6.3. Todos os parâmetros a serem configurados deverão ser alinhados entre as partes em reuniões de pré-projeto, devendo a CONTRATADA sugerir as configurações de acordo com normas técnicas e boas práticas, cabendo à contratante a sua aceitação expressa ou recusa nos casos de não atendimento das condições estabelecidas;

7.2.6.4. Os serviços deverão ser realizados por pessoal técnico experiente e certificado pelo fabricante dos equipamentos. Em momento anterior à migração e/ou instalação, a contratante poderá solicitar os comprovantes da qualificação profissional do

técnico que executará os serviços, sendo direito da mesma a sua aceitação ou exigência de troca de profissional no caso de este não satisfizer às condições supramencionadas;

7.2.6.5. Ao término dos serviços deve ser criado um relatório detalhado, por cliente da CONTRATANTE, contendo todos os itens configurados no projeto (relatório as-built), etapas de execução e toda informação pertinente para posterior continuidade e manutenção da solução instalada, como usuários e endereços de acesso, configurações realizadas e o resumo das configurações dos equipamentos. Este relatório deve ser enviado com todas as informações em até 10 (dez) dias corridos após a finalização dos serviços;

7.2.6.6. A CONTRATADA deverá fornecer documentação completa da solução, incluindo especificação do equipamento, características e funcionalidades implementadas, desenho lógico da implantação, comentários e configurações executadas. Deverá conter também todas as configurações executadas em equipamentos de terceiros, quando for o caso;

7.3. Prestação dos Serviços Contínuos

7.3.1. Os serviços deverão ser prestados remotamente, a partir de Centros de Operação de Segurança (SOC) e Rede (NOC) próprios, localizados no Brasil, estritamente de acordo com as especificações deste documento;

7.3.2. Os serviços de monitoração remota da segurança deverão ser realizados pela CONTRATADA, na modalidade 24x7 (vinte e quatro horas por dia, sete dias na semana);

7.3.3. Para a manutenção do hardware e software ofertados, bem como para a prestação de suporte aos serviços de monitoração remota, a CONTRATADA deve possuir infraestrutura de suporte técnico, disponível em período integral, ou seja, 24x7 (vinte e quatro horas por dia, sete dias por semana), nos

seguintes modelos:

7.3.3.1. Suporte técnico remoto: suporte prestado por meio de Central de Atendimento 0800, web, e-mail e fax, para:

- Esclarecimento de dúvidas relacionadas à prestação dos serviços, políticas e regras implementadas, funcionalidade da solução e incidentes de segurança, sendo este atendimento imediato;
- Atendimento às solicitações de alterações (inclusão e exclusão) de políticas e regras;
- Análise e tomada de decisão proativa ou quando solicitado pela CONTRATANTE de ataques e/ou vulnerabilidades de segurança da informação;
- Atendimento às solicitações de log e relatórios;

7.3.3.2. Suporte técnico local: atendimento in-loco, prestados por técnicos capacitados e certificado para a solução de problemas relacionados aos equipamentos e softwares;

7.3.4. As versões dos softwares ofertados pela CONTRATADA sempre deverão estar com a versão mais atual disponível no mercado. A versão anterior:

7.3.4.1. Não poderá permanecer instalada mais do que 03 (três) meses, após o lançamento da última versão homologada ou poderá permanecer instalada por tempo maior, desde que acordado com a CONTRATANTE;

7.3.5. A CONTRATADA deverá disponibilizar, nas instalações da CONTRATANTE, o acesso de leitura ao Serviço de Gestão de Logs e do IPS, que permita aos técnicos da CONTRATANTE de terem acesso aos alarmes de eventos e de correlação dos logs gerados pelos dispositivos de tecnologia da informação e segurança lógica;

7.3.6. O Serviço de Gestão de Logs disponibilizado pela CONTRATADA deverá, de

acordo com a Lei 12.965/2014 (Marco Civil da Internet) Art.15, reter no mínimo 06 (seis) meses de registro de acesso a aplicações de internet (o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados);

7.3.7. O Serviço de Gestão de Logs disponibilizado pela CONTRATADA deverá, de acordo com a Lei 12.965/2014 (Marco Civil da Internet) Art.13, reter no mínimo 01 (um) ano de registro de conexões (o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados);

7.3.8. A CONTRATADA deverá prover, através do Serviço de Gestão de Logs, relatórios de todos os sistemas, portais, websites e serviços hoespedados e providos pela CONTRATANTE que contenham, no mínimo, os seguintes itens:

7.3.8.1. Endereço IP do terminal acessando o Serviço;

7.3.8.2. Informação do Header X-Forward-For, quando aplicável;

7.3.8.3. Porta de Origem do acesso, endereço IP do Destino, Porta de Destino do Acesso;

7.3.8.4. Horário em timestamp EPOCH ou UTC que é logado;

7.3.8.5. URL Logada em acessos do método GET;

7.3.8.6. POST ou Request Body logados;

7.3.9. Serão apresentados pela CONTRATADA, no mínimo, relatórios analíticos mensais contendo o diagnóstico dos ambientes monitorados, obtido através do cruzamento das informações coletadas pelos softwares. Tais relatórios deverão estar disponíveis para a CONTRATANTE a qualquer momento, se solicitado, devendo ser disponibilizados em até 12 (doze) horas após a solicitação;

7.3.10. Os recursos humanos envolvidos na atividade de monitoração remota da segurança deverão ser dedicados às atividades de monitoração, ou seja, os mesmos não poderão executar outras atividades na CONTRATADA;

7.3.11. Os recursos humanos envolvidos na prestação de serviço de monitoração, remota da segurança deverão estar capacitados na solução envolvida. Entende-se por capacitação: profissionais com certificados emitidos pelos fabricantes ou instituições independentes;

7.3.12. A CONTRATADA deverá interagir com os analistas e técnicos da CONTRATANTE para dirimir dúvidas relacionadas ao serviço prestado;

7.3.13. A CONTRATADA deverá disponibilizar 0800 e portal WEB para abertura e acompanhamento de chamados;

7.3.14. Os chamados abertos somente poderão ser fechados após autorização dos analistas designados pela CONTRATANTE;

7.3.15. O fechamento por parte da CONTRATADA que não tenha sido previamente autorizado pela CONTRATANTE, poderá ensejar aplicação de multa a CONTRATADA no valor conforme termo de contrato do valor mensal pelos serviços por ocorrência;

7.3.16. A CONTRATANTE deverá informar as pessoas autorizadas para abrir e fechar chamados junto a CONTRATADA, bem como o meio pelo qual a autorização de fechamento será formalizada;

7.4. Manutenção das Regras e Políticas de versões dos Softwares

7.4.1. Toda e qualquer alteração na configuração da solução (aplicação de novas regras, exclusão de regras, atualização de versões, aplicações de “patches”, etc.) deverão ocorrer mediante autorização formal da CONTRATANTE;

7.4.2. A CONTRATANTE, no momento da migração e/ou implantação da solução, indicará as pessoas que poderão autorizar as referidas alterações;

7.4.3. A CONTRATADA implementará mecanismos que garantem a identificação destas pessoas;

7.4.4. As alterações das configurações deverão ocorrer em horários determinados pela CONTRATANTE;

7.4.5. O tempo de atendimento das solicitações de alterações das políticas e regras feitas pela CONTRATANTE não deverá ultrapassar o SLA (acordo de nível de serviço) especificado neste documento, a contar da efetivação da solicitação;

7.4.6. A CONTRATADA deverá efetuar, em laboratório próprio, os testes necessários antes de implementar qualquer alteração no ambiente de monitoração (políticas, regras, versões, etc.), evitando impactos negativos nos serviços da CONTRATANTE;

7.4.7. A CONTRATANTE poderá solicitar, por escrito, o acesso às senhas de configuração dos equipamentos disponibilizados pela CONTRATADA em regime de comodato;

7.4.8. A CONTRATANTE deverá designar, no mínimo, 02 (duas) pessoas para que possam ter acesso a (s) senha (s), que devem ser fornecidas de forma segura;

7.4.9. A CONTRATANE deverá seguir os procedimentos documentais acordado entre as partes, caso venha a fazer uso deste acesso, e se responsabilizará pelas consequências que porventura possam advir deste acesso;

7.5. Controle dos Serviços Realizados pela CONTRATADA

7.5.1. Para o controle e administração dos serviços realizados pela CONTRATADA, a CONTRATANTE poderá nomear até 02 (dois) representantes autorizados a interagir com aquela. Tais representantes serão responsáveis por:

7.5.1.1. Manter as informações técnicas (configuração do ambiente) atualizadas, bem como dar suporte na implantação e manutenção da solução;

7.5.1.2. Definir as estratégias, políticas e regras a serem implantadas, e analisar os relatórios gerados pelos softwares que compõem a solução;

7.5.1.3. Tomar providências necessárias em caso da ocorrência de algum incidente (análise dos logs, rastreamento da ocorrência).

7.5.2. Para cada solução implantada a CONTRATADA emitirá relatórios definidos pela CONTRATANTE;

7.5.3. A CONTRATADA realizará reuniões mensais, nas dependências da CONTRATANTE, para dirimir dúvidas sobre o serviço contratado, análise e entendimento dos relatórios gerenciais e administrativos e revisão das configurações e procedimentos implementados;

7.5.4. A CONTRATANTE poderá realizar auditoria nas instalações do Centro de Operações de Segurança (SOC) e no Centro de Operações de Rede (NOC), com o objetivo de verificar as instalações físicas, a segurança física e lógica do ambiente, e demais itens exigidos neste documento, desde que previamente acordada com a CONTRATADA;

7.5.5. A CONTRATADA deverá ministrar workshop visando treinar a equipe da CONTRATANTE quanto a: Solução de monitoração remota da segurança implantada;

7.5.6. Apresentação da funcionalidade e dos recursos de cada produto que faz parte da solução.

7.5.7. Armazenamento dos logs de auditoria:

7.5.8. A CONTRATANTE, caso julgue insuficiente as informações gravadas nos arquivos de logs, poderá solicitar alterações na configuração junto à CONTRATADA;

7.5.9. O tempo de retenção dos logs gerados deverá ser conforme definido no item 7.3.6 e 7.3.7 deste Termo. Ao final do contrato, a CONTRATADA não deverá ficar com nenhuma cópia dos mesmos, repassando-os para a CONTRATANTE em meio magnético antes da sua destruição.

7.6. Ocorrência de Incidentes

7.6.1. No caso de detecção de algum incidente de segurança, a CONTRATADA

deverá informar a CONTRATANTE e tomar as devidas providências para conter. Após a contenção do incidente, deverá acionar a CONTRATANTE imediatamente, para que sejam tomadas as medidas corretivas e legais necessárias, de acordo com o procedimento de resposta a incidentes;

7.6.2. Serão considerados incidentes de segurança: os acessos indevidos, instalação de códigos maliciosos, indisponibilização dos serviços (DoS), vazamento de dados pessoais, ataques por força bruta, ou qualquer outra ação que vise prejudicar a funcionalidade dos serviços da CONTRATANTE;

7.6.3. Nos casos onde a CONTRATADA identifique as tentativas de acessos indevidos, de instalação de códigos maliciosos, ou de qualquer outra ação que venham pôr em risco a segurança do ambiente da CONTRATANTE, sem sucesso, mas que seja detectada insistência por parte da pessoa mal-intencionada, deverá realizar ações para garantir a contenção e comunicar imedia- tamente a CONTRATANTE para que possam ser tomadas ações preventivas;

7.6.4. A CONTRATADA deverá disponibilizar todas as informações necessárias (origem do ataque, tipo de ataque, data e hora, logs, etc.) para que sejam apurados os incidentes de segurança reportados;

7.6.5. Dependendo do grau do incidente onde o técnico residente não consiga dar suporte, a CONTRATADA deverá deslocar recurso técnico capaz de dar suporte ao problema, para compor o tempo de resposta da CONTRATANTE, visando dirimir quaisquer dúvidas e dar suporte nas providências a serem customizadas;

7.7. Solução de Hardware e Software da CONTRATADA

7.7.1. Todos os equipamentos ou componentes necessários à prestação dos serviços deverão ser novos e de primeiro uso e não constar, no momento da apresentação da proposta, em listas de end-of-sale, end-of-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. Caso o equipamento venha ser descontinuado, a CONTRATADA deverá substitui-lo antes sem custos adicionais para a CONTRATANTE;

7.7.2. A CONTRATADA deverá apresentar juntamente a sua Proposta uma Carta de cada Fabricante do item proposto declarando que seja Revenda Autorizada/Parceiro e uma empresa capacitada, com profissionais certificados, como Prestador de Serviços do Fabricante;

7.7.3. A CONTRATADA também será responsável pela administração e manutenção do serviço em regime de 24x7x365 para atendimentos remotos e o regime 8x5 para atendimentos que possam ser necessários na forma presencial, durante todo o período do serviço comtemplado nesse Termo de Referência. As tarefas atinentes ao transporte, deslocamento e remessa necessários, seja na implementação, substituição e/ ou remoção de equipamentos defeituosos será de responsabilidade da CONTRATADA;

7.7.4. Os software e hardware necessários para implantação do serviço de monitoração, gerência e administração remota da segurança fazem parte dos serviços a serem prestados pela CONTRATADA durante o prazo do contrato;

7.7.5. A manutenção das licenças do hardware e software necessários, junto aos fabricantes, será de responsabilidade da CONTRATADA, devendo esta, apresentar cópia autenticada das mesmas anualmente à CONTRATANTE;

7.7.6. O hardware e software ofertados deverão ser compatíveis com o ambiente operacional da CONTRATANTE;

7.7.7. A CONTRATADA é responsável pela manutenção preventiva e corretiva do hardware por ela ofertado;

7.7.8. O hardware e o software devem ser fornecidos em regime de comodato;

7.8. Encerramento dos Serviços de Operações de Segurança

7.8.1. Quando do encerramento da prestação do serviço de Operações de Segurança remota e presencial, a CONTRATADA deverá retirar os componentes da solução, comunicando a retirada à CONTRATANTE, por

escrito, com 90 dias de antecedência;

7.8.2. Todas as informações de customização, políticas e regras, logs de auditoria serão disponibilizadas para a CONTRATANTE, em mídia magnética ou via rede, e em seguida eliminadas da base de dados da CONTRATADA.

8. Justificativa para o parcelamento ou não da solução

8.1. O agrupamento dos itens em um lote único, levou em consideração questões técnicas, bem como o ganho de economia em escala, sem prejuízo a ampla competitividade, uma vez que existem no mercado vários fabricantes com capacidade de fornecer a solução na forma em que está agrupada nesta contratação.

8.2. O agrupamento encontra ainda justificativa em decisões já deliberadas pelo TCU sobre a matéria, tais como, o informativo 106 do TCU que traz decisão que “A aquisição de itens diversos em lotes deve estar respaldada em critérios justificantes“, adotando o entendimento do acórdão 5260/2011 – TCU – 1a câmara, de 06/07/2011, que decidiu que “Inexiste ilegalidade na realização de pregão com previsão de adjudicação por lotes, e não por itens, desde que os lotes sejam integrados por itens de uma mesma natureza e que guardem correlação entre si.“

9. CONDIÇÕES PARA PRESTAÇÃO DO SERVIÇO

9.1. A CONTRATADA deve ser revenda autorizada e/ou canal integrador qualificado pelos fabricantes das soluções por ela ofertadas. Sua comprovação será realizada através de declaração do fabricante dirigido especificamente à CONTRATANTE e a este processo licitatório;

9.2. A CONTRATADA deverá possuir equipe especializada e certificada na solução ofertada no acompanhamento dos trabalhos lotados na CONTRATANTE até a conclusão da implantação e transferência de conhecimento;

9.3. A CONTRATADA deverá possuir uma solução de gerenciamento centralizado, gerenciamento centralizado de logs e relatoria conforme ANEXO 1-B;

9.4. A CONTRATANTE poderá solicitar qualquer relatório da solução com uma frequência mensal o que deverá ser provido pela CONTRATADA num prazo máximo de 2 dias úteis;

9.5. Todos os equipamentos ou componentes necessários à prestação dos serviços deverão ser novos e de primeiro uso e não constar, no momento da apresentação da proposta, em listas de end-of-sale, end-of-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. Caso o equipamento venha ser descontinuado, a CONTRATADA deverá substitui-lo antes sem custos adicionais para a CONTRATANTE;

9.6. A CONTRATADA deverá apresentar juntamente a sua Proposta uma Carta de cada Fabricante do item proposto declarando que seja Revenda Autorizada/Parceiro e uma empresa capacitada como Prestador de Serviços do Fabricante;

9.7. A CONTRATADA também será responsável pela administração e manutenção do serviço em regime de 24x7x365 para atendimentos remotos e o regime 8x5 para atendimentos realizados pelo técnico residente e/ou para aqueles atendimentos que possa ser necessário a vinda de um especialista na forma presencial, durante todo o período do serviço comtemplado nesse Edital. As tarefas atinentes ao transporte, deslocamento e remessa necessários, seja na implementação, substituição e/ ou remoção de equipamentos defeituosos será de responsabilidade da CONTRATADA;

9.8. A garantia e cobertura dos serviços será de mesmo prazo do contrato em meses e em caso de necessidade de reparo ou substituição de equipamentos e componentes de algum item fornecido nesse contrato, o mesmo será de responsabilidade da CONTRATADA, devendo ela ainda atender aos critérios/características do equipamento substituído, por outro equivalente ou mesmo superior. O equipamento ou componente que vier a substituir um outro defeituoso, estará sob as mesmas condições de garantia e assistência técnica especificada do que for substituído;

9.9. A CONTRATADA substituirá qualquer solução em que o hardware seja avariado por acidentes, operação indevida ou negligente, transporte, intempéries climáticas, vandalismo, descargas elétricas provenientes de raios e trovões, furações, ventanias, inundações, desabamentos e outros desastres naturais dentro de um percentual estipulado de até 5% dos ativos instalados pela CONTRATADA, acima deste

percentual a CONTRATANTE se responsabilizará pela aquisição dentro da vigência do contrato;

9.10. O percentual de 5% é calculado por item de um contrato que tenha sido efetivamente instalado (emitida uma OS);

9.11. O CONTRATANTE deixará de fazer os pagamentos daqueles itens que estiverem dentro do percentual de 5% até que este item seja substituído pela CONTRATATADA;

9.12. O CONTRATANTE continuará fazendo os pagamentos daqueles itens que superar o percentual de 5% que tenha sido avariado independente se o item tenha sido adquirido ou não;

9.13. Para garantir a qualidade e disponibilidade do serviço, deverá ser disponibilizado pela empresa CONTRATADA uma solução de gerência e relatoria, bem como solução de monitoramento, com estrutura dedicada para a CONTRATANTE, para dar visibilidade e que atenda as características mínimas descritas no ANEXO 1-B. Essas características deverão constar na comprovação ponto-a-ponto que será entregue;

9.14. Fica a critério da CONTRATANTE a solicitação desta ferramenta a qualquer momento após a contratação da solução deste Termo de Referência;

9.15. A ferramenta deve ser acompanhada de todos os itens necessários para operacionalização, tais como: softwares de apoio (sistema operacional, etc) e licenças de softwares;

9.16. A ferramenta deve ser fornecida em forma de appliance físico;

9.17. O *Appliance* Físico ofertado, no mínimo, deve possuir:

9.17.1. Pelo menos 2 interfaces 1000Base-T com conectores RJ-45;

9.17.2. Porta console padrão RJ-45, USB ou RS-232 para permitir o gerenciamento completo através de linha de comando;

9.17.3. Possuir indicadores luminosos (led) para a indicação do status;

9.17.4. Fonte de alimentação com capacidade para operar em tensões de 110V/220V com comutação automática. Deve acompanhar fonte de alimentação redundante interna com operação N+1;

9.17.5. Capacidade para retenção de LOGs de acordo com os mínimos exigidos nos itens 7.3.6 e 7.3.7.

9.18. O serviço de monitoramento 24x7 deverá ser prestado OBRIGATÓRIA E INDISPENSAVELMENTE através de NOCs (Network Operation Center) e SOCs (Security Operation Center) redundantes da empresa CONTRATADA que já deverão estar em pleno funcionamento até a data da assinatura do contrato. Será o ponto único de contato com a equipe técnica da CONTRATANTE para abertura de chamados, incidentes, problemas, dúvidas e requisições relacionadas aos serviços contratados, atuando como a primeira instância de atendimento à CONTRATANTE. Os serviços prestados pelo NOC compreendem, entre outros, no mínimo os seguintes procedimentos:

9.18.1. Monitoramento proativo do ambiente de rede WAN do CONTRATANTE;

9.18.2. Suporte técnico para identificação e resolução de problemas em software e hardware;

9.18.3. Resolução de problemas oriundos de acesso à internet, sites remotos, serviços de rede oferecidos aos funcionários do CONTRATANTE;

9.18.4. Resolução de problemas referente aos meios de Acesso WAN como MPLS e Ethernet;

9.18.5. Suporte em criação de políticas, configurações, parametrizações de quaisquer ordens relativas aos equipamentos ofertados;

9.18.6. Resolução de problemas referente a políticas, configurações, parametrizações de quaisquer ordens relativas aos equipamentos ofertados;

9.18.7. Suporte à criação, geração e parametrização de relatórios e eventos de segurança de quaisquer naturezas detectados e prevenidos pelos equipamentos ofertados;

9.18.8. Encaminhar incidentes ao fabricante da solução;

9.18.9. Suporte em demais configurações de segurança, redundância e gerência;

9.18.10. Suporte, administração e monitoramento das políticas e tarefas de

backup das configurações;

9.18.11. Apoio técnico para tarefas de auditoria e análise de logs;

9.18.12. Agir de forma reativa para incidentes, restabelecimento do serviço o mais rápido possível minimizando o impacto, seja por meio da uma solução de contorno ou definitiva;

9.18.13. Agir de forma proativa aplicando medidas para a boa manutenção a fim de garantir a regularidade da operação do serviço;

9.18.14. Atualização de firmware quando disponibilizado exclusivamente pelo próprio fabricante dos equipamentos deverá ser executada pela CONTRATADA sem custo adicional, sempre mediante autorização da CONTRATANTE;

9.18.15. Fornecimento mensal de indicadores e métricas que permitam quantificar o desempenho e a disponibilidade da operação do serviço;

9.18.16. Fornecimento de relatórios gerenciais, implantação/instalação, configuração, ativação, suporte técnico remoto em regime 24x7 com utilização de central de serviços de atendimento integrado e monitoramento automatizado (24x7x365) aos equipamentos detalhados neste estudo;

9.18.17. Comunicar ao CONTRATANTE, os casos de eminente falha operacional dos equipamentos ou de qualquer outra ação que possa vir a colocar em risco a operação da rede da mesma;

9.18.18. Permitir que a CONTRATANTE defina pessoas do seu Quadro de Funcionários que terão acesso de Administração nos equipamentos disponibilizados e essas pessoas deverão comunicar à empresa CONTRATADA qualquer alteração de configuração realizada nos equipamentos fornecidos nessa contratação e, nessa situação, se responsabilizarão pelos riscos relacionadas as intervenções efetuadas.

10. ACORDO DO NÍVEL DE SERVIÇO

10.1. A CONTRATADA deverá respeitar os tempos máximos de ATENDIMENTOS e ANS (Acordo de Nível de Serviço) abaixo descritos, sob a pena de multa no caso de falhas

em seu integral cumprimento:

TABELA DE ACORDO DE NÍVEL DE SERVIÇO - ANS	
Tipo de Contrato	**Tempo de Atendimento**
Monitoramento	24x7x365
Suporte Técnico	24x7x365
Serviços	**Tempo de Atendimento**
Requisição de Informação, parecer ou relatórios	8h
Requisição de serviço	4h
Incidentes	**Tempo de Atendimento**
Produção impactada	2h
Produção parada	1h
Mudanças	**Tempo de Atendimento**
Substituição de Produto	02 (dois) dias
Requisição de Mudança	24h

11. Treinamento

11.1. TREINAMENTO DE FIREWALL DE PRÓXIMA GERAÇÃO

11.1.1. A CONTRATADA deverá prover treinamento “OFICIAL” de capacitação para até 03 (três) turmas de no mínimo 05 (cinco) colaboradores por turma pertencente exclusivamente ao time técnico da CONTRATANTE;

11.1.2. O treinamento deverá ser executado pelo próprio fabricante ou empresa por ele certificada para essa finalidade;

11.1.3. O treinamento deverá ser promovido em local físico dentro das dependências da CONTRATANTE (Modalidade IN COMPANY) ou local por ela definido;

11.1.4. Ao final dos treinamentos, deverá ser emitido um certificado oficial a todos os participantes e um voucher, também por participante, de realização da prova de certificação oficial da solução adquirida;

11.1.5. O treinamento deverá ocorrer antes da entrega/implantação/migração dos equipamentos;

11.1.6. Realizar a transferência de conhecimento nas etapas de implantação e migração do equipamento;

12. Execução do Contrato

12.1. O Regime de execução do contrato será por empreitada por preço unitário;

12.2. Os serviços deverão ser demandados através de Autorização de Execução de Serviços emitidos pelo setor de compras da PRODAM e autorizados pela Diretoria;

12.3. Uma vez demandado, o serviço terá a duração máxima de vigência do contrato;

12.4. Todos os serviços executados pela empresa CONTRATADA serão acompanhados e fiscalizados pela GESIQ (Gerência de Segurança da Informação e Qualidade), com autoridade para exercer em nome da CONTRATANTE, toda e qualquer ação de orientação geral, controle e fiscalização dos serviços;

12.5. À fiscalização compete, entre outras atribuições:

12.5.1. Verificar a conformidade da execução dos serviços com as normas especificadas e se os procedimentos, materiais e acessórios empregados, são adequados para garantir a qualidade desejada dos serviços, caberá também o direito de rejeitar os materiais que não satisfaçam aos padrões especificados;

12.5.2. Ordenar à CONTRATADA que corrija, refaça ou reconstrua as partes dos serviços executados com erros, imperfeições, que estejam em desacordo com as especificações;

12.5.3. A ação da fiscalização exercida pela CONTRATANTE, não desobriga a empresa CONTRATADA de suas responsabilidades contratuais;

12.6. Não obstante a CONTRATADA seja a única e exclusiva responsável pela execução de todos os serviços, ao CONTRATANTE é reservado o direito de, sem que de

qualquer forma restrinja a plenitude dessa responsabilidade, exercer a mais ampla e completa fiscalização sobre os serviços, por meio de sua Gerência de Segurança da Informação e Qualidade (GESIQ) ou por Comissão de Fiscalização designada pelo CONTRATANTE, podendo para isso:

12.6.1. Exercer a fiscalização dos serviços contratados, de modo a assegurar o efetivo cumprimento da execução do escopo contratado, cabendo-lhe, também realizar a supervisão das atividades desenvolvidas pela CONTRATADA, efetivando avaliação periódica;

12.6.2. Ordenar a imediata retirada do local, bem como a substituição de funcionário da CONTRATADA que estiver sem uniforme ou crachá, que embaraçar ou dificultar a sua fiscalização ou cuja permanência na área, a seu exclusivo critério, julgar inconveniente;

12.6.3. Examinar a (s) Carteira (s) Profissional (is) do (s) funcionário (s) colocado (s) a seu serviço, para comprovar o registro de função profissional;

12.6.4. Executar o aceite dos serviços efetivamente prestados, descontando o equivalente aos não realizados bem como aqueles não aprovados por inconformidade aos padrões estabelecidos, desde que por motivos imputáveis à CONTRATADA, sem prejuízo das demais sanções disciplinadas neste Contrato.

12.6.5. Correrão por conta da CONTRATADA as despesas para efetivo atendimento ao objeto contratado, tais como materiais, equipamentos, acessórios, transporte, tributos, encargos trabalhistas e previdenciários decorrentes de sua execução;

12.7. A CONTRATADA deverá indicar para a Comissão de Fiscalização, antes do início dos serviços e, em até 5 (cinco) dias úteis após a publicação no Diário Oficial do Estado do Amazonas do extrato deste Contrato, preposto que a representará durante a sua vigência, com, no mínimo, as seguintes informações: nome, número do RG, número do telefone e endereço de e-mail;

12.8. A Comissão de Fiscalização terá 5 (cinco) dias úteis para analisar os documentos

entregues e emitir a Autorização para Início dos Serviços.

12.9. As atividades deverão transcorrer em conformidade com o disposto no Termo de Referência, e obedecerão ao seguinte planejamento:

12.9.1. A CONTRATADA realizará a instalação dos equipamentos e softwares, migração, execução de testes de segurança, configuração das regras de detecção e prevenção, transferência de conhecimento e entrega da documentação do serviço no prazo de até 30 (trinta) dias CORRIDOS contados da data indicada pela Comissão de Fiscalização na Autorização para Início dos Serviços;

12.9.2. Na conclusão desta Etapa, a CONTRATADA deverá comunicar à Comissão de Fiscalização o término destas atividades através de um ofício protocolado na secretaria geral da CONTRATANTE;

12.9.3. O CONTRATANTE, por meio do seu Fiscal do contrato, executará a conferência do objeto segundo o Termo de Referência;

12.9.4. Não sendo constatados vícios, funcionamento inadequado ou divergências em relação à especificação e proposta da CONTRATADA, o Fiscal do Contrato comunicará o término desta etapa à Comissão de Fiscalização através da emissão do respectivo Questionário de Avaliação do Fornecedor de Serviços no prazo de até 5 (cinco) dias da comunicação de encerramento desta atividade;

12.9.5. Caso seja constatado qualquer vício, funcionamento inadequado ou divergência em relação à especificação e proposta da CONTRATADA, será expedido um comunicado estabelecendo o prazo máximo de até 15 (quinze) dias corridos e improrrogáveis para que ela solucione os vícios apontados, após o qual será reiniciado o prazo máximo de 5 (cinco) dias corridos para nova conferência e testes de aceite;

12.10. A operação assistida será executada durante os 5 (cinco) dias úteis seguintes, contados da data de emissão do Questionário de Avaliação do Fornecedor;

12.11. Em caso de conformidade com o estabelecido no Termo de Referência, o

CONTRATANTE, por meio do Fiscal do Contrato, comunicará o término desta Etapa à Comissão de Fiscalização através da emissão do respectivo Questionário de Avaliação do Fornecedor de Serviços no prazo de até 5 (cinco) dias da comunicação de encerramento desta atividade;

12.12. Os treinamentos oficiais, conforme descrito no item 10, deverão ser agendados pela CONTRATADA em datas a serem definidas pelo CONTRATANTE, respeitando o limite máximo de 30 (trinta) dias corridos contados a partir da data de emissão do Questionário de Avaliação do Fornecedor;

12.13. Os treinamentos só serão aceitos como concluídos pela CONTRATANTE após o recebimento do certificado oficial da fabricante e recebimento dos vouchers para realização da prova oficial de certificação;

12.14. Após a conclusão dos treinamentos, o CONTRATANTE, por meio do Fiscal do Contrato, comunicará o seu término à Comissão de Fiscalização através da emissão de um Questionário de Avaliação referente ao seu cumprimento no prazo de até 5 (cinco) dias úteis, caso não seja constatada qualquer irregularidade;

12.15. A CONTRATADA prestará os serviços contínuos gerenciados de segurança da informação, compreendendo monitoramento remoto através do NOC, em regime 24x7, durante 36 (trinta e seis) meses contados da data de emissão do Termo de Aceite Técnico;

12.16. Após o término de cada período mensal em que os serviços forem prestados, o Fiscal do Contrato, em posse de todos os relatórios periódicos exigidos no Termo de Referência, a serem produzidos e entregues pela CONTRATADA ao CONTRATANTE, comunicará a sua satisfatória através da emissão do correspondente “Questionário de Avaliação de fornecedor de Serviços” no prazo de até 5 (cinco) dias úteis, caso não seja constatada qualquer irregularidade;

12.17. Eventual indisponibilidade ou irregularidade dos serviços prestados por motivos imputáveis à CONTRATADA ensejarão aplicação de multa por atraso e/ou inexecução dos serviços contratados, previstas na cláusula 6 deste Termo de Referência e na Lei n.º 13.303 de 30 de junho de 2016, e demais sanções cabíveis;

12.18. Para a execução do serviço de treinamento oficial, será permitida a subcontratação desde que atenda todos os critérios do Item 10;

12.19. A proposta de subcontratação, no ato da execução, deverá ser apresentada por escrito, e somente após a aprovação da Comissão de Fiscalização do contrato os serviços a serem realizados pela subcontratada poderão ser iniciados;

12.20. O CONTRATANTE não reconhecerá qualquer vínculo com empresas subcontratadas, sendo que qualquer contato porventura necessário, de natureza técnica, administrativa, financeira ou jurídica que decorra dos trabalhos realizados será mantido exclusivamente com a CONTRATADA, que responderá por seu pessoal técnico e operacional e, também, por prejuízos e danos que eventualmente estas causarem;

12.21. A cada 12 meses, a contar da data de assinatura do contrato, a CONTRATADA poderá solicitar reajustamento de preços dos itens de serviços (itens 2 e 3), considerando seu valor básico atualizado até esta data, visando a manutenção do equilíbrio econômico-financeiro do contrato, devendo para isso apresentar tabelas de custos que evidencie tal necessidade para devida avaliação por parte da CONTRATANTE;

12.22. Será considerado o Índice de Custos de Tecnologia da Informação – ICTI como índice de reajuste de preços;

13. CONDIÇÕES DE PAGAMENTO

13.1. O pagamento ocorrerá mensalmente, de acordo com a apuração da quantidade de serviços demandados na Autorização de Execução de Serviço - AES e devidamente atestados, conforme apresentação de relatório de execução de serviço;

13.2. O pagamento será efetuado mediante apresentação da Nota Fiscal/Fatura e ocorrerá até o 15º (décimo quinto) dia útil do mês subsequente, com os descontos legais (retenções);

13.3. Será de responsabilidade da contratada disponibilizar relatório de execução de serviço junto com a Nota Fiscal/Fatura para apuração de valores;

13.4. A CONTRATADA poderá solicitar reajuste de preços dos itens a cada 12 meses,

visando manter o equilíbrio econômico-financeiro do contrato, desde que apresente tabela de custos justificando a necessidade.

13.5. O reajuste de preços se dará com base no Índice de Custo de Tecnologia da Informação (ICTI) acumulado de 12 (doze) meses, calculado e divulgado pelo Instituto de Pesquisa Econômica Aplicada (IPEA).

14. QUALIFICAÇÃO TÉCNICA

14.1. A LICITANTE deve apresentar no mínimo 03 (três) ATESTADOS de CAPACIDADE TÉCNICA focados em prestação de Serviços Gerenciados de Segurança, 24x7x365, onde foram prestados os serviços: Firewall/VPN, IPS, Filtro Web, conferido por empresas públicas ou privadas e que possuam, pelo menos, 300 (trezentos) hosts gerenciados, devidamente emitidos por entidades públicas e/ou privadas. Os atestados deverão conter as seguintes informações:

14.1.1. Nome, CNPJ e endereço completo do emitente;

14.1.2. Nome da empresa que prestou o serviço ao emitente;

14.1.3. Data de emissão do atestado ou da certidão;

14.1.4. Assinatura e identificação do signatário (nome, cargo ou função que exerce junto à emitente);

14.1.5. Descrição do tipo do serviço executado (ou nome do evento realizado e sua descrição, em caso de licitação para área de turismo, cultura, esporte e lazer) ou dos produtos fornecidos.

14.2. A LICITANTE deverá apresentar documento comprovando ser parceira qualificada dos fabricantes das soluções por ela ofertadas.

15. APRESENTAÇÃO DA PROPOSTA

Tabela de Preços

Item	Descrição	A. Qtd.	Unid	B. Valor Mensal Unitário (R$)	C. Valor Mensal Total(R$) (A*B)	D. Valor Instalação Unitario (R$)	E. Valor Total Global (R$) (C*36)+(A*D)

1	SERVIÇO DE PROTEÇÃO DE PERÍMETRO PEQUENO PORTE POR 36 MESES	30	Mês				
2	SERVIÇO DE PROTEÇÃO DE PERÍMETRO MÉDIO PORTE POR 36 MESES	20	Mês				
3	SERVIÇO DE PROTEÇÃO DE PERÍMETRO GRANDE PORTE POR 36 MESES	20	Mês				
4	SERVIÇO DE PROTEÇÃO DE DATACENTER PEQUENO PORTE POR 36 MESES	25	Mês				
5	SERVIÇO DE PROTEÇÃO DE DATACENTER MÉDIO PORTE POR 36 MESES	20	Mês				
6	SERVIÇO DE PROTEÇÃO DE DATACENTER GRANDE PORTE POR 36 MESES	4	Mês				

Total global da proposta... R$ xxxx,xx

15.1. O valor global da proposta deverá ser a soma da coluna E. Total Global;

15.2. O Total Geral será o valor a ser utilizado como base para os lances do pregão e serão considerados para os 36 meses;

16. OBRIGAÇÕES DA CONTRATADA

16.1. Sujeitar-se a mais ampla e irrestrita fiscalização por parte do CONTRATANTE, prestando todos os esclarecimentos necessários, atendendo às reclamações formuladas e cumprindo todas as orientações, do mesmo, visando fiel desempenho das atividades;

16.2. Responder por quaisquer danos, pessoais ou materiais, ocasionados em face do contrato;

16.3. Aceitar, nas mesmas condições contratuais, os acréscimos ou supressões no objeto do contrato, até o limite de 25% (vinte e cinco por cento) de seu valor atualizado;

16.4. Não transferir a outrem, no todo ou em parte, os serviços contratados, sem prévia e

expressa anuência do CONTRATANTE;

16.5. Repor qualquer material ou bem, pertencente à CONTRATANTE, que for danificado, roubado ou furtado por negligência de seus prepostos;

16.6. Agir segundo as diretrizes do CONTRATANTE e legislação pertinente;

16.7. Cumprir horários e periodicidade para execução dos serviços conforme definido pela CONTRATANTE;

16.8. Proceder ao atendimento extraordinário, em caso de necessidade, respeitada a legislação trabalhista;

16.9. Utilizar, sob sua inteira responsabilidade, toda a compete e indispensável mão-de-obra, devidamente habilitada, treinada e certificada na solução entregue para execução dos serviços contratados, correndo por sua conta o cumprimento das obrigações trabalhistas, sociais, previdenciárias, tributárias e todas as outras previstas nas normas legais pertinentes;

16.10. A inadimplência da CONTRATADA, com referência à encargos, não transfere ao CONTRATANTE a responsabilidade de seu pagamento, nem poderá onerar o objeto deste contrato;

16.11. Indicar preposto do contrato, que a representará durante a vigência do contrato, no prazo de até 5 (cinco) dias úteis da data da publicação do extrato deste contrato, com no mínimo as seguintes informações: nome, número do RG, número do telefone e endereço de e-mail;

16.12. O preposto do contrato realizará todos os atos necessários e compatíveis com os compromissos assumidos no presente ajuste, garantindo seu fiel cumprimento perante o CONTRATANTE;

16.13. A mudança de preposto do Contrato deverá ser formalmente comunicada ao Gestor do Contrato;

16.14. Responsabilizar-se integralmente pelos serviços prestados contratados, nos termos da legislação vigente;

16.15. Manter disciplina nos locais dos serviços, substituindo logo após notificação, qualquer empregado considerado com conduta inconveniente pela CONTRATANTE;

16.16. Responsabilizar seus empregados pelo cumprimento das normas disciplinares determinadas pela CONTRATANTE;

16.17. Fornecer documentação de todas as atividades realizadas;

16.18. Assumir todas as responsabilidades e tomar as medidas necessárias ao atendimento dos seus empregados, acidentados ou com mal súbito;

16.19. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança da CONTRATANTE;

16.20. Atender prontamente quaisquer exigências do representante da Administração, inerentes ao objeto da contratação;

16.21. Manter sigilo de informações que por qualquer meio venha a ter acesso referentes ao CONTRATANTE ou a seus servidores e assinar o “Termo - Termo de Responsabilidade - Fornecedores e Parceiros – Processamento” presente no ANEXO 1-C deste Termo de Referência;

16.22. Manter, durante toda a execução deste Contrato, todas as condições que culminaram em sua habilitação;

16.23. Responsabilizar-se pelos danos causados diretamente ao CONTRATANTE ou a terceiros, decorrentes de culpa ou dolo, na execução deste contrato;

16.24. Refazer os serviços considerados inadequados pelo Comissão de Fiscalização;

16.25. A CONTRATADA em situação de recuperação judicial/extrajudicial deverá comprovar o cumprimento das obrigações do plano de recuperação judicial/extrajudicial sempre que solicitada pela Comissão de Fiscalização e, ainda, na hipótese de substituição ou impedimento do administrador judicial, comunicar imediatamente, por escrito, à Comissão de Fiscalização;

16.26. A CONTRATADA deverá possuir na sua equipe profissionais com as seguintes certificações obrigatórias e indispensáveis em face da complexidade da prestação dos serviços requeridos e ainda mais da rede computacional:

16.26.1. 03 (três) profissionais com nível máximo na solução ofertada;

16.26.2. 05 (cinco) profissionais com nível expert na solução ofertada;

16.26.3. 02 (dois) profissionais com certificação ITIL Foudation;

16.26.4. 01 (um) profissional com certificação PMP (Project Management Professional);

17. OBRIGAÇÕES DA CONTRATANTE

17.1. Proporcionar todas as condições para que a CONTRATADA possa desempenhar seus serviços dentro das normas estabelecidas neste TERMO;

17.2. Exercer a Fiscalização e o acompanhamento do contrato, através do GESIN, por meio de servidores especialmente designados para este fim, independente, do acompanhamento e controle exercidos diretamente pela CONTRATADA;

17.3. Atestar os serviços executados, através do técnico responsável por seu acompanhamento e fiscalização;

17.4. Notificar a CONTRATADA, quando for o caso, sobre a aplicação de eventuais sanções previstas em contrato;

17.5. Notificar a CONTRATADA por meio de seu responsável técnico toda e qualquer ocorrência relacionada com o contrato, tais como, eventuais imperfeições durante sua vigência;

18. SANÇÕES ADMINISTRATIVAS

18.1. O descumprimento injustificado nos prazos de entrega, substituição ou de assistência técnica sujeita a CONTRATADA à multa de 2% (dois por cento) ao dia até o limite de 05 (cinco) dias corridos, contados do encerramento dos prazo estabelecidos neste instrumento, incidentes sobre o valor da obrigação descumprida;

18.2. A partir do 6º (sexto) dia consecutivo de atraso injustificado poderá ser caracterizada a inexecução total da obrigação;

18.3. Poderão ser aplicadas à contratada, nas hipóteses de inexecução total ou parcial das obrigações estipuladas neste instrumento, as seguintes penalidades:

18.3.1. Advertência;

18.3.2. Multa de 10% (dez por cento) sobre o valor da proposta;

18.3.3. Suspensão temporária de participação em licitação e impedimento de contratar com a Administração, por prazo não superior a 02 (dois) anos;

18.3.4. Declaração de inidoneidade para licitar ou contratar com a Administração

Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que o contratado ressarcir a Administração pelos prejuízos resultantes e depois de decorrido o prazo da sanção aplicada com base no inciso anterior;

18.4. A multa, eventualmente imposta à CONTRATADA, será automaticamente descontada da fatura a que fizer jus, acrescida de juros moratórios de 1% (um por cento) ao mês. Caso a CONTRATADA não tenha nenhum valor a receber desta CONTRATANTE, ser-lhe-á concedido o prazo de 05 (cinco) dias úteis, contados de sua intimação, para efetuar o pagamento da multa. Após esse prazo, não sendo efetuado o pagamento, seus dados serão encaminhados ao Órgão competente para que seja inscrita na dívida ativa da União, podendo, ainda a Administração proceder à cobrança judicial da multa;

18.5. As multas previstas nesta seção não eximem a adjudicatária ou contratada da reparação dos eventuais danos, perdas ou prejuízos que seu ato punível venha causar à Administração contratante;

18.6. Por inexecução de quaisquer das obrigações estipuladas, a CONTRATADA estará sujeita, a exclusivo juízo do CONTRATANTE, à indenização dos prejuízos que resultarem da paralisação dos serviços;

19. MATRIZ DE RISCO

19.1. O mapa de risco poderá necessitar de revisão durante a gestão do contrato porque no desenvolvimento dos serviços, situações não previstas por ocasião da elaboração do termo de referência podem ocorrer, vale lembrar que mais perfeito que seja o termo de referência, o mesmo ainda guarda um percentual de 10% de margem de falha, margem esta admissível em termos de gestão de projetos;

19.2. Análise de riscos para cada etapa ou evento de uma contratação, devem ser utilizadas as escalas a seguir para a avaliação dos riscos:

Definir o tratamento para os riscos cuja importância seja superior a 6.

Importância = Probabilidade x Impacto

Risco 1	**Risco:**	Interromper na prestação do Serviço de proteção deFirewall				
	Probabilidade:	3	**Id**	**Dano**	**Impacto**	**Importância do risco**
			1	Ataque à rede da CONTRATANTE	4	12
			2	Interrupção dos serviços prestados	4	12
	Id	**Ação Preventiva**			**Responsável**	
	1	Adquirir a solução com alta disponibilidade			GINFS	
	2	Incluir a contratação do serviço de instalação, suporte, reparo e substituiçãocom SLA no TR			GINFS	
	Id	**Ação de Contingência**			**Responsável**	
	1	Contratar o serviço de instalação, suporte, reparo e substituição			GINFS	
	2	Habilitar o firewall de contingência			GINFS	
Risco 2	**Risco:**	Equipamento não atender a especificação técnica				
	Probabilidade:	3	**Id**	**Dano**	**Impacto**	**Importância do risco**
			1	Funcionalidade contratada não disponível	4	12
			2	Prejuízo financeiro	4	12
	Id	**Ação Preventiva**			**Responsável**	
	1	Realizar parecer técnico			DPSEO	
	Id	**Ação de Contingência**			**Responsável**	
	1	Chamar o 2º colocado			SPACIN	
	Risco:	Equipamento não ser configurado corretamente				
			Id	**Dano**	**Impacto**	**Importância do risco**

Nível de Classificação	Grupo de acesso
Público	**PRODAM**

Risco 3	**Probabilidade:**	2	1	Característica de segurança não habilitada	4	8
			2	Processo judicial e/ou prejuízo financeiro	4	8

Id	**Ação Preventiva**	**Responsável**
1	Validar comprovação de qualificação da mão de obra de suporte técnico durante a fase de classificação	DPSEO
2	Solicitar declaração de capacidade de empresa de porte e serviço semelhante aoda CONTRATANTE	DPSEO

Id	**Ação de Contingência**	**Responsável**
1	Solicitar substituição de técnico indicado	DPSEO

Risco 4	**Risco:**	Serviço não ser entregue corretamente				
	Probabilidade:	2	**Id**	**Dano**	**Impacto**	**Importância do risco**
			1	Deixar a rede vulnerável	4	8
			2	Processo judicial e/ou prejuízo financeiro	4	8

Id	**Ação Preventiva**	**Responsável**
1	Validar comprovação de qualificação da mão de obra de suporte técnico durante afase de classificação	DPSEO
2	Incluir a contratação do serviço com SLA no TR	DPSEO

Id	**Ação de Contingência**	**Responsável**
1	Aplicar sanções	DPSEO

	Risco:	Descumprimento dos prazos na execução dos serviços				
			Id	**Dano**	**Impacto**	**Importância do risco**

Risco 5	**Probabilidade:**	2	1	Não cumprir SLA	4	8
			2	Não solucionar incidente de SI	4	8

Id	**Ação Preventiva**	**Responsável**
1	Incluir sanções no processo licitatório	DPSEO

Id	**Ação de Contingência**	**Responsável**
1	Aplicar sanções previstas em contrato ou legislação aplicável	DPSEO

Risco 6	**Risco:**	Cobrar valores indevidos				
	Probabilidade:	2	**Id**	**Dano**	**Impacto**	**Importância do risco**
			1	Prejuízo Financeiro	1	2

Id	**Ação Preventiva**	**Responsável**
1	Incluir previsão de glosa na fatura	DPSEO

Id	**Ação de Contingência**	**Responsável**
1	Notificar o fornecedor e solicitar correção	DPSEO
2	Aplicar glosa	DPSEO

Quanto ao disposto nas alíneas “b” e “c” do Art. 42-X (Matriz de Riscos) da Lei 13.303/16 (Lei das Estatais), não há, identificada neste Termo de Referência, qualquer fração do objeto em que haverá liberdade da CONTRATADA para inovar em soluções metodológicas ou tecnológicas, em obrigações de resultado ou em termos de modificação das soluções previamente delineadas neste documento.

Manaus, 20 de março de 2024

Jeimy Lima de Oliveira

(DPSEO-Departamento de Segurança e Operações)

Nível de Classificação	Grupo de acesso
Público	**PRODAM**

Salim Silva David

(GINFS-Gerência de Infraestrutura e Serviços de TI)

ANEXO 1-A – ESPECIFICAÇÕES TÉCNICAS

1. QUANTIDADES

Item	Total
SERVIÇO DE PROTEÇÃO DE PERÍMETRO PEQUENO PORTE	**30**
SERVIÇO DE PROTEÇÃO DE PERÍMETRO MÉDIO PORTE	**20**
SERVIÇO DE PROTEÇÃO DE PERÍMETRO GRANDE PORTE	**20**
SERVIÇO DE PROTEÇÃO DE DATACENTER PEQUENO PORTE	**25**
SERVIÇO DE PROTEÇÃO DE DATACENTER MÉDIO PORTE	**20**
SERVIÇO DE PROTEÇÃO DE DATACENTER GRANDE PORTE	**4**

2. ESPECIFICAÇÕES TÉCNICAS

2.1. SERVIÇO DE PROTEÇÃO DE PERÍMETRO PEQUENO PORTE

2.1.1. CARACTERÍSTICAS GERAIS

2.1.1.1. É permitida a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;

2.1.1.2. A solução deverá ser compatível com SNMPv2 e SNMPv3;

2.1.1.3. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos equipamentos desde que obedeçam a todos os requisitos desta especificação;

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

2.1.1.5. Os appliances de segurança devem suportar operar em cluster ativo-ativo e ativo-passivo sem a necessidade de licenças adicionais;

2.1.1.6. Não serão aceitos modelos em listas de end-of-sale, cuja data do fim de vendas seja anterior à data da proposta.

2.1.1.7. Não serão aceitos modelos em lista de end-of-support, cuja data do fim do suporte seja anterior ao fim da vigência do contrato e/ou

do fim do período de garantia e suporte exigido no edital.

2.1.2. CAPACIDADE E QUANTIDADES

2.1.2.1. Throughput de, no mínimo, 650 (seiscentos e cinquenta) Mbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, anti-malware e prevenção de ameaças avançadas (dia zero) habilitados simultaneamente;

2.1.2.2. Suporte a, no mínimo, 700.000 (setecentas mil) conexões ou sessões simultâneas;

2.1.2.3. Suporte a, no mínimo, 15.000 (quinze mil) novas conexões ou sessões por segundo;

2.1.2.4. Throughput de, no mínimo, 1,9 (um vírgula nove) Gbps para conexões VPN;

2.1.2.5. Licenciado ou permitir, pelo menos, 100 conexões ou sessões simultâneas de VPN client-to-site;

2.1.2.6. Possuir, pelo menos, 10 (dez) interfaces de rede 1Gbps UTP;

2.1.2.7. Possuir 1 (uma) interface do tipo console ou similar;

2.1.2.8. O Throughput e as interfaces solicitados neste item deverão ser comprovados através de datasheet público na internet. Não serão aceitas declarações de fabricantes informando números de performance e interfaces. Caso um mesmo Throughput seja apresentado mais de uma vez em diferentes métricas, será considerado o de maior valor;

2.1.3. FUNCIONALIDADES DE FIREWALL

2.1.3.1. Deve suportar autenticação para o serviço NTP.

2.1.3.2. Deve ser possível definir por quais origens de rede são permitidas as conexões do administrador.

2.1.3.3. Deve ser possível restringir o acesso à gerência do equipamento por, pelo menos, endereço IP e Rede.

2.1.3.4. Deve suportar SNMP v2 e v3.

2.1.3.5. Deve ser possível realizar captura de pacotes diretamente na gerência do equipamento.

2.1.3.6. Deve ser possível monitorar a utilização de CPU e memória diretamente na gerência do equipamento.

2.1.3.7. Deve ser possível realizar a configuração do cluster diretamente na gerência do equipamento.

2.1.3.8. Deve ser possível conectar a serviços de DDNS;

2.1.3.9. Deve ser possível configurar o timeout da sessão do administrador na interface web.

2.1.3.10. Deve ser possível configurar a complexidade da senha do administrador e dias para expirar.

2.1.3.11. A solução deve ser capaz de trabalhar com identidades de usuários para propósitos de configurações e logs.

2.1.3.12. A solução deve possibilitar ao administrador realizar a integração com o AD (Active Directory) na própria interface gráfica do produto;

2.1.3.13. A solução deve identificar usuários das seguintes fontes pelo menos:

2.1.3.14. Active Directory: o gateway de segurança deve realizar consulta aos servidores AD para obter informação dos usuários;

2.1.3.15. Autenticação via navegador: para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador;

2.1.3.16. A identificação do usuário registrado no Microsoft Active Directory, deverá ocorrer sem qualquer tipo de agente instalado nos controladores de domínio e estações dos usuários;

2.1.3.17. Na operação para integração com o AD, a operação de cadastro

deve ser realizada na própria gerência do equipamento, de maneira simples e sem utilização de scripts de comando;

2.1.4. FUNCIONALIDADE DE PREVENÇÃO DE AMEAÇAS

2.1.4.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS integrados no próprio equipamento sem a necessidade de uso de quaisquer interfaces ou dispositivos externos.

2.1.4.2. Deve ser possível agendar para que o mecanismo de inspeção receba e implemente atualizações para os ataques emergentes sem a necessidade de reiniciar o equipamento;

2.1.4.3. Deve ser possível realizar a atualização manualmente sem necessidade de internet através da importação do pacote de atualização.

2.1.4.4. Deve incluir a habilidade de detectar e bloquear ataques conhecidos, protegendo, pelo menos, os seguintes ataques conhecidos: SQL Injection, ICMP Denial of Service, força bruta, scanning de portas, CIFS Port overflow, Non Compliant DNS, Non Compliant SMTP, Non Compliant CIFS, Non Compliant MS SQL Server, IKE aggressive Exchange;

2.1.4.5. Deve ser capaz de bloquear tráfego SSH em DNS tunneling;

2.1.4.6. A solução deverá ser capaz de inspecionar e proteger apenas hosts internos ou inspecionar todo o tráfego;

2.1.4.7. A solução deve proteger contra-ataques do tipo envenenamento de cache DNS (DNS Cache Poisoning);

2.1.4.8. A solução deverá possuir pelo menos dois perfis pré-configurados de fábrica para uso imediato e permitir a customização de um perfil;

2.1.4.9. Em cada proteção de segurança, devem estar inclusas

informações como: categoria, tipo de impacto na ferramenta, severidade, e tipo de ação que a solução irá executar;

2.1.4.10. A solução de IPS deve possuir um modo de solução de problemas, que define o uso de perfil de detecção sem modificar as proteções individuais já criadas e customizadas;

2.1.4.11. Deve ser possível criar regras de exceção no IPS para que a solução não faça a inspeção de um tráfego específico por pelo menos proteção, origem, destino, serviço ou porta.

2.1.4.12. Deve ser possível visualizar a lista de proteções disponíveis no equipamento com os detalhes.

2.1.4.13. A solução deve incluir ferramenta própria ou solução de terceiros para mitigar/bloquear a comunicação entre os hosts infectados com bot e operador remoto (command & contrai).

2.1.4.14. A solução deve bloquear arquivos potencialmente maliciosos infectados com malware.

2.1.4.15. A solução de proteção contra malware e bot podem compartilhar a mesma política para facilitar o gerenciamento.

2.1.4.16. A solução de proteção contra malware e bot deve possuir um modo de solução de problemas, que define o uso de perfil de detecção, sem modificar as proteções individuais já criadas e customizadas;

2.1.4.17. Deve ser possível habilitar a trilha das proteções para não logar, criar um log ou gerar um alerta;

2.1.4.18. Deve ser possível criar regras de exceção para que a solução não faça a inspeção de um tráfego específico por escopo, proteção e definir a ação e log para cada uma delas.

2.1.4.19. A solução de anti-malware deve suportar protocolos SMTP e POP 3, FTP, HTTP em qualquer porta;

2.1.4.20. Deve ser possível definir uma política de inspeção para os tipos de arquivos por:

- Inspecionar tipos de arquivos conhecidos que contenham malware;
- Inspecionar todos os tipos de arquivos;
- Inspecionar tipos de arquivos de famílias específicas;

2.1.4.21. Deve bloquear acesso a URLs com malware;

2.1.4.22. Deve ser possível customizar a página exibida para o usuário quando a URL contiver um malware e o acesso for bloqueado;

2.1.5. FILTRO DE CONTEÚDO WEB

2.1.5.1. A solução deverá contar com ferramentas de visibilidade e controle de aplicações web e filtro URL integrada no próprio appliance de segurança que permita a criação de políticas de liberação ou bloqueio baseando-se em aplicações web e URL;

2.1.5.2. A gerência das políticas de segurança de controle de aplicação e controle de URL's deverá ser realizada na mesma interface web de gerenciamento;

2.1.5.3. Deve ser possível configurar o bloqueio a sites e aplicações que representem um risco de segurança e estão categorizadas como spyware, phishing, botnet, spam, anonymizer ou hacking.

2.1.5.4. Deve ser possível configurar o bloqueio a sites com conteúdo inapropriado como sexo, violência, armas, jogos e álcool.

2.1.5.5. Deve configurar regras para permitir ou bloquear aplicações ou páginas da Internet por pelo menos:

- Usuário do Active Directory
- IP
- Rede

2.1.5.6. Deve ser possível configurar o bloqueio de compartilhamento de

arquivos com origem usualmente ilegais como aplicações torrents e peer-to-peer.

2.1.5.7. Deve ser possível configurar manualmente o bloqueio de aplicações ou categorias de sites de aplicações indesejadas.

2.1.5.8. Deve ainda ser possível adicionar uma URL ou aplicação que não está na base de dados.

2.1.5.9. Deve ser possível limitar o consumo de banda de aplicações.

2.1.5.10. A base de aplicações deve ser superior a 2900 aplicações, reconhecendo, pelo menos, as seguintes aplicações: bittorrent, gnutella, skype, facebook, linkedin, twitter, gmail, dropbox, whatsapp, etc;

2.1.5.11. Deve ser possível realizar a recategorização de uma URL através da gerência do equipamento.

2.1.5.12. Deve ser possível customizar e definir a frequência com que serão exibidas as mensagens para os usuários nas seguintes ações:

- Aceitar e informar
- Perguntar

2.1.6. IDENTIFICAÇÃO DE USUÁRIOS

2.1.6.1. A solução deve ser capaz de trabalhar com identidades de usuários para propósitos de configurações e logging.

2.1.6.2. A solução deve possibilitar ao administrador realizar a integração com o AD na própria interface gráfica do produto;

2.1.6.3. A solução deve identificar usuários das seguintes fontes:

2.1.6.4. Active Directory o gateway de segurança deve realizar consulta aos servidores AD para obter informação dos usuários;

2.1.6.5. Autenticação via navegador Para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de

fornecer uma autenticação baseada em navegador;

2.1.6.6. A identificação do usuário registrado no Microsoft Active Directory, deverá ocorrer sem qualquer tipo de agente instalado nos controladores de domínio e estações dos usuários;

2.1.6.7. Na operação para integração com o AD, a operação de cadastro deve ser realizada na própria interface web de gerência, de maneira simples e sem utilização de scritps de comando;

2.1.7. FUNCIONALIDADES DE ACESSO REMOTO

2.1.7.1. A solução deve prover acesso seguro encriptado aos usuários remotos através da Internet;

2.1.7.2. A solução deve prover conectividade através de um cliente instalado no computador do usuário e através do navegador do usuário com conexão segura (HTTPS).

2.1.7.3. Deve suportar pelo menos os seguintes métodos de conexão:

2.1.7.4. Conexão através de cliente instalado no laptop ou desktop do usuário.

2.1.7.5. Conexão através de cliente instalado no smartphone e tablets.

2.1.7.6. Conexão através de navegador com SSL.

2.1.7.7. Conexão através de cliente nativo Windows L2TP.

2.1.7.8. Solução deve suportar alterar a porta padrão 443 para estabelecimento de VPN SSL.

2.1.7.9. A solução deve permitir conexão VPN aos seguintes usuários:

2.1.7.10. Usuários locais na própria base do appliance.

2.1.7.11. Grupos de usuários locais na própria base do appliance.

2.1.7.12. Grupos de usuários do Active Directory.

2.1.7.13. Grupos de usuários Radius.

2.1.7.14. A solução deve permitir atribuir um endereço específico para o usuário remoto.

2.1.8. FUNCIONALIDADE DE VPN SITE-TO-SITE

2.1.8.1. A solução deve prover acesso seguro criptografado entre duas localidades através da Internet;

2.1.8.2. A solução deve estabelecer VPN com o site remoto do próprio fabricante ou de terceiros;

2.1.8.3. A solução deve suportar autenticação com senha ou certificado;

2.1.8.4. Deve suportar, pelo menos, criptografia AES 128 e 256;

2.1.8.5. Deve possuir mecanismo para monitorar a saúde do túnel remoto;

2.2. SERVIÇO DE PROTEÇÃO DE PERÍMETRO MÉDIO PORTE

2.2.1. CARACTERÍSTICAS GERAIS

2.2.1.1. É permitida a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;

2.2.1.2. A solução deverá ser compatível com SNMPv2 e SNMPv3;

2.2.1.3. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos equipamentos desde que obedeçam a todos os requisitos desta especificação;

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

2.2.1.5. Os appliances de segurança devem suportar operar em cluster ativo-ativo e ativo- passivo sem a necessidade de licenças adicionais;

2.2.1.6. Não serão aceitos modelos em listas de end-of-sale, cuja data do fim de vendas seja anterior à data da proposta.

2.2.1.7. Não serão aceitos modelos em lista de end-of-support, cuja data do fim do suporte seja anterior ao fim da vigência do contrato e/ou do fim do período de garantia e suporte exigido no edital.

2.2.2. CAPACIDADE E QUANTIDADES

2.2.2.1. Throughput de, no mínimo, 2 (dois) Gbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, anti-malware e prevenção de ameaças avançadas (dia zero) habilitados simultaneamente;

2.2.2.2. Suporte a, no mínimo, 2.200.000 (duas milhões e duzental mil) conexões ou sessões simultâneas;

2.2.2.3. Suporte a, no mínimo, 66.000 (sessenta e seis mil) novas conexões ou sessões por segundo;

2.2.2.4. Throughput de, no mínimo, 4 (quatro) Gbps para conexões VPN;

2.2.2.5. Licenciado ou permitir, pelo menos, 200 conexões ou sessões simultâneas de VPN client-tosite;

2.2.2.6. Possuir, pelo menos, 10 (dez) interfaces de rede 1Gbps UTP;

2.2.2.7. Possuir, pelo menos, 1 (uma) interface de rede 10Gbps SFP+;

2.2.2.8. Possuir 1 (uma) interface do tipo console ou similar;

2.2.2.9. O Throughput e as interfaces solicitados neste item deverão ser comprovados através de datasheet público na internet. Não serão aceitas declarações de fabricantes informando números de performance e interfaces. Caso um mesmo Throughput seja apresentado mais de uma vez em diferentes métricas, será considerado o de maior valor;

2.2.3. FUNCIONALIDADES DE FIREWALL

2.2.3.1. Deve suportar autenticação para o serviço NTP.

2.2.3.2. Deve ser possível definir por quais origens de rede são permitidas as conexões do administrador.

2.2.3.3. Deve ser possível restringir o acesso à gerência do equipamento por, pelo menos, endereço IP e Rede.

2.2.3.4. Deve suportar SNMP v2 e v3.

2.2.3.5. Deve ser possível realizar captura de pacotes diretamente na gerência do equipamento.

2.2.3.6. Deve ser possível monitorar a utilização de CPU e memória diretamente na gerência do equipamento.

2.2.3.7. Deve ser possível realizar a configuração do cluster diretamente na gerência do equipamento.

2.2.3.8. Deve ser possível conectar a serviços de DDNS;

2.2.3.9. Deve ser possível configurar o timeout da sessão do administrador na interface web.

2.2.3.10. Deve ser possível configurar a complexidade da senha do administrador e dias para expirar.

2.2.3.11. A solução deve ser capaz de trabalhar com identidades de usuários para propósitos de configurações e logs.

2.2.3.12. A solução deve possibilitar ao administrador realizar a integração com o AD (Active Directory) na própria interface gráfica do produto;

2.2.3.13. A solução deve identificar usuários das seguintes fontes pelo menos:

2.2.3.14. Active Directory: o gateway de segurança deve realizar consulta aos servidores AD para obter informação dos usuários;

2.2.3.15. Autenticação via navegador: para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador;

2.2.3.16. A identificação do usuário registrado no Microsoft Active Directory, deverá ocorrer sem qualquer tipo de agente instalado nos controladores de domínio e estações dos usuários;

2.2.3.17. Na operação para integração com o AD, a operação de cadastro deve ser realizada na própria gerência do equipamento, de

maneira simples e sem utilização de scripts de comando;

2.2.4. FUNCIONALIDADE DE PREVENÇÃO DE AMEAÇAS

2.2.4.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS integrados no próprio equipamento sem a necessidade de uso de quaisquer interfaces ou dispositivos externos.

2.2.4.2. Deve ser possível agendar para que o mecanismo de inspeção receba e implemente atualizações para os ataques emergentes sem a necessidade de reiniciar o equipamento;

2.2.4.3. Deve ser possível realizar a atualização manualmente sem necessidade de internet através da importação do pacote de atualização.

2.2.4.4. Deve incluir a habilidade de detectar e bloquear ataques conhecidos, protegendo, pelo menos, os seguintes ataques conhecidos: SQL Injection, ICMP Denial of Service, força bruta, scanning de portas, CIFS Port overflow, Non Compliant DNS, Non Compliant SMTP, Non Compliant CIFS, Non Compliant MS SQL Server, IKE aggressive Exchange;

2.2.4.5. Deve ser capaz de bloquear tráfego SSH em DNS tunneling;

2.2.4.6. A solução deverá ser capaz de inspecionar e proteger apenas hosts internos ou inspecionar todo o tráfego;

2.2.4.7. A solução deve proteger contra-ataques do tipo envenenamento de cache DNS (DNS Cache Poisoning);

2.2.4.8. A solução deverá possuir pelo menos dois perfis pré-configurados de fábrica para uso imediato e permitir a customização de um perfil;

2.2.4.9. Em cada proteção de segurança, devem estar inclusas informações como: categoria, tipo de impacto na ferramenta,

severidade, e tipo de ação que a solução irá executar;

2.2.4.10. A solução de IPS deve possuir um modo de solução de problemas, que define o uso de perfil de detecção sem modificar as proteções individuais já criadas e customizadas;

2.2.4.11. Deve ser possível criar regras de exceção no IPS para que a solução não faça a inspeção de um tráfego específico por pelo menos proteção, origem, destino, serviço ou porta.

2.2.4.12. Deve ser possível visualizar a lista de proteções disponíveis no equipamento com os detalhes.

2.2.4.13. A solução deve incluir ferramenta própria ou solução de terceiros para mitigar/bloquear a comunicação entre os hosts infectados com bot e operador remoto (command & contrai).

2.2.4.14. A solução deve bloquear arquivos potencialmente maliciosos infectados com malware.

2.2.4.15. A solução de proteção contra malware e bot podem compartilhar a mesma política para facilitar o gerenciamento.

2.2.4.16. A solução de proteção contra malware e bot deve possuir um modo de solução de problemas, que define o uso de perfil de detecção, sem modificar as proteções individuais já criadas e customizadas;

2.2.4.17. Deve ser possível habilitar a trilha das proteções para não logar, criar um log ou gerar um alerta;

2.2.4.18. Deve ser possível criar regras de exceção para que a solução não faça a inspeção de um tráfego específico por escopo, proteção e definir a ação e log para cada uma delas.

2.2.4.19. A solução de anti-malware deve suportar protocolos SMTP e POP 3, FTP, HTTP em qualquer porta;

2.2.4.20. Deve ser possível definir uma política de inspeção para os tipos

de arquivos por:

- Inspecionar tipos de arquivos conhecidos que contenham malware;
- Inspecionar todos os tipos de arquivos;
- Inspecionar tipos de arquivos de famílias específicas;

2.2.4.21. Deve bloquear acesso a URLs com malware;

2.2.4.22. Deve ser possível customizar a página exibida para o usuário quando a URL contiver um malware e o acesso for bloqueado;

2.2.5. FILTRO DE CONTEÚDO WEB

2.2.5.1. A solução deverá contar com ferramentas de visibilidade e controle de aplicações web e filtro URL integrada no próprio appliance de segurança que permita a criação de políticas de liberação ou bloqueio baseando-se em aplicações web e URL;

2.2.5.2. A gerência das políticas de segurança de controle de aplicação e controle de URL's deverá ser realizada na mesma interface web de gerenciamento;

2.2.5.3. Deve ser possível configurar o bloqueio a sites e aplicações que representem um risco de segurança e estão categorizadas como spyware, phishing, botnet, spam, anonymizer ou hacking.

2.2.5.4. Deve ser possível configurar o bloqueio a sites com conteúdo inapropriado como sexo, violência, armas, jogos e álcool.

2.2.5.5. Deve configurar regras para permitir ou bloquear aplicações ou páginas da Internet por pelo menos:

- Usuário do Active Directory
- IP
- Rede

2.2.5.6. Deve ser possível configurar o bloqueio de compartilhamento de arquivos com origem usualmente ilegais como aplicações torrents

e peer-to-peer.

2.2.5.7. Deve ser possível configurar manualmente o bloqueio de aplicações ou categorias de sites de aplicações indesejadas.

2.2.5.8. Deve ainda ser possível adicionar uma URL ou aplicação que não está na base de dados.

2.2.5.9. Deve ser possível limitar o consumo de banda de aplicações.

2.2.5.10. A base de aplicações deve ser superior a 2900 aplicações, reconhecendo, pelo menos, as seguintes aplicações: bittorrent, gnutella, skype, facebook, linkedin, twitter, gmail, dropbox, whatsapp, etc;

2.2.5.11. Deve ser possível realizar a recategorização de uma URL através da gerência do equipamento.

2.2.5.12. Deve ser possível customizar e definir a frequência com que serão exibidas as mensagens para os usuários nas seguintes ações:

- Aceitar e informar
- Perguntar

2.2.6. IDENTIFICAÇÃO DE USUÁRIOS

2.2.6.1. A solução deve ser capaz de trabalhar com identidades de usuários para propósitos de configurações e logging.

2.2.6.2. A solução deve possibilitar ao administrador realizar a integração com o AD na própria interface gráfica do produto;

2.2.6.3. A solução deve identificar usuários das seguintes fontes:

2.2.6.4. Active Directory o gateway de segurança deve realizar consulta aos servidores AD para obter informação dos usuários;

2.2.6.5. Autenticação via navegador Para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador;

2.2.6.6. A identificação do usuário registrado no Microsoft Active Directory, deverá ocorrer sem qualquer tipo de agente instalado nos controladores de domínio e estações dos usuários;

2.2.6.7. Na operação para integração com o AD, a operação de cadastro deve ser realizada na própria interface web de gerência, de maneira simples e sem utilização de scritps de comando;

2.2.7. FUNCIONALIDADES DE ACESSO REMOTO

2.2.7.1. A solução deve prover acesso seguro encriptado aos usuários remotos através da Internet;

2.2.7.2. A solução deve prover conectividade através de um cliente instalado no computador do usuário e através do navegador do usuário com conexão segura (HTTPS).

2.2.7.3. Deve suportar pelo menos os seguintes métodos de conexão:

2.2.7.4. Conexão através de cliente instalado no laptop ou desktop do usuário.

2.2.7.5. Conexão através de cliente instalado no smartphone e tablets.

2.2.7.6. Conexão através de navegador com SSL.

2.2.7.7. Conexão através de cliente nativo Windows L2TP.

2.2.7.8. Solução deve suportar alterar a porta padrão 443 para estabelecimento de VPN SSL.

2.2.7.9. A solução deve permitir conexão VPN aos seguintes usuários:

2.2.7.10. Usuários locais na própria base do appliance.

2.2.7.11. Grupos de usuários locais na própria base do appliance.

2.2.7.12. Grupos de usuários do Active Directory.

2.2.7.13. Grupos de usuários Radius.

2.2.7.14. A solução deve permitir atribuir um endereço específico para o usuário remoto.

2.2.8. FUNCIONALIDADE DE VPN SITE-TO-SITE

2.2.8.1. A solução deve prover acesso seguro criptografado entre duas localidades através da Internet;

2.2.8.2. A solução deve estabelecer VPN com o site remoto do próprio fabricante ou de terceiros;

2.2.8.3. A solução deve suportar autenticação com senha ou certificado;

2.2.8.4. Deve suportar, pelo menos, criptografia AES 128 e 256;

2.2.8.5. Deve possuir mecanismo para monitorar a saúde do túnel remoto;

2.3. SERVIÇO DE PROTEÇÃO DE PERÍMETRO GRANDE PORTE

2.3.1. CARACTERÍSTICAS GERAIS

2.3.1.1. É permitida a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;

2.3.1.2. A solução deverá ser compatível com SNMPv2 e SNMPv3;

2.3.1.3. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos equipamentos desde que obedeçam a todos os requisitos desta especificação;

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

2.3.1.5. Os appliances de segurança devem suportar operar em cluster ativo-ativo e ativo- passivo sem a necessidade de licenças adicionais;

2.3.1.6. Não serão aceitos modelos em listas de end-of-sale, cuja data do fim de vendas seja anterior à data da proposta.

2.3.1.7. Não serão aceitos modelos em lista de end-of-support, cuja data do fim do suporte seja anterior ao fim da vigência do contrato e/ou do fim do período de garantia e suporte exigido no edital.

2.3.2. CAPACIDADE E QUANTIDADES

2.3.2.1. Throughput de, no mínimo, 2,8 (dois vírgula oito) Gbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, anti-malware e prevenção de ameaças avançadas (dia zero) habilitados simultaneamente;

2.3.2.2. Suporte a, no mínimo, 3.000.000 (três milhões) conexões ou sessões simultâneas;

2.3.2.3. Suporte a, no mínimo, 90.000 (noventa mil) novas conexões ou sessões por segundo;

2.3.2.4. Throughput de, no mínimo, 5 (cinco) Gbps para conexões VPN;

2.3.2.5. Licenciado ou permitir, pelo menos, 500 conexões ou sessões simultâneas de VPN client-to-site;

2.3.2.6. Possuir, pelo menos, 12 (doze) interfaces de rede 1Gbps UTP;

2.3.2.7. Possuir, pelo menos, 4 (quatro) interface de rede 10Gbps SFP+;

2.3.2.8. Possuir 1 (uma) interface do tipo console ou similar;

2.3.2.9. O Throughput e as interfaces solicitados neste item deverão ser comprovados através de datasheet público na internet. Não serão aceitas declarações de fabricantes informando números de performance e interfaces. Caso um mesmo Throughput seja apresentado mais de uma vez em diferentes métricas, será considerado o de maior valor;

2.3.3. FUNCIONALIDADES DE FIREWALL

2.3.3.1. Deve suportar autenticação para o serviço NTP.

2.3.3.2. Deve ser possível definir por quais origens de rede são permitidas as conexões do administrador.

2.3.3.3. Deve ser possível restringir o acesso à gerência do equipamento por, pelo menos, endereço IP e Rede.

2.3.3.4. Deve suportar SNMP v2 e v3.

2.3.3.5. Deve ser possível realizar captura de pacotes diretamente na

gerência do equipamento.

2.3.3.6. Deve ser possível monitorar a utilização de CPU e memória diretamente na gerência do equipamento.

2.3.3.7. Deve ser possível realizar a configuração do cluster diretamente na gerência do equipamento.

2.3.3.8. Deve ser possível conectar a serviços de DDNS;

2.3.3.9. Deve ser possível configurar o timeout da sessão do administrador na interface web.

2.3.3.10. Deve ser possível configurar a complexidade da senha do administrador e dias para expirar.

2.3.3.11. A solução deve ser capaz de trabalhar com identidades de usuários para propósitos de configurações e logs.

2.3.3.12. A solução deve possibilitar ao administrador realizar a integração com o AD (Active Directory) na própria interface gráfica do produto;

2.3.3.13. A solução deve identificar usuários das seguintes fontes pelo menos:

2.3.3.14. Active Directory: o gateway de segurança deve realizar consulta aos servidores AD para obter informação dos usuários;

2.3.3.15. Autenticação via navegador: para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador;

2.3.3.16. A identificação do usuário registrado no Microsoft Active Directory, deverá ocorrer sem qualquer tipo de agente instalado nos controladores de domínio e estações dos usuários;

2.3.3.17. Na operação para integração com o AD, a operação de cadastro deve ser realizada na própria gerência do equipamento, de maneira simples e sem utilização de scripts de comando;

2.3.4. FUNCIONALIDADE DE PREVENÇÃO DE AMEAÇAS

2.3.4.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS integrados no próprio equipamento sem a necessidade de uso de quaisquer interfaces ou dispositivos externos.

2.3.4.2. Deve ser possível agendar para que o mecanismo de inspeção receba e implemente atualizações para os ataques emergentes sem a necessidade de reiniciar o equipamento;

2.3.4.3. Deve ser possível realizar a atualização manualmente sem necessidade de internet através da importação do pacote de atualização.

2.3.4.4. Deve incluir a habilidade de detectar e bloquear ataques conhecidos, protegendo, pelo menos, os seguintes ataques conhecidos: SQL Injection, ICMP Denial of Service, força bruta, scanning de portas, CIFS Port overflow, Non Compliant DNS, Non Compliant SMTP, Non Compliant CIFS, Non Compliant MS SQL Server, IKE aggressive Exchange;

2.3.4.5. Deve ser capaz de bloquear tráfego SSH em DNS tunneling;

2.3.4.6. A solução deverá ser capaz de inspecionar e proteger apenas hosts internos ou inspecionar todo o tráfego;

2.3.4.7. A solução deve proteger contra-ataques do tipo envenenamento de cache DNS (DNS Cache Poisoning);

2.3.4.8. A solução deverá possuir pelo menos dois perfis pré-configurados de fábrica para uso imediato e permitir a customização de um perfil;

2.3.4.9. Em cada proteção de segurança, devem estar inclusas informações como: categoria, tipo de impacto na ferramenta, severidade, e tipo de ação que a solução irá executar;

2.3.4.10. A solução de IPS deve possuir um modo de solução de problemas, que define o uso de perfil de detecção sem modificar as proteções individuais já criadas e customizadas;

2.3.4.11. Deve ser possível criar regras de exceção no IPS para que a solução não faça a inspeção de um tráfego específico por pelo menos proteção, origem, destino, serviço ou porta.

2.3.4.12. Deve ser possível visualizar a lista de proteções disponíveis no equipamento com os detalhes.

2.3.4.13. A solução deve incluir ferramenta própria ou solução de terceiros para mitigar/bloquear a comunicação entre os hosts infectados com bot e operador remoto (command & contrai).

2.3.4.14. A solução deve bloquear arquivos potencialmente maliciosos infectados com malware.

2.3.4.15. A solução de proteção contra malware e bot podem compartilhar a mesma política para facilitar o gerenciamento.

2.3.4.16. A solução de proteção contra malware e bot deve possuir um modo de solução de problemas, que define o uso de perfil de detecção, sem modificar as proteções individuais já criadas e customizadas;

2.3.4.17. Deve ser possível habilitar a trilha das proteções para não logar, criar um log ou gerar um alerta;

2.3.4.18. Deve ser possível criar regras de exceção para que a solução não faça a inspeção de um tráfego específico por escopo, proteção e definir a ação e log para cada uma delas.

2.3.4.19. A solução de anti-malware deve suportar protocolos SMTP e POP 3, FTP, HTTP em qualquer porta;

2.3.4.20. Deve ser possível definir uma política de inspeção para os tipos de arquivos por:

2.3.4.21. Inspecionar tipos de arquivos conhecidos que contenham malware;

2.3.4.22. Inspecionar todos os tipos de arquivos;

2.3.4.23. Inspecionar tipos de arquivos de famílias específicas;

2.3.4.24. Deve bloquear acesso a URLs com malware;

2.3.4.25. Deve ser possível customizar a página exibida para o usuário quando a URL contiver um malware e o acesso for bloqueado;

2.3.5. FILTRO DE CONTEÚDO WEB

2.3.5.1. A solução deverá contar com ferramentas de visibilidade e controle de aplicações web e filtro URL integrada no próprio appliance de segurança que permita a criação de políticas de liberação ou bloqueio baseando-se em aplicações web e URL;

2.3.5.2. A gerência das políticas de segurança de controle de aplicação e controle de URL's deverá ser realizada na mesma interface web de gerenciamento;

2.3.5.3. Deve ser possível configurar o bloqueio a sites e aplicações que representem um risco de segurança e estão categorizadas como spyware, phishing, botnet, spam, anonymizer ou hacking.

2.3.5.4. Deve ser possível configurar o bloqueio a sites com conteúdo inapropriado como sexo, violência, armas, jogos e álcool.

2.3.5.5. Deve configurar regras para permitir ou bloquear aplicações ou páginas da Internet por pelo menos:

- Usuário do Active Directory
- IP
- Rede

2.3.5.6. Deve ser possível configurar o bloqueio de compartilhamento de arquivos com origem usualmente ilegais como aplicações torrents e peer-to-peer.

2.3.5.7. Deve ser possível configurar manualmente o bloqueio de aplicações ou categorias de sites de aplicações indesejadas.

2.3.5.8. Deve ainda ser possível adicionar uma URL ou aplicação que não está na base de dados.

2.3.5.9. Deve ser possível limitar o consumo de banda de aplicações.

2.3.5.10. A base de aplicações deve ser superior a 2900 aplicações, reconhecendo, pelo menos, as seguintes aplicações: bittorrent, gnutella, skype, facebook, linkedin, twitter, gmail, dropbox, whatsapp, etc;

2.3.5.11. Deve ser possível realizar a recategorização de uma URL através da gerência do equipamento.

2.3.5.12. Deve ser possível customizar e definir a frequência com que serão exibidas as mensagens para os usuários nas seguintes ações:

- Aceitar e informar
- Perguntar

2.3.6. IDENTIFICAÇÃO DE USUÁRIOS

2.3.6.1. A solução deve ser capaz de trabalhar com identidades de usuários para propósitos de configurações e logging.

2.3.6.2. A solução deve possibilitar ao administrador realizar a integração com o AD na própria interface gráfica do produto;

2.3.6.3. A solução deve identificar usuários das seguintes fontes:

2.3.6.4. Active Directory o gateway de segurança deve realizar consulta aos servidores AD para obter informação dos usuários;

2.3.6.5. Autenticação via navegador Para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador;

2.3.6.6. A identificação do usuário registrado no Microsoft Active

Directory, deverá ocorrer sem qualquer tipo de agente instalado nos controladores de domínio e estações dos usuários;

2.3.6.7. Na operação para integração com o AD, a operação de cadastro deve ser realizada na própria interface web de gerência, de maneira simples e sem utilização de scritps de comando;

2.3.7. FUNCIONALIDADES DE ACESSO REMOTO

2.3.7.1. A solução deve prover acesso seguro encriptado aos usuários remotos através da Internet;

2.3.7.2. A solução deve prover conectividade através de um cliente instalado no computador do usuário e através do navegador do usuário com conexão segura (HTTPS).

2.3.7.3. Deve suportar pelo menos os seguintes métodos de conexão:

2.3.7.4. Conexão através de cliente instalado no laptop ou desktop do usuário.

2.3.7.5. Conexão através de cliente instalado no smartphone e tablets.

2.3.7.6. Conexão através de navegador com SSL.

2.3.7.7. Conexão através de cliente nativo Windows L2TP.

2.3.7.8. Solução deve suportar alterar a porta padrão 443 para estabelecimento de VPN SSL.

2.3.7.9. A solução deve permitir conexão VPN aos seguintes usuários:

2.3.7.10. Usuários locais na própria base do appliance.

2.3.7.11. Grupos de usuários locais na própria base do appliance. Grupos de usuários do Active Directory.

2.3.7.12. Grupos de usuários Radius.

2.3.7.13. A solução deve permitir atribuir um endereço específico para o usuário remoto.

2.3.8. FUNCIONALIDADE DE VPN SITE-TO-SITE

2.3.8.1. A solução deve prover acesso seguro criptografado entre duas

localidades através da Internet;

2.3.8.2. A solução deve estabelecer VPN com o site remoto do próprio fabricante ou de terceiros;

2.3.8.3. A solução deve suportar autenticação com senha ou certificado;

2.3.8.4. Deve suportar, pelo menos, criptografia AES 128 e 256;

2.3.8.5. Deve possuir mecanismo para monitorar a saúde do túnel remoto;

2.4. SERVIÇO DE PROTEÇÃO DE DATACENTER PEQUENO PORTE

2.4.1. CARACTERÍSTICAS GERAIS

2.4.1.1. É permitida a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;

2.4.1.2. A solução deverá ser compatível com SNMPv2 e SNMPv3;

2.4.1.3. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos equipamentos desde que obedeçam a todos os requisitos desta especificação;

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

2.4.1.5. Os appliances de segurança devem suportar operar em cluster ativo-ativo e ativo- passivo sem a necessidade de licenças adicionais;

2.4.1.6. Não serão aceitos modelos em listas de end-of-sale, cuja data do fim de vendas seja anterior à data da proposta.

2.4.1.7. Não serão aceitos modelos em lista de end-of-support, cuja data do fim do suporte seja anterior ao fim da vigência do contrato e/ou do fim do período de garantia e suporte exigido no edital.

2.4.2. CAPACIDADE E QUANTIDADES

2.4.2.1. Throughput de, no mínimo, 9 (nove) Gbps, com as

funcionalidades de firewall, prevenção de intrusão, controle de aplicação, anti-malware e prevenção de ameaças avançadas (dia zero) habilitados simultaneamente;

2.4.2.2. Suporte a, no mínimo, 5.000.000 (cinco milhões) conexões ou sessões simultâneas;

2.4.2.3. Suporte a, no mínimo, 270.000 (duzentos e setenta mil) novas conexões ou sessões por segundo;

2.4.2.4. Throughput de, no mínimo, 20 (vinte) Gbps para conexões VPN;

2.4.2.5. Licenciado ou permitir, pelo menos, 500 conexões ou sessões simultâneas de VPN client-tosite;

2.4.2.6. Possuir, pelo menos, 8 (oito) interfaces de rede 1Gbps UTP;

2.4.2.7. Possuir, pelo menos, 8 (oito) interfaces de rede 10Gbps SFP+;

2.4.2.8. Possuir fonte de alimentação redundante e hot-swap;

2.4.2.9. Possuir 1 (uma) interface do tipo console ou similar;

2.4.2.10. O Throughput e as interfaces solicitados neste item deverão ser comprovados através de datasheet público na internet. Não serão aceitas declarações de fabricantes informando números de performance e interfaces. Caso um mesmo Throughput seja apresentado mais de uma vez em diferentes métricas, será considerado o de maior valor;

2.4.3. FUNCIONALIDADES DE FIREWALL

2.4.3.1. Deve suportar autenticação para o serviço NTP.

2.4.3.2. Deve ser possível definir por quais origens de rede são permitidas as conexões do administrador.

2.4.3.3. Deve ser possível restringir o acesso à gerência do equipamento por, pelo menos, endereço IP e Rede.

2.4.3.4. Deve suportar SNMP v2 e v3.

2.4.3.5. Deve ser possível realizar captura de pacotes diretamente na

gerência do equipamento.

2.4.3.6. Deve ser possível monitorar a utilização de CPU e memória diretamente na gerência do equipamento.

2.4.3.7. Deve ser possível realizar a configuração do cluster diretamente na gerência do equipamento.

2.4.3.8. Deve ser possível conectar a serviços de DDNS;

2.4.3.9. Deve ser possível configurar o timeout da sessão do administrador na interface web.

2.4.3.10. Deve ser possível configurar a complexidade da senha do administrador e dias para expirar.

2.4.3.11. A solução deve ser capaz de trabalhar com identidades de usuários para propósitos de configurações e logs.

2.4.3.12. A solução deve possibilitar ao administrador realizar a integração com o AD (Active Directory) na própria interface gráfica do produto;

2.4.3.13. A solução deve identificar usuários das seguintes fontes pelo menos:

2.4.3.14. Active Directory: o gateway de segurança deve realizar consulta aos servidores AD para obter informação dos usuários;

2.4.3.15. Autenticação via navegador: para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador;

2.4.3.16. A identificação do usuário registrado no Microsoft Active Directory, deverá ocorrer sem qualquer tipo de agente instalado nos controladores de domínio e estações dos usuários;

2.4.3.17. Na operação para integração com o AD, a operação de cadastro deve ser realizada na própria gerência do equipamento, de maneira simples e sem utilização de scripts de comando;

2.4.4. FUNCIONALIDADE DE PREVENÇÃO DE AMEAÇAS

2.4.4.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS integrados no próprio equipamento sem a necessidade de uso de quaisquer interfaces ou dispositivos externos.

2.4.4.2. Deve ser possível agendar para que o mecanismo de inspeção receba e implemente atualizações para os ataques emergentes sem a necessidade de reiniciar o equipamento;

2.4.4.3. Deve ser possível realizar a atualização manualmente sem necessidade de internet através da importação do pacote de atualização.

2.4.4.4. Deve incluir a habilidade de detectar e bloquear ataques conhecidos, protegendo, pelo menos, os seguintes ataques conhecidos: SQL Injection, ICMP Denial of Service, força bruta, scanning de portas, CIFS Port overflow, Non Compliant DNS, Non Compliant SMTP, Non Compliant CIFS, Non Compliant MS SQL Server, IKE aggressive Exchange;

2.4.4.5. Deve ser capaz de bloquear tráfego SSH em DNS tunneling;

2.4.4.6. A solução deverá ser capaz de inspecionar e proteger apenas hosts internos ou inspecionar todo o tráfego;

2.4.4.7. A solução deve proteger contra-ataques do tipo envenenamento de cache DNS (DNS Cache Poisoning);

2.4.4.8. A solução deverá possuir pelo menos dois perfis pré-configurados de fábrica para uso imediato e permitir a customização de um perfil;

2.4.4.9. Em cada proteção de segurança, devem estar inclusas informações como: categoria, tipo de impacto na ferramenta, severidade, e tipo de ação que a solução irá executar;

2.4.4.10. A solução de IPS deve possuir um modo de solução de problemas, que define o uso de perfil de detecção sem modificar as proteções individuais já criadas e customizadas;

2.4.4.11. Deve ser possível criar regras de exceção no IPS para que a solução não faça a inspeção de um tráfego específico por pelo menos proteção, origem, destino, serviço ou porta.

2.4.4.12. Deve ser possível visualizar a lista de proteções disponíveis no equipamento com os detalhes.

2.4.4.13. A solução deve incluir ferramenta própria ou solução de terceiros para mitigar/bloquear a comunicação entre os hosts infectados com bot e operador remoto (command & contrai).

2.4.4.14. A solução deve bloquear arquivos potencialmente maliciosos infectados com malware.

2.4.4.15. A solução de proteção contra malware e bot podem compartilhar a mesma política para facilitar o gerenciamento.

2.4.4.16. A solução de proteção contra malware e bot deve possuir um modo de solução de problemas, que define o uso de perfil de detecção, sem modificar as proteções individuais já criadas e customizadas;

2.4.4.17. Deve ser possível habilitar a trilha das proteções para não logar, criar um log ou gerar um alerta;

2.4.4.18. Deve ser possível criar regras de exceção para que a solução não faça a inspeção de um tráfego específico por escopo, proteção e definir a ação e log para cada uma delas.

2.4.4.19. A solução de anti-malware deve suportar protocolos SMTP e POP 3, FTP, HTTP em qualquer porta;

2.4.4.20. Deve ser possível definir uma política de inspeção para os tipos de arquivos por:

- Inspecionar tipos de arquivos conhecidos que contenham malware;
- Inspecionar todos os tipos de arquivos;
- Inspecionar tipos de arquivos de famílias específicas;

2.4.4.21. Deve bloquear acesso a URLs com malware;

2.4.4.22. Deve ser possível customizar a página exibida para o usuário quando a URL contiver um malware e o acesso for bloqueado;

2.4.5. FILTRO DE CONTEÚDO WEB

2.4.5.1. A solução deverá contar com ferramentas de visibilidade e controle de aplicações web e filtro URL integrada no próprio appliance de segurança que permita a criação de políticas de liberação ou bloqueio baseando-se em aplicações web e URL;

2.4.5.2. A gerência das políticas de segurança de controle de aplicação e controle de URL's deverá ser realizada na mesma interface web de gerenciamento;

2.4.5.3. Deve ser possível configurar o bloqueio a sites e aplicações que representem um risco de segurança e estão categorizadas como spyware, phishing, botnet, spam, anonymizer ou hacking.

2.4.5.4. Deve ser possível configurar o bloqueio a sites com conteúdo inapropriado como sexo, violência, armas, jogos e álcool.

2.4.5.5. Deve configurar regras para permitir ou bloquear aplicações ou páginas da Internet por pelo menos:

- Usuário do Active Directory
- IP
- Rede

2.4.5.6. Deve ser possível configurar o bloqueio de compartilhamento de arquivos com origem usualmente ilegais como aplicações torrents e peer-to-peer.

2.4.5.7. Deve ser possível configurar manualmente o bloqueio de aplicações ou categorias de sites de aplicações indesejadas.

2.4.5.8. Deve ainda ser possível adicionar uma URL ou aplicação que não está na base de dados.

2.4.5.9. Deve ser possível limitar o consumo de banda de aplicações.

2.4.5.10. A base de aplicações deve ser superior a 2900 aplicações, reconhecendo, pelo menos, as seguintes aplicações: bittorrent, gnutella, skype, facebook, linkedin, twitter, gmail, dropbox, whatsapp, etc;

2.4.5.11. Deve ser possível realizar a recategorização de uma URL através da gerência do equipamento.

2.4.5.12. Deve ser possível customizar e definir a frequência com que serão exibidas as mensagens para os usuários nas seguintes ações:

- Aceitar e informar
- Perguntar

2.4.6. IDENTIFICAÇÃO DE USUÁRIOS

2.4.6.1. A solução deve ser capaz de trabalhar com identidades de usuários para propósitos de configurações e logging.

2.4.6.2. A solução deve possibilitar ao administrador realizar a integração com o AD na própria interface gráfica do produto;

2.4.6.3. A solução deve identificar usuários das seguintes fontes:

2.4.6.4. Active Directory o gateway de segurança deve realizar consulta aos servidores AD para obter informação dos usuários;

2.4.6.5. Autenticação via navegador Para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador;

2.4.6.6. A identificação do usuário registrado no Microsoft Active

Directory, deverá ocorrer sem qualquer tipo de agente instalado nos controladores de domínio e estações dos usuários;

2.4.6.7. Na operação para integração com o AD, a operação de cadastro deve ser realizada na própria interface web de gerência, de maneira simples e sem utilização de scritps de comando;

2.4.7. FUNCIONALIDADES DE ACESSO REMOTO

2.4.7.1. A solução deve prover acesso seguro encriptado aos usuários remotos através da Internet;

2.4.7.2. A solução deve prover conectividade através de um cliente instalado no computador do usuário e através do navegador do usuário com conexão segura (HTTPS).

2.4.7.3. Deve suportar pelo menos os seguintes métodos de conexão:

2.4.7.4. Conexão através de cliente instalado no laptop ou desktop do usuário.

2.4.7.5. Conexão através de cliente instalado no smartphone e tablets.

2.4.7.6. Conexão através de navegador com SSL.

2.4.7.7. Conexão através de cliente nativo Windows L2TP.

2.4.7.8. Solução deve suportar alterar a porta padrão 443 para estabelecimento de VPN SSL.

2.4.7.9. A solução deve permitir conexão VPN aos seguintes usuários:

2.4.7.10. Usuários locais na própria base do appliance.

2.4.7.11. Grupos de usuários locais na própria base do appliance.

2.4.7.12. Grupos de usuários do Active Directory.

2.4.7.13. Grupos de usuários Radius.

2.4.7.14. A solução deve permitir atribuir um endereço específico para o usuário remoto.

2.4.8. FUNCIONALIDADE DE VPN SITE-TO-SITE

2.4.8.1. A solução deve prover acesso seguro criptografado entre duas

localidades através da Internet;

2.4.8.2. A solução deve estabelecer VPN com o site remoto do próprio fabricante ou de terceiros;

2.4.8.3. A solução deve suportar autenticação com senha ou certificado;

2.4.8.4. Deve suportar, pelo menos, criptografia AES 128 e 256;

2.4.8.5. Deve possuir mecanismo para monitorar a saúde do túnel remoto;

2.5. SERVIÇO DE PROTEÇÃO DE DATACENTER MÉDIO PORTE

2.5.1. CARACTERÍSTICAS GERAIS

2.5.1.1. É permitido a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;

2.5.1.2. A solução deverá ser compatível com SNMPv2 e SNMPv3;

2.5.1.3. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos equipamentos desde que obedeçam a todos os requisitos desta especificação;

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

2.5.1.5. Os appliances de segurança devem suportar operar em cluster ativo-ativo e ativo- passivo sem a necessidade de licenças adicionais;

2.5.1.6. Não serão aceitos modelos em listas de end-of-sale, cuja data do fim de vendas seja anterior à data da proposta.

2.5.1.7. Não serão aceitos modelos em lista de end-of-support, cuja data do fim do suporte seja anterior ao fim da vigência do contrato e/ou do fim do período de garantia e suporte exigido no edital.

2.5.2. CAPACIDADE E QUANTIDADES

2.5.2.1. Throughput de, no mínimo, 20 (vinte) Gbps, com as

funcionalidades de firewall, prevenção de intrusão, controle de aplicação, anti-malware e prevenção de ameaças avançadas (dia zero) habilitados simultaneamente;

2.5.2.2. Suporte a, no mínimo, 7.000.000 (sete milhões) de conexões ou sessões simultâneas;

2.5.2.3. Suporte a, no mínimo, 370.000 (trezentas e setenta mil) novas conexões ou sessões por segundo;

2.5.2.4. Throughput de, no mínimo, 28 (vinte e oito) Gbps, para conexões VPN;

2.5.2.5. Armazenamento de, no mínimo, 400GB SSD;

2.5.2.6. Possuir, no mínimo, 6 (seis) interfaces de rede 1Gbps UTP;

2.5.2.7. Possuir, no mínimo, 4 (quatro) interfaces de rede 10 Gbps SFP+;

2.5.2.8. Possuir, no mínimo, 4 (quatro) interfaces de rede 25 Gbps SFP28;

2.5.2.9. Capacidade para suportar, pelo menos, 10 contextos virtuais;

2.5.2.10. Possuir fonte de alimentação redundante e hot-swap;

2.5.2.11. Possuir 1 (uma) interface de rede dedicada ao gerenciamento;

2.5.2.12. Possuir 1 (uma) interface de rede dedicada para sincronismo;

2.5.2.13. Possuir 1 (uma) interface do tipo console ou similar;

2.5.2.14. A solução deve possuir mecanismo para dedicar processamento no equipamento de segurança para funções e ações de gerenciamento, mesmo que o equipamento esteja com alto processamento de CPU. Assim evitando a falta de acesso do administrador para qualquer mitigação de problema e aplicação de política para solução de problema. Entre as funções, deve suportar no mínimo: acesso SSH, acesso WEB, alterações de política.

2.5.2.15. O Throughput e as interfaces solicitados neste item deverão ser comprovados através de datasheet público na internet. Não serão

aceitas declarações de fabricantes informando números de performance e interfaces;

2.5.3. FUNCIONALIDADE DE FIREWALL

2.5.3.1. A solução deve consistir de appliance de proteção de rede com funcionalidades de proteção de próxima geração;

2.5.3.2. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação técnica;

2.5.3.3. O hardware e software que executem as funcionalidades de proteção de rede deve ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

2.5.3.4. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19'', incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;

2.5.3.5. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

2.5.3.6. Suporte a, no mínimo, 1024 VLAN Tags 802.1q, agregação de links 802.3ad, policy based routing ou policy based forwarding, roteamento multicast (PIM-SM), DHCP Relay, DHCP Server e Jumbo Frames;

2.5.3.7. A solução deve possuir mecanismo onde identifica o volume de conexões que foi trafegada na regra, assim identificando as regras mais utilizadas;

2.5.3.8. Deve suportar os seguintes tipos de NAT:

2.5.3.9. Nat dinâmico (Many-to-1), Nat estático (1-to-1), Tradução de porta (PAT), NAT de Origem, NAT de Destino e suportar NAT de Origem e NAT de Destino simultaneamente;

2.5.3.10. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

2.5.3.11. Deve suportar NAT64 e NAT46;

2.5.3.12. Enviar logs para sistemas de monitoração externos, simultaneamente;

2.5.3.13. Deve possuir mecanismos de proteção anti-spoofing;

2.5.3.14. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

2.5.3.15. O firewall deve ter a capacidade de operar de forma simultânea em uma única instancia de Firewall, mediante o uso das suas interfaces físicas nos seguintes modos:

2.5.3.16. Transparente, modo sniffer (monitoramento e análise o tráfego de rede), camada 2 (L2) e camada 3 (L3);

2.5.3.17. Para IPv6, deve suportar roteamento estático e dinâmico (OSPF);

2.5.3.18. Suportar OSPF graceful restart;

2.5.3.19. Autenticação via Kerberos.

2.5.3.20. Cada regra deve, obrigatoriamente, funcionar nas versões de endereço IP 4 e 6 sem duplicação da base de objetos e regras;

2.5.3.21. Não serão aceitas soluções nas quais as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou obrigatoriamente listadas nas configurações de regras;

2.5.4. FUNCIONALIDADE DE CONTROLE DE DADOS E FILTRO DE CONTEÚDO WEB

2.5.4.1. A solução deverá contar com ferramentas de visibilidade e controle de aplicações WEB e Filtro URL integrada no próprio appliance de segurança que permite a criação de políticas de liberação ou bloqueio baseando-se em aplicações WEB e URL;

2.5.4.2. Controle de políticas por usuários, grupos de usuários, IPs e redes;

2.5.4.3. Deve de-criptografar tráfego de entrada e saída em conexões negociadas com TLS 1.2;

2.5.4.4. Será aceito soluções de outros fabricantes diferentes do firewall ofertado pela licitante desde que atendido todos os requisitos desta especificação;

2.5.4.5. Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

2.5.4.6. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

2.5.4.7. Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;

2.5.4.8. Reconhecer pelo menos 3.000 (Três mil) 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;

2.5.4.9. Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do pay load para checagem de assinaturas de aplicações conhecidas;

2.5.4.10. A solução deve suportar a recategorização de URLs local;

2.5.4.11. Atualizar a base de assinaturas de aplicações automaticamente;

2.5.4.12. A solução deve permitir a solicitação da contratada com o fabricante para categorização de URL na base do fabricante;

2.5.4.13. Limitar a banda (download/upload) usada por aplicações,

baseado no IP de origem, usuários e grupos do LDAP/AD;

2.5.4.14. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Aclive Directory, sem a necessidade de instalação de agente no controlador de do mínio, nem nas estações dos usuários;

2.5.4.15. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;

2.5.4.16. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;

2.5.4.17. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

2.5.4.18. Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

2.5.4.19. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;

2.5.4.20. Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

2.5.4.21. Deve bloquear o acesso a sites com conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, mesmo que a opção "Safe Search" esteja desabilitada no navegador do usuário;

2.5.4.22. Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs. Caso a solução ofertada não suporte localmente, será aceito produto externo

desde que não seja solução de software livre;

2.5.4.23. Suportar a criação de categorias de URLs customizadas;

2.5.4.24. Permitir a customização de página de bloqueio;

2.5.4.25. Como melhor prática do uso do acesso a internet e respeitando as políticas de segurança do orgão, a ferramenta deve criar uma página customizada ou pop-up onde o usuário será questionado ou informado no momento do acesso a uma página URL ou applicação WEB de acordo com as políticas de acesso estabelecidas pela área de TI;

2.5.4.26. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via Radius, para a identificação de endereços IP e usuários;

2.5.4.27. 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);

2.5.4.28. A solução de controle de dados deve trazer de fábrica vários tipos de arquivos reconhecidos nativamente, permitindo a reconhecimento de pelo menos os seguintes tipos de dados e arquivos:

2.5.4.29. PCI números de cartão de crédito;

2.5.4.30. Arquivos PDF;

2.5.4.31. Arquivos executáveis;

2.5.4.32. Arquivos de banco de dados ou similar;

2.5.4.33. Arquivos do tipo documento;

2.5.4.34. Arquivos do tipo apresentação;

2.5.4.35. Arquivos do tipo planilha;

2.5.4.36. A solução de controle de dados deve permitir que as direções do

tráfego inspecionado sejam defini das no momento da criação da politica, tais como: "Upload", "Download" e "Download e Upload".

2.5.4.37. A solução de controle de dados deve permitir que o usuário receba uma notificação, redirect de uma página web, sempre que um arquivo reconhecido por match em uma regra em uma das categorias acima, seja feito.

2.5.4.38. A solução de controle de dados deve permitir, inspecionar e prevenir vazamentos de arquivos mesmo quando estes estes sendo trafegados pela Web em páginas utilizando o protocolo HTTPS.

2.5.5. FUNCIONALIDADES DE PREVENÇÃO DE AMEAÇAS

2.5.5.1. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS e suportar os módulos de: Antivírus e Anti-Malware integrados no próprio equipamento de firewall;

2.5.5.2. Possuir capacidade de detecção de, no mínimo, 7.000 (sete mil) assinaturas de ataques pré-defini dos;

2.5.5.3. A solução deve sincronizar ou aplicar as assinaturas de IPS, Antivírus, Anti- Malware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;

2.5.5.4. A fim de não criar indisponibilidade no appliance de segurança, a solução de IPS deve possuir mecanismo de fail-open baseado em software, configurável baseado em thresholds de CPU e memória do dispositivo;

2.5.5.5. Deve suportar granularidade nas políticas de Antivírus e Anti-malware, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

2.5.5.6. A solução de IPS deve possuir análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

2.5.5.7. Detectar e bloquear a origem de portscans;

2.5.5.8. Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;

2.5.5.9. A solução de IPS deve suportar a inclusão de novas assinaturas e customização no formato SNORT ou formato proprietário onde seja possível definir o protocolo (TCP, UDP, ICMP, IP), serviço, conteúdo do pacote (payload), tipo do arquivo e severidade;

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

2.5.5.11. Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;

2.5.5.12. Suportar bloqueio de arquivos por tipo;

2.5.5.13. Identificar e bloquear comunicação com botnets;

2.5.5.14. Deve suportar referência cruzada com CVE;

2.5.5.15. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

2.5.5.16. O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;

2.5.5.17. Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware, através da console de gerência centralizada;

2.5.5.18. Os eventos devem identificar o país de onde partiu a ameaça;

2.5.5.19. Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);

2.5.5.20. Possuir a capacidade de prevenção de ameaças não

conhecidas;

2.5.5.21. Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/ Países seja bloqueado;

2.5.5.22. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

2.5.5.23. A solução de anti-malware, deve ser capaz de detectar e bloquear ações de callbacks;

2.5.6. FUNCIONALIDADES DE CONTROLE DE QUALIDADE DE SERVIÇO

2.5.6.1. Suportar a criação de políticas de QoS por:

2.5.6.2. Endereço de origem, endereço de destino e por porta;

2.5.6.3. O QoS deve possibilitar a definição de classes por:

2.5.6.4. Banda garantida;

2.5.6.5. Banda máxima ;

2.5.6.6. Fila de prioridade;

2.5.6.7. Disponibilizar estatísticas RealTime para classes de QoS;

2.5.7. FUNCIONALIDADES DE VPN

2.5.7.1. Suportar VPN Site-to-Site e Cliente-To-Site;

2.5.7.2. Suportar IPSec VPN;

2.5.7.3. Suportar SSL VPN;

2.5.7.4. A VPN IPSEc deve suportar:

2.5.7.5. 3DES, Autenticação MOS e SHA-1, Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Algoritmo Internet Key Exchange (IKE), AES 128 e 256 (Advanced Encryption Standard) e Autenticação via certificado IKE PKI;

2.5.7.6. A solução deve suportar a importação de certificados de CA Interna e CA Externa de terceiros;

2.5.7.7. Solução deve suportar a configuração VPN através de uma interface do tipo GUI (console do fabricante ou interface web);

2.5.8. SOLUÇÃO DE PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS

2.5.8.1. A solução deverá prover as funcionalidades de inspeção de artefatos de entrada com malwares não conhecidos ou do tipo APT com filtro de ameaças avançadas e análise de execução em tempo real, sendo essa análise executada na nuvem proprietária do próprio fabricante ou appliance dedicada para sandboxing;

2.5.8.2. Prevenir através do bloqueio efetivo do malware desconhecido (Dia Zero), oriundo da comunicação Web (HTTP e HTTPS) ou E-mail (SMTP/TLS), sem que o mesmo seja entregue parcialmente ao cliente.

2.5.8.3. A solução deve ser capaz de inspecionar e prevenir malware desconhecido em tráfego criptografado SSL;

2.5.8.4. A solução deve fornecer a capacidade de emular ataques em sistemas operacionais Windows e Linux;

2.5.8.5. Implementar atualização da base de dados de forma automática, permitindo agendamentos diários, dias da semana ou automáticos como o período de cada atualização;

2.5.8.6. A solução deve suportar as seguintes topologias de implantação: Inline ou Mirror/TAP;

2.5.8.7. A tecnologia de máquina virtual deverá possuir diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso, não sendo baseado apenas em assinaturas;

2.5.8.8. A solução de prevenção de ameaças avançadas (Sandboxing) contra ataques persistentes e Zero-Day, quando habilitada, pode funcionar de forma integrada a engines de antivírus;

2.5.8.9. Todas as máquinas virtuais (Windows e Linux) utilizadas na solução e solicitadas neste edital, devem estar integralmente

instaladas e licenciadas, sem a necessidade de intervenções por parte do administrador do sistema. As atualizações deverão ser providas pelo fabricante;

2.5.8.10. Para a emulação de arquivos, a solução deve suportar arquivos com tamanho máximo de emulação de até 30Mb.

2.5.8.11. Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endereço IP;

2.5.8.12. Implementar a emulação, detecção e bloqueio de qualquer malware e/ou código malicioso detecta do como desconhecido. A solução deve permitir a análise e bloqueio dos seguintes tipos de arquivos caso tenham malware desconhecido: pdf, tar, zip, rar, 7z, exe, rtf, xls, xlsx, xlt, xltx, xlsm, xltm, xlsb, ppt, pptx, pps, pptm, ppsx, ppsm, doc, docx;

2.5.8.13. A solução deve permitir a criação de Whitelists baseado no MD5 do arquivo;

2.5.8.14. Para melhor administração da solução, a solução deve possibilitar as seguintes

2.5.8.15. visualizações a nível de monitoração:

2.5.8.16. Quantidade de arquivos que estão em emulação;

2.5.8.17. Número de arquivos emulados;

2.5.8.18. A solução deve possuir os indicadores abaixo referente ao último dia, última semana ou últimos 30 dias:

2.5.8.19. Arquivos scaneados;

2.5.8.20. Arquivos maliciosos;

2.6. SERVIÇO DE PROTEÇÃO DE DATACENTER GRANDE PORTE

2.6.1. CARACTERÍSTICAS GERAIS

2.6.1.1. É permitido a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;

2.6.1.2. A solução deverá ser compatível com SNMPv2 e SNMPv3;

2.6.1.3. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos equipamentos desde que obedeçam a todos os requisitos desta especificação;

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

2.6.1.5. Os appliances de segurança devem suportar operar em cluster ativo-ativo e ativo- passivo sem a necessidade de licenças adicionais;

2.6.1.6. Não serão aceitos modelos em listas de end-of-sale, cuja data do fim de vendas seja anterior à data da proposta.

2.6.1.7. Não serão aceitos modelos em lista de end-of-support, cuja data do fim do suporte seja anterior ao fim da vigência do contrato e/ou do fim do período de garantia e suporte exigido no edital.

2.6.2. CAPACIDADE E QUANTIDADES

2.6.2.1. Throughput de, no mínimo, 25 (vinte e cinco) Gbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, anti-malware e prevenção de ameaças avançadas (dia zero) habilitados simultaneamente;

2.6.2.2. Suporte a, no mínimo, 9.000.000 (nove milhões) de conexões ou sessões simultâneas;

2.6.2.3. Suporte a, no mínimo, 380.000 (trezentas e oitenta mil) novas conexões ou sessões por segundo;

2.6.2.4. Throughput de, no mínimo, 42 (quarenta e dois) Gbps, para conexões VPN;

2.6.2.5. Armazenamento redundante de, no mínimo, 960GB SSD;

2.6.2.6. Possuir, no mínimo, 8 (oito) interfaces de rede 10 Gbps UTP;

2.6.2.7. Possuir, no mínimo, 8 (oito) interfaces de rede 10 Gbps SFP+;

2.6.2.8. Possuir, no mínimo, 4 (quatro) interfaces de rede 25 Gbps SFP28, com suporte a conectores 10 Gbps SFP+;

2.6.2.9. Possuir, no mínimo, 4 (quatro) interfaces de rede 100 Gbps QFP28, com suporte a conectores 40 Gbps QSFP+;

2.6.2.10. Capacidade para suportar, pelo menos, 30 contextos virtuais;

2.6.2.11. Possuir fonte de alimentação redundante e hot-swap;

2.6.2.12. Possuir 1 (uma) interface de rede dedicada ao gerenciamento;

2.6.2.13. Possuir 1 (uma) interface de rede dedicada para sincronismo;

2.6.2.14. Possuir 1 (uma) interface do tipo console ou similar;

2.6.2.15. A solução deve possuir mecanismo para dedicar processamento no equipamento de segurança para funções e ações de gerenciamento, mesmo que o equipamento esteja com alto processamento de CPU. Assim evitando a falta de acesso do administrador para qualquer mitigação de problema e aplicação de política para solução de problema. Entre as funções, deve suportar no mínimo: acesso SSH, acesso WEB, alterações de política.

2.6.2.16. O Throughput e as interfaces solicitados neste item deverão ser comprovados através de datasheet público na internet. Não serão aceitas declarações de fabricantes informando números de performance e interfaces;

2.6.3. FUNCIONALIDADE DE FIREWALL

2.6.3.1. A solução deve consistir de appliance de proteção de rede com funcionalidades de proteção de próxima geração;

2.6.3.2. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação técnica;

2.6.3.3. O hardware e software que executem as funcionalidades de proteção de rede deve ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

2.6.3.4. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;

2.6.3.5. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

2.6.3.6. Suporte a, no mínimo, 1024 VLAN Tags 802.1q, agregação de links 802.3ad, policy based routing ou policy based forwarding, roteamento multicast (PIM-SM), DHCP Relay, DHCP Server e Jumbo Frames;

2.6.3.7. A solução deve possuir mecanismo onde identifica o volume de conexões que foi trafegada na regra, assim identificando as regras mais utilizadas;

2.6.3.8. Deve suportar os seguintes tipos de NAT:

2.6.3.9. Nat dinâmico (Many-to-1), Nat estático (1-to-1), Tradução de porta (PAT), NAT de Origem, NAT de Destino e suportar NAT de Origem e NAT de Destino simultaneamente;

2.6.3.10. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

2.6.3.11. Deve suportar NAT64 e NAT46;

2.6.3.12. Enviar logs para sistemas de monitoração externos, simultaneamente;

2.6.3.13. Deve possuir mecanismos de proteção anti-spoofing;

2.6.3.14. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

2.6.3.15. O firewall deve ter a capacidade de operar de forma simultânea

em uma única instancia de Firewall, mediante o uso das suas interfaces físicas nos seguintes modos:

2.6.3.16. Transparente, modo sniffer (monitoramento e análise o tráfego de rede), camada 2 (L2) e camada 3 (L3);

2.6.3.17. Para IPv6, deve suportar roteamento estático e dinâmico (OSPF);

2.6.3.18. Suportar OSPF graceful restart;

2.6.3.19. Autenticação via Kerberos.

2.6.3.20. Cada regra deve, obrigatoriamente, funcionar nas versões de endereço IP 4 e 6 sem duplicação da base de objetos e regras;

2.6.3.21. Não serão aceitas soluções nas quais as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou obrigatoriamente listadas nas configurações de regras;

2.6.4. FUNCIONALIDADE DE CONTROLE DE DADOS E FILTRO DE CONTEÚDO WEB

2.6.4.1. A solução deverá contar com ferramentas de visibilidade e controle de aplicações WEB e Filtro URL integrada no próprio appliance de segurança que permite a criação de políticas de liberação ou bloqueio baseando-se em aplicações WEB e URL;

2.6.4.2. Controle de políticas por usuários, grupos de usuários, IPs e redes;

2.6.4.3. Deve de-criptografar tráfego de entrada e saída em conexões negociadas com TLS 1.2;

2.6.4.4. Será aceito soluções de outros fabricantes diferentes do firewall ofertado pela licitante desde que atendido todos os requisitos desta especificação;

2.6.4.5. Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-

definidos automaticamente;

2.6.4.6. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

2.6.4.7. Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;

2.6.4.8. Reconhecer pelo menos 3.000 (Três mil) 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;

2.6.4.9. Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do pay load para checagem de assinaturas de aplicações conhecidas;

2.6.4.10. A solução deve suportar a recategorização de URLs local;

2.6.4.11. Atualizar a base de assinaturas de aplicações automaticamente;

2.6.4.12. A solução deve permitir a solicitação da contratada com o fabricante para categorização de URL na base do fabricante;

2.6.4.13. Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;

2.6.4.14. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Aclive Directory, sem a necessidade de instalação de agente no controlador de do mínio, nem nas estações dos usuários;

2.6.4.15. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;

2.6.4.16. Permitir nativamente a criação de assinaturas personalizadas

para reconhecimento de aplicações proprietárias, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;

2.6.4.17. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

2.6.4.18. Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

2.6.4.19. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;

2.6.4.20. Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

2.6.4.21. Deve bloquear o acesso a sites com conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, mesmo que a opção "Safe Search" esteja desabilitada no navegador do usuário;

2.6.4.22. Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs. Caso a solução ofertada não suporte localmente, será aceito produto externo desde que não seja solução de software livre;

2.6.4.23. Suportar a criação de categorias de URLs customizadas;

2.6.4.24. Permitir a customização de página de bloqueio;

2.6.4.25. Como melhor prática do uso do acesso a internet e respeitando as políticas de segurança do orgão, a ferramenta deve criar uma página customizada ou pop-up onde o usuário será questionado ou informado no momento do acesso a uma página URL ou applicação WEB de acordo com as políticas de acesso estabelecidas pela área de TI;

2.6.4.26. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via Radius, para a identificação de endereços IP e usuários;

2.6.4.27. 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);

2.6.4.28. A solução de controle de dados deve trazer de fábrica vários tipos de arquivos reconhecidos nativamente, permitindo a reconhecimento de pelo menos os seguintes tipos de dados e arquivos:

2.6.4.29. PCI números de cartão de crédito;

2.6.4.30. Arquivos PDF;

2.6.4.31. Arquivos executáveis;

2.6.4.32. Arquivos de banco de dados ou similar;

2.6.4.33. Arquivos do tipo documento;

2.6.4.34. Arquivos do tipo apresentação;

2.6.4.35. Arquivos do tipo planilha;

2.6.4.36. A solução de controle de dados deve permitir que as direções do tráfego inspecionado sejam defini das no momento da criação da politica, tais como: "Upload", "Download" e "Download e Upload".

2.6.4.37. A solução de controle de dados deve permitir que o usuário receba uma notificação, redirect de uma página web, sempre que um arquivo reconhecido por match em uma regra em uma das categorias acima, seja feito.

2.6.4.38. A solução de controle de dados deve permitir, inspecionar e prevenir vazamentos de arquivos mesmo quando estes estes sendo trafegados pela Web em páginas utilizando o protocolo

HTTPS.

2.6.5. FUNCIONALIDADES DE PREVENÇÃO DE AMEAÇAS

2.6.5.1. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS e suportar os módulos de: Antivírus e Anti-Malware integrados no próprio equipamento de firewall;

2.6.5.2. Possuir capacidade de detecção de, no mínimo, 7.000 (sete mil) assinaturas de ataques pré-defini dos;

2.6.5.3. A solução deve sincronizar ou aplicar as assinaturas de IPS, Antivírus, Anti- Malware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;

2.6.5.4. A fim de não criar indisponibilidade no appliance de segurança, a solução de IPS deve possuir mecanismo de fail-open baseado em software, configurável baseado em thresholds de CPU e memória do dispositivo;

2.6.5.5. Deve suportar granularidade nas políticas de Antivírus e Anti-malware, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

2.6.5.6. A solução de IPS deve possuir análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

2.6.5.7. Detectar e bloquear a origem de portscans;

2.6.5.8. Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;

2.6.5.9. A solução de IPS deve suportar a inclusão de novas assinaturas e customização no formato SNORT ou formato proprietário onde

seja possível definir o protocolo (TCP, UDP, ICMP, IP), serviço, conteúdo do pacote (payload), tipo do arquivo e severidade;

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

2.6.5.11. Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;

2.6.5.12. Suportar bloqueio de arquivos por tipo;

2.6.5.13. Identificar e bloquear comunicação com botnets;

2.6.5.14. Deve suportar referência cruzada com CVE;

2.6.5.15. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

2.6.5.16. O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;

2.6.5.17. Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware, através da console de gerência centralizada;

2.6.5.18. Os eventos devem identificar o país de onde partiu a ameaça;

2.6.5.19. Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);

2.6.5.20. Possuir a capacidade de prevenção de ameaças não conhecidas;

2.6.5.21. Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/ Países seja bloqueado;

2.6.5.22. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

2.6.5.23. A solução de anti-malware, deve ser capaz de detectar e bloquear ações de callbacks;

2.6.6. FUNCIONALIDADES DE CONTROLE DE QUALIDADE DE SERVIÇO

2.6.6.1. Suportar a criação de políticas de QoS por:

2.6.6.2. Endereço de origem, endereço de destino e por porta;

2.6.6.3. O QoS deve possibilitar a definição de classes por:

2.6.6.4. Banda garantida;

2.6.6.5. Banda máxima ;

2.6.6.6. Fila de prioridade;

2.6.6.7. Disponibilizar estatísticas RealTime para classes de QoS;

2.6.7. FUNCIONALIDADES DE VPN

2.6.7.1. Suportar VPN Site-to-Site e Cliente-To-Site;

2.6.7.2. Suportar IPSec VPN;

2.6.7.3. Suportar SSL VPN;

2.6.7.4. A VPN IPSEc deve suportar:

2.6.7.5. 3DES, Autenticação MOS e SHA-1, Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Algoritmo Internet Key Exchange (IKE), AES 128 e 256 (Advanced Encryption Standard) e Autenticação via certificado IKE PKI;

2.6.7.6. A solução deve suportar a importação de certificados de CA Interna e CA Externa de terceiros;

2.6.7.7. Solução deve suportar a configuração VPN através de uma interface do tipo GUI (console do fabricante ou interface web);

2.6.8. SOLUÇÃO DE PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS

2.6.8.1. A solução deverá prover as funcionalidades de inspeção de artefatos de entrada com malwares não conhecidos ou do tipo APT com filtro de ameaças avançadas e análise de execução em tempo real, sendo essa análise executada na nuvem proprietária do próprio fabricante ou appliance dedicada para sandboxing;

2.6.8.2. Prevenir através do bloqueio efetivo do malware desconhecido (Dia Zero), oriundo da comunicação Web (HTTP e HTTPS) ou E-mail (SMTP/TLS), sem que o mesmo seja entregue parcialmente

ao cliente.

2.6.8.3. A solução deve ser capaz de inspecionar e prevenir malware desconhecido em tráfego criptografado SSL;

2.6.8.4. A solução deve fornecer a capacidade de emular ataques em sistemas operacionais Windows e Linux;

2.6.8.5. Implementar atualização da base de dados de forma automática, permitindo agendamentos diários, dias da semana ou automáticos como o período de cada atualização;

2.6.8.6. A solução deve suportar as seguintes topologias de implantação: lnline ou Mirror/TAP;

2.6.8.7. A tecnologia de máquina virtual deverá possuir diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso, não sendo baseado apenas em assinaturas;

2.6.8.8. A solução de prevenção de ameaças avançadas (Sandboxing) contra ataques persistentes e Zero-Day, quando habilitada, pode funcionar de forma integrada a engines de antivírus;

2.6.8.9. Todas as máquinas virtuais (Windows e Linux) utilizadas na solução e solicitadas neste edital, devem estar integralmente instaladas e licenciadas, sem a necessidade de intervenções por parte do administrador do sistema. As atualizações deverão ser providas pelo fabricante;

2.6.8.10. Para a emulação de arquivos, a solução deve suportar arquivos com tamanho máximo de emulação de até 30Mb.

2.6.8.11. Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endereço IP;

2.6.8.12. Implementar a emulação, detecção e bloqueio de qualquer malware e/ou código malicioso detecta do como desconhecido. A

solução deve permitir a análise e bloqueio dos seguintes tipos de arquivos caso tenham malware desconhecido: pdf, tar, zip, rar, 7z, exe, rtf, xls, xlsx, xlt, xltx, xlsm, xltm, xlsb, ppt, pptx, pps, pptm, ppsx, ppsm, doc, docx;

2.6.8.13. A solução deve permitir a criação de Whitelists baseado no MD5 do arquivo;

2.6.8.14. Para melhor administração da solução, a solução deve possibilitar as seguintes

2.6.8.15. visualizações a nível de monitoração:

2.6.8.16. Quantidade de arquivos que estão em emulação;

2.6.8.17. Número de arquivos emulados;

2.6.8.18. A solução deve possuir os indicadores abaixo referente ao último dia, última semana ou últimos 30 dias:

2.6.8.19. Arquivos scaneados;

2.6.8.20. Arquivos maliciosos;

ANEXO 1-B – GERENCIAMENTO

GERENCIAMENTO CENTRALIZADO E RELATORIA

1. Deve permitir o gerenciamento e administração centralizado, possibilitando o gerenciamento de diversos equipamentos de proteção de rede desde que não sejam software livre;
2. O módulo de gerência deve ser capaz de gerenciar e administrar as soluções dos itens 1 a 6, descrito nesse termo.
3. Caso a solução possua licenciamento por número de equipamentos gerenciados, deve ser licenciada para o número necessário de equipamentos a serem gerenciados;
4. Caso a solução possua licenças relacionadas a armazenamento, deve ser ofertado a sua maior capacidade suportada ou ilimitada;
5. Caso a solução possua módulo de relatórios estendida, deve ser também entregue junto com a solução;
6. A solução de gerenciamento deverá ser entregue como appliance físico, no ambiente da CONTRATANTE;
7. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança;
8. Centralizar a administração de regras e políticas dos equipamentos de proteção de rede, usando uma única interface de gerenciamento;
9. O gerenciamento da solução deve suportar acesso via SSH, cliente do próprio fabricante ou WEB (HTTPS);
10. O gerenciamento deve permitir/possuir monitoração de logs, ferramentas de investigação de logs e acesso concorrente de administradores.
11. Deve possuir um mecanismo de preenchimento automático de comandos no gerenciamento via SSH, facilitando a localização de comandos;
12. Suportar criação de regras que fiquem ativas em horário definido e suportar criação de regras com data de expiração;
13. Suportar backup das configurações e rollback de configuração para a última configuração

salva;

14. Suportar validação de regras antes da aplicação;
15. Suportar validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
16. Deve possibilitar a integração com outras soluções de SIEM de mercado desde que não sejam software livre;
17. Suportar geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;
18. De acordo com o Item 7.3.6 E 7.3.7, deve garantir a retenção dos Logs conforme determina a Lei 12.965/2014 (Marco Civil da Internet) Arts 13 e 15;
19. De acordo com o Item 7.3.8, deve prover relatórios de todos os sistemas, portais, websites e serviços hoespedados e providos pela CONTRATANTE que contenham, no mínimo, os seguintes itens
20. Endereço IP do terminal acessando o Serviço;
21. Informação do Header X-Forward-For, quando aplicável;
22. Porta de Origem do acesso, endereço IP do Destino, Porta de Destino do Acesso;
23. Horário em timestamp EPOCH ou UTC que é logado;
24. URL Logada em acessos do método GET;
25. POST ou Request Body logados;
26. Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-Malware), etc;
27. Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus, Anti-Malware), e URLs que passaram pela solução;
28. Deve ser possível exportar os logs em CSV;
29. Deve possibilitar a geração de relatórios de eventos no formato PDF;
30. Possibilitar rotação do log;
31. Suportar geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:
32. Resumo gráfico de aplicações utilizadas, principais aplicações por utilização de largura de banda, principais aplicações por taxa de transferência de bytes, principais hosts por

número de ameaças identificadas, atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-Malware), de rede vinculadas a este tráfego;

33. Deve permitir a criação de relatórios personalizados;
34. Suportar enviar os relatórios de forma automática via PDF:
35. Deve consolidar logs e relatórios de todos os dispositivos administrados;
36. Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura;
37. Deverá possuir mecanismo de Drill-Down para navegação e análise dos logs em tempo real;
38. Nas opções de Drill-Down, deve ser possível identificar o usuário que fez determinado acesso;
39. Permitir que os relatórios possam ser salvos, enviados e impressos;
40. Deve incluir uma ferramenta do próprio fabricante ou de outro, desde que não seja software livre, ou em composição com terceiros, para correlacionar os eventos de segurança das funcionalidades adquiridas de todos os equipamentos e softwares ofertados;
41. 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.;
42. A solução deve prover, no mínimo, as seguintes funcionalidades para análise avançada dos incidentes:
43. Visualizar quantidade de tráfego utilizado de aplicações e navegação;
44. Gráficos com principais eventos de segurança de acordo com a funcionalidade selecionada;
45. A solução de correlação deve possuir mecanismo para detectar login de administradores em horários irregulares;
46. A solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credencias;

47. Deve suportar a geração de relatório gerencial para apresentar aos executivos os eventos de ataque de forma completamente visual, utilizando, para tanto, gráficos, consumo de banda utilizado pelos ataques e quantidade de eventos gerados e protegidos;
48. Deve permitir a integração com servidores de autenticação LDAP Microsoft Active Directory e Radius;
49. Permitir criações de políticas de acesso de usuários autenticada no Active Directory, de forma que reconheça os usuários de forma transparente;
50. Permitir o download de assinaturas, atualizações e firmwares para distribuição centralizada aos dispositivos de segurança integrados a mesma;
51. Permitir a visualização de gráficos e mapa de ameaças;
52. Possuir mecanismo para que logs antigos sejam removidos automaticamente;
53. Deve permitir a criação de dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino;
54. Deve possuir a capacidade de visualizar na interface gráfica da solução, informações do sistema como licenças, memória, disco e uso de CPU;
55. A solução deve ser capaz de correlacionar eventos de todas as fontes de log em tempo real;
56. A solução deve fornecer conteúdo de correlação pré-definido organizado por categoria;
57. A solução deve possuir painéis de eventos em tempo real com possibilidade de configuração das atualizações e frequências;
58. Deve disponibilizar a geração de pelo menos os seguintes tipos de relatórios:
59. Máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas e categorias Web mais acessadas;
60. Deve permitir a integração com sistemas terceiros através de API;
61. Deve permitir a criação de objetos e políticas compartilhadas;
62. Deve suportar configuração em alta disponibilidade para fins de redundância;

Nível de Classificação	Grupo de acesso
Público	**PRODAM**

ANEXO 1-C

TERMO DE RESPONSABILIDADE E CONFIDENCIALIDADE PARA FORNECEDORES E PARCEIROS

PRODAM – PROCESSAMENTO DE DADOS AMAZONAS S.A., pessoa jurídica de direito privado (sociedade de economia mista), criada pela Lei nº 941, de 10/07/1970, com seus atos constitutivos registrados na Junta Comercial do Estado, sob o nº 13300001038, e com Inscrição Estadual nº 05.341.162-5 e CNPJ nº 04.407.920/0001-80, neste ato representada por seu Diretor Presidente, Sr. LINCOLN NUNES DA SILVA, brasileiro, em união estável, administrador de empresas, portador da Cédula de Identidade nº 0748852-1 SSP/AM, inscrito no CPF/MF sob o nº 033.699.748-51, residente e domiciliado nesta cidade, no uso das atribuições que lhe confereo inciso XVI do artigo 34 do Estatuto Social, arquivado na JUCEA/AM, em data de 07/06/2018, sob o nº 970752, conforme atesta a Ata da Reunião Extraordinária do Conselho de Administraçãoda PRODAM, datada de 30/11/2020, arquivada na JUCEA, em data de 18/12/2020, sob o nº 1085793, doravante designada simplesmente CONTRATANTE, e

[NOME DA EMPRESA CONTRATADA], situada na [ENDEREÇO COMPLETO], na cidade de [CIDADE], [UF], inscrita no CNPJ sob o nº [CNPJ], neste ato devidamente representada por seu [CARGO], o Sr. [NOME COMPLETO], [NACIONALIDADE], [ESTADO CIVIL], [PROFISSÃO], portador da cédula de identidade nº [RG], [ÓRGÃO EMISSOR], e do CPF nº [CPF], doravante denominada simplesmente **CONTRATADA**, Considerando:

(i) a intenção das partes de realizar acordo comercial ou acordo de cooperação técnica a título oneroso ou não oneroso;

(ii) a possibilidade de que a CONTRATADA tenha acesso a informações confidenciais técnicas e ou estratégicas das quais a CONTRATANTE é proprietária e ou custodiante;

(iii) a necessidade, da CONTRATANTE, de resguardar a segurança de tais informações,

garantindo sua confidencialidade; e

(iv) a necessidade, da CONTRATANTE, de estabelecer regras para o manuseio e tratamento de tais informações, bem com definir o modo como estas poderão ser usadas e deverão ser protegidas.

Resolvem, na presença das testemunhas adiante nominadas, firmar o presente instrumento, vinculado ao [contrato, acordo, convênio ou ajuste], com os seguintes termos e condições:

DO OBJETO

CLÁUSULA PRIMEIRA. O objeto deste Termo é a proteção de informações confidenciais disponibilizadas pela CONTRATANTE em razão da celebração de contrato para prestação de serviços com a CONTRATADA.

DAS DEFINIÇÕES

CLÁUSULA SEGUNDA. Para os fins deste instrumento, considera-se:

(i) CONTRATO: todo e qualquer ajuste entre órgãos ou entidades da Administração Pública e particulares, em que haja acordo de vontades para a formação de vínculo e estipulação de obrigações recíprocas, seja qual for a denominação utilizada;

(ii) CONTRATANTE: órgão ou entidade da Administração Pública signatária do instrumento contratual;

(iii) CONTRATADA: pessoa física ou jurídica signatária de contrato com a Administração Pública;

(iv) INFORMAÇÃO DA CONTRATANTE: qualquer informação, elaborada ou não por parte da CONTRATADA, ou ainda, revelada pela CONTRATANTE à CONTRATADA, que esteja relacionada às atividades de prestação de serviços à CONTRATANTE, seus clientes ou fornecedores e das quais a CONTRATANTE seja proprietária e ou custodiante, e que por determinação legal seja classificada como “dados pessoais” ou confidenciais.

CLÁUSULA TERCEIRA. Não são consideradas informações da CONTRATANTE:

(i) habilidades gerais, ou experiência adquirida durante o período da execução do contrato ao qual este Termo está vinculado, quando a CONTRATADA poderia razoavelmente ter tido a expectativa de adquiri-las em situação similar ou prestando serviços a outras empresas;

(ii) informação conhecida publicamente sem a violação deste Termo ou de instrumentos similares; ou

(iii) informação cuja revelação seja exigida por lei ou regulamento, autoridade governamental ou judiciária, devendo a CONTRATADA providenciar para que, antes de tal revelação, seja a CONTRATANTE notificada da exigência (dentro dos limites possíveis diante das circunstâncias)e lhe seja proporcionada oportunidade de discuti-la.

DA INEXISTÊNCIA DE OBRIGAÇÕES CONFLITUOSAS

CLÁUSULA QUARTA. A CONTRATADA declara que:

(i) o cumprimento de seus deveres como prestadora de serviços da CONTRATANTE não violará nenhum acordo ou outra obrigação de manter informações de propriedade de terceiros, não importando a natureza de tais informações;

(ii) não está vinculada a nenhum acordo ou obrigação com terceiros, o qual esteja ou possa estar em conflito com as obrigações assumidas perante a CONTRATANTE ou que possa afetar os interesses desta nos serviços por ela realizados; e

(iii) não trará ao conhecimento de qualquer empregado, administrador ou consultor da CONTRATANTE informações confidenciais – técnicas e ou estratégicas – de propriedade de terceiros, bem como não utilizará tais informações enquanto persistir qualquer espécie de vínculo contratual entre a CONTRATANTE e a CONTRATADA e mesmo após encerrado este vínculo.

DA INFORMAÇÃO DA CONTRATANTE

CLÁUSULA QUINTA. Para os propósitos deste Termo, toda e qualquer informação da CONTRATANTE repassada à CONTRATADA, por qualquer meio, durante a execução dos serviços contratados, constitui informação privilegiada e, como tal, tem caráter de estrita confidencialidade, e que por determinação legal seja classificada como “dados pessoais” ou confidenciais, só podendo ser utilizada para fins de execução do contrato ao qual este Termo é vinculado.

CLÁUSULA SEXTA. Para os propósitos deste Termo, toda e qualquer informação incluída para processamento pela CONTRATANTE no sistema da CONTRATADA é e permanecerá de propriedade exclusiva da CONTRATANTE. Essa informação será tratada e protegida como tal,

de acordo com o estabelecido neste Termo e legislação pertinente e que por determinação legal seja classificada como “dados pessoais” ou confidenciais.

CLÁUSULA SÉTIMA. Como consequência do conhecimento de informação da CONTRATANTE, a CONTRATADA deverá guardar segredo a respeito dos negócios realizados, obrigando-se desde já a:

(i) não destruir, usar, copiar, transferir ou revelar a nenhuma pessoa ou entidade qualquer informação da CONTRATANTE, sem a sua prévia e expressa autorização;
(ii) tomar todas as precauções razoáveis para impedir a destruição, uso, cópia, transferência ou revelação inadvertida de qualquer informação da CONTRATANTE;
(iii) providenciar a devolução de todas as informações da CONTRATANTE, em qualquer meio em que estiverem armazenadas, que estejam sob sua posse e controle, dentro do prazo de 05 (cinco) dias úteis, a contar da data da extinção do vínculo contratual.
CLÁUSULA OITAVA. É expressamente vedado à CONTRATADA repassar qualquer informação da CONTRATANTE, inclusive a terceiros contratados para executar atividades decorrentes do contrato ao qual este Termo está vinculado, exceto mediante autorização prévia e expressa da CONTRATANTE, ou quando amparada por Lei ou determinação Judicial.

DAS DISPOSIÇÕES GERAIS
CLÁUSULA NONA. A CONTRATADA declara-se inteiramente responsável pelos atos praticados por seus empregados, durante e após a execução do contrato ao qual este Termo está vinculado, que impliquem no descumprimento de suas cláusulas.

CLÁUSULA DÉCIMA. **CLÁUSULA DÉCIMA**. As obrigações da CONTRATADA produzirão efeitos a partir da data da assinatura do instrumento contratual ao qual este Termo está vinculado. Qualquer violação ou ameaça de violação a este Termo irá constituir justa causa para imediata rescisão do contrato de prestação de serviços firmado, assegurados a ampla defesa e o contraditório. A rescisão não exime o infrator das penalidades previstas nos artigos 927 e seguintes do Código Civil, artigos 153 e 154 do Código Penal, assegurado o contraditório garantido pelo artigo 5º, inciso IV, da Constituição Federal da República.

CLÁUSULA DÉCIMA PRIMEIRA. As obrigações da CONTRATADA derivadas deste Termo permanecerão em vigor e produzirão seus regulares efeitos pelos próximos 5 anos ou por prazo determinado por lei, mesmo após a extinção do contrato ao qual este Termo está vinculado, conforme cada uma de suas disposições, continuando válidas e com efeito, a despeito de qualquer violação de suas cláusulas ou do contrato de prestação de serviços firmado.

CLÁUSULA DÉCIMA SEGUNDA. A CONTRATADA compromete-se a treinar os seus empregados envolvidos na prestação dos serviços à CONTRATANTE, de forma a que os mesmos estejam comprometidos e aptos a resguardar toda e qualquer informação da CONTRATANTE, nas condições estabelecidas neste Termo.

CLÁUSULA DÉCIMA TERCEIRA. A omissão ou tolerância da CONTRATANTE em exigir da CONTRATADA o estrito cumprimento das condições deste Termo não constituirá novação ou renúncia, nem afetará os seus direitos, que poderão ser exercidos a qualquer tempo.

CLÁUSULA DÉCIMA QUARTA. As Partes elegem o foro da Comarca de Manaus, Capital do Estado do Amazonas, para dirimir quaisquer dúvidas originadas do presente Termo, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

E, por assim estarem de acordo, assinam o presente instrumento em 02 (duas) vias de igual teor e para um só efeito, na presença de 02 (duas) testemunhas.

Manaus,_____/_____/_____

PRODAM – Processamento de Dados Amazonas S.A.

Nível de Classificação	Grupo de acesso
Público	**PRODAM**

CONTRATANTE

_____

[NOME DA EMPRESA CONTRATADA]

CONTRATADA

_____

Nome Testemunha 1

CPF__._____._____-_____

_____

Nome Testemunha 2

CPF__._____._____-_____

Nível de Classificação	Grupo de acesso
Público	**PRODAM**

PREGÃO ELETRÔNICO SRP 09/2024

Anexo 01-A – MODELO DE PROPOSTA DE PREÇOS

O preço deverá ser composto de acordo com a tabela abaixo:

Item	Descrição	A. Qtd.	Unid	B. Valor Mensal Unitário (R$)	C. Valor Mensal Total(R$) (A*B)	D. Valor Instalação Unitario (R$)	E. Valor Total Global (R$) (C*36)+(A*D)
1	SERVIÇO DE PROTEÇÃO DE PERÍMETRO PEQUENO PORTE POR 36 MESES	30	Mês				
2	SERVIÇO DE PROTEÇÃO DE PERÍMETRO MÉDIO PORTE POR 36 MESES	20	Mês				
3	SERVIÇO DE PROTEÇÃO DE PERÍMETRO GRANDE PORTE POR 36 MESES	20	Mês				
4	SERVIÇO DE PROTEÇÃO DE DATACENTER PEQUENO PORTE POR 36 MESES	25	Mês				
5	SERVIÇO DE PROTEÇÃO DE DATACENTER MÉDIO PORTE POR 36 MESES	20	Mês				
6	SERVIÇO DE PROTEÇÃO DE DATACENTER GRANDE PORTE POR 36 MESES	4	Mês				

Total global da proposta..... R$ xxxx,xx

O valor global da proposta deverá ser a soma da coluna E. Total Global;

Para a sessão pública, deverão ser utilizados os valores da coluna E Total Global para cada item;

Validade da Proposta: 90 (noventa) dias.

Nível de Classificação	Grupo de acesso
Público	**PRODAM**

PREGÃO ELETRÔNICO SRP Nº 09/2024

ANEXO 2 - DOCUMENTOS PARA HABILITAÇÃO

1. DOCUMENTOS PARA HABILITAÇÃO

1.1. A arrematante será avaliada quanto ao cumprimento dos requisitos de participação no certame através de consulta efetuada pelo pregoeiro em algum dos seguintes cadastros:

1.1.1. Cadastro Nacional de Empresas Inidôneas e Suspensas – CEIS, no endereço eletrônico: www.portaldatransparencia.gov.br/sancoes/ceis;

1.1.2. Cadastro Nacional de Empresas Punidas – CNEP, no endereço eletrônico: www.portaldatransparencia.gov.br/sancoes/cnep

1.1.3. Outros sistemas cadastrais pertinentes com disposição para consulta.

1.2. Constatada a existência de sanção, o Pregoeiro reputará o licitante inabilitado, por falta de condição de participação e examinará as mesmas circunstâncias para o segundo colocado.

1.3. Caso atendidas as condições de participação, a arrematante terá seus documentos de habilitação verificada por meio do SICAF, nos documentos por ele abrangidos em relação à habilitação jurídica, à regularidade fiscal e trabalhista, à qualificação econômica financeira e habilitação técnica.

1.4. É dever do licitante atualizar previamente as comprovações constantes do SICAF para que estejam vigentes na data de abertura da sessão pública, ou encaminhar, em conjunto com a apresentação da proposta, a respectiva documentação atualizada.

1.5. Havendo a necessidade de envio de documentos de habilitação complementares, necessários à confirmação daqueles exigidos neste Edital e já apresentados, o licitante será convocado a encaminhá-los, em formato digital, via sistema, no prazo de 2 (duas) horas.

1.6. Se o arrematante desatender às exigências habilitatórias, o pregoeiro examinará a documentação do licitante subsequente e, assim, sucessivamente até a apuração de documentação que atenda os termos do edital.

1.7. **Habilitação Jurídica:**

1.7.1. Registro comercial, no caso de empresa individual;

1.7.2. Ato constitutivo (Estatuto ou Contrato Social em vigor), devidamente registrado no Órgão competente, acompanhado de documento comprobatório da eleição dos atuais administradores;

1.7.3. Inscrição do Ato Constitutivo, no caso de Sociedades Civis, acompanhada de prova de designação da diretoria em exercício.

1.8. **Qualificação Econômico-Financeira:**

1.8.1. Certidão negativa ou positiva com efeito negativa de existência de ação de recuperação judicial de falência ou concordata, expedida pelo Cartório de Distribuição da sede da licitante;

1.8.2. Cópia do balanço patrimonial, demonstração de resultado de exercício e demais

demonstrações contábeis da licitante, dos 2 (dois) últimos exercícios sociais, devidamente registrados na Junta Comercial, **na forma da lei**[1]. Em se tratando de empresas regidas pela Lei 6.404 de 15/12/1976, essa comprovação deverá ser feita através da publicação na Imprensa Oficial, apresentando a boa situação financeira da licitante, vedada a sua substituição por balancetes ou balanços provisórios. Os demonstrativos poderão ser atualizados por índices oficiais quando encerrado há mais de três meses da data prevista para realização desta licitação. (Devem-se incluir no balanço patrimonial os Termos de Abertura e Encerramento). **Deverá comprovar que possui capital social registrado ou patrimônio líquido mínimo igual ou superior, a 5% do valor global de sua proposta.**

1.8.2.1. A comprovação do subitem 1.8.2 deverá ser feita através do Balanço Patrimonial do último exercício publicado (contendo termo de abertura e encerramento), assinado por profissional devidamente habilitado pelo conselho de classe **OU** através da alteração do capital social em momento anterior à apresentação da proposta**.**

1.8.3. Comprovação da boa situação financeira da licitante, aferida com base nos índices de Liquidez Geral (ILG), iguais ou maiores que um (>1), aplicando a seguinte fórmula:

$$\frac{\text{ATIVO CIRCULANTE + REALIZÁVEL A LONGO PRAZO}}{\text{PASSIVO CIRCULANTE + PASSIVO NÃO CIRCULANTE}}$$

1.8.3.1. A comprovação do subitem 1.8.3 deverá ser feita através do Balanço Patrimonial do último exercício publicado (contendo termo de abertura e encerramento), assinado por profissional devidamente habilitado pelo conselho de classe.

1.8.4. A comprovação de que o profissional está devidamente habilitado, exigida nos itens 1.8.2.1 e 1.8.3.1, deverá ser comprovada por meio de emissão de certidão de regularidade profissional no devido conselho de classe.

1.9. **Regularidade Fiscal e Trabalhista:**

1.9.1. Inscrição no Cadastro Nacional de Pessoa Jurídica (CNPJ), do Ministério da Fazenda;

1.9.2. Certidões de regularidade fiscal e previdenciária apresentando Certidão Negativa de ou Positiva com Efeitos de Negativa de Débitos relativos a Créditos Tributários Federais e

---

[1] ***Na forma da lei:***

- Indicação do número das páginas e número do livro onde estão inscritos o Balanço Patrimonial e as Demonstrações Contábeis no Livro Diário, acompanhados do respectivo Termo de Abertura e Termo de Encerramento do mesmo - § 2º do art. 1.184 da Lei 10.406/02; Art. 1.180, lei 10.406/02; art. 177 da lei 6.404/76;

- Assinatura do contador e do titular ou representante legal da Entidade no Balanço Patrimonial e a Demonstração do Resultado do Exercício - § 2º do art. 1.184 da lei 10.406/02; § 4º do art. 177 da lei 6.404/76.

- Prova de registro na Junta Comercial ou Cartório (carimbo, etiqueta ou chancela da Junta Comercial) – art. 1.181, lei 10.406/02; resolução CFC nº 563/83; § 2º do art. 1.184 da lei 10.406/02.

- Demonstração de escrituração Contábil/Fiscal/Pessoal regular – NBC T 2 (Resolução CFC 563/83; art. 179, lei 10.406/02; art. 177 da lei 6.404/76; OU as empresas obrigadas ao envio do SPED CONTÁBIL deverão apresentar o recibo de entrega e o termos de abertura e de encerramento constantes na escrituração contábil digital.

- Boa situação financeira – art. 7.1, inciso V da IN/MARE 05/95

à Dívida Ativa da União **(portaria conjunta PGFN/RFB nº 1751/2014)**, Fazendas Estadual e Municipal ou do Distrito Federal, conforme domicílio/sede da licitante.

1.9.3. Prova de regularidade relativa ao Fundo de Garantia Por Tempo de Serviço (FGTS) demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei;

1.9.4. 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 artigo 642-A da Consolidação das Leis do Trabalho, acrescentado pelo Decreto-Lei nº 12.440 de 7 de julho de 2011, e na Resolução Administrativa nº 1470/2011 do Tribunal Superior do Trabalho, de 24 de agosto de 2011, em validade.

1.10. **Qualificação Técnico-operacional:**

1.10.1. A LICITANTE deve apresentar no mínimo 03 (três) ATESTADOS de CAPACIDADE TÉCNICA focados em prestação de Serviços Gerenciados de Segurança, 24x7x365, onde foram prestados os serviços: Firewall/VPN, IPS, Filtro Web, conferido por empresas públicas ou privadas e que possuam, pelo menos, 300 (trezentos) hosts gerenciados, devidamente emitidos por entidades públicas e/ou privadas. Os atestados deverão conter as seguintes informações:

- Nome, CNPJ e endereço completo do emitente;
- Nome da empresa que prestou o serviço ao emitente;
- Data de emissão do atestado ou da certidão;
- Assinatura e identificação do signatário (nome, cargo ou função que exerce junto à emitente);
- Descrição do tipo do serviço executado (ou nome do evento realizado e sua descrição, em caso de licitação para área de turismo, cultura, esporte e lazer) ou dos produtos fornecidos.

1.10.2. A LICITANTE deverá apresentar documento comprovando ser parceira qualificada dos fabricantes das soluções por ela ofertadas.

1.11. Declaração de inexistência de fato superveniente impeditivo de habilitação, conforme Anexo 4 – Modelo de Declaração de Fato Superveniente Impeditivo da Habilitação.

1.12. Declaração da empresa de que não possui, em seu quadro de pessoal, empregado (s) menor (es) de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e, menores de 16 (dezesseis) anos em qualquer trabalho, salvo na condição de aprendiz, a partir de 14 (quatorze) anos, nos termos do artigo 7º, inciso XXXIII, da Constituição Federal, conforme Anexo 5 – Modelo de Declaração Quanto ao Cumprimento às Normas Relativas ao Trabalho do Menor.

1.13. O Pregoeiro reserva-se o direito de solicitar das licitantes, em qualquer tempo, no curso da licitação, quaisquer esclarecimentos sobre documentos já entregues, fixando-lhes prazo para atendimento.

1.14. O pregoeiro poderá convocar o licitante para enviar documento complementar, em formato digital, por meio de funcionalidade disponível no sistema, no prazo de 2 (duas) horas, sob pena de desclassificação.

1.15. Dentre os documentos passíveis de solicitação pelo Pregoeiro, destacam-se os que contenham

as características do material ofertado, a exemplo de catálogos, folhetos ou propostas, ou planilhas de custos retificadas (em caso de contratação de serviços), encaminhados por meio eletrônico, ou, se for o caso, por outro meio e prazo indicados pelo pregoeiro, sem prejuízo do seu ulterior envio pelo sistema eletrônico, sob pena de não aceitação da proposta.

1.16. Sem prejuízo da obrigatoriedade de envio por meio do sistema do site https://www.gov.br/compras/, o pregoeiro poderá solicitar o envio para o e-mail: licitacoes@prodam.am.gov.br.

1.17. Os documentos de habilitação deverão estar em nome da licitante, com o número do CNPJ e respectivo endereço referindo-se ao local da sede da empresa licitante. Se o licitante for matriz, todos os documentos deverão estar em nome da matriz, e se o licitante for a filial, todos os documentos deverão estar em nome da filial, exceto aqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

PREGÃO ELETRÔNICO SRP Nº 09/2024

ANEXO 3 – ATA DE REGISTRO DE PREÇOS Nº XX/20XX

Ao xxxx dia do mês de xxxxx do ano de dois mil e xxxxxxx (xx/xx/20xx), nesta cidade de Manaus, Capital do Estado do Amazonas, República Federativa do Brasil, presentes, de um lado, a PRODAM – Processamento de Dados Amazonas S.A., pessoa jurídica de direito privado, sociedade de economia mista, criada pela Lei n.º 941, de 10/07/1970, com seus atos constitutivos registrados na Junta Comercial do Estado do Amazonas, sob o n.º 13300001038, e com inscrição estadual n.º 05.341.162-5, inscrição municipal n.º 673801 e C.N.P.J. n.º 04.407.920/0001-80, neste ato representada por seu Diretor-Presidente, conforme Portaria Interna n.º 159.2019 de 27 de maio de 2019, Sr. XXXXXXXXXXXXXXXXXXXXXX, nacionalidade, estado civil, profissão, portador da Cédula de Identidade n.º xxxxxxxxxxxxxxxxxx e do CPF n.º xxxxxxxxxxxxxxxxxxx, residente e domiciliado nesta cidade, no uso das atribuições que lhe confere o Estatuto Social, em seu artigo 34, inciso XVI, conforme atesta a Ata de Reunião Extraordinária do Conselho de Administração da PRODAM, datada de 31/01/2019 e registrada na JUCEA sob o n.º 979877, considerando julgamento da licitação na modalidade de Pregão, na forma XXXXXXXXXX, para REGISTRO DE PREÇOS n° XX/20XX, publicada no Diário Oficial do Estado do Amazonas de xx/xx/2019, processo administrativo SPROWEB XXXX/20XX, RESOLVE registrar os preços da(s) empresa(s) indicada(s) e qualificada(s) nesta ATA, de acordo com a classificação por ela(s) alcançada(s) e na(s) quantidade(s) cotada(s), sujeitando-se as partes às normas contidas na Lei nº 13.303, de 30.06.2016, Decreto Estadual nº 39.032, de 24.05.2018, Lei nº 10.520, de 17.07.2002, Lei Complementar nº 123, de 14.12.2006, Decreto Estadual nº 21.178, de 27.09.2000, Decreto nº. 5.450, de 31 de maio de 2005, Decreto Estadual nº 24.818, de 27.01.2005, Decreto Estadual nº 40.674, de 14.05.2019, Decreto nº 10.024 de 20.09.2019 e alterações e RILC - Regulamento Interno de Licitações e Contratos da PRODAM e ainda, pelo estabelecido no presente Edital e seus Anexos, e em conformidade com as disposições a seguir:

1. **DO OBJETO:**
   XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

   XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

   XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

   XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

2. **DO FORNECEDOR REGISTRADO:** a partir desta data, fica registrado na PRODAM, observada a ordem de classificação, os preços dos fornecedores a seguir relacionados, objetivando o compromisso discriminado no Anexo deste instrumento, nas condições estabelecidas no ato convocatório:

   2.1. Fornecedor: **XXXXXXXXXXXXXXXXXXXXXXXXXXXX**, CNPJ nº xxxxxxxxx/xxxxx-xx, com sede na xxxxxxxxxx, nº xxx, bairro, CEP xxxxxxx, Cidade/ESTADO, telefone (XX) XXXXXXXX/ XXXXXXXX, E-mail: xxxxxxxxxxxxxxxxxxxxxxxx, representada por xxxxxxxxxx, Xx. **XXXXXXXXXXXXXXXX**, nacionalidade, profissão, estado civil, residente e domiciliado xxxxxxxxxx, nº xxx, bairro, CEP xxxxxxx, Cidade/ESTADO, RG nº xxxxxxx XXX/XXe CPF nº XXXXXXXXXXX.

   2.2. Fornecedor: **XXXXXXXXXXXXXXXXXXXXXXXXXXXX**, CNPJ nº xxxxxxxxx/xxxxx-xx, com sede na xxxxxxxxxx, nº xxx, bairro, CEP xxxxxxx, Cidade/ESTADO, telefone (XX) XXXXXXXX/ XXXXXXXX, E-mail: xxxxxxxxxxxxxxxxxxxxxxxx, representada por xxxxxxxxxx, Xx. **XXXXXXXXXXXXXXXX**, nacionalidade, profissão, estado civil, residente e domiciliado xxxxxxxxxx, nº xxx, bairro, CEP xxxxxxx, Cidade/ESTADO, RG nº xxxxxxx XXX/XXe CPF nº XXXXXXXXXXX.

   2.3. (...)

3. **CADASTRO DE RESERVA**

   3.1. A PRODAM utilizará o cadastro de reserva, no caso de impossibilidade de atendimento pelo primeiro colocado da ata, nas hipóteses previstas nos art. 24 do Decreto Estadual nº 40.674, de 14.05.2019.

   3.2. As empresas que integrarem o cadastro de reserva somente terão sua proposta, bem como sua documentação habilitatória, analisada, para fins de aceitação e habilitação, quando houver necessidade de contratação de fornecedor remanescente, nas hipóteses mencionadas.

4. **DA EXPECTATIVA DO FORNECIMENTO:** o ajuste com o fornecedor registrado será formalizado pela PRODAM mediante emissão de Pedido de Compra e ou Autorização para Execução do Serviço, observadas as disposições contidas no **Edital do Pregão SRP nº XX/20XX.**

   4.1. O compromisso de entrega só estará caracterizado mediante o comprovado recebimento, pelo Fornecedor, de Pedido de Compra e ou Autorização para Execução do Serviço, decorrente desta Ata de Registro de Preços e Edital do Pregão SRP nº XX/20XX.

   4.2. O fornecedor registrado fica obrigado a atender todos os pedidos efetuados durante a validade desta Ata de Registro de Preços.

5. **DO CONTROLE DOS PREÇOS REGISTRADOS:** a PRODAM adotará a prática de todos os atos necessários ao controle e administração da presente Ata.

   5.1. Os preços registrados e a indicação dos respectivos fornecedores detentores da Ata serão publicados na imprensa oficial e divulgados em meio eletrônico.

6. **DA READEQUAÇÃO DOS PREÇOS REGISTRADOS:** a qualquer tempo, o preço registrado poderá ser revisto em decorrência de eventual redução daqueles existentes no mercado, cabendo a PRODAM convocar os fornecedores registrados para negociar o novo valor.
   6.1. Caso o fornecedor registrado se recuse a baixar os preços registrados, a PRODAM poderá cancelar o registro ou convocar todos os fornecedores registrados para oferecerem novos envelopes de propostas, gerando novo julgamento e adjudicação para esse fim.
   6.2. Durante o período de validade da Ata de Registro de Preços, os preços não serão reajustados, ressalvada a superveniência de normas gerais ou estaduais aplicáveis à espécie.
   6.3. O diferencial de preço entre a proposta inicial do fornecedor detentor da Ata e a pesquisa de mercado efetuada pela PRODAM à época da abertura da proposta, bem como eventuais descontos por ela concedidos, serão mantidos durante a vigência da Ata de Registro de Preços.

7. **DO CANCELAMENTO DO REGISTRO DE PREÇOS:** o fornecedor registrado terá o seu registro cancelado quando:
   7.1. Descumprir as condições da Ata de Registro de Preços;
   7.2. Não aceitar reduzir seus preços registrados na hipótese de se tornarem superiores aos praticados no mercado;
   7.3. Houver razões de interesse público.
   7.4. O cancelamento de registro, nas hipóteses previstas, assegurados o contraditório e a ampla defesa e, será formalizado por despacho da autoridade competente.
   7.5. O fornecedor registrado poderá solicitar o cancelamento de seu registro de preço na ocorrência de caso fortuito ou de força maior comprovados.

8. **DA VALIDADE DA ATA DE REGISTRO DE PREÇOS:** A presente Ata terá validade de 12 (doze) meses contada a partir da data de sua assinatura, podendo ser prorrogada uma única vez por igual período.

9. **DO PRAZO DE ENTREGA:** o prazo de entrega será de 30 (trinta) dias corridos contados a partir da emissão do Pedido de Compra.

10. **DA DIVULGAÇÃO DA ATA DE REGISTRO DE PREÇOS:** A presente Ata será divulgada no portal da internet www.prodam.am.gov.br.

11. **DO FORO:** as dúvidas decorrentes da presente Ata serão dirimidas no Foro de Manaus, com renúncia de qualquer outro.

E por estarem de acordo com as disposições contidas na presente Ata, assinam este instrumento a PRODAM e o fornecedor registrado, na pessoa dos seus representantes legais, que vai assinada, em 2 (duas) vias, de igual e teor e forma.

Nível de Classificação	Grupo de acesso
Público	**PRODAM**

MANAUS, xx de xxxxxxx de 201X.

Pela **PRODAM S.A.**

XXXXXXXXXXXXXXXX

Diretor-Presidente

Pela **XXXXXXXXXXXXXXXXXXXXXXXXXXXX**

XXXXXXXXXXXXXXXX

Representante legal

REVISÃO E APROVAÇÃO:

XXXXXXXXXXXX

Assessor Jurídico

OAB/AM – XXXXXXXXXXXXXX

Nível de Classificação	Grupo de acesso
Público	**PRODAM**

ANEXO DA ATA DE REGISTRO DE PREÇOS Nº XX/202X

PREGÃO ELETRÔNICO SRP Nº 09/2024

VALOR TOTAL DA ATA: R$ XXXXXXXXXX (xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)

Pela **PRODAM S.A.**

XXXXXXXXXXXXXXXX
Diretor-Presidente

Pela **XXXXXXXXXXXXXXXXXXXXXXXXXXX**

XXXXXXXXXXXXXXXX
Representante legal

Nível de Classificação	Grupo de acesso
Público	**PRODAM**

PREGÃO ELETRÔNICO SRP Nº 09/2024

ANEXO 4 – MODELO DE DECLARAÇÃO DE FATO SUPERVENIENTE IMPEDITIVO DE HABILITAÇÃO

_____

(Nome da Empresa)

CNPJ/MF Nº _____, sediada

_____

(Endereço Completo)

declara, sob as penas da Lei, que até a presente data inexistem fatos impeditivos para sua habilitação no presente processo ciente da obrigatoriedade de declarar ocorrências posteriores.

_____

(Local e Data)

_____

(Nome e Número da Carteira de Identidade do Declarante)

OBS: Está declaração deverá ser emitida em papel timbrado da empresa proponente e carimbada com o número do CNPJ.

Nível de Classificação	Grupo de acesso
Público	**PRODAM**

PREGÃO ELETRÔNICO SRP Nº 09/2024

ANEXO 5 - MODELO DE DECLARAÇÃO QUANTO AO CUMPRIMENTO ÀS NORMAS RELATIVAS AO TRABALHO DO MENOR

(Nome da Empresa)

CNPJ/MF Nº _____, sediada.

(Endereço Completo)

Declaro que não possuímos, em nosso Quadro de Pessoal, empregados menores de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e em qualquer trabalho, menores de 16 (dezesseis) anos, salvo na condição de aprendiz, a partir de 14 (quatorze) anos, em observância ao artigo 7º, inciso XXXIII, da Constituição Federal

(Local e Data)

(Nome e Número da Carteira de Identidade do Declarante)

OBS: 1) Esta declaração deverá ser emitida em papel timbrado da empresa proponente e carimbada com o número do CNPJ.

2) Se a empresa licitante possuir menores de 14 anos aprendizes deverá declarar essa condição.

Nível de Classificação	Grupo de acesso
Público	**PRODAM**

PREGÃO ELETRÔNICO SRP Nº 09/2024

ANEXO 6 - TABELA DE PREÇO MÁXIMO

Item	Descrição	A. Qtd.	Unid	B. Valor Mensal Unitário (R$)	C. Valor Mensal Total(R$) (A*B)	D. Valor Instalação Unitario(R$)	E. Valor Total Global (R$) (C*36)+(A*D)
1	SERVIÇO DE PROTEÇÃO DE PERÍMETRO PEQUENO PORTE POR 36 MESES	30	Mês	508,84	15.265,20	7.190,49	765.261,90
2	SERVIÇO DE PROTEÇÃO DE PERÍMETRO MÉDIO PORTE POR 36 MESES	20	Mês	1.794,68	35.893,60	9.317,23	1.478.514,20
3	SERVIÇO DE PROTEÇÃO DE PERÍMETRO GRANDE PORTE POR 36 MESES	20	Mês	2.368,26	47.368,20	11.406,66	1.933.280,40
4	SERVIÇO DE PROTEÇÃO DE DATACENTER PEQUENO PORTE POR 36 MESES	25	Mês	9.660,16	241.504,00	29.034,90	9.420.016,50
5	SERVIÇO DE PROTEÇÃO DE DATACENTER MÉDIO PORTE POR 36 MESES	20	Mês	22.171,30	443.426,00	64.066,08	17.244.657,60
6	SERVIÇO DE PROTEÇÃO DE DATACENTER GRANDE PORTE POR 36 MESES	4	Mês	67.540,66	270.162,64	185.702,83	10.468.666,36

Deverá ser respeitado o valor máximo de cada ITEM, sob pena de desclassificação.

Nível de Classificação	Grupo de acesso
Público	**PRODAM**

PREGÃO ELETRÔNICO Nº 09/2024

ANEXO 7 – MODELO DE DECLARAÇÃO – SOMENTE PARA MICRO E PEQUENAS EMPRESAS

(NOME DA EMPRESA), com sede (endereço completo), inscrita no CNPJ sob o nº..... DECLARA à PRODAM – Processamento de Dados Amazonas S.A., para fins de **não incidência** na fonte da Contribuição Social sobre o Lucro Líquido (CSLL), da Contribuição para o Financiamento da Seguridade Social (Cofins), e da Contribuição para o PIS/Pasep, a que se refere o art. 30 da Lei nº 10.833, de 29 de dezembro de 2003, que é regularmente inscrita no Regime Especial Unificado de Arrecadação de Tributos e Contribuições devidos pelas Microempresas e Empresas de Pequeno Porte - Simples Nacional, de que trata o art. 12 da Lei Complementar nº 123, de 14 de dezembro de 2006.
Para esse efeito, a declarante informa que:

I – Preenche os seguintes requisitos:

a) Conserva em boa ordem, pelo prazo de cinco anos, contado na data de emissão, os documentos que comprovam a origem de suas receitas e a efetivação de suas despesas, bem assim a realização de quaisquer outros atos ou operações que venham a modificar sua situação profissional;
b) Cumpre as obrigações acessórias a que está sujeita, em conformidade com a legislação pertinente;

II – O signatário é representante legal desta empresa, **assumindo o compromisso de informar** à Secretaria da Receita Federal do Brasil e à PRODAM – Processamento de Dados Amazonas S.A., **imediatamente**, eventual desenquadramento da presente situação e está ciente de que a falsidade na prestação destas informações, sem prejuízo do disposto no art. 32 da Lei nº 9.430, de 1996, o sujeitará, juntamente com as demais pessoas que para ela concorrem, às penalidades previstas na legislação criminal e tributária, relativas à falsidade ideológica (art. 299 do Código Penal) e ao crime contra a ordem tributária (art.1º da Lei nº 8.137, de 27 de dezembro de 1990).

Local e Data

Assinatura do Representante

Nível de Classificação	Grupo de acesso
Público	**PRODAM**

PREGÃO ELETRÔNICO Nº 09/2024

ANEXO 8 – CHECKLIST– PROGRAMA DE INTEGRIDADE

Item	Atendido?		
	Sim	**Não**	**Não se Aplica**
1 - O grau de comprometimento da alta direção da pessoa jurídica, incluídos os Conselhos, quando aplicado, está evidenciado pelo apoio visível e inequívoco ao Programa? (participação em reuniões e avaliações periódicas, elaboração de dispositivos de controle, etc.)			
2 – Os padrões de conduta, código de ética, políticas e procedimentos de integridade apresentados pela entidade são de conhecimento dos funcionários (cópia de documento entregue na contratação, publicação na empresa, etc.)?			
3 – O nível de adesão dos padrões de conduta, código de ética e políticas de integridade estendidos, quando necessário, a terceiros, tais como, fornecedores, prestadores de serviço, agentes intermediários e associados, está sendo monitorado?			
4 – A realização dos treinamentos periódicos sobre o Programa de Integridade está devidamente registrada?			
5 – Os mecanismos de acompanhamento da análise periódica de riscos para realizar adaptações necessárias ao Programa de Integridade estão disponíveis e tem um cronograma estabelecido?			
6 – Os controles internos que asseguram a pronta elaboração e confiabilidade de relatórios e demonstrações financeiras estão atualizados e em conformidade com os padrões das demonstrações contábeis?			
7 – Os canais de denúncia de irregularidades, abertos e amplamente divulgados a funcionários e terceiros, e de mecanismos destinados à proteção de denunciantes de boa-fé são efetivamente monitorados? (relatórios periódicos, reuniões de avaliação, documentação relativa a tomada de providências, etc.)			
8 – Existem medidas disciplinares em caso de violação do Programa de Integridade e sua efetividade (monitoramento das violações documentadas, relatórios de acompanhamento das medidas, registro e acompanhamento de medidas tomadas, etc.)?			

9 – Os procedimentos internos quanto ao Programa de Integridade, asseguram a pronta interrupção de irregularidades ou infrações detectadas e a tempestiva remediação dos danos gerados?			
10 – As diligências apropriadas para contratação e, conforme o caso, supervisão de terceiros, tais como, fornecedores, prestadores de serviço, agentes intermediários e associados, são devidamente registradas e seu acompanhamento periódico é documentado?			

Atesto para os devidos fins que a Contratada atende aos requisitos relacionados no Checklist referente a implantação do Programa de Integridade.

Contrato nº.: _____

Fiscal do Contrato: _____

Cargo: _____ CPF.:_____

Nível de Classificação	Grupo de acesso
Público	**PRODAM**

PREGÃO ELETRÔNICO Nº 09/2024

ANEXO 9 – MINUTA DE CONTRATO

CONTRATO N.º XXX/2024

TERMO DE CONTRATO DE PRESTAÇÃO XXXXXXXXXXXXXXXXXXXXXXXXXXXX, FIRMADO ENTRE A PRODAM - PROCESSAMENTO DE DADOS AMAZONAS S/A E A XXXXXXXXXXXXX, NA FORMA ABAIXO:

Na data da assinatura eletrônica [ou "Aos XX dias do mês de XXXX do ano de dois mil e xxxxx (xx/xx/xxxx)], nesta cidade de Manaus, Capital do Estado do Amazonas, República Federativa do Brasil, presentes, de um lado, a **PRODAM – Processamento de Dados Amazonas S.A.**, doravante designada **CONTRATANTE**, pessoa jurídica de direito privado, sociedade de economia mista, criada pela Lei N.º 941, de 10/07/1970, com seus atos constitutivos registrados na Junta Comercial do Estado do Amazonas, sob o N.º 13300001038, e com inscrição estadual N.º 05.341.162-5 e CNPJ N.º 04.407.920/0001-80, neste ato representada por seu Diretor-Presidente, **XXXXXX**, xxxx, xxxx, xxxx, portador da Cédula de Identidade N.º xxxx e do CPF N.º xxxx, residente e domiciliado nesta cidade, no uso das atribuições que lhe confere o Estatuto Social, em seu artigo 34, inciso XVI, conforme atesta a Ata de Reunião Extraordinária do Conselho de Administração datada de 05/05/2022 e Ata Registrada na Junta Comercial do Estado do Amazonas sob o N.º 1196758 em 10/05/2022 e, de outro lado, **XXXXXX**, doravante designada simplesmente **CONTRATADA**, com sede em xxxx, na Rua xxxx, N.º xxx, Bairro xxxx, CEP xx.xxx-xxx, sob o NIRE N.º xxxx com inscrição municipal N.º xxxx e inscrita no CNPJ N.º xxxx, neste ato representada pelo Sr. **XXXXXX**, xxxx, xxxx, xxxx, portador da Cédula de Identidade N.º xxxx e do CPF N.º xxxx, residente e domiciliado em xxxx tendo em vista o que consta no **Processo de Licitação – Pregão Eletrônico N.º xx/xxxx**, devidamente homologado em xx/xx/xxxx e publicado no Diário Oficial do Estado do Amazonas datado de xx/xx/xxxx, tudo em conformidade com a Lei N.º 13.303 de 30 de junho de 2016, e demais alterações, e o RILC - Regulamento Interno de Licitações e **CONTRATO**s da **CONTRATANTE**, aplicando-se subsidiariamente as disposições estabelecidas no presente instrumento convocatório, seus anexos e proposta encaminhada pela **CONTRATADA**, resolvem as partes celebrar o presente **CONTRATO**, doravante simplesmente denominado "**CONTRATO**", que se regerá de acordo com as seguintes cláusulas e condições, abaixo descritas, mutuamente aceitas e reciprocamente outorgadas, por si e seus sucessores:

Nível de Classificação	Grupo de acesso
Público	**PÚBLICO**

1. CLÁUSULA PRIMEIRA: DO OBJETO

1.1. Contratação de Serviços Gerenciados de Segurança da Informação destinados a proteção das redes computacionais dos clientes da **CONTRATANTE**, compreendendo a alocação de equipamentos Firewall de Próxima Geração (Next Generation Firewall - NGFW), operação e monitoramento remoto em regime 24x7, software para o gerenciamento centralizado e emissão de relatórios, prestação de serviços para instalação e configuração da solução, suporte técnico do fabricante para o hardware com garantia da solução e licenciamento do software para atualizações pelo período de 36 meses, **TREINAMENTO OFICIAL DO FABRICANTE** e transferência de conhecimento da solução para a equipe da **CONTRATANTE**.

2. CLÁUSULA SEGUNDA - DO DETALHAMENTO DO OBJETO

2.1. **Dos Serviços a Serem Contratados.**

2.1.1. **Dos Serviços Gerenciados de Segurança da Informação destinados a proteção das redes computacionais**

2.1.1.1 Os quantitativos dos serviços objeto deste **CONTRATO** estão descritos conforme tabela abaixo:

ITEM	DESCRIÇÃO	QTDE
1	SERVIÇO DE PROTEÇÃO DE PERÍMETRO PEQUENO PORTE	30
2	SERVIÇO DE PROTEÇÃO DE PERÍMETRO MÉDIO PORTE	20
3	SERVIÇO DE PROTEÇÃO DE PERÍMETRO GRANDE PORTE	20
4	SERVIÇO DE PROTEÇÃO DE DATACENTER PEQUENO PORTE	25
5	SERVIÇO DE PROTEÇÃO DE DATACENTER MÉDIO PORTE	20
6	SERVIÇO DE PROTEÇÃO DE DATACENTER GRANDE PORTE	4

2.1.1.2 **Especificações Técnicas**

2.1.1.2.1 Todas as especificações Técnicas estão contidas no **item 7 e no ANEXO I-A** do Termo de Referência do Edital do Pregão Eletrônico N.º xx/xxxx, parte integrante deste CONTRATO;

2.1.1.2.2 A CONTRATADA se responsabiliza por atender todas as condições existentes neste CONTRATO e no Termo de Referência do Edital do Pregão Eletrônico N.º xx/xxxx, parte integrante deste CONTRATO.

2.1.2. **Do Treinamento Oficial do Fabricante**

2.1.1.3 A **CONTRATADA** deverá prover **TREINAMENTO OFICIAL" de capacitação para até 03 (três) turmas de no mínimo 05 (cinco) colaboradores por turma** pertencente exclusivamente ao time técnico da **CONTRATANTE**;

2.1.1.4 O treinamento deverá ser executado pelo próprio fabricante ou empresa por ele certificada para essa finalidade;

2.1.1.5 O treinamento deverá ser promovido em local físico dentro das dependências da **CONTRATANTE** (Modalidade IN COMPANY) ou local por ela definido;

2.1.1.6 Ao final dos treinamentos, deverá ser emitido um certificado oficial a todos os participantes e um voucher, também por participante, de realização da prova de certificação oficial da solução adquirida;

2.1.1.7 O treinamento deverá ocorrer antes da entrega/implantação/migração dos equipamentos;

2.1.1.8 Realizar a transferência de conhecimento nas etapas de implantação e migração do equipamento;

2.1.3. **Da Prestação do Serviço**

2.1.1.9 Todos os equipamentos ou componentes necessários à prestação dos serviços deverão ser novos e de primeiro uso e não constar, no momento da apresentação da proposta, em listas de end-of-sale, end-of-support ou end-of-life do fabricante.

2.1.1.10 Os equipamentos ou componentes necessários à prestação dos serviços não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante.

2.1.1.11 Caso o equipamento venha ser descontinuado, a **CONTRATADA** deverá substitui-lo sem custos adicionais para a **CONTRATANTE;**

2.1.1.12 A **CONTRATADA** também será responsável pela administração e manutenção do serviço em regime de 24x7x365 para atendimentos remotos e o regime 8x5 para atendimentos realizados pelo técnico residente e/ou para aqueles atendimentos que possam ser necessários a vinda de um especialista na forma presencial, durante todo o período do serviço objeto deste **CONTRATO**.

2.1.1.13 As tarefas atinentes ao transporte, deslocamento e remessa necessários, seja na implementação, substituição e/ ou remoção de equipamentos defeituosos será de responsabilidade da **CONTRATADA;**

2.1.1.14 As demais disposições sobre o detalhamento da prestação do serviço estão contidas no item 8 – **CONDIÇÕES PARA A PRESTAÇÃO DE SERVIÇO** -, no Termo de Referência do Edital do Pregão Eletrônico SRP N.º 09/2024, parte integrante deste **CONTRATO**;

3. CLÁUSULA TERCEIRA – DO REGIME DE EXECUÇÃO DO CONTRATO

3.1. Os serviços ora contratados serão executados sob o **regime de empreitada por preço unitário.**

4. CLÁUSULA QUARTA – DOS PREÇOS E CONDIÇÕES DE PAGAMENTO

4.1. O **Valor Mensal Estimado** do serviço contratado é de **R$ xxxx** (xxxx reais) perfazendo o **Valor Global Estimado** de **R$ xxxx** (xxxx reais).

4.2. O pagamento ocorrerá **MENSALMENTE**, de acordo com a apuração da quantidade de serviços demandados na **Autorização de Execução de Serviço** - AES e devidamente atestados pela **CONTRATANTE**, conforme apresentação de relatório de execução de serviço;

4.3. O pagamento será efetuado mediante apresentação da Nota Fiscal/Fatura e ocorrerá até o 15º (décimo quinto) dia útil do mês subsequente, com os descontos legais (retenções);

4.4. Será de responsabilidade da **CONTRATADA** disponibilizar relatório de execução de serviço junto com a Nota Fiscal/Fatura para apuração de valores.

5. CLÁUSULA QUINTA – DO REAJUSTAMENTO

5.1. A **CONTRATADA** poderá solicitar reajuste de preços dos itens a cada 12 meses, visando manter o equilíbrio econômico-financeiro do **CONTRATO**, desde que apresente tabela de custos justificando a necessidade;

5.2. O reajuste de preços se dará com base no **Índice de Custo de Tecnologia da Informação** (ICTI) acumulado de 12 (doze) meses, calculado e divulgado pelo Instituto de Pesquisa Econômica Aplicada (IPEA).

6. CLÁUSULA SEXTA – DA VIGÊNCIA DO CONTRATO

6.1. O prazo da prestação dos serviços ora contratados é de **36 (trinta e seis) meses**, contados a partir da data da assinatura do **CONTRATO**, podendo ser prorrogado mediante justificativa por escrito e prévia autorização da **CONTRATANTE**, se conveniente para a Administração, nos termos do Art. 71 da Lei N.º 13.303/2016 e legislação pertinente.

7. CLÁUSULA SÉTIMA – DOS RECURSOS FINANCEIROS

7.1. As despesas com a execução do presente **CONTRATO** correrão à conta de recursos próprios da **CONTRATANTE**.

8. CLÁUSULA OITAVA – DAS OBRIGAÇÕES DA CONTRATADA

8.1. A **CONTRATADA** se responsabiliza por atender todas as condições existentes no Termo de Referência do Edital do Pregão Eletrônico SRP N.º 09/2024, parte integrante deste **CONTRATO**, bem como todas as condições pactuadas neste instrumento além das obrigações seguintes:

8.1.1. Como parte integrante de suas obrigações, e em atendimento à legislação pertinente e à Política de Segurança da Informação e Comunicação da **CONTRATANTE**, a **CONTRATADA** deverá assinar o "Termo de Responsabilidade e Confidencialidade para Fornecedores e Parceiros", constante no Anexo “I” deste **CONTRATO**;

8.1.2. Sujeitar-se a mais ampla e irrestrita fiscalização por parte do **CONTRATANTE**, prestando todos os esclarecimentos necessários, atendendo às reclamações formuladas e cumprindo todas as orientações, do mesmo, visando fiel desempenho das atividades;

8.1.3. Responder por quaisquer danos, pessoais ou materiais, ocasionados em face do **CONTRATO**;

8.1.4. Aceitar, nas mesmas condições contratuais, os acréscimos ou supressões no objeto do **CONTRATO**, até o limite de 25% (vinte e cinco por cento) de seu valor atualizado;

8.1.5. Não transferir a outrem, no todo ou em parte, os serviços contratados, sem prévia e expressa anuência do **CONTRATANTE**;

8.1.6. Repor qualquer material ou bem, pertencente à **CONTRATANTE**, que for danificado, roubado ou furtado por negligência de seus prepostos;

8.1.7. Agir segundo as diretrizes do **CONTRATANTE** e legislação pertinente;

8.1.8. Cumprir horários e periodicidade para execução dos serviços conforme definido pela **CONTRATANTE**;

8.1.9. Proceder ao atendimento extraordinário, em caso de necessidade, respeitada a legislação trabalhista;

8.1.10. Utilizar, sob sua inteira responsabilidade, toda a compete e indispensável mão-de- obra, devidamente habilitada, treinada e certificada na solução entregue para execução dos serviços contratados, correndo por sua conta o cumprimento das obrigações trabalhistas, sociais, previdenciárias, tributárias e todas as outras previstas nas normas legais pertinentes;

8.1.11. A inadimplência da **CONTRATADA**, com referência à encargos, não transfere ao **CONTRATANTE** a responsabilidade de seu pagamento, nem poderá onerar o objeto deste **CONTRATO**;

8.1.12. Indicar preposto do **CONTRATO**, que a representará durante a vigência do **CONTRATO**, no prazo de até 5 (cinco) dias úteis da data da publicação do extrato deste **CONTRATO**, com no mínimo as seguintes informações: nome, número do RG, número do telefone e endereço de e-mail;

8.1.13. O preposto do **CONTRATO** realizará todos os atos necessários e compatíveis com os compromissos assumidos no presente ajuste, garantindo seu fiel cumprimento perante o **CONTRATANTE**;

8.1.14. A mudança de preposto do **CONTRATO** deverá ser formalmente comunicada ao Gestor do **CONTRATO**;

8.1.15. Responsabilizar-se integralmente pelos serviços prestados contratados, nos termos da legislação vigente;

8.1.16. Manter disciplina nos locais dos serviços, substituindo logo após notificação, qualquer empregado considerado com conduta inconveniente pela **CONTRATANTE**;

8.1.17. Responsabilizar seus empregados pelo cumprimento das normas disciplinares determinadas pela **CONTRATANTE**;

8.1.18. Fornecer documentação de todas as atividades realizadas;

8.1.19. Assumir todas as responsabilidades e tomar as medidas necessárias ao atendimento dos seus empregados, acidentados ou com mal súbito;

8.1.20. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança da **CONTRATANTE**;

8.1.21. Atender prontamente quaisquer exigências do representante da Administração, inerentes ao objeto da contratação;

8.1.22. Manter, durante toda a execução deste **CONTRATO**, todas as condições que culminaram em sua habilitação;

8.1.23. Responsabilizar-se pelos danos causados diretamente a **CONTRATANTE** ou a terceiros, decorrentes de culpa ou dolo, na execução deste **CONTRATO**;

8.1.24. Refazer os serviços considerados inadequados pelo Comissão de Fiscalização;

8.1.25. A **CONTRATADA** em situação de recuperação judicial/extrajudicial deverá comprovar o cumprimento das obrigações do plano de recuperação judicial/extrajudicial sempre que solicitada pela Comissão de Fiscalização e, ainda, na hipótese de substituição ou impedimento do administrador judicial, comunicar imediatamente, por escrito, à Comissão de Fiscalização;

8.1.26. A **CONTRATADA** deverá possuir na sua equipe profissionais com as seguintes certificações obrigatórias e indispensáveis em face da complexidade da prestação dos serviços requeridos e ainda mais da rede computacional:

8.8.26.1 **03 (três)** profissionais com nível máximo na solução ofertada;

8.8.26.2 **05 (cinco)** profissionais com nível expert na solução ofertada;

8.8.26.3 **02 (dois)** profissionais com certificação ITIL Foudation;

8.8.26.4 **01 (um)** profissional com certificação PMP (Project Management Professional).

9. CLÁUSULA NONA - DAS OBRIGAÇÕES DA CONTRATANTE

9.1. Prestar as informações e os esclarecimentos solicitados pela **CONTRATADA** para a fiel execução do **CONTRATO**;

9.2. Solicitar a correção ou substituição do objeto contratado em que se verificarem vícios, defeitos ou incorreções;

9.3. Acompanhar e fiscalizar a execução do **CONTRATO** e efetuar os pagamentos nas condições, prazos e preços pactuados no presente **CONTRATO**;

9.4. Rejeitar o objeto em desacordo com as obrigações assumidas pela **CONTRATADA** exigindo sua imediata correção, sob pena de aplicação das penalidades previstas em lei e nas clausulas desse **CONTRATO**, ressalvados os casos fortuitos ou de força maior, devidamente justificados e aceitos pela **CONTRATANTE**;

9.5. Comunicar à **CONTRATADA** toda e qualquer ocorrência relacionada com o objeto do **CONTRATO**;

9.6. Fornecer à **CONTRATADA** todos os documentos, informações e demais elementos que sejam pertinentes à vigência do **CONTRATO**;

9.7. Aplicar as penalidades previstas na lei e nas clausulas deste **CONTRATO**, na hipótese da **CONTRATADA** não cumprir no todo ou em parte o objeto contratado.

10. CLÁUSULA DÉCIMA - DA SUBCONTRATAÇÃO

10.1. A proposta de subcontratação, no ato da execução, deverá ser apresentada por escrito, e somente após a aprovação da Comissão de Fiscalização do **CONTRATO** os serviços a serem realizados pela subcontratada poderão ser iniciados;

10.2. Para a execução do serviço de **TREINAMENTO OFICIAL**, será permitida a subcontratação desde que atenda todos os critérios do Item **10 - TREINAMENTO DE FIREWALL DE PRÓXIMA GERAÇÃO** -, constante do Termo de Referência do Edital do Pregão Eletrônico N.º xx/xxxx, parte integrante deste **CONTRATO.**

11. CLÁUSULA DÉCIMA PRIMEIRA – ACORDO DE NÍVEL DE SERVIÇO

11.1. A **CONTRATADA** deverá respeitar os tempos máximos de ATENDIMENTOS e ANS (Acordo de Nível de Serviço) abaixo descritos, sob a pena de multa no caso de falhas em seu integral cumprimento:

TABELA DE ACORDO DE NÍVEL DE SERVIÇO - ANS	
Tipo de CONTRATO	**Tempo de Atendimento**
Monitoramento	**24x7x365**
Suporte Técnico	**24x7x365**
Serviços	**Tempo de Atendimento**
Requisição de Informação, parecer ou relatórios	**8h**
Requisição de serviço	**4h**
Incidentes	**Tempo de Atendimento**
Produção impactada	**2h**
Produção parada	**1h**
Mudanças	**Tempo de Atendimento**
Substituição de Produto	**02 (dois) dias**
Requisição de Mudança	**24h**

12. CLÁUSULA DÉCIMA SEGUNDA – DA SUSTENTABILIDADE E RESPONSABILIDADE SOCIOAMBIENTAL - ESG

12.1. A **CONTRATADA** concorda em cumprir e fazer cumprir, conforme o caso, e declarar-se ciente e disposto a seguir:

12.1.1. Respeitar e promover a diversidade, abstendo-se de todas as formas de preconceito e discriminação, de modo que nenhum empregado ou potencial empregado receba tratamento discriminatório em função de sua raça, cor de pele, origem étnica, nacionalidade, posição social, idade, religião, gênero, orientação sexual, estética pessoal, condição física, mental ou psíquica, estado civil, opinião, convicção política, ou qualquer outro fator de diferenciação;

12.1.2. Adotar medidas de combate à prática de lavagem de dinheiro e à corrupção em todas as suas formas, inclusive extorsão e propina;

12.1.3. Adotar conduta justa e ética, respeitando os princípios estabelecidos no Código de Conduta Ética da **CONTRATANTE**;

12.1.4. Proteger e preservar o meio ambiente, bem como evitar quaisquer práticas que possam lhe causar danos, executando seus serviços em estrita observância às normas legais e regulamentares, federais, estaduais ou municipais, aplicáveis ao assunto, incluindo, mas não se limitando à:

- Lei nº 6.938/1981, que institui a Política Nacional do Meio Ambiente;
- Lei nº 9.605/1998, a chamada “Lei dos Crimes Ambientais”;
- Lei nº 12.305/2010, que institui a Política Nacional de Resíduos Sólidos, assim como as demais normas relacionadas ao gerenciamento, ao manuseio e ao descarte adequado dos resíduos sólidos resultantes de suas atividades, privilegiando todas as formas de reuso, reciclagem e de descarte adequado, de acordo com as normas antes mencionadas.

13. CLÁUSULA DÉCIMA TERCEIRA – DAS PENALIDADES E SANÇÕES ADMINISTRATIVAS

13.1. O serviço a ser prestado deverá seguir as especificações contidas neste **CONTRATO**;

13.2. O descumprimento total ou parcial de qualquer obrigação estabelecida sujeitará a **CONTRATADA** às sanções legais aplicáveis, garantido o contraditório e a ampla defesa;

13.3. O descumprimento injustificado nos prazos de entrega, substituição ou de assistência técnica sujeita a **CONTRATADA** à multa de **2% (dois por cento)** ao dia

até o limite de 05 (cinco) dias corridos, contados do encerramento dos prazo estabelecido neste instrumento, incidentes sobre o valor da obrigação descumprida;

13.4. A partir do 6º (sexto) dia consecutivo de atraso injustificado poderá ser caracterizada a inexecução total da obrigação;

13.5. Poderão ser aplicadas à **CONTRATADA**, nas hipóteses de inexecução total ou parcial das obrigações estipuladas neste instrumento, as seguintes penalidades:

13.5.1. Advertência;

13.5.2. Multa de **10% (dez por cento)** sobre o valor da proposta;

13.5.3. Suspensão temporária de participação em licitação e impedimento de contratar com a Administração, por prazo não superior a 02 (dois) anos;

13.5.4. Declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que o contratado ressarcir a Administração pelos prejuízos resultantes e depois de decorrido o prazo da sanção aplicada com base no inciso anterior;

13.6. A multa, eventualmente imposta à **CONTRATADA**, será automaticamente descontada da fatura a que fizer jus, acrescida de juros moratórios de 1% (um por cento) ao mês. Caso a **CONTRATADA** não tenha nenhum valor a receber desta **CONTRATANTE**, ser-lhe-á concedido o prazo de 05 (cinco) dias úteis, contados de sua intimação, para efetuar o pagamento da multa. Após esse prazo, não sendo efetuado o pagamento, seus dados serão encaminhados ao Órgão competente para que seja inscrita na dívida ativa da União, podendo, ainda a Administração proceder à cobrança judicial da multa;

13.7. As multas previstas nesta seção não eximem a adjudicatária ou **CONTRATADA** da reparação dos eventuais danos, perdas ou prejuízos que seu ato punível venha causar à Administração **CONTRATANTE**;

13.8. Por inexecução de quaisquer das obrigações estipuladas, a **CONTRATADA** estará sujeita, a exclusivo juízo do **CONTRATANTE**, à indenização dos prejuízos que resultarem da paralisação dos serviços;

14. CLÁUSULA DÉCIMA QUARTA – DOS RECURSOS

14.1. A **CONTRATADA**, notificada da sanção que poderá lhe ser aplicada, terá o prazo de 5 (cinco) dias úteis, a contar do recebimento da Notificação, para apresentar defesa prévia;

14.2. Contra as decisões que tiverem aplicado penalidades, a **CONTRATADA** poderá, sempre com efeito suspensivo:

14.2.1. Interpor recursos para a autoridade imediatamente superior, no prazo de 5 (cinco) dias úteis da ciência que tiver da decisão que aplicar as penalidades de advertência e de multa;

14.2.2. Interpor recursos para a autoridade imediatamente superior, no prazo de 5 (cinco) dias úteis de publicação no Diário Oficial da decisão de suspensão do direito de licitar, impedimento de contratar ou rescindir administrativamente o **CONTRATO**;

14.2.3. Formular pedido de reconsideração à autoridade que aplicou a sanção de declaração de inidoneidade para licitar ou contratar, no prazo de 10 (dez) dias úteis da publicação no Diário Oficial do Estado;

14.3. A autoridade competente, ouvida a **FISCALIZAÇÃO**, decidirá pela procedência ou não do Recurso. A decisão deverá ser comunicada à **CONTRATADA**.

15. CLÁUSULA DÉCIMA QUINTA - DA RESCISÃO

15.1. Constituem motivos para a rescisão do presente **CONTRATO**:

15.1.1. **UNILATERALMENTE**, pela **CONTRATANTE** em razão:

15.1.1.1 Do não cumprimento por parte da **CONTRATADA** de cláusulas contratuais, especificações ou prazos;

15.1.1.2 Do cumprimento irregular de cláusulas contratuais, especificações ou prazos;

15.1.1.3 Da lentidão do seu cumprimento, levando a **CONTRATANTE** a comprovar a impossibilidade da conclusão da obra, do serviço ou do fornecimento, nos prazos estipulados;

15.1.1.4 Do atraso injustificado no início da prestação dos serviços;

15.1.1.5 Da paralisação dos serviços sem justa causa e prévia comunicação à **CONTRATANTE**;

15.1.1.6 Da subcontratação feita contrariamente ao artigo 78 da Lei N.º 13.303, de 30 de junho de 2016, assim como a associação do fornecedor com outrem, a cessão ou transferência, total ou parcial, bem como a fusão, cisão ou incorporação, quando não admitidas no instrumento convocatório e no **CONTRATO** ou, quando admitidas, se causarem prejuízo à execução do **CONTRATO**;

15.1.1.7 Do desatendimento das determinações regulares da **FISCALIZAÇÃO** ou de seus superiores;

15.1.1.8 Do cometimento reiterado de faltas na sua execução, anotadas pelo Gestor ou Fiscal do **CONTRATO**;

15.1.1.9 Da decretação de falência ou a instauração de insolvência civil;

15.1.1.10 Da dissolução da sociedade ou o falecimento do contratado;

15.1.1.11 De alteração social ou de modificação da finalidade ou da estrutura da empresa que prejudique a execução do **CONTRATO**;

15.1.1.12 De interesse público, ou pela ocorrência de caso fortuito ou de força maior, regularmente comprovada, impeditiva da execução deste **CONTRATO**.

15.1.2. **AMIGAVELMENTE** pelas partes, desde que haja conveniência para a **CONTRATANTE**;

15.1.3. **JUDICIALMENTE**, nos termos da legislação em vigor.

15.2. A rescisão de que trata o item 15.1.1, desta cláusula, será determinada por ato unilateral e escrito da **CONTRATANTE**, não cabendo à **CONTRATADA** indenização de qualquer natureza;

15.3. A declaração de rescisão administrativa, precedida de autorização escrita e fundamentada da autoridade competente, será sempre feita independentemente de prévia notificação ou interpelação judicial ou extrajudicial e operará seus efeitos a partir da publicação do ato administrativo no órgão de divulgação oficial estadual;

15.4. A rescisão amigável, precedida de autorização escrita e fundamentada da autoridade competente, será reduzida a termo no processo administrativo;

15.5. Qualquer um desses casos de rescisão contratual serão formalmente motivados nos autos do processo, assegurado o **CONTRADITÓRIO** e a **AMPLA DEFESA;**

15.6. Os casos fortuitos e/ou motivos de força maior serão excludentes da responsabilidade das Partes de acordo com o disposto no artigo 393 do Código Civil Brasileiro;

15.7. A **CONTRATADA DEVERÁ** se responsabilizar por quaisquer prejuízos advindos de não cumprimento dos serviços contratados, isentando a **CONTRATANTE** de quaisquer responsabilidades de seus atos; e ainda estará sujeita a todas as multas e penalidades legais previstas neste **CONTRATO** e na legislação vigente;

16. CLÁUSULA DÉCIMA SEXTA – DO RECONHECIMENTO DOS DIREITOS DA CONTRATANTE

16.1. As causas de rescisão previstas neste instrumento acarretam, no que couber, as seguintes consequências, sem prejuízo das sanções pertinentes, reconhecendo a **CONTRATADA**, desde já, os direitos da **CONTRATANTE** de:

16.1.1. Assunção imediata do objeto deste **CONTRATO** no estado em que se encontrar, por ato seu;

16.1.2. Ocupação e utilização dos equipamentos, material e pessoal empregados na execução do **CONTRATO**, necessários à sua continuidade, os quais serão devolvidos ou ressarcidos posteriormente, mediante avaliação, inclusive na hipótese da necessidade de acautelar apuração administrativa de faltas contratuais da **CONTRATADA**;

16.1.3. Retenção dos créditos decorrentes do **CONTRATO**, até o limite dos prejuízos causados à **CONTRATANTE**.

17. CLÁUSULA DÉCIMA SÉTIMA - DAS ALTERAÇÕES DO PRESENTE CONTRATO

17.1. O Presente **CONTRATO** poderá ser alterado conforme artigo 81 da Lei N.º 13.303 de 30 de junho de 2016;

17.2. As alterações poderão ser realizadas por Termos Aditivos;

17.3. Nenhuma alteração poderá ser realizada sem o acordo da **CONTRATANTE** e **CONTRATADA**, vedada a alteração que viole a obrigação de licitar;

17.4. De comum acordo, as partes poderão suspender a execução do objeto deste **CONTRATO**, quando, justificadamente, por motivo imperioso e extraordinário, se fizer necessário;

17.5. A suspensão será formalizada através de Termo Aditivo, onde será definida a expectativa de prazo do reinício da execução, bem como dos correspondentes pagamentos, devendo, quando aplicável, ser firmado novo Cronograma de execução;

17.6. É admissível a fusão, cisão ou incorporação da **CONTRATADA** com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do **CONTRATO**; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do **CONTRATO**.

18. CLÁUSULA DÉCIMA OITAVA – DO CONTROLE

18.1. A **CONTRATANTE** providenciará, nos prazos legais, a remessa de informações do presente **CONTRATO** via sistema ao **TRIBUNAL DE CONTAS DO ESTADO DO AMAZONAS**.

19. CLÁUSULA DÉCIMA NONA – DA DOCUMENTAÇÃO

19.1. A **CONTRATADA** fica obrigada a manter, durante toda a vigência do **CONTRATO**, em compatibilidade com as obrigações por ela assumidas, inclusive na possibilidade

de renovação contratual, todas as condições de habilitação e qualificação exigidas na assinatura do Presente Instrumento.

20. CLÁUSULA VIGÉSIMA – DA MATRIZ DE RISCO

20.1. A **MATRIZ DE RISCO** poderá necessitar de revisão durante a gestão do **CONTRATO**, diante de situações supervenientes, não previstas por ocasião de sua elaboração;

20.2. A **CONTRATADA** e a **CONTRATANTE** deverão observar e acompanhar durante a execução do objeto contratado os riscos inerentes a matriz abaixo:

Risco 01	**Risco:**	**Interrupção na prestação do Serviço de proteção de Firewall**				
	Probabilidade:	3	**Id**	**Dano**	**Impacto**	**Importância do risco**
			1	Ataque à rede da **CONTRATANTE**	4	**12**
			2	Interrupção dos serviços prestados	4	**12**
	Id	**Ação Preventiva**			**Responsável**	
	1	Adquirir a solução com alta disponibilidade			**GINFS**	
	2	Incluir a contratação do serviço de instalação, suporte, reparo e substituiçãocom SLA no TR			**GINFS**	
	Id	**Ação de Contingência**			**Responsável**	
	1	Contratar o serviço de instalação, suporte, reparo e substituição			**GINFS**	
	2	Habilitar o firewall de contingência			**GINFS**	
Risco 02	**Risco:**	**Equipamento não atender a especificação técnica**				
	Probabilidade:	3	**Id**	**Dano**	**Impacto**	**Importância do risco**
			1	Funcionalidade **CONTRATADA** não disponível	4	**12**
			2	Prejuízo financeiro	4	**12**

	Id	**Ação Preventiva**				**Responsável**
	1	Realizar parecer técnico				**DPSEO**
	Id	**Ação de Contingência**				**Responsável**
	1	Chamar o próximo colocado				**SPACIN**
Risco 03	**Risco:**	**Equipamento não ser configurado corretamente**				
	Probabilidade:	2	**Id**	**Dano**	**Impacto**	**Importância do risco**
			1	Característica de segurança não habilitada	4	**8**
			2	Processo judicial e/ou prejuízo financeiro	4	**8**
	Id	**Ação Preventiva**				**Responsável**
	1	Validar comprovação de qualificação da mão de obra de suporte técnico durante a fase de classificação				**DPSEO**
	2	Solicitar declaração de capacidade de empresa de porte e serviço semelhante ao da **CONTRATANTE**				**DPSEO**
	Id	**Ação de Contingência**				**Responsável**
	1	Solicitar substituição de técnico indicado				**DPSEO**
Risco 04	**Risco:**	**Serviço não ser entregue corretamente**				
	Probabilidade:	2	**Id**	**Dano**	**Impacto**	**Importância do risco**
			1	Deixar a rede vulnerável	4	**8**
			2	Processo judicial e/ou prejuízo financeiro	4	**8**
	Id	**Ação Preventiva**				**Responsável**

	1	Validar comprovação de qualificação da mão de obra de suporte técnico durante a fase de classificação				**DPSEO**
	2	Incluir a contratação do serviço com SLA no **CONTRATO**				**DPSEO**
	Id	**Ação de Contingência**				**Responsável**
	1	Aplicar sanções				**DPSEO**
Risco 05	**Risco:**	**Descumprimento dos prazos na execução dos serviços**				
	Probabilidade:	2	**Id**	**Dano**	**Impacto**	**Importância do risco**
			1	Não cumprir SLA	4	**8**
			2	Não solucionar incidente de SI	4	**8**
	Id	**Ação Preventiva**				**Responsável**
	1	Incluir sanções definida em processo licitatório				**DPSEO**
	Id	**Ação de Contingência**				**Responsável**
	1	Aplicar sanções previstas em **CONTRATO** e/ou legislação aplicável				**DPSEO**
Risco 06	**Risco:**	**Cobrar valores indevidos**				
	Probabilidade:	2	**Id**	**Dano**	**Impacto**	**Importância do risco**
			1	Prejuízo Financeiro	1	**2**
	Id	**Ação Preventiva**				**Responsável**
	1	Incluir previsão de glosa na fatura				**DPSEO**
	Id	**Ação de Contingência**				**Responsável**
	1	Notificar o fornecedor e solicitar correção				**DPSEO**
	2	Aplicar glosa				**DPSEO**

- Definir o tratamento para os riscos cuja importância seja superior a 6.

- Importância = Probabilidade x Impacto

Quanto ao disposto nas alíneas “b” e “c” do Art. 42-X (Matriz de Riscos) da Lei 13.303/16 (Lei das Estatais), não há, identificada neste **CONTRATO** qualquer fração do objeto em que haverá liberdade da **CONTRATADA** para inovar em soluções metodológicas ou tecnológicas, em obrigações de resultado ou em termos de modificação das soluções previamente delineadas neste documento.

21. CLÁUSULA VIGÉSIMA PRIMEIRA – DA GESTÃO E FISCALIZAÇÃO DO CONTRATO

21.1. Durante a vigência do **CONTRATO** Todos os serviços executados pela empresa **CONTRATADA** serão acompanhados e fiscalizados pela GESIQ (Gerência de Segurança da Informação e Qualidade), com autoridade para exercer em nome da **CONTRATANTE**, toda e qualquer ação de orientação geral, controle e fiscalização dos serviços;

21.2. À fiscalização compete, entre outras atribuições:

21.2.1. Verificar a conformidade da execução dos serviços com as normas especificadas e se os procedimentos, materiais e acessórios empregados, são adequados para garantir a qualidade desejada dos serviços, caberá também o direito de rejeitar os materiais que não satisfaçam aos padrões especificados;

21.2.2. Ordenar à **CONTRATADA** que corrija, refaça ou reconstrua as partes dos serviços executados com erros, imperfeições, que estejam em desacordo com as especificações;

21.2.3. A ação da fiscalização exercida pela **CONTRATANTE**, não desobriga a empresa **CONTRATADA** de suas responsabilidades contratuais;

21.3. Não obstante a **CONTRATADA** seja a única e exclusiva responsável pela execução de todos os serviços, ao **CONTRATANTE** é reservado o direito de, sem que de qualquer forma restrinja a plenitude dessa responsabilidade, exercer a mais ampla e completa fiscalização sobre os serviços, por meio de sua Gerência de Segurança da Informação e Qualidade (GESIQ) ou por Comissão de Fiscalização designada pelo **CONTRATANTE**, podendo para isso:

21.3.1. Exercer a fiscalização dos serviços contratados, de modo a assegurar o efetivo cumprimento da execução do escopo contratado, cabendo-lhe, também realizar a supervisão das atividades desenvolvidas pela **CONTRATADA**, efetivando avaliação periódica;

21.3.2. Ordenar a imediata retirada do local, bem como a substituição de funcionário da **CONTRATADA** que estiver sem uniforme ou crachá, que embaraçar ou dificultar a sua fiscalização ou cuja permanência na área, a seu exclusivo critério, julgar inconveniente;

21.3.3. Examinar a (s) Carteira (s) Profissional (is) do (s) funcionário (s) colocado (s) a seu serviço, para comprovar o registro de função profissional;

21.3.4. Executar o aceite dos serviços efetivamente prestados, descontando o equivalente aos não realizados bem como aqueles não aprovados por inconformidade aos padrões estabelecidos, desde que por motivos imputáveis à **CONTRATADA**, sem prejuízo das demais sanções disciplinadas neste **CONTRATO**;

21.3.5. Correrão por conta da **CONTRATADA** as despesas para efetivo atendimento ao objeto contratado, tais como materiais, equipamentos, acessórios, transporte, tributos, encargos trabalhistas e previdenciários decorrentes de sua execução;

21.4. A **CONTRATADA** deverá indicar para a Comissão de Fiscalização, antes do início dos serviços e, em até 5 (cinco) dias úteis após a publicação no Diário Oficial do Estado do Amazonas do extrato deste **CONTRATO**, preposto que a representará durante a sua vigência, com, no mínimo, as seguintes informações: nome, número do RG, número do telefone e endereço de e-mail;

21.5. A Comissão de Fiscalização terá 5 (cinco) dias úteis para analisar os documentos entregues e emitir a Autorização para Início dos Serviços;

21.6. Caso seja constatado qualquer vício, funcionamento inadequado ou divergência em relação à especificação e proposta da **CONTRATADA**, será expedido um comunicado estabelecendo o prazo máximo de até 15 (quinze) dias corridos e improrrogáveis para que ela solucione os vícios apontados, após o qual será reiniciado o prazo máximo de 5 (cinco) dias corridos para nova conferência e testes de aceite;

21.7. Eventual indisponibilidade ou irregularidade dos serviços prestados por motivos imputáveis à **CONTRATADA** ensejarão aplicação de multa por atraso e/ou inexecução dos serviços contratados, previstas na cláusula 13 deste **CONTRATO** e na Lei n.º 13.303 de 30 de junho de 2016, e demais sanções cabíveis;

21.8. O **CONTRATANTE** não reconhecerá qualquer vínculo com empresas subcontratadas, sendo que qualquer contato porventura necessário, de natureza técnica, administrativa, financeira ou jurídica que decorra dos trabalhos realizados será mantido exclusivamente com a **CONTRATADA**, que responderá por seu pessoal técnico e operacional e, também, por prejuízos e danos que eventualmente estas causarem;

22. CLÁUSULA VIGÉSIMA SEGUNDA – DO FORO

22.1. O foro do presente **CONTRATO** é o desta cidade de Manaus/AM, com expressa renúncia da **CONTRATADA** a qualquer outro que tenha ou venha a ter, por mais privilegiado que seja.

23. CLÁUSULA VIGÉSIMA TERCEIRA – DOS CASOS OMISSOS

23.1. Os casos omissos serão decididos pela **CONTRATANTE**, segundo as disposições contidas na Lei N.º 13.303 de 30 de junho de 2016 e demais alterações, pelas normas de Direito Privado e no Regulamento Interno de Licitações e Contratos da **CONTRATANTE** e demais normas aplicáveis.

24. CLÁUSULA VIGÉSIMA QUARTA – DA PUBLICAÇÃO

24.1. A **CONTRATANTE** deve, nesta data, providenciar a publicação, em forma de extrato, do presente **CONTRATO**, no Diário Oficial do Estado do Amazonas, na forma do artigo 31 da Lei N.º 13.303 de 30 de junho de 2016.

25. CLÁUSULA VIGÉSIMA QUINTA – DAS NORMAS APLICÁVEIS

25.1. O presente **CONTRATO** rege-se por toda a legislação aplicável à espécie e ainda pelas disposições que a complementarem, alterarem ou regulamentarem, inclusive nos casos omissos, cujas normas, desde já, entendem-se como integrantes do presente termo, especialmente a Lei N.º 13.303 de 30 de junho de 2016 e o Regulamento de Licitações e Contratos da **CONTRATANTE**.

25.2. A **CONTRATANTE** e a **CONTRATADA** declaram conhecer todas essas normas e concordam em sujeitar-se às estipulações, sistemas de penalidades e demais regras delas constantes, mesmo que não expressamente transcritas no presente instrumento.

De tudo, para constar, foi lavrado o presente termo, em 02 (duas) vias de igual teor e forma, na presença das testemunhas abaixo, para que produza seus legítimos e legais efeitos.

Manaus, na data da assinatura eletrônica [ou xx de xxxx de xxxx].

Pela CONTRATANTE

xxxxxxxx

Diretor-Presidente

Pela CONTRATADA

xxxxxx

Representante Legal

Nível de Classificação	Grupo de acesso
Público	**PÚBLICO**

REVISÃO E APROVAÇÃO:

Assessor Jurídico