



**CONTRATO DE ADESÃO CARONA Nº 045/2026/SES/MT**  
**ORIGEM: ARP Nº 2025/03636/ETICE/CE - PREGÃO ELETRÔNICO Nº 20240008**  
**PROCESSO ADMINISTRATIVO Nº SES-PRO-2025/85193**

**AQUISIÇÃO DE SOLUÇÃO DE SEGURANÇA DE APLICAÇÕES WEB (WAF) DE DATA CENTER, ACOMPANHADA DOS SERVIÇOS ESPECIALIZADOS DE IMPLANTAÇÃO, LICENCIAMENTO E SUPORTE TÉCNICO 24X7X365, CONTEMPLANDO UTILIZAÇÃO DE EQUIPAMENTOS OBRIGATORIEDADE TODOS NOVOS E DE PRIMEIRO USO, PELO PERÍODO DE 36 MESES, CONFORME ANEXO I, POR MEIO DE ADESÃO A ATA DE REGISTRO DE PREÇOS Nº. 2025/03636, PROCEDIMENTO ADMINISTRATIVO N.º 30032.000154/2024-71, PREGÃO ELETRÔNICO Nº. 20240008, VISANDO ATENDER ÀS NECESSIDADES DA SECRETARIA ESTADUAL DE SAÚDE.**

**CONTRATANTE: O ESTADO DE MATO GROSSO** por meio da **SECRETARIA ESTADUAL DE SAÚDE**, com sede no Centro Político Administrativo, bloco 05, Cuiabá/MT, inscrita no CNPJ sob n. 57.252.971/0001-46, neste ato representado pelo Secretário de Estado de Saúde **JULIANO SILVA MELO**, brasileiro, portador da cédula de identidade RG nº \*\*\*536715 - SSP/RO, inscrito no CPF sob o nº \*\*\*180.542-15, residente e domiciliado nesta Capital.

**CONTRATADA:** A empresa **NTSEC SOLUCOES EM TELEINFORMATICA LTDA**, inscrita no CNPJ n.º 09.137.728/0002-15, sediada na avenida Rua Ary Barroso, 70, Salas 801 a 818, Torre 01, Papicu, Fortaleza-CE, CEP: 60175-705, telefone: (61)3248-3829,(85) 30353540e-mail: comercial@ntsec.com.br, neste ato representada por **SRA. PATRÍCIA ANGELINA DA CONCEIÇÃO**, portador da Cédula de Identidade RG nº \*\*\*021-5 SSP/SP, inscrita no CPF sob o nº \*\*\*94.838-01.

**FIRMAM O PRESENTE CONTRATO:** Têm entre si justa e acordada a celebração do presente contrato, mediante as cláusulas e condições seguintes:

Palácio Paiaguás, Rua D, s/n, Bloco 5, Centro Político Administrativo – CEP: 78.049-902  
Cuiabá – Mato Grosso – Telefone: (65) 3613-5344 – E-mail: [contratos@ses.mt.gov.br](mailto:contratos@ses.mt.gov.br).

Página 1 de 82





### CLÁUSULA PRIMEIRA – DA FUNDAMENTAÇÃO

1.1. O presente contrato tem como fundamento o Pregão Eletrônico nº 20240008, e seus anexos, os preceitos do direito público, Lei Federal nº 14.133, de 1º de abril de 2021, e demais legislação aplicável ao cumprimento de seu objeto.

### CLÁUSULA SEGUNDA – DA VINCULAÇÃO AO EDITAL E A PROPOSTA

2.1. O cumprimento deste contrato está vinculado aos termos do edital do Pregão Eletrônico nº 20240008, o Termo de Referência, a proposta do contratado e eventuais anexos dos respectivos documentos os quais constituem parte deste instrumento, independente de sua transcrição.

### CLÁUSULA TERCEIRA – DO OBJETO

3.1. Registro de preços para futuras e eventuais aquisições de solução de proteção de redes, incluindo aquisições de hardware e software e respectivo serviço de implantação, posterior monitoramento e suporte técnico 24x7x365, contemplando utilização de equipamentos obrigatoriamente todos novos e de primeiro uso, nas condições estabelecidas neste contrato e no Termo de Referência do edital e na proposta do CONTRATADO.

ITEM	SIAG	ESPECIFICAÇÃO	UND	QTD	VALOR UNITÁRIO R\$	VALOR TOTAL R\$
21	0016120	Firewall de Aplicação Web – WAF – Datacenter Tipo II F5 Networks - Appliance R5800 com licenciamento Best Bundle e suporte e garantia do fabricante por 36 meses	Pcs.	2	R\$ 1.989.800,00	R\$ 3.979.600,00
28	0012741	Instalação Firewall de Aplicação Web – WAF – Datacenter	Pcs.	2	R\$ 123.630,50	R\$ 247.261,00
34	0001173	Serviço de Monitoramento e Suporte Técnico 24x7 de Firewall de Aplicação Web – Datacenter – 36 Meses	Pcs.	2	R\$ 541.494,10	R\$ 1.082.988,20
35	0001173	Serviço de SOC 24x7 com SIEM – Pacotes de 200 EPS – 36 Meses	Pcs.	10	R\$ 323.476,00	R\$ 3.234.760,00
<b>VALOR TOTAL DO CONTRATO</b>						<b>R\$ 8.544.609,20</b>





#### CLÁUSULA QUARTA – DA VIGÊNCIA E PRORROGAÇÃO

4.1. O prazo de vigência do contrato é de 36 (trinta e seis) meses, **tendo início em 13/04/2026 e término em 12/04/2029**, na forma do art. 94 c/c o art. 105 da Lei Federal nº 14.133/2021, admitindo-se a prorrogação desde que a autoridade competente ateste que as condições e os preços permanecem vantajosos para a Administração, permitida a negociação com o CONTRATADO.

#### CLÁUSULA QUINTA – DO FORNECIMENTO

5.1. A forma de fornecimento, assim como os prazos e condições de conclusão, entrega, recebimento do objeto, obrigações e demais condições constam no Termo de Referência, anexo a este contrato.

#### CLÁUSULA SEXTA – DA SUBCONTRATAÇÃO

6.1. Será admitida a subcontratação do objeto contratual nos termos estabelecidos no subitem 21.7 do edital.

#### CLÁUSULA SÉTIMA – DO PREÇO

7.1. O valor total da contratação é de R\$ **R\$ 8.544.609,20 (oito milhões, quinhentos e quarenta e quatro mil, seiscentos e nove reais e vinte centavos.)**

7.1.1. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

#### CLÁUSULA OITAVA – DO PAGAMENTO E DO RECEBIMENTO

8.1. O prazo para pagamento ao CONTRATADO e demais condições a ele referentes, bem como, as condições de recebimento, se encontram definidos no Termo de Referência, anexo a este instrumento de contrato.

#### CLÁUSULA NONA – DO REAJUSTE

9.1. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do orçamento estimado, ou seja, a data da pesquisa constante no Mapa Comparativo de Preços.

9.2. Após o interregno de um ano, os preços iniciais poderão ser reajustados, mediante a aplicação, do índice IPCA, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

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

9.4. No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o CONTRATANTE pagará ao CONTRATADO a importância calculada pela última variação conhecida, liquidando a diferença





correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

9.5. Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

9.6. Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

9.7. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

9.8. O reajuste será realizado por apostilamento.

#### **CLÁUSULA DÉCIMA – DAS OBRIGAÇÕES DO CONTRATANTE E DO CONTRATADO**

10.1. As obrigações referentes ao CONTRATANTE e ao CONTRATADO encontram-se, respectivamente, definidas no Termo de Referência, parte integrante deste termo.

#### **CLÁUSULA DÉCIMA PRIMEIRA – DAS OBRIGAÇÕES PERTINENTES À LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)**

11.1. O CONTRATADO declara que tem ciência da existência da LGPD e se compromete a adequar todos os procedimentos internos ao disposto na legislação, com o intuito de proteger os dados pessoais que lhe forem repassados, cumprindo, a todo momento, as normas de proteção de dados pessoais, jamais colocando, por seus atos ou por sua omissão, o CONTRATANTE em situação de violação de tais regras.

11.1.1. O CONTRATADO somente poderá tratar dados pessoais nos limites e finalidades exclusivas do cumprimento de suas obrigações com base no presente contrato e jamais poderá realizar o tratamento para fins distintos da execução dos serviços especificados no certame ou no contrato administrativo.

11.2. O tratamento de dados pessoais será realizado de acordo com as hipóteses de tratamento previstas nos arts. 7º, 11, 14, 23, 24 e 26 da LGPD e somente para propósitos legítimos, específicos, explícitos e informados ao titular, observando a persecução do interesse público e os princípios do art. 6º da LGPD e 37 da Constituição Federal de 1988.

11.3. O CONTRATADO deverá indicar, no prazo máximo de 5 ( cinco) dias úteis da publicação do Aditivo, a identidade e informações de contato do seu Encarregado de Proteção de Dados, bem como, se aplicável, o endereço da página eletrônica onde essa designação é realizada, conforme estabelecido no § 1º do art. 41 da LGPD e se compromete a manter o CONTRATANTE informado sobre os dados atualizados de contato de seu Encarregado de Tratamento de Dados Pessoais, sempre que for substituído, independentemente das alterações em sua página eletrônica.

11.4. O CONTRATADO deverá cooperar com a Administração Direta e Indireta do Estado do Mato Grosso no cumprimento das obrigações referentes ao exercício dos direitos dos Titulares previstos na LGPD e nas Leis e Regulamentos de Proteção de Dados em vigor e também no atendimento de





requisições e determinações do Poder Judiciário, Ministério Público e Órgãos de Controle, quando relacionados ao objeto contratual.

11.5. O CONTRATADO não poderá disponibilizar ou transmitir a terceiros, sem prévia autorização por escrito, informação, dados pessoais ou base de dados a que tenha acesso em razão do cumprimento do objeto deste instrumento contratual.

11.5.1. Caso autorizada transmissão de dados pelo CONTRATADO a terceiros, as informações fornecidas e/ou compartilhadas devem se limitar ao estritamente necessário para o fiel desempenho da execução do instrumento contratual, adotando procedimentos de segurança que assegurem a sua confidencialidade, integridade e disponibilidade dos dados.

11.5.2. As PARTES se obrigam a zelar pelo sigilo dos dados, garantindo que apenas as pessoas que efetivamente precisam acessá-los o façam, submetendo-as, em todo caso, ao dever de confidencialidade.

11.6. Ocorrendo o término do tratamento dos dados nos termos do art. 15 da LGPD é dever do CONTRATADO eliminá-los, com exceção das hipóteses do art. 16 da mesma lei, incluindo aquelas em que houver necessidade de guarda de documentação para fins de comprovação do cumprimento de obrigações legais ou contratuais e somente enquanto não prescritas essas obrigações.

11.6.1. O CONTRATADO não poderá deter cópias ou backups, informações, dados pessoais e/ou base de dados a que tenha tido acesso durante a execução do cumprimento do objeto deste instrumento contratual.

11.6.2. O CONTRATADO deverá eliminar os dados pessoais a que tiver conhecimento ou posse em razão do cumprimento do objeto deste instrumento contratual tão logo não haja necessidade de seu tratamento.

11.6.3. O CONTRATADO fica obrigado a devolver todos os documentos, registros e cópias que contenham informação, dados pessoais, e/ou base de dados a que tenha tido acesso durante a execução do cumprimento do objeto deste instrumento contratual, no prazo de 30 (trinta) dias corridos, contados da data de qualquer uma das hipóteses de extinção do contrato, restando autorizada a conservação apenas nas hipóteses legalmente previstas,

11.7. Caso as PARTES necessitem subcontratar atividades relacionadas ao certame/contrato em que haja tratamento dos dados, deverão exigir a vinculação do SUBCONTRATADO (suboperador) aos critérios definidos neste instrumento, fazendo-o assinar um termo de adesão ao presente contrato.

11.7.1. O CONTRATANTE deverá ser informado no prazo de 5 (cinco) dias úteis sobre todos os contratos de subcontratação (suboperadores) firmados ou que venham a ser celebrados pelo CONTRATADO.

11.7.2. Em caso de subcontratação, o CONTRATADO e o SUBCONTRATADO responderão em regime de solidariedade por eventuais danos causados aos titulares, o CONTRATANTE e a terceiros, em virtude de qualquer conduta comissiva ou omissiva inerente ao tratamento dos dados.

11.7.3. O CONTRATADO deverá assegurar que o subcontratado oferecerá o mesmo nível de segurança dos dados, produzindo e guardando evidências disso;



11.8. As PARTES devem adotar boas práticas de governança e medidas técnicas e administrativas em relação ao tratamento dos dados, compatíveis com a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados.

11.8.1. É dever do CONTRATADO orientar e treinar seus empregados sobre os deveres, requisitos e responsabilidades decorrentes da LGPD, inclusive dará conhecimento formal aos seus empregados das obrigações e condições acordadas nesta cláusula.

11.8.2. O CONTRATADO se responsabilizará por assegurar que todos os seus colaboradores, consultores, e/ou prestadores de serviços que, no exercício das suas atividades, tenham acesso e/ou conhecimento da informação e/ou dos dados pessoais, agirão de acordo com o presente contrato, com as leis de proteção de dados e que estes respeitem o dever de proteção, confidencialidade e sigilo, devendo estes assumir compromisso formal de preservar a confidencialidade e segurança de tais dados, documento que estar disponível em caráter permanente para exibição do CONTRATANTE, mediante solicitação.

11.8.3. O CONTRATADO deverá promover a revogação de todos os privilégios de acesso aos sistemas, informações e recursos do CONTRATANTE, em caso de desligamento de funcionário das atividades inerentes à execução do presente Contrato.

11.9. Em caso de incidente de segurança em relação aos dados tratados neste certame/contrato, que comprometa a confidencialidade, a integridade e a disponibilidade dos dados, a PARTE que sofreu o incidente deverá comunicar imediatamente a ocorrência a partir de uma notificação que conterà, no mínimo:

- a) Data e hora do incidente;
- b) Data e hora da ciência pela PARTE responsável;
- c) Descrição dos dados pessoais afetados;
- d) Número de titulares afetados;
- e) Relação dos titulares envolvidos;
- f) Riscos relacionados ao incidente;
- g) Indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados;
- h) Motivos da demora, no caso de a comunicação não haver sido imediata;
- i) Medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo;
- j) O contato do Encarregado de Proteção de Dados ou de outra pessoa junto a qual seja possível obter maiores informações sobre o ocorrido;

11.9.1. Na hipótese descrita acima, as PARTES atuarão em regime de cooperação para:

- a) Definir e implementar as medidas necessárias para fazer cessar o incidente e minimizar seus impactos;
- b) Prover as informações necessárias à apuração do ocorrido no menor prazo possível;





c) Definir o padrão de respostas a serem dadas aos titulares, terceiros, à ANPD e demais autoridades competentes.

11.10. Os dados obtidos em razão deste contrato serão armazenados em um banco de dados seguro, com garantia de registro das transações realizadas na aplicação de acesso (log), adequado controle baseado em função (role based access control) e com transparente identificação do perfil dos credenciados, tudo estabelecido como forma de garantir inclusive a rastreabilidade de cada transação e a franca apuração, a qualquer momento, de desvios e falhas, vedado o compartilhamento dessas informações com terceiros;

11.11. A critério do CONTRATANTE, o CONTRATADO poderá ser provocado a colaborar na elaboração do Relatório de Impacto à Proteção de Dados Pessoais, conforme a sensibilidade e o risco inerente dos serviços objeto deste contrato, no tocante a dados pessoais.

11.12. O CONTRATADO indenizará o CONTRATANTE, em razão do não cumprimento das obrigações previstas nas leis, normas, regulamentos e recomendações das autoridades de proteção de dados com relação ao presente contrato, de quaisquer danos, prejuízos, custos e despesas, incluindo-se honorários advocatícios, multas, penalidades e eventuais dispêndios investigativos relativos a demandas administrativas ou judiciais propostas em face do CONTRATANTE a esse título.

11.13. Em caso de responsabilização do Estado por danos e/ou violações à LGPD decorrentes do objeto do contrato, deverá ser apurado os danos que efetivamente cada uma das partes causarem ao titular dos dados, para fins de assegurar o direito de regresso do Estado nos termos da legislação.

11.13.1. O CONTRATANTE poderá realizar diligência para aferir o cumprimento dessa cláusula, devendo o Contratado atender prontamente eventuais pedidos de comprovação formulados.

11.14. Os contratos e convênios de que trata o § 1º do art. 26 da Lei nº 13.709/2018 deverão ser comunicados à ANPD.

11.15. Este instrumento pode ser alterado nos procedimentos pertinentes ao tratamento de dados pessoais, quando indicado pela autoridade competente, em especial a ANPD por meio de opiniões técnicas ou recomendações, editadas na forma da LGPD.

## CLÁUSULA DÉCIMA SEGUNDA – DA GARANTIA DE EXECUÇÃO

12.1. A contratação conta com garantia de execução, nos moldes do art. 96 da Lei nº 14.133/2021, em valor correspondente a 5% (cinco por cento) do valor contratual, que deverá ser prestada até 10 (dez) dias úteis a contar da assinatura deste instrumento.

12.2. A apólice do seguro-garantia deverá acompanhar as modificações referentes à vigência do contrato principal mediante a emissão do respectivo endosso pela seguradora.

12.3. Será permitida a substituição da apólice de seguro-garantia na data de renovação ou de aniversário, desde que mantidas as condições e coberturas da apólice vigente e nenhum período fique descoberto, ressalvado o disposto no subitem 12.5, deste instrumento de contrato.

12.4. A garantia somente será liberada ou restituída após a fiel execução do contrato ou após a sua extinção por culpa exclusiva da Administração e, quando em dinheiro, será atualizada monetariamente.





12.5. Na hipótese de suspensão do contrato por ordem ou inadimplemento da Administração, o CONTRATADO ficará desobrigado de renovar a garantia ou de endossar a apólice de seguro até a ordem de reinício da execução ou o adimplemento pela Administração.

12.6. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

12.6.1. Prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

12.6.2. Multas moratórias e punitivas aplicadas pela Administração ao CONTRATADO; e

12.6.3. Obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pelo CONTRATADO, quando couber.

12.7. A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no subitem 12.6, observada a legislação que rege a matéria.

12.8. A garantia em dinheiro deverá ser efetuada em favor do CONTRATANTE, em conta específica no Banco Bradesco S.A., com correção monetária.

12.9. Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Economia.

12.10. No caso de garantia na modalidade de fiança bancária, deverá ser emitida por banco ou instituição financeira devidamente autorizada a operar no País pelo Banco Central do Brasil, e deverá constar expressa renúncia do fiador aos benefícios do art. 827 do Código Civil.

12.11. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada ou renovada, seguindo os mesmos parâmetros utilizados quando da contratação.

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

12.13. O CONTRATANTE executará a garantia na forma prevista na legislação que rege a matéria.

12.14. O emitente da garantia ofertada pelo CONTRATADO deverá ser notificado pelo CONTRATANTE quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.

12.15. Caso se trate da modalidade seguro-garantia, ocorrido o sinistro durante a vigência da apólice, sua caracterização e comunicação poderão ocorrer fora desta vigência, não caracterizando fato que justifique a negativa do sinistro, desde que respeitados os prazos prescricionais aplicados ao contrato de seguro, nos termos da lei.

12.16. Extinguir-se-á a garantia com a restituição da apólice, carta fiança ou autorização para a liberação de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração do CONTRATANTE, mediante termo circunstanciado, de que o CONTRATADO cumpriu todas as cláusulas do contrato.





12.17. O garantidor não é parte para figurar em processo administrativo instaurado pelo CONTRATANTE com o objetivo de apurar prejuízos e/ou aplicar sanções ao CONTRATADO.

12.18. O CONTRATADO autoriza o CONTRATANTE a reter, a qualquer tempo, a garantia, na forma prevista neste contrato.

12.19. Além da garantia de que tratam os arts. 96 e seguintes da Lei nº 14.133/2021, a presente contratação possui previsão de garantia do serviço a ser fornecido, incluindo manutenção e assistência técnica, conforme o caso e condições estabelecidas no Termo de Referência.

### CLÁUSULA DÉCIMA TERCEIRA – DAS INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

13.1. Comete infração administrativa, nos termos da Lei nº 14.133/2021, o CONTRATADO que :

13.1.1. Der causa à inexecução parcial do contrato;

13.1.2. Der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;

13.1.3. Der causa à inexecução total do contrato;

13.1.4. Ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;

13.1.5. Apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;

13.1.6. Praticar ato fraudulento na execução do contrato;

13.1.7. Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

13.1.8. Praticar ato lesivo previsto no art. 5º da Lei nº 12.846/2013.

13.2. Serão aplicadas ao CONTRATADO que incorrer nas infrações acima descritas as seguintes sanções:

13.2.1. Advertência, quando o CONTRATADO der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave;

13.2.2. Impedimento de licitar e contratar, quando praticadas as condutas descritas nos subitens 13.1.2, 13.1.3 e 13.1.4, deste contrato, sempre que não se justificar a imposição de penalidade mais grave;

13.2.3. Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nos subitens 13.1.5, 13.1.6, 13.1.7 e 13.1.8 deste contrato, bem como nos subitens 13.1.2, 13.1.3 e 13.1.4, que justifiquem a imposição de penalidade mais grave.

13.2.4. Multa:

13.2.4.1. Moratória de 0,2% (dois décimos por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 25 (vinte e cinco) dias.

13.2.4.2. Moratória de 0,07% (sete centésimos por cento) por dia de atraso injustificado sobre o valor total do contrato, até o máximo de 2% (dois por cento) pela inobservância do prazo fixado para





apresentação, suplementação ou reposição da garantia.

13.2.4.2.1. O atraso superior a 30 (trinta) dias autoriza a Administração a promover a extinção do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe o inciso I do art. 137 da Lei n. 14.133/2021.

13.2.4.3. Compensatória de 20% (vinte por cento) sobre o valor total do contrato, no caso de inexecução total do objeto.

13.3. A aplicação das sanções previstas neste contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao CONTRATANTE.

13.4. Todas as sanções previstas neste contrato poderão ser aplicadas cumulativamente com a multa.

13.4.1. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

13.5. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao CONTRATADO, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei nº 14.133/2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

13.6. Na aplicação das sanções serão considerados:

13.6.1. A natureza e a gravidade da infração cometida;

13.6.2. As peculiaridades do caso concreto;

13.6.3. As circunstâncias agravantes ou atenuantes;

13.6.4. Os danos que dela provierem para o CONTRATANTE;

13.6.5. A implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

13.7. Os atos previstos como infrações administrativas na Lei nº 14.133/2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846/2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei.

13.8. A personalidade jurídica do CONTRATADO poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o CONTRATADO, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia.

13.9. O CONTRATANTE deverá, no prazo máximo 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ele aplicados, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no





Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal e no Certificado de Registro Cadastral(CRC) do Estado do Ceará.

13.10. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133/2021.

13.11. Os débitos do CONTRATADO para com o CONTRATANTE, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes deste mesmo contrato ou de outros contratos administrativos que o CONTRATADO possua com o mesmo órgão ora CONTRATANTE.

13.11.1. Na impossibilidade do pagamento da multa por meio de descontos dos créditos existentes ou da garantia contratual, o CONTRATADO recolherá a multa por meio de Documento de Arrecadação Estadual (DAE), podendo ser substituído por outro instrumento legal, em nome do CONTRATANTE, se não o fizer, será cobrada em processo de execução.

#### CLÁUSULA DÉCIMA QUARTA – DA EXTINÇÃO CONTRATUAL

14.1. Este contrato se extingue nas seguintes hipóteses:

I- Quando cumpridas as obrigações de ambas as partes, ainda que isso ocorra antes do prazo estipulado para tanto, e.

II- Quando mesmo não cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, ocorrer algum dos motivos previstos no art. 137 da Lei nº 14.133/2021, bem como amigavelmente, assegurados o contraditório e a ampla defesa.

a) Na hipótese do inciso II, aplicam-se também os arts. 138 e 139 da mesma Lei.

14.2. A alteração social ou a modificação da finalidade ou da estrutura da empresa não ensejará a rescisão se não restringir sua capacidade de concluir o contrato.

14.2.1. Se a operação implicar mudança da pessoa jurídica CONTRATADA, deverá ser formalizado termo aditivo para alteração subjetiva.

14.3. O termo de rescisão, sempre que possível, será precedido:

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

14.3.2. Relação dos pagamentos já efetuados e ainda devidos;

14.3.3. Indenizações e multas.

14.4. A extinção do contrato não configura óbice para o reconhecimento do desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório.

14.5. Este contrato poderá ser rescindido a qualquer tempo pelo CONTRATANTE, mediante aviso prévio de no mínimo 30 (trinta) dias, nos casos das rescisões decorrentes do previsto no inciso VIII, do art. 137, da Lei Federal nº 14.133/2021, sem que caiba ao CONTRATADO, direito à indenização de qualquer espécie.





### CLÁUSULA DÉCIMA QUINTA – DA DOTAÇÃO ORÇAMENTÁRIA

15.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral do Estado deste exercício, na dotação abaixo discriminada, conforme o caso:

ÓRGÃO/ ENTIDADE	UNIDADE ORÇAMENTÁRIA	PROJETO/ ATIVIDADE	NATUREZA DE DESPESA	VALOR R\$	FONTE
SES/MT	21.601	2569	4.4.90.52.014	1.790.820,00	1.500.1002
			3.3.90.40.006	6.753.789,20	

15.2. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

### CLÁUSULA DÉCIMA SEXTA – DAS ALTERAÇÕES

16.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 14.133/2021.

16.2. O CONTRATADO é obrigado a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

16.3. Registros que não caracterizam alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do art. 136 da Lei nº 14.133/2021.

### CLÁUSULA DÉCIMA SÉTIMA – DOS CASOS OMISSOS

17.1. Os casos omissos serão decididos pelo CONTRATANTE, segundo as disposições contidas na Lei nº 14.133/2021, e demais normas estaduais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078/1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

### CLÁUSULA DÉCIMA OITAVA – DA PUBLICAÇÃO

18.1. Incumbirá ao CONTRATANTE divulgar o presente instrumento no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no art. 94 da Lei 14.133/2021, bem como no respectivo sítio oficial na Internet, em atenção a Lei nº 12.527/2011, regulamentada no Estado de Mato Grosso por norma estadual.

### CLÁUSULA DÉCIMA NONA – DO FORO

19.1. Fica eleito o foro do município da sede do CONTRATANTE, para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não puderem ser compostos pela conciliação,





conforme art. 92, §1º, da Lei nº 14.133/2021.

E, por estarem de acordo, foi mandado lavrar o presente contrato, que está visado pela Assessoria Jurídica do CONTRATANTE, e do qual se extraíram 1(uma) via de igual teor e forma, para um só efeito, a qual, depois de lida e achada conforme, vão assinadas pelos representantes das partes e pelas testemunhas abaixo.

Cuiabá/MT, 06 de abril de 2026.

**JULIANO SILVA MELO**  
*Secretário de Estado de Saúde*

PATRICIA ANGELINA DA  
CONCEICAO:34699483  
801

Assinado de forma digital  
por PATRICIA ANGELINA DA  
CONCEICAO:34699483801  
Dados: 2026.04.07 15:23:15  
-03'00'

**PATRÍCIA ANGELINA DA CONCEIÇÃO**  
*Nisec Solucoes Em Teleinformatica Ltda*

**Testemunhas:**





## ANEXO I – TERMO DE REFERÊNCIA

### 3ª RETIFICAÇÃO AO TERMO DE REFERÊNCIA N.º 005/2025/COIETI/STI/GBSAITI/SES-MT BENS DE CONSUMO/PERMANENTE/SERVIÇOS Processo Administrativo n.º SES-PRO-2025/85193

**A. Termo de Referência n.º 005/2025/ COIETI/STI/GBSAITI/SES-MT**

**B. Órgão:** Secretaria de Estado de Saúde de Mato Grosso – SES/MT

**C. Número da Unidade Orçamentária:** 21.601

**D. Unidade Administrativa Demandante:** Coordenadoria de Infraestrutura de TI/ Superintendência de Tecnologia da Informação

**E. Estudo Técnico Preliminar n.º 005/2025/COIETI/STI/GBSAITI/SES-MT**

#### 1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Aquisição de Solução de Segurança de Aplicações Web (WAF) de Data Center, acompanhada dos serviços especializados de implantação, licenciamento e suporte técnico 24X7X365, contemplando utilização de equipamentos obrigatoriedade todos novos e de primeiro uso, pelo período de 36 meses, conforme ANEXO I, por meio de adesão a **Ata de Registro de Preços n.º. 2025/03636, Procedimento Administrativo n.º 30032.000154/2024-71, Pregão Eletrônico n.º. 20240008**, visando atender às necessidades da Secretaria Estadual de Saúde, nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

ITEM	SIAG	ESPECIFICAÇÃO	UND	QTD	VALOR UNITÁRIO R\$	VALOR TOTAL R\$
21	0016120	Firewall de Aplicação Web – WAF – Datacenter Tipo II F5 Networks - Appliance R5800 com	Pcs.	2	R\$ 1.989.800,00	R\$ 3.979.600,00





		licenciamento Best Bundle e suporte e garantia do fabricante por 36 meses				
28	0012741	Instalação Firewall de Aplicação Web – WAF – Datacenter	Pcs.	2	R\$ 123.630,50	R\$ 247.261,00
34	0001173	Serviço de Monitoramento e Suporte Técnico 24x7 de Firewall de Aplicação Web – Datacenter – 36 Meses	Pcs.	2	R\$ 541.494,10	R\$ 1.082.988,20
35	0001173	Serviço de SOC 24x7 com SIEM – Pacotes de 200 EPS – 36 Meses	Pcs.	10	R\$ 323.476,00	R\$ 3.234.760,00
<b>VALOR TOTAL</b>						<b>R\$ 8.544.609,20</b>

1.2. O custo estimado total deste termo de referência é de **R\$ 8.544.609,20 (oito milhões, quinhentos e quarenta e quatro mil, seiscientos e nove reais e vinte centavos).**

1.3. O contratante declara que o objeto desta contratação não se enquadra na definição de bem de luxo, conforme Decreto Estadual nº 1.525/2022.

1.4. Os custos estimados foram determinados conforme pesquisa de preços realizada na forma do Decreto Estadual n.º 1.525/2022 e juntada a este processo administrativo, conforme tópico **6 do ETP**.

1.5. O quantitativo a ser adquirido foi dimensionado conforme **tópico 4 do ETP**.

1.6. A Categoria de despesa do objeto a ser contratado enquadra-se em:

- Bens Permanentes (patrimoniáveis)
- Bens de Consumo (não patrimoniáveis)
- Equipamento de Apoio
- Equipamentos, Insumos, Serviços de TI

## 2. VIGÊNCIA DA CONTRATAÇÃO

2.1. O prazo de vigência do contrato é de 36 (trinta e seis) meses, contado da sua assinatura, na forma do art. 94 c/c o art. 105 da Lei Federal nº 14.133/2021, e para as empresas públicas e sociedades de economia mista, o disposto no art. 71 da Lei Federal nº 13.303/2016.

2.2. O contrato poderá ser alterado pela disciplina dos arts. 124 e seguintes da Lei Federal nº 14.133/2021, e para as empresas públicas e sociedades de economia mista, nos casos previstos nos arts.





72 e 81 da Lei Federal nº 13.303/2016 e conforme dispuser o Regulamento Interno de Licitações e Contratos do contratante.

### 3. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

3.1 O presente estudo trata da aquisição de uma Solução de Segurança e Proteção de Aplicações Web (WAF), composta pelo appliance F5 Networks R5800, licenciamento Best Bundle, e serviços especializados de Instalação e Suporte Técnico 24x7.

3.2 Essa aquisição é mandatória para **fortalecer a segurança cibernética** do Datacenter da Secretaria de Saúde do Estado de Mato Grosso (SES-MT), mitigando riscos nas aplicações que atendem às crescentes demandas de seus usuários internos, externos.

3.3 Eventos recentes de ataques cibernéticos contra órgãos dos Poderes demonstram o poder desses atacantes e a necessidade cada vez maior de implementarmos ações preventivas, detectivas e corretivas, de forma organizada e colaborativa para minimizar os impactos desses ataques. No Brasil, a escalada de ataques cibernéticos motivou a criação de diversos normativos que impõem uma série de novas responsabilidades e um conjunto inexplorado de atividades técnicas que teriam o objetivo de estabelecer um novo paradigma de segurança cibernética para todos os órgãos de governo.

3.4 A Superintendência de Tecnologia da Informação tem a missão de oferecer às unidades administrativas da SES-MT as melhores e mais eficientes ferramentas de mercado com o objetivo de superar a qualidade dos serviços prestados pela SES-MT à sociedade. O foco da instituição está em investir em Tecnologia da Informação e Comunicação para alcançar rapidez, segurança e eficiência em toda a cadeia produtiva.

3.5 Nossa entidade estadual é responsável pelo fornecimento diretamente e indiretamente de serviços à população mato-grossense através de 45 (quarenta e cinco) unidades, distribuídas em 16 (dezesseis) regiões de saúde. Desse total 13 (treze) são hospitais, sendo 09 (nove) em operação e 04 (quatro) em construção. Atualmente esta instituição possui uma equipe de infraestrutura capacitada para conduzir todas as necessidades desta instituição onde, após um esforço de checagem, levantamento e dimensionamento dos recursos, constatou a necessidade crítica de insumos de TI focados em segurança de aplicação para proteger o ambiente.





3.6 Após uma análise técnica detalhada, a equipe de TI da SES-MT identificou que a Solução WAF F5 Networks R5800 é a mais adequada para atender às necessidades atuais e futuras de segurança. O WAF é crucial por atuar na Camada Aplicação do modelo OSI, onde os firewalls de rede tradicionais não possuem visibilidade. Esta tecnologia de borda é essencial para garantir a proteção e a eficiência na prestação dos serviços públicos, defendendo os aplicativos web contra diversos tipos de ataques na camada de aplicação, como Cross-Site Scripting (XSS), injeção de SQL e envenenamento de cookies, entre outros.

3.7 A SECRETARIA DE SAÚDE DE MT trata diariamente um grande volume de dados sensíveis e processos de trabalho, para os quais precisa garantir confidencialidade, disponibilidade e integridade destas informações. De outro lado, a partir da ampliação da transformação digital e a disponibilização das soluções de software baseadas nos protocolos que constituem a Web, principalmente, HTTP (HyperText Transfer Protocol) e HTTPS (HyperText Transfer Protocol Secure) para acessos externos e internos, respectivamente, via Internet e Intranet, tornou-se necessário reduzir a superfície de ataque, ampliando a segurança da informação deste egrégia Secretaria de Saúde de MT, uma vez que tais aplicações são vetores potenciais para exploração de falhas, principalmente ao se considerar a complexidade das arquiteturas de softwares e plataformas utilizadas.

3.8 A SES-MT possui Data Center nas suas dependências onde hospeda aplicações e dados relevantes, pois, como responsável pela política estadual de saúde, pelos serviços de média e alta complexidade como os hospitais de emergência, hospitais de referência, centros especializados, hemocentros, e pela regulação estadual (que deve transferir os pacientes atendidos na rede de emergência para tratamentos especializados), a SES-MT suporta as demandas de seus usuários internos (usuários administrativos, unidades hospitalares e de saúde) e por conseguinte a população do Estado do Mato Grosso.

3.9 Neste ambiente a SES-MT hospeda diversas aplicações como a HOME PAGE DA SAÚDE, DW (DATA WARE HOUSE), INDICASUS, AGHUSE, SIEGES, SVS, SIMAP, GAL, CATMED, RESME, AGENDAMENTO DE DOAÇÃO DE SANGUE, SIGEP, MT HEMOVIDA, RTC, SAP, SGS, SIARQ,





SIMAP, SROA, HELP DESK, SADH, SGBR, NGSN, PORTAL COVID, PORTAL VACINAÇÃO, GENESIS, CONSULTA PLANTÃO, GESIAS, GPAC, PREDIS, E-SAMU, CIEVS, E-SUS, ATENÇÃO BÁSICA, entre. Estes sistemas acessíveis via *web* processam dados relevantes e sensíveis, exigindo o mais alto nível de proteção contra tentativas de invasão e manipulação.

3.10 Neste contexto, a aquisição de 2 (duas) unidades do WAF F5 Networks R5800 (com licença Best Bundle) é uma medida de Segurança Preventiva e de Compliance (em especial com a LGPD) que visa ampliar a proteção dos recursos computacionais para o atendimento das demandas atuais e futuras, garantindo a integridade e a continuidade dos serviços de saúde prestados à população do Estado do Mato Grosso. A contratação do Suporte Técnico 24x7 e da Instalação é vital para manter a eficácia e a alta disponibilidade da solução de segurança.

#### 4 DESCRIÇÃO DA AQUISIÇÃO

4.1 A descrição da aquisição como um todo, encontra-se pormenorizada, no anexo I.

#### 5 FUNDAMENTAÇÃO PARA ESCOLHA DA MODALIDADE LICITATÓRIA

Considerando a necessidade de aquisição de solução de proteção de redes, incluindo aquisições de hardware e software e respectivo serviço de implantação, posterior monitoramento e suporte técnico 24x7x365, contemplando utilização de equipamentos obrigatoriamente todos novos e de primeiro uso, de acordo com as especificações e quantitativos previstos, identificou-se a existência de Ata de Registro de Preços vigente, regularmente formalizada por nº. 2025/03636, por meio do processo licitatório n.º 30032.000154/2024-71, modalidade Pregão Eletrônico n.º. 20240008.

5.1 A modalidade licitatória adotada para contratação é a adesão a Ata de Registro de Preços.

5.2 A Lei nº 14.133/2021 (Nova Lei de Licitações e Contratos Administrativos) rege a utilização de Atas de Registro de Preços e, conforme o art. 58, autoriza a adesão a Atas de Registro de Preços firmadas por outros órgãos ou entidades, desde que atendam aos requisitos legais. A adesão a Atas de Registro de Preço ocorre para permitir que órgãos públicos adquiram bens ou contratem serviços sob as mesmas condições, preços e prazos acordados no processo licitatório original, sem a necessidade de nova licitação.



5.3 O artigo 58 da Lei nº 14.133/2021 estabelece as seguintes condições para a adesão:

5.3.1 Compatibilidade do objeto: a aquisição da solução de segurança do tipo Firewall de Aplicação Web (WAF), incluindo fornecimento, licenciamento, implantação, configuração, suporte técnico 24x7 e garantia de 36 meses visa atender às necessidades e devem ser compatíveis com as especificações e demandas da Secretaria de Estado de Saúde de Mato Grosso;

5.3.2 Conformidade com as condições da Ata: A adesão deve ocorrer dentro das condições acordadas entre o órgão responsável pela Ata (Empresa de Tecnologia da Informação do Ceará - ETICE) e o fornecedor vencedor, com descrição das especificações detalhadas neste Termo de Referência;

5.3.3 Não implicação de aumento de custo: A adesão à Ata de Registro de Preços não pode resultar em aumento do valor originalmente contratado ou em custos adicionais para o órgão aderente, ou seja, o preço pago pela solução de segurança do tipo Firewall de Aplicação Web (WAF), incluindo fornecimento, licenciamento, implantação, configuração, suporte técnico 24x7 e garantia de 36 meses deve ser o mesmo que foi registrado na Ata original.

#### DA EXECUÇÃO DO OBJETO

6.1 O prazo de execução do objeto contratual será de 12 (doze) meses para os itens 1 a 28 e de 36 (trinta e seis) meses para os itens 29 a 35, contado a partir do recebimento da ordem de serviço ou instrumento equivalente.

6.1.1 O prazo de execução poderá ser prorrogado, nos termos da Lei Federal nº 14.133/2021, e para as empresas públicas e sociedades de economia mista, o disposto na Lei Federal nº 13.303/2016.

#### 6.2 Condições de Entrega

6.2.1 Os itens 1 a 21 do objeto contratual deverão ser entregues na Contratante em conformidade com as especificações e condições estabelecidas neste termo, no prazo de 90 (noventa) dias úteis, contado do recebimento da ordem de fornecimento ou instrumento equivalente, nos locais, horários e dias estabelecidos no respectivo documento.

6.2.2 Os atrasos ocasionados por motivo de força maior ou caso fortuito, desde que justificados e aceitos pelo contratante, não serão considerados como inadimplemento contratual.

#### 6.3 Das Condições de Instalação





6.3.1 É/será de inteira responsabilidade da CONTRATADA a correta instalação, configuração e funcionamento dos equipamentos e componentes da solução ofertada, caso um dos serviços de instalação (itens 22 a 28) seja contratado. 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.

6.3.2 A instalação e configuração dos equipamentos será de responsabilidade da CONTRATANTE caso nenhum dos itens 22 a 28 seja contratado.

6.3.3 Em processos de implantação de Firewall de Aplicação Web Virtual ou Datacenter (itens 19 a 21), Firewall SEDE (itens 5 a 7), Firewall DATA CENTER (itens 8 a 10) ou mais de 10 unidades de Firewall UNIDADE REMOTA (itens 1 a 4) deverão ser realizadas as seguintes atividades:

6.3.4 Deverá ser realizada uma reunião de kick-off do projeto, nas instalações do CONTRATANTE, com a participação do gerente técnico do projeto, dos responsáveis comercial, de design da solução, pelo técnico responsável pela implementação do projeto;

6.3.5 O planejamento dos serviços de instalação deve resultar num documento tipo SOW (Scope of Work, em tradução livre, escopo de trabalho). Neste documento devem conter 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;

6.3.6 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;

6.3.7 Os serviços deverão ser realizados por pessoal técnico experiente e certificado pelo fabricante dos equipamentos. Em momento anterior à 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;

6.3.8 Ao término dos serviços deve ser criado um relatório detalhado 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 15 (quinze) dias após a finalização dos serviços;

6.3.9 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;

6.3.10 Em processos de implantação de até 10 unidades de Firewall UNIDADE REMOTA (itens 1 a 4) os processos detalhados podem ser executados de maneira simplificada sendo, no entanto, obrigatório:

6.3.10.1 Os serviços deverão ser realizados por pessoal técnico experiente e certificado pelo fabricante dos equipamentos. Em momento anterior à 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;

6.3.10.2 Relatório as-built simplificado;

6.3.10.3 Documentação completa da solução, incluindo especificação do equipamento, características e funcionalidades implementadas, comentários e configurações executadas.

#### **6.4 Do Local de Entrega**

6.4.1 Os bens deverão ser entregues no seguinte endereço Centro Político Administrativo, Palácio Paiaguás, Rua Júlio Domingos de Campos “Seo Fiote”, S/N, Bloco 5, CEP: 78050-970, Cuiabá-MT, Telefone: 3613-5332/5454/5460/5461, E-mail: [sti@ses.mt.gov.br](mailto:sti@ses.mt.gov.br).

6.4.2 A CONTRATADA deverá comunicar, previamente, a CONTRATANTE com o propósito de agendar todos os aspectos correlatos a entrega e as execuções dos serviços.





## 6.5 Do recebimento provisório e definitivo

6.5.1 Os bens serão recebidos provisoriamente, de forma sumária, no ato da entrega, juntamente com a nota fiscal ou instrumento de cobrança equivalente, pelo(a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes neste termo e na proposta.

6.5.2. Os bens poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes neste termo e na proposta, devendo ser substituídos no prazo de 90 (noventa) dias, a contar da notificação do contratado, às suas custas, sem prejuízo da aplicação das penalidades.

6.5.3. O recebimento definitivo ocorrerá no prazo de 10(dez) dias úteis, a contar do recebimento da nota fiscal ou instrumento de cobrança equivalente pela Administração, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo detalhado.

6.6.4. O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

6.7.5. No caso de controvérsia sobre a execução do objeto, quanto à qualidade e quantidade, deverá ser comunicando-se ao contratado para emissão de nota fiscal no que pertine à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento. 30/194

6.8.6. O prazo para a solução, pelo contratado, de inconsistências na execução do objeto ou de saneamento da nota fiscal ou de instrumento de cobrança equivalente, verificadas pela Administração durante a análise prévia à liquidação de despesa, não será computado para os fins do recebimento definitivo.

6.9.7. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança dos bens objeto da contratação, nem a responsabilidade ético-profissional pela perfeita execução do contrato.

## MODELO DE GESTÃO DE CONTRATO

7.1 O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

7.2 Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.





7.3 As comunicações entre o órgão ou entidade e o contratado devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

7.4 O contratante poderá convocar representante do contratado para adoção de providências que devam ser cumpridas de imediato.

7.5 Após a assinatura do contrato ou instrumento equivalente, o contratado poderá convocar o representante do contratado para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução do contratado, quando houver, do método de aferição dos resultados, quando houver, e das sanções aplicáveis, dentre outros.

7.6 A execução do contrato deverá ser acompanhada e fiscalizada pelo fiscal do contrato, ou pelo respectivo substituto, nos termos da lei.

7.7 A fiscalização se responsabilizará pelo acompanhamento da execução do objeto contratual, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração.

7.7.1 O fiscal do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados.

7.7.2 Identificada qualquer inexecução ou irregularidade, o fiscal emitirá notificações para a correção da execução do contrato, determinando prazo para a correção.

7.7.3 O fiscal informará ao gestor do contrato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso.

7.7.4 No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprezadas, o fiscal comunicará o fato imediatamente ao gestor do contrato.

7.7.5 O fiscal comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual.

7.8 O gestor do contrato coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais,





elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração.

7.9 O gestor do contrato acompanhará a manutenção das condições de habilitação do contratado, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais.

7.10 O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência.

7.11 O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, quando for o caso, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações.

7.12 O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido por comissão constituída para este fim.

## 8 DO CONTRATO

8.1 O CONTRATADO terá o prazo de 5 (cinco) dias úteis, contados a partir da convocação, para a assinatura do contrato. Este prazo poderá ser prorrogado uma vez por igual período, desde que solicitado durante o seu transcurso e, ainda assim, se devidamente justificado e aceito.

8.2 O contrato poderá ser assinado por certificação digital, com autenticidade reconhecida pelo ICP-Brasil.

8.3 Na assinatura do contrato será exigida a comprovação das condições de habilitação exigidas neste instrumento, as quais deverão ser mantidas pelo contratado durante todo o período da contratação, bem como a apresentação do Certificado de Registro Cadastral – CRC, emitido pela Secretaria de Planejamento e Gestão do Estado do MT.

8.4 Quando o adjudicatário não comprovar as condições habilitatórias consignadas neste instrumento, ou recusar-se a assinar o contrato.





## 9 FISCALIZAÇÃO CONTRATUAL

9.1 O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas do Decreto Estadual nº 1.525/2022 e da Lei nº 14.133/21, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

9.2 Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostilamento.

9.3 A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou, em caso de afastamentos legais, pelos respectivos substitutos.

9.4 Os gestores e fiscais de contrato devem ser previamente designados, por portaria geral ou específica, respeitadas as exigências do art. 308 do Decreto Estadual nº 1.525/2022, e cientificados de forma expressa, preferencialmente por meio eletrônico, bem como os titulares e substitutos, conforme § 4º do art. 308 do Decreto Estadual nº 1.525/2022.

9.5 Não obstante o Contratado seja o único e exclusivo responsável pela execução do Contrato, o contratante reserva-se o direito de, sem que de qualquer forma restrinja a plenitude dessa responsabilidade, exercer a mais ampla e completa fiscalização sobre a execução do objeto contratado.

9.6 Para efeito de gestão dos contratos originados desta operação, quando for o caso, serão utilizadas as seguintes definições:

9.6.1 **Gestor do Contrato** – Trata-se de servidor da unidade administrativa de controle ou equivalente, diretamente responsável pela disponibilização do bem às demais unidades administrativas do órgão ou entidade, devendo ser indicado em Contrato, sendo responsável por aplicar as ações estabelecidas no art. 14 do Decreto Estadual nº 1.525/2022, bem como:

9.6.1.1 Aplicar todas as determinações e normas de conduta, acompanhamento e fiscalização de contrato previstas em manual de gerenciamento de contrato, caso houver, e aquelas decorrentes da legislação aplicável.

9.6.1.2 Aplicar as orientações e determinações oriundas dos Órgãos de Controle Interno e Externo e as previstas nos instrumentos legais





9.6.2 **Fiscal do Contrato** – Trata-se de agente público indicado pelo Gestor do Contrato, preferencialmente, entre servidores que preencham os requisitos técnicos-profissionais aplicáveis, sendo responsável por aplicar as ações estabelecidas no art. 15 do Decreto Estadual nº 1.525/2022, bem como:

9.6.2.1 Prestar informações e esclarecimentos ao preposto do contratado, sempre que for preciso.

9.6.2.2 Desempenhar com eficiência e zelo todas as atribuições a ele incumbidas na legislação aplicável, em especial aquelas indicadas no art. 312 do Decreto Estadual nº 1.525/2022.

9.7 A fiscalização deverá emitir informação ou relatório a respeito de todos os atos do contratado relativos à execução do Contrato, quando couber, em especial quanto à aplicação de sanções, alterações, prorrogações e rescisão do Contrato;

9.8 A fiscalização deverá, em seu relatório de avaliação da qualidade dos bens, identificar e quantificar as ocorrências eventualmente praticadas pelo contratado no período de faturamento, com vistas a aplicar multas/glosas no pagamento da fatura.

9.9 Todas as ocorrências devem ser documentalmente comprovadas e anexadas ao Relatório a ser elaborado conforme estabelecido no art. 294 do Decreto Estadual nº 1.525/2022.

9.10 O Relatório é o ato administrativo que concretiza o recebimento provisório.

9.11 O fiscal do contrato anotará em registro próprio todas as ocorrências relacionadas à execução do contrato, determinando o que for necessário para a regularização das faltas ou dos defeitos observados.

9.12 O fiscal do contrato informará a seus superiores, em tempo hábil para a adoção das medidas convenientes, a situação que demandar decisão ou providência que ultrapasse sua competência.

## 10 HABILITAÇÃO ECONÔMICO E FINANCEIRA

10.1 A empresa deverá apresentar:

10.1.1 Certidão negativa de falência expedida pelo distribuidor da sede da pessoa jurídica, dentro do prazo de validade previsto na própria certidão, ou, na omissão desta, expedida há no máximo 90 (noventa) dias anteriores à data de abertura do certame;



- 10.1.2 Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, comprovando: índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um);
- 10.1.3 Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, comprovando: índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um);
- 10.1.4 As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura;
- 10.1.5 Os documentos referidos acima limitar-se-ia ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos;
- 10.1.6 Os documentos referidos acima deverão ser exigidos com base no limite definido pela Receita Federal do Brasil para transmissão da Escrituração Contábil Digital - ECO ao Sped;
- 10.1.7 As empresas criadas no exercício financeiro da licitação deverá atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura. (Lei nº 14.133, de 2021, art. 65, §1º);
- 10.1.8 Caso a empresa licitante apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral {SG) e Liquidez Corrente (LC), será exigido para fins de habilitação (capital mínimo) ou patrimônio líquido mínimo de (até 10%) do valor estimado do lote ou os itens pertinentes.
- 10.1.9 O atendimento dos índices econômicos previsto, neste item deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo fornecedor.
- 10.1.10 Critérios técnicos obrigatórios de habilitação
- a) Considerando-se a natureza dos bens e serviços a serem contratados, os padrões de excelência que se deseja alcançar e os resultados esperados, é significativo que as empresas candidatas demonstrem por meio de atestados de capacidade técnica, em proporção razoável de experiência comprovada, o fornecimento e a prestação de serviços compatíveis em características, quantidades e prazos com o objeto desta contratação.
- b) Os atestados devem conter: a identificação da entidade que emitiu o atestado; os sistemas





implantados ou serviços executados; a qualidade do serviço ou produto fornecido; a data da emissão do atestado; o nome, endereço e o telefone de contato dos atestadores, ou qualquer outro meio pelo qual a SES/MT possa valer-se para manter contato com os declarantes;

c) Todos os atestados apresentados poderão vir a ser objeto de diligência a ser efetuada pela SES/MT, que poderá demandar todos os contratos e devidas alterações que originam o atestado, acompanhados de seus aditivos, apostilamentos ou quaisquer outros itens que se obriguem a constar como parte integrante do contrato, bem como outras demonstrações cabíveis comprovação inequívoca do atestado em questão;

d) A licitante que não apresentar tais evidências será desclassificada por descumprimento de norma editalícia.

#### 10.1.11 Dos atestados de capacidade técnica a serem apresentados

Deverá ser apresentado, no mínimo, 01 (um) Atestado de Capacidade Técnica de fornecimento emitido por pessoa jurídica de direito público ou privado, comprovando o fornecimento, de objeto com características similares ou compatíveis com as do objeto deste Termo de Referência.

a) Observa-se que todas as comprovações poderão ser apresentadas por meio de um único atestado de capacidade técnica, caso seja passível de ser apresentado pela licitante;

b) Entende-se por similar ou compatível em características: Atestado que demonstre em sua individualidade, ou soma de atestados, a entrega de solução de segurança do tipo Firewall de Aplicação Web (WAF), incluindo fornecimento, licenciamento, implantação, configuração, suporte técnico 24x7 e garantia de 36 meses;

c) Quanto aos serviços solicitados, as Licitantes deverão apresentar atestados de capacidade técnica que demonstrem a execução bem-sucedida da instalação de solução de segurança do tipo Firewall de Aplicação Web (WAF), incluindo fornecimento, licenciamento, implantação, configuração, suporte técnico 24x7 e garantia de 36 meses;

d) Quanto ao fornecimento, as licitantes deverão apresentar atestados que em sua individualidade ou soma que contemplem que a licitante prestou/forneceu os serviços condizentes com o objeto desta licitação, no percentual de 50% (cinquenta por cento) do quantitativo total do objeto desta licitação;





- e) O(s) atestado(s) de capacidade técnica apresentado(s) estará(ão) sujeito(s) a confirmação de autenticidade, exatidão e veracidade conforme previsto na Lei Federal nº 14.133/2021, sujeitando o emissor às penalidades previstas em lei caso ateste informações inverídicas;
- f) Os atestados de capacidade técnica deverão ser obrigatoriamente emitidos por pessoa jurídica de direito público ou privado, contendo nome, cargo e número de telefone institucional, para contato do emitente. Adicionalmente, deverão informar os dados do contrato de referência, a saber: número, período de vigência, contratante e local da prestação dos serviços, além da descrição do objeto e quantidades;
- g) Serão aceitos atestados de capacidade técnica com vigência de garantia distinta dessa solicitada, desde que correlatos a soluções similares ao objeto desta contratação;
- h) Serão aceitos atestados de capacidade técnica de contratações ainda em vigor, tanto em condições de fornecimento quanto em condições de comodato, desde que similares ao objeto da contratação;
- i) Não serão aceitos "protocolos de entrega" ou "solicitação de documento" em substituição aos documentos requeridos neste instrumento;
- j) No caso de atestados emitidos por empresa da iniciativa privada, não serão considerados aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da empresa proponente;
- k) Serão consideradas como pertencentes ao mesmo grupo empresarial, empresas controladas ou controladoras da empresa proponente, ou que tenham pelo menos uma mesma pessoa física ou jurídica que seja sócio da empresa emitente e da empresa proponente.

## 11 ADEQUAÇÃO ORÇAMENTÁRIA

11.1 As despesas decorrentes da presente contratação designadas da Secretaria de Estado de Saúde correrão à conta de recursos específicos consignados no Orçamento da STI/SES/MT e serão atendidas pela seguinte dotação:

ÓRGÃO/ ENTIDADE	UNIDADE ORÇAMENTÁRIA	PROJETO/ ATIVIDADE	NATUREZA DE DESPESA	VALOR R\$	FONTE
SES/MT	21.601	2569	4.4.90.52.014	1.790.820,00	15001002





			3.3.90.40.006	6.753.789,20
--	--	--	---------------	--------------

**11.2 O objeto da contratação está previsto no Plano Anual de Contratações 2025, conforme detalhamento a seguir:**

ITEM	POS	TIPO DE CONTRATAÇÃO	DESCRIÇÃO DO ITEM/POSTO	TIPO DO ITEM	CODIGO DO ITEM	UNIDADE DE MEDIDA	QUANTIDADE	DEPENDENCIA DE OUTRO ITEM	COMO A SER CONTRATADO	VALOR UN. LÍQUIDO ESTIMADO	VALOR ESTIMADO DO CONTRATO	FONTE	MOTIVAZ	INDICAÇÃO DE CONTRATO	NECESSIDADE ATUALIZADA	DATA PREVISÃO PARA A CONTRATAÇÃO	GRAU DE PRIORIDADE	JUSTIFICATIVA RESUMIDA
17	2568	C	Atividade de monitoramento e supervisão de qualidade Web (Portal de Trans. Contas)	SERVICO		un.	240		Atividade de monitoramento e supervisão de qualidade Web (Portal de Trans. Contas) - 240 unidades de medida.	R\$ 1.700,00	R\$ 408.000,00	1-989-1007	140815581	Sim	Não	2025/01	ALTA	Atividade de monitoramento e supervisão de qualidade Web (Portal de Trans. Contas) - 240 unidades de medida.

## 12 DA GARANTIA DOS PRODUTOS E/OU SERVIÇOS ENTREGUES

12.1 A CONTRATADA dará suporte e assistência técnica 24x7 conforme descrito abaixo caso um dos itens 29 a 34 seja contratado, pelo período de 36 (trinta e seis) meses.

12.1 O suporte e assistência técnica se dará conforme as condições especificadas a partir do item 12.9.12 deste TR caso nenhum dos itens 29 a 34 seja contratado.

12.2 A CONTRATADA deverá possuir uma solução de monitoramento conforme **Anexo II**.

12.3 A CONTRATANTE poderá solicitar qualquer relatório da solução com uma frequência mensal o que deverá ser provido pela contratada num prazo de 5 dias úteis.

12.4 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 contemplado nesse instrumento. As tarefas atinentes ao transporte, deslocamento e remessa necessários, seja na implementação, substituição e/ou remoção de equipamentos defeituosos será de responsabilidade da CONTRATADA.

12.5 Para garantir a qualidade e disponibilidade do serviço, deverá ser disponibilizado pela empresa CONTRATADA uma ferramenta de monitoramento com estrutura dedicada para a STI/SES/MT que atenda as características mínimas descritas no **Anexo II**. Essas características deverão constar na comprovação ponto-a-ponto que será entregue.





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

12.7 O serviço de monitoramento 24x7 deverá ser prestado OBRIGATÓRIA E INDISPENSAVELMENTE através de NOCs (Network 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.

12.8 Os serviços prestados pelo NOC compreendem, entre outros, os seguintes procedimentos:

12.8.1 Monitoramento pró-ativo do ambiente de rede WAN do CONTRATANTE;

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

12.8.3 Resolução de problemas quanto acesso à internet, sites remotos, serviços de rede oferecidos aos funcionários do CONTRATANTE;

12.8.4 Resolução de problemas referente aos meios de Acesso WAN, tais como: MPLS e Ethernet;

12.8.5 Suporte em criação de políticas, configurações, parametrizações de quaisquer ordens relativos aos equipamentos ofertados;

12.8.6 Resolução de problemas referente a políticas, configurações, parametrizações de quaisquer ordens relativos aos equipamentos ofertados;

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

12.8.8 Encaminhar incidentes ao fabricante da solução;

12.8.9 Suporte em demais configurações de segurança, redundância e gerência;

12.8.10 Suporte, administração e monitoramento das políticas e tarefas de backup das configurações;

12.8.11 Apoio técnico para tarefas de auditoria e análise de logs.

12.8.12 A CONTRATADA deverá agir de forma reativa para incidentes, restabelecimento do serviço o mais rápido possível minimizando o impacto, seja por meio de uma solução de contorno ou definitiva.

Ainda caberá a CONTRATADA agir de forma proativa aplicando medidas para a boa manutenção afim de garantir a regularidade da operação do serviço.





12.8.13 O atendimento e suporte técnico especializado de 1º (primeiro nível) será sempre telefônico e remoto em regime 24x7 e assim, responsável pelo acompanhamento e gestão dos chamados, controle dos Indicadores de monitoramento, atuando como ponto único de contato entre a CONTRATANTE e profissionais da equipe da CONTRATADA.

12.8.14 O atendimento e suporte técnico especializado de 2º (segundo nível) poderá ser presencial ou remoto em regime 8x5 em todo estado do MT caso o suporte remoto não seja suficiente para resolução do problema. Responsável pela prevenção e resolução de incidentes, problemas e requisições, identificando a causa raiz de eventual problema e buscando sua solução. Execução de atividades remotas e/ou presenciais em incidentes, solicitações de maior complexidade.

12.8.15 Os Técnicos deverão ser capacitados e certificados para prestação dos serviços, resolução de incidentes, problemas e solicitações nos equipamentos ofertados. O comparecimento de um técnico ao local da necessidade será de no máximo 48 (quarenta e oito) horas para atendimentos na área que abrange e define a Região de Cuiabá e de até 5 (cinco) dias para as outras demais localidades (interior do Estado) e devendo sempre atender aos critérios de SLA determinados nesse instrumento/edital.

12.8.16 Para abertura dos chamados de suporte, a CONTRATADA deverá disponibilizar número telefônico 0800 (ou equivalente a ligação local), também serviço via portal WEB e/ou e-mail (em português). Na abertura do chamado, o órgão ao fazê-lo, receberá naquele momento, o número, data e hora de abertura do chamado. Este será considerado o início para contagem dos SLAS. O fechamento do chamado deverá ser comunicado pela CONTRATADA para fins de contagem do tempo de atendimento e resolução do chamado.

12.8.17 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:

12.8.17.1 02 (dois) profissionais com certificação de nível técnico fornecida pelo fabricante das soluções de Next Generation Firewall ofertadas;

12.8.17.2 02 (dois) profissionais com certificação de nível técnico fornecida pelo fabricante das soluções de Firewall de Aplicação Web – WAF;

12.8.17.3 02 (dois) profissionais com certificação ITIL Foundation;

12.8.17.4 01 (um) profissional com certificação PMP;





12.8.17.5 A Comprovação de que o(s) profissional(is) indicado(s) pela contratado pertence(m) ao seu quadro permanente, se dará mediante:

12.8.17.5.1 Apresentação de vínculo trabalhista (registro em carteira de trabalho e previdência social CTPS e ficha de empregado) em sendo o profissional empregado da licitante ou;

12.8.17.5.2 Apresentação de contrato social, em sendo o profissional integrante do quadro societário da licitante ou;

12.8.17.5.3 Apresentação de contrato de prestação de serviço regido pela legislação civil, celebrado entre o profissional e a contratada.

12.8.17.5.4 A CONTRATANTE poderá, em qualquer momento durante a execução do contrato, exigir a apresentação das documentações referidas nos subitens **16.9.17**, concedendo à CONTRATADA o prazo improrrogável de 30 (trinta) dias corridos, contados a partir da data do requerimento, para comprovar o atendimento das exigências. Ademais, a CONTRATADA deverá, na fase de habilitação, assumir compromisso formal quanto à disponibilidade de corpo técnico especializado, devidamente capacitado para a execução dos serviços previstos no contrato, sob pena de desclassificação.

12.8.17.5.5 A atualização de firmware quando disponibilizado exclusivamente pelo próprio fabricante dos equipamentos deverá ser executada pela CONTRATADA sem custo adicional, sempre que requisitado pela CONTRATANTE. Toda e qualquer atualização só poderá ser aplicada mediante autorização da CONTRATANTE. As atualizações deverão ocorrer em data e horário determinado pela CONTRATADA em comum acordo e autorização da CONTRATANTE visando manter em normal funcionamento a rede onde estiverem funcionando.

12.8.17.5.6 A CONTRATADA deverá fornecer informações de monitoramento on-line, via dashboard que permita o acompanhamento em tempo real do estado dos ativos. Deverá ainda apresentar relatórios mensais, por meio digital (DOCX, XLSX ou PDF), com o diagnóstico e controle dos equipamentos monitorados (dados, informações, descrição, indicadores e métricas que permitam quantificar o desempenho e a disponibilidade da operação do serviço).

12.8.17.5.7 A CONTRATADA deverá disponibilizar uma ferramenta de Service Desk comprovadamente aderente as boas práticas do ITIL e que contenha o detalhamento dos chamados com no mínimo as seguintes informações: o funcionário do órgão/entidade que realizou a abertura do chamado, data e hora de abertura, data e hora de atendimento, data e hora de solução, o funcionário do





órgão/entidade que realizou o encerramento do chamado, descrição detalhada do problema e das ações tomadas para sua resolução e a relação dos equipamentos ou componentes substituídos, especificando marca, modelo, fabricante e número de série).

12.8.17.5.8 Os relatórios de chamados abertos poderão ser solicitados a qualquer instante pela CONTRATANTE dentro das condições estipuladas, respeitando, no entanto, um prazo de até 48 (quarenta e oito) horas uteis. Esses relatórios deverão ser retidos pelo tempo mínimo equivalente a vigência do contrato e após o seu encerramento inutilizados.

12.8.17.5.9 A CONTRATADA deverá 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 dela, mesmo que a falha não tenha sido consumada, mas que tenha sido detectada a existência do risco.

12.8.17.5.10 A CONTRATANTE deverá definir 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 respondendo por sua conta e risco pelas intervenções que possam ter efetuado.

12.8.17.5.11 A CONTRATADA deverá respeitar os tempos máximos de ATENDIMENTOS e SLA (Nível de Acordo de Serviço) abaixo descritos, sob a pena de multa no caso de falhas em seu integral cumprimento:

12.8.17.5.11.1 Operação parada (incidente que gere parada total de algum serviço contemplado nesse contrato) o tempo de atendimento será de até 2 (duas) horas.

12.8.17.5.11.2 Operação impactada (incidente que gere parada parcial de algum serviço contemplado nesse contrato) o tempo de atendimento será de até 4 (quatro) horas.

12.8.17.5.11.3 Requisição de serviço (solicitações de mudanças nos equipamentos ou serviços do contrato) o tempo de atendimento será de até 8 (oito) horas.

12.8.17.5.11.4 Informações de contrato (solicitação de informação, parecer ou relatório de algum serviço contemplado no contrato) o tempo de atendimento será de até 12 (doze) horas.

12.8.17.6 Os itens 1 a 21 deste TR devem oferecer as condições de garantia conforme descrito abaixo:





12.8.17.7 A garantia deverá ser integral de, no mínimo, 36 (trinta e seis) meses do fabricante, com cobertura total para peças, atualização de versão e assistência técnica.

12.8.17.8 A Assistência Técnica deverá disponibilizar número telefônico 0800 (ou equivalente ao serviço gratuito) e serviço WEB ou e-mail (em português), para registro do chamado de assistência técnica e suporte. Em relação a abertura do chamado, o órgão ao fazê-lo, receberá neste momento, o número, data e hora de abertura do chamado. Este será considerado o início para contagem dos prazos estabelecidos;

12.8.17.9 Caso seja impossível a substituição dos equipamentos, componentes, materiais ou peças por outras que não as que compõem o item proposto, esta substituição obedecerá ao critério de compatibilidade, que poderá ser encontrado no site do fabricante, através de equivalência e semelhança, e só poderá ser efetuada mediante expressa autorização por escrito do órgão/entidade, para cada caso particular. Caso o órgão/entidade recuse o equipamento, componente, material e ou peça a ser substituído, o licitante deverá apresentar alternativas, porém o prazo para solução do problema não será alterado.

### 13 GARANTIA CONTRATUAL

13.1 Será exigida garantia contratual nos termos e prazos estabelecidos na cláusula décima segunda da minuta do contrato. A não prestação de garantia equivale à recusa injustificada para a contratação, caracterizando descumprimento total da obrigação assumida, ficando a adjudicatária sujeita às penalidades legalmente estabelecidas, inclusive multa.

13.2 Adotada a modalidade seguro-garantia, prevista no inciso II do § 1º do art. 96 da Lei nº 14.133/2021, o licitante deverá apresentá-la no valor correspondente a 5% (cinco por cento) do valor contratado, no prazo de 1(um) mês, contado da data de homologação da licitação e anterior à assinatura do contrato conforme § 3º do mesmo artigo suprarreferido.





## 14 OBRIGAÇÕES DO CONTRATADO

14.1 O contratado deve cumprir todas as obrigações constantes neste instrumento, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas;

14.1.1 Entregar o objeto, quando for o caso, acompanhado do manual do usuário, com uma versão em português, e da relação da rede de assistência técnica autorizada;

14.1.2 Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com o Código de Defesa do Consumidor;

14.1.3 Comunicar ao contratante, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;

14.1.4 Atender às determinações regulares emitidas pelo fiscal ou gestor do contrato ou autoridade superior e prestar todo esclarecimento ou informação por eles solicitados;

14.1.5 Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os bens nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

14.1.6 Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo contratante, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida, o valor correspondente aos danos sofridos;

14.1.7 Quando não for possível a verificação da regularidade no Sistema de Cadastramento Unificado de Fornecedores (SICAF) ou no Certificado de Registro Cadastral (CRC) do Estado do MT, o contratado deverá entregar ao setor responsável pela fiscalização do contrato, junto com a nota fiscal para fins de pagamento, os seguintes documentos: 1) prova de regularidade relativa à Seguridade Social; 2) Certidão Conjunta relativa aos Tributos Federais e à Dívida Ativa da União; 3) certidões que comprovem a regularidade perante a Fazenda Estadual ou Distrital do domicílio ou sede do contratado; 4) Certidão de Regularidade do FGTS – CRF; e 5) Certidão Negativa de Débitos Trabalhistas – CNDT;





14.1.8 Responsabilizar-se pelo cumprimento de todas as obrigações trabalhistas, previdenciárias, fiscais, comerciais e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao contratante e não poderá onerar o objeto do contrato;

14.1.9 Comunicar ao fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local da execução do objeto.

14.1.10 Paralisar, por determinação do contratante, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros.

14.1.11 Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação na licitação.

14.1.12 Cumprir, durante todo o período de execução do contrato e desde que regulamentado, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas em outras normas específicas. Esta obrigação não se aplica às contratações decorrentes da Lei nº 13.303/2016.

14.1.12.1 Comprovar as reservas de cargos e vagas a que se referem o subitem acima, no prazo fixado pelo fiscal do contrato, com a indicação dos empregados que preencheram as referidas vagas.

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

14.1.14 Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da contratação, exceto para restabelecer o equilíbrio econômico-financeiro inicial do contrato em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução do contrato tal como pactuado, respeitada, em qualquer caso, a repartição objetiva de risco estabelecida no contrato.

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

14.1.16 Promover, se for o caso, a guarda, manutenção e vigilância de materiais, ferramentas, tudo o que for necessário à execução do objeto, durante a vigência do contrato.





14.1.17 Providenciar a substituição de qualquer profissional envolvido na execução do objeto contratual, cuja conduta seja considerada indesejável pela fiscalização do contratante.

14.1.18 Respeitar os princípios de proteção de dados pessoais elencados na Lei Geral de Proteção de Dados, Lei nº 13.709 de 14 de agosto de 2018 e suas alterações.

14.1.19 Realizar os serviços de manutenção e assistência técnica nos locais indicados pela CONTRATANTE;

14.1.19.1 O técnico deverá se deslocar ao local da execução do serviço, salvo se puder ser realizado a distância.

## 15 OBRIGAÇÕES DO CONTRATANTE

15.1 Exigir o cumprimento de todas as obrigações assumidas pelo contratado, de acordo com este instrumento e seus anexos;

15.2 Receber o objeto no prazo e condições estabelecidas neste Termo;

15.3 Notificar o contratado, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto contratado, para que seja por ele substituído, reparado ou corrigido, no total ou em parte, às suas expensas;

15.4 Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pelo contratado;

15.5 Comunicar o contratado para emissão de nota fiscal relativa à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento, quando houver controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade;

15.6 Efetuar o pagamento ao contratado do valor correspondente a execução do objeto, no prazo, forma e condições estabelecidos neste termo;

15.7 Aplicar as sanções previstas na lei e neste instrumento, quando do descumprimento de obrigações pelo contratado;

15.8 Emitir explicitamente decisão sobre todas as solicitações e reclamações relacionadas à execução do contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do contrato.

15.8.1 A Administração terá o prazo de 10 (dez) dias, a contar da data do protocolo do requerimento para decidir sobre a solicitação de prorrogação motivada.





15.8.2 Responder eventuais pedidos de restabelecimento do equilíbrio econômico-financeiro feitos pelo contratado no prazo máximo de 30 (trinta) dias.

15.8.3 Não responder por quaisquer compromissos assumidos pelo contratado com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato do contratado, de seus empregados, prepostos ou subordinados.

## 16 PAGAMENTO

16.1 Não haverá pagamento antecipado.

16.2 O pagamento será realizado de acordo com a execução do objeto do contrato, mediante emissão da respectiva Nota Fiscal devidamente atestada, e análise dos documentos que compõem o processo de pagamento.

16.3 As operações de vendas destinadas a Órgão Público da Administração Federal, Estadual e Municipal, deverão ser acobertadas por Nota Fiscal Eletrônica, conforme Protocolo ICMS 42/2009, regulamentado pelo Artigo 355, §6º do RICMS. Informações através do site [www.sefaz.mt.gov.br/nfe](http://www.sefaz.mt.gov.br/nfe).

16.4 O contratado deverá indicar no corpo da Nota Fiscal, o número do Contrato/Ordem de Fornecimento, a descrição do objeto, o número e nome do banco, agência e número da conta na qual deverá ser feito o pagamento, via ordem bancária.

16.5 As despesas bancárias decorrentes de transferência de valor(es) para outra(s) praça(s) será(ão) de responsabilidade do contratado.

16.6 O contratante não efetuará pagamento de título descontado, ou por meio de cobrança em banco, bem como, os que forem negociados com terceiros, por intermédio da operação de “factoring”.

16.7 O pagamento será efetuado mediante a apresentação dos seguintes documentos:

16.8 Prova de regularidade junto à Fazenda Estadual, expedida pela Secretaria de Estado de Fazenda da sede ou domicílio do credor e do Estado de Mato Grosso, abrangendo inclusive débitos inscritos em dívida ativa;

16.9 Prova de regularidade junto à Dívida Ativa do Estado, expedida pela Procuradoria-Geral do Estado da sede ou domicílio do credor e do Estado de Mato Grosso;





- 16.10 Prova de regularidade perante o Fundo de Garantia do Tempo de Serviço – FGTS, em plena validade e relativa ao contratado.
- 16.11 Prova de regularidade fiscal perante a Fazenda Federal e Instituto Nacional do Seguro Social – INSS;
- 16.12 Prova de regularidade perante a Justiça do Trabalho;
- 16.13 Prova de regularidade junto à Fazenda Municipal da sede ou domicílio do credor.
- 16.14 O pagamento será efetuado pelo contratante em favor do contratado em até 30 dias úteis, mediante ordem bancária a ser depositada em conta corrente, no valor correspondente, após a apresentação da Nota Fiscal devidamente atestada pela fiscalização do contratante
- 16.15 O(s) pagamento(s) não realizado(s) dentro do prazo por eventos decorrentes do contratado, não será(ão) gerador(es) de direito a qualquer acréscimo financeiro;
- 16.16 Caso o atraso no pagamento seja motivado exclusivamente pelo contratante, o valor devido será corrigido pelo IPCA, conforme apuração desde a data prevista para o pagamento até a data de sua efetiva realização;
- 16.17 A efetivação dos pagamentos não isentará o contratado das suas responsabilidades e das suas obrigações contratuais, especialmente aquelas relacionadas à qualidade e à garantia dos produtos entregues.
- 16.18 Caso constatada alguma irregularidade ou incorreção na Nota Fiscal/Fatura, esta será devolvida ao contratado para as necessárias correções, acompanhada dos motivos que deram ensejo à sua rejeição, interrompendo-se o prazo para o pagamento, que começa a fluir somente a partir da data do protocolo da nova Nota Fiscal e demais documentos, devidamente corrigidos. O prazo somente voltará a fluir, desde o começo e de maneira integral, a partir da data do protocolo da nova Nota Fiscal e dos demais documentos exigíveis, devidamente corrigidos.
- 16.19 Constatando-se qualquer outra circunstância que desaconselha o pagamento, em razão de circunstância devidamente justificada e informada ao contratante, o prazo para pagamento ficará suspenso e voltará a partir da respectiva data de regularização.





16.20 Nos casos de aplicação de penalidade ao contratado, em virtude de inadimplência contratual, não serão efetuados pagamentos a esta, enquanto perdurar pendência de liquidação das respectivas obrigações.

16.21 As Notas Fiscais a serem pagas deverão sofrer desconto devido à aplicação de multas/glosas previstas no Contrato e já identificadas pela fiscalização.

16.22 O contratado deverá, durante toda a execução do Contrato, manter atualizada a vigência da garantia contratual.

## 17 REAJUSTE

17.1 Os preços inicialmente contratados são fixos e irremovíveis pelo prazo de um ano contado da data de empenho estimado.

17.2 Após o interregno de um ano, os preços iniciais poderão ser reajustados, mediante a aplicação, do índice IPCA, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade;

17.3 Os reajustes deverão ser precedidos de solicitação do contratado, acompanhada de memorial do cálculo, conforme for a variação de custos, objeto do reajuste.

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

17.5 No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o contratante pagará ao contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

17.6 O reajuste será realizado por apostilamento.

## 18 SANÇÕES

18.1 Comete infração administrativa, nos termos da Lei nº 14.133/2021 (art. 155) e do Decreto Estadual nº 1.525/2022 (art. 370 e 371), o contratado que:

18.1.1 Dar causa à inexecução parcial do contrato.

18.1.2 Dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo.





- 18.1.3 Dar causa à inexecução total do contrato.
- 18.1.4 Não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta.
- 18.1.5 Ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado.
- 18.1.6 Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato.
- 18.1.7 Fraudar a licitação ou praticar ato fraudulento na execução do contrato.
- 18.1.8 Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza.
- 18.1.9 Praticar atos ilícitos com vistas a frustrar os objetivos da licitação.
- 18.1.10 Praticar ato lesivo previsto no art. 5º, da Lei nº 12.846/2013.
- 18.2 Serão aplicadas ao contratado que incorrer nas infrações acima descritas as seguintes sanções:
- 18.2.1 Advertência, quando o contratado der causa à inexecução parcial do contrato que não implique em prejuízo ou dano à administração, bem como na hipótese de descumprimento de pequena relevância praticado pelo contratado e que não justifique imposição de penalidade mais grave.
- 18.3 Multa:
- 18.3.1 Moratória de 0,2% (dois décimos por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 25 (vinte e cinco) dias.
- 18.3.2 Moratória de 0,07% (sete centésimos por cento) por dia de atraso injustificado sobre o valor total do contrato, até o máximo de 2% (dois por cento) pela inobservância do prazo fixado para apresentação, suplementação ou reposição da garantia.
- 18.3.3 O atraso superior a 30 (trinta) dias autoriza a Administração a promover a extinção do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe o inciso I do art. 137 da Lei n. 14.133/2021.
- 18.3.3.1 Em casos de inexecução parcial do contrato, que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo, a multa será de 0,5% a 15% do valor do contrato licitado.
- 18.4 Compensatória de 20% (vinte por cento) sobre o valor total do contrato, no caso de inexecução total do objeto.
- 18.5 No caso de inexecução total, a multa será aplicada independentemente da existência ou não do prejuízo ao contratante, implicando ainda na possibilidade de rescisão do contrato.





- 18.6 A aplicação das sanções previstas neste contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao CONTRATANTE.
- 18.7 Todas as sanções previstas neste contrato poderão ser aplicadas cumulativamente com a multa.
- 18.8 Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.
- 18.9 A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa, observando-se o procedimento previsto na Lei nº 14.133/2021, no Decreto Estadual nº 1.525/2022 e, subsidiariamente, na Lei Estadual nº 7.692/2002.
- 18.10 A autoridade competente, na aplicação das sanções, levará em consideração:
- 18.10.1 a natureza e a gravidade da infração cometida;
  - 18.10.2 as peculiaridades do caso concreto;
  - 18.10.3 as circunstâncias agravantes ou atenuantes;
  - 18.10.4 os danos que dela provierem para o contratante;
  - 18.10.5 a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.
- 18.11 Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei e nos regulamentos estaduais complementares.
- 18.12 A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia.
- 18.13 Antes da remessa à Procuradoria-Geral do Estado para cobrança de créditos oriundos de contrato administrativo, o contratante deve optar, preferencialmente, pela compensação com eventuais pagamentos devidos ao contratado, independentemente de estes ou aqueles decorrerem de contratos distintos e/ou de Secretarias distintas, nos termos da ORIENTAÇÃO JURÍDICO-NORMATIVA 014/CPPGE/2022.
- 18.14 Após a apuração dos fatos e responsabilização da empresa, as penalidades aplicadas constarão registradas nos sistemas informatizado do Estado de Mato Grosso (Cadastro de Fornecedores) e do Poder





Executivo Federal, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep).

18.15 As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133/2021.

## 19 SUBCONTRATAÇÃO

19.1 É permitida a subcontratação parcial do objeto, até o limite de 25% (vinte e cinco por cento) do valor total do contrato.

19.2 É vedada a subcontratação integral do objeto.

19.3 Em qualquer hipótese de subcontratação, permanece a responsabilidade integral do contratado pela perfeita execução contratual, cabendo-lhe realizar a supervisão e coordenação das atividades do subcontratado, bem como responder perante o contratante pelo rigoroso cumprimento das obrigações contratuais correspondentes ao objeto da subcontratação.

19.4 A subcontratação depende de autorização prévia do contratante, a quem incumbe avaliar se o subcontratado cumpre os requisitos de qualificação técnica necessários para a execução do objeto.

19.5 O contratado apresentará à Administração documentação que comprove a capacidade técnica do subcontratado, que será avaliada e juntada aos autos do processo correspondente.

19.6 É vedada a subcontratação de pessoa física ou jurídica, se aquela ou os dirigentes desta mantiverem vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na contratação ou atue na fiscalização ou na gestão do contrato, ou se deles forem cônjuge, companheiro ou parente em linha reta, colateral, ou por afinidade, até o terceiro grau.

**20 ADEQUAÇÕES DE ACORDO COM DESPACHO: SES-DES-2026/21053 - INCLUSÃO DA CLAUSULA DECIMA SEGUNDA A CLAUSULA DECIMA NONA, PRESENTE NO EDITAL DO PREGÃO ELETRÔNICO, PÁGINAS 182-186, TENDO EM VISTA QUE SÃO CLAUSULAS ESSENCIAIS PARA ELABORAÇÃO DO CONTRATO. RESSALTA-SE QUE AS REFERIDAS RETIFICAÇÕES DIZEM RESPEITO AO ANEXO IV-A – MINUTA DE CONTRATO DO REFERIDO EDIATL. SENDO OS SEGUINTE ITENS 21 A 28.**





21 DA GARANTIA DE EXECUÇÃO

**21.1 A contratação conta com garantia de execução, nos moldes do art. 96 da Lei nº 14.133/2021, em valor correspondente a 5% (cinco por cento) do valor contratual, que deverá ser prestada até 10 (dez) dias úteis a contar da assinatura deste instrumento.**

**21.2 A apólice do seguro-garantia deverá acompanhar as modificações referentes à vigência do contrato principal mediante a emissão do respectivo endosso pela seguradora.**

**21.3 Será permitida a substituição da apólice de seguro-garantia na data de renovação ou de aniversário, desde que mantidas as condições e coberturas da apólice vigente e nenhum período fique descoberto, ressalvado o disposto no subitem 25.5, deste instrumento de contrato.**

**21.4 A garantia somente será liberada ou restituída após a fiel execução do contrato ou após a sua extinção por culpa exclusiva da Administração e, quando em dinheiro, será atualizada monetariamente.**

**21.5 Na hipótese de suspensão do contrato por ordem ou inadimplemento da Administração, o CONTRATADO ficará desobrigado de renovar a garantia ou de endossar a apólice de seguro até a ordem de reinício da execução ou o adimplemento pela Administração.**

**21.6 A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:**

**21.6.1 Prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;**

**21.6.2 Multas moratórias e punitivas aplicadas pela Administração ao CONTRATADO; e**

**21.6.3 Obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pelo CONTRATADO, quando couber.**

**21.7 A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no subitem 25.6, observada a legislação que rege a matéria.**

**21.8 A garantia em dinheiro deverá ser efetuada em favor do CONTRATANTE, em conta específica no Banco Brasil, com correção monetária.**





- 21.9** Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos sob forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Economia.
- 21.10** No caso de garantia na modalidade de fiança bancária, deverá ser emitida por banco ou instituição financeira devidamente autorizada a operar no País pelo Banco Central do Brasil, e deverá constar expressa renúncia do fiador aos benefícios do art. 827 do Código Civil.
- 21.11** No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada ou renovada, seguindo os mesmos parâmetros utilizados quando da contratação.
- 21.12** Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, o CONTRATADO obriga-se a fazer a respectiva reposição no prazo máximo de \_\_\_\_ (\_\_\_\_) dias úteis, contados da data em que for notificada.
- 21.13** O CONTRATANTE executará a garantia na forma prevista na legislação que rege a matéria.
- 21.14** O emitente da garantia ofertada pelo CONTRATADO deverá ser notificado pelo CONTRATANTE quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.
- 21.15** Caso se trate da modalidade seguro-garantia, ocorrido o sinistro durante a vigência da apólice, sua caracterização e comunicação poderão ocorrer fora desta vigência, não caracterizando fato que justifique a negativa do sinistro, desde que respeitados os prazos prescricionais aplicados ao contrato de seguro, nos termos do art. 20 da Circular Susep nº 662, de 11 de abril de 2022.
- 21.16** Extinguir-se-á a garantia com a restituição da apólice, carta fiança ou autorização para a liberação de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração do CONTRATANTE, mediante termo circunstanciado, de que o CONTRATADO cumpriu todas as cláusulas do contrato.





**21.17 O garantidor não é parte para figurar em processo administrativo instaurado pelo CONTRATANTE com o objetivo de apurar prejuízos e/ou aplicar sanções ao CONTRATADO.**

**21.18 O CONTRATADO autoriza o CONTRATANTE a reter, a qualquer tempo, a garantia, na forma prevista neste contrato.**

**21.19 Além da garantia de que tratam os arts. 96 e seguintes da Lei nº 14.133/2021, a presente contratação possui previsão de garantia do serviço a ser fornecido, incluindo manutenção e assistência técnica, conforme o caso e condições estabelecidas no Termo de Referência.**

## 22 DAS INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

22.1 Comete infração administrativa, nos termos da Lei nº 14.133/2021, o CONTRATADO que:

22.1.1 Der causa à inexecução parcial do contrato;

22.1.2 Der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;

22.1.3 Der causa à inexecução total do contrato;

22.1.4 Ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;

22.1.5 Apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato; 22.1.6 Praticar ato fraudulento na execução do contrato;

22.1.7 Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

22.1.8 Praticar ato lesivo previsto no art. 5º da Lei nº 12.846/2013.

22.2. Serão aplicadas ao CONTRATADO que incorrer nas infrações acima descritas as seguintes sanções:

22.2.1. Advertência, quando o CONTRATADO der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave;

22.2.2. Impedimento de licitar e contratar, quando praticadas as condutas descritas nos subitens 22.1.2, 23.1.3 e 23.1.4, deste contrato, sempre que não se justificar a imposição de penalidade mais grave;

22.2.3. Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nos subitens 22.1.5, 22.1.6, 22.1.7 e 22.1.8 deste contrato, bem como nos subitens 22.1.2, 22.1.3 e 22.1.4,

 



que justifiquem a imposição de penalidade mais grave.

#### 22.2.4. Multa:

22.2.4.1. Moratória de 0,2% (dois décimos por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 25 (vinte e cinco) dias.

22.2.4.2. Moratória de 0,07% (sete centésimos por cento) por dia de atraso injustificado sobre o valor total do contrato, até o máximo de 2% (dois por cento) pela inobservância do prazo fixado para apresentação, suplementação ou reposição da garantia.

22.2.4.2.1. O atraso superior a 30 (trinta) dias autoriza a Administração a promover a extinção do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe o inciso I do art. 137 da Lei n. 14.133/2021.

22.2.4.3. Compensatória de 20% (vinte por cento) sobre o valor total do contrato, no caso de inexecução total do objeto.

22.3. A aplicação das sanções previstas neste contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao CONTRATANTE.

22.4. Todas as sanções previstas neste contrato poderão ser aplicadas cumulativamente com a multa.

22.4.1. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

22.5. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao CONTRATADO, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei nº 14.133/2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

22.6. Na aplicação das sanções serão considerados:

22.6.1. A natureza e a gravidade da infração cometida;

22.6.2. As peculiaridades do caso concreto;

22.6.3. As circunstâncias agravantes ou atenuantes;

22.6.4. Os danos que dela provierem para o CONTRATANTE;

22.6.5. A implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

22.7. Os atos previstos como infrações administrativas na Lei nº 14.133/2021, ou em outras leis de





licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846/2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei.

22.8. A personalidade jurídica do CONTRATADO poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o CONTRATADO, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia.

22.9. O CONTRATANTE deverá, no prazo máximo 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ele aplicados, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal e no Certificado de Registro Cadastral (CRC) do Estado do Mato Grosso.

22.10. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133/ 2021.

22.11. Os débitos do CONTRATADO para com o CONTRATANTE, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes deste mesmo contrato ou de outros contratos administrativos que o CONTRATADO possua com o mesmo órgão ora CONTRATANTE.

22.11.1. Na impossibilidade do pagamento da multa por meio de descontos dos créditos existentes ou da garantia contratual, o CONTRATADO recolherá a multa por meio de Documento de Arrecadação Estadual (DAE), podendo ser substituído por outro instrumento legal, em nome do CONTRATANTE, se não o fizer, será cobrada em processo de execução.

## 23 DA EXTINÇÃO CONTRATUAL

23.1 Este contrato se extingue nas seguintes hipóteses:





23.1.1 Quando cumpridas as obrigações de ambas as partes, ainda que isso ocorra antes do prazo estipulado para tanto, e.

23.1.2 Quando mesmo não cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, ocorrer algum dos motivos previstos no art. 137 da Lei nº 14.133/2021, bem como amigavelmente, assegurados o contraditório e a ampla defesa.

23.1.3 Na hipótese do inciso II, aplicam-se também os arts. 138 e 139 da mesma Lei.

23.2 A alteração social ou a modificação da finalidade ou da estrutura da empresa não ensejará a rescisão se não restringir sua capacidade de concluir o contrato.

23.2.1 Se a operação implicar mudança da pessoa jurídica CONTRATADA, deverá ser formalizado termo aditivo para alteração subjetiva.

23.3 O termo de rescisão, sempre que possível, será precedido:

23.3.1 Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

23.3.2 Relação dos pagamentos já efetuados e ainda devidos;

23.3.3 Indenizações e multas.

23.4 A extinção do contrato não configura óbice para o reconhecimento do desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório.

23.5 Este contrato poderá ser rescindido a qualquer tempo pelo CONTRATANTE, mediante aviso prévio de no mínimo 30 (trinta) dias, nos casos das rescisões decorrentes do previsto no inciso VIII, do art. 137, da Lei Federal nº 14.133/2021, sem que caiba ao CONTRATADO, direito à indenização de qualquer espécie.

#### 24 DA DOTAÇÃO ORÇAMENTÁRIA

24.1 As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral do Estado deste exercício, na dotação abaixo discriminada, conforme o caso:

24.1.1 Gestão/Unidade:

24.1.2 Fonte de Recursos:





24.1.3 Programa de Trabalho:

24.1.4 Elemento de Despesa:

24.1.5 Nota de Empenho:

24.2 A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

## 25 DAS ALTERAÇÕES

25.1 Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 14.133/2021.

25.2 O CONTRATADO é obrigado a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

25.3 Registros que não caracterizam alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do art. 136 da Lei nº 14.133/2021.

## 26 DOS CASOS OMISSOS

26.1 Os casos omissos serão decididos pelo CONTRATANTE, segundo as disposições contidas na Lei nº 14.133/2021, e demais normas estaduais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078/1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

## 27 DA PUBLICAÇÃO

27.1 Incumbirá ao CONTRATANTE divulgar o presente instrumento no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no art. 94 da Lei 14.133/2021, bem como no respectivo sítio oficial na Internet, em atenção a Lei nº 12.527/2011, regulamentada no Estado do MT pelo Decreto Estadual nº 806/2021.

 



## 28 DO FORO

28.1 Fica eleito o foro do município da sede do CONTRATANTE, para dirimir os litígios que decorrerem da execução deste instrumento que não puderem ser compostos pela conciliação, conforme art. 92, §1º, da Lei nº 14.133/ 2021.

## 29 LEGISLAÇÃO APLICADA

29.1 Lei nº 14.133/2021 e alterações – Lei de Licitações e Contratos Administrativos.

29.2 Lei Estadual nº 7.692/2002 - Regula o processo administrativo.

29.3 Decreto Estadual nº 1.131, de 30 de setembro de 2021.

29.4 Decreto Estadual nº 1.525/2022 – Regulamenta a Lei nº 14.133/2021, no âmbito da Administração Pública estadual direta, autárquica e fundacional do Estado de Mato Grosso.

29.5 Decreto Estadual nº 806/2021 - Regulamenta a aplicação da Lei Federal nº 12.527, de 18 de novembro de 2011, no âmbito do Poder Executivo, disciplina a proteção de dados pessoais sensíveis e prevê salvaguardas à identidade dos denunciantes.

29.6 Lei complementar nº 116/2003 - Dispõe sobre o Imposto Sobre Serviços de Qualquer Natureza, de competência dos Municípios e do Distrito Federal.

29.7 Instrução Normativa nº 1.234/2012 - Dispõe sobre a retenção de tributos nos pagamentos efetuados pelos Órgãos da Administração Pública.

29.8 Instrução Normativa SLTI/MPOG nº 01/2010 - Práticas de sustentabilidade ambiental.

## 30 PÚBLICO ALVO

30.1 Os itens a serem adquiridos destinam-se ao atendimento da Infraestrutura de T.I. na SES-MT.

## 31 ANEXOS

São partes integrantes deste Termo de Referência:

31.1 DESCRIÇÃO DA AQUISIÇÃO - ANEXO I;

31.2 PLATAFORMA DE MONITORAMENTO - ANEXO II.

**Cuiabá-MT, 11 de fevereiro de 2026.**

Página 52 de 82





**Elaborado por:**

**ANDRE VALENTE DO COUTO**  
Superintendente de Tecnologia da Informação  
STI/SES/MT  
(Assinado digitalmente)

**MANOEL ABREU DE OLIVEIRA NETO**  
COIETI/SES/MT  
Coordenador de Infraestrutura de T.I.  
(Assinado digitalmente)

**De acordo:**

**MAYARA GALVÃO NASCIMENTO**  
Secretária Adjunta de Infraestrutura de  
Tecnologia e Informação - GBSAITI  
(Assinado Digitalmente)

**TERMO DE ANÁLISE, APROVAÇÃO E AUTORIZAÇÃO**

**1. DA ANÁLISE E APROVAÇÃO:**

1.1. Analisamos e aprovamos a 3ª Retificação ao **Termo de Referência nº 005/2025/COIETI/STI/GBSAITI/SES-MT**, seus anexos e constatamos a regularidade dos autos.

**2. DA AUTORIZAÇÃO:**

2.1. Analisado e aprovado a 3ª Retificação ao **Termo de Referência nº 005/2025/COIETI/STI/GBSAITI/SES-MT**, inerente e face aos processos e documentos vinculantes, **AUTORIZO** os procedimentos legais para realização de **adesão à Ata de Registro de Preços nº 2025/03636, Procedimento Administrativo n.º -30032.000154/2024-71, Pregão Eletrônico nº. 20240008**, cujos atos procedimentais e contratação devem obediência às condições e termos previstos no Termo de Referência supracitado, processo administrativo inerente e legislação vigente.

**Cuiabá-MT, 11 de fevereiro de 2026.**

**MAYARA GALVÃO NASCIMENTO**  
Secretária Adjunta de Infraestrutura de Tecnologia e Informação - GBSAITI  
(Assinado Digitalmente)

**ANEXO I – DESCRIÇÃO DA AQUISIÇÃO**

**1.1.21. ITEM 21 – FIREWALL DE APLICAÇÃO WEB – WAF – DATACENTER TIPO**





## II

1.1.21.1. Os appliances físicos devem ser novos e de primeiro uso;

1.1.21.2. Os equipamentos devem ser fornecidos em modo appliance, com conjunto de hardware e software dedicados, não podendo ser servidor de uso genérico, e que atendam todas as funcionalidades descritas neste Termo de Referência;

1.1.21.3. Devem ser novos, sem uso prévio e entregues em perfeito estado de funcionamento. Não devem ser remanufaturados, reconicionados ou possuir reparos de qualquer espécie;

1.1.21.4. Não serão aceitos equipamentos ou softwares que constem em anúncio ou lista do tipo end-of-sale, end-of-support ou end-of-life do fabricante, ou seja, produtos que serão descontinuados, perderão suporte e garantia oficiais do fabricante;

1.1.21.5. Deverão ser fornecidos todos os cabos, suportes (se necessários, "gavetas", "braços" e "trilhos"), incluindo todos os cabos de ligação lógica e elétrica necessários à instalação e perfeito funcionamento do equipamento no rack;

1.1.21.6. Dispor de fonte de alimentação redundante com tensão de entrada de 110V a 220V AC automática e frequência de 60Hz;

1.1.21.7. Possuir sistema operacional customizado especificamente para funções de Web Application Firewall, não podendo ser entregue appliance do tipo NGFW;

1.1.21.8. A solução deve ser licenciada para uso perpétuo. As funcionalidades da solução devem permanecer ativas após o período de garantia mesmo que desatualizadas e com todas as atualizações e assinaturas que forem disponibilizadas até data final do período que foram aplicadas ou instaladas na solução;

1.1.21.9. Possuir, no mínimo, 08 (oito) interfaces de 10GE SFP+. Serão aceitas interfaces de maior capacidade, desde que possibilitem ser transformados em 10 GE (incluindo os cabos "breakout" de no mínimo 3 metros);

1.1.21.10. Possuir, pelo menos, 02 (duas) interfaces 100G/40G QSFP+/QSFP28;

1.1.21.11. Possuir 01 interfaces 1GE, incluso interfaces de gerência com conectores padrão RJ45;

1.1.21.12. Todas as interfaces fornecidas devem estar licenciadas e habilitadas para uso imediato;

1.1.21.13. Deve possuir capacidade de inspecionar, no mínimo, 82 (oitenta e dois) Gbps de tráfego web em camada 7;





- 1.1.21.14. Suportar no mínimo 45.000 (quarenta e cinco mil) transações por segundo (TPS) SSL utilizando curva elíptica (ECDHE) com chaves RSA 2048 bits;
- 1.1.21.15. Suportar 80.000.000 (oitenta milhões) de conexões concorrentes em camada 4;
- 1.1.21.16. Possuir no mínimo compressão de 35.000 Mbps em tráfego HTTP/HTTPS;
- 1.1.21.17. Recursos de agregação de portas baseado no protocolo LACP, segundo o padrão IEEE 802.3ad;
- 1.1.21.18. Memória RAM mínima de 128 GB;
- 1.1.21.19. Disco rígido com capacidade de armazenamento interno e retenção de logs para análise com capacidade mínima de 1TB;
- 1.1.21.20. Deve vir acompanhado de todas as licenças de software ou hardware necessárias para atendimento das funcionalidades exigidas neste caderno de especificações técnicas;
- 1.1.21.21. Garantir que na aceleração de SSL, tanto a troca de chaves quanto a criptografia dos dados seja realizada com aceleração em hardware, para não onerar o sistema;
- 1.1.21.22. Deve permitir a configuração da solução em alta disponibilidade, permitindo o funcionamento em cluster do tipo ativo-passivo e ativo-ativo;
- 1.1.21.23. A solução deve suportar mais do que dois elementos no cluster para sincronização de configuração de forma nativa a fim de permitir escalabilidade no futuro;
- 1.1.21.24. Implementar a sincronização entre os equipamentos redundantes, assegurando que não haverá "downtime" e queda de sessões em caso de falha de uma das unidades;
- 1.1.21.25. Possuir recurso para o transporte de múltiplas VLANs por uma única porta (ou por um conjunto agregado de portas) utilizando o protocolo 802.1q;
- 1.1.21.26. Deve suportar, no mínimo, 1000 VLANs simultaneamente;
- 1.1.21.27. Analisar e proteger tráfego HTTP/1.0, HTTP/1.1, HTTP/2.0 e/ou HTTP/3;
- 1.1.21.28. Possuir suporte a IPv6;
- 1.1.21.29. A solução deve permitir o encapsulamento, em camada 3, do tráfego entre o balanceador e o servidor para tráfego IPv4 e IPv6, quando o balanceamento é realizado apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente;
- 1.1.21.30. Possuir suporte à funcionalidade de VXLAN para integração com o ambiente de virtualização (Software Defined Network);





- 1.1.21.31. Assinar cookies digitalmente e editar endereços de URL (“URL Rewriting”);
- 1.1.21.32. Os usuários de gerência deverão poder ser autenticados em bases remotas. No mínimo RADIUS, LDAP e TACACS+ deverão ser suportados;
- 1.1.21.33. Deverá possuir uma funcionalidade de criação automática de políticas, para proteção DDOS e ataques zero-day onde a política de segurança é criada e atualizada automaticamente baseando-se no tráfego real observado à aplicação;
- 1.1.21.34. Restringir métodos HTTP/ HTTPS permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de cookies;
- 1.1.21.35. Permitir as seguintes opções de implementação:
- 1.1.21.36. Monitoramento (sem bloqueio);
- 1.1.21.37. Proxy (reverso e transparente);
- 1.1.21.38. Permitir que novas políticas fiquem apenas monitorando o tráfego, sem bloqueá-lo, indicando caso aconteça algum evento;
- 1.1.21.39. Remover as mensagens de erro do conteúdo que será enviado aos usuários;
- 1.1.21.40. Proteger contra-ataques automatizados, incluindo bots e web scraping, identificando comportamento não humano, navegadores operados por scripts ou qualquer outra forma que não operados por humanos;
- 1.1.21.41. Possuir firewall XML integrado com suporte a filtro e validação de funções XML específicas da aplicação;
- 1.1.21.42. A solução deve suportar e fazer a proteção do tráfego de protocolo WebSocket;
- 1.1.21.43. Permitir a utilização de modelo positivo de segurança para proteger contra ataques às aplicações HTTP e HTTPS, além de proteção contra- ataques conhecidos aos protocolos HTTP e HTTPS;
- 1.1.21.44. Criação de políticas automáticas que bloqueiam o endereço IP que realizar violações;
- 1.1.21.45. Possuir mecanismo de aprendizado automatizado capaz de identificar todos os conteúdos das aplicações, incluindo URLs, parâmetros URLs, campos de formulários, o que se espera de cada campo (tipo de dado, tamanho de caracteres, se é um campo obrigatório), cookies, ações SOAP e elementos XML. Identificar e criar perfil de utilização dos aplicativos, inclusive desenvolvidos em Javascript, CGI, ASP e PHP;



1.1.21.46. Deve possuir tecnologia para mitigação de DDoS em camada 7 baseado em análise comportamental, usando o aprendizado;

1.1.21.47. A solução deve possuir a capacidade de capturar tráfego no formato TCP Dump relativos a ataques DoS L7, Web Scraping e força bruta permitindo uma análise mais aprofundada por parte do administrador;

1.1.21.48. Detectar ataques de força bruta por meio dos seguintes métodos:

1.1.21.49. Aumento do tempo de resposta da aplicação monitorada ou bloqueio temporário do atacante;

1.1.21.50. Quantidade de transações por segundo (TPS), monitorando a quantidade de transações por segundo por endereço IP;

1.1.21.51. Permitir a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes;

1.1.21.52. Apresentar proteção contra-ataques, como:

1.1.21.53. Brute Force Login;

1.1.21.54. Buffer Overflow;

1.1.21.55. Cookie Injection;

1.1.21.56. Cookie Poisoning;

1.1.21.57. Cross Site Request Forgery (CSRF);

1.1.21.58. Cross Site Scripting (XSS);

1.1.21.59. Server Side Request Forgery (SSRF);

1.1.21.60. Directory Traversal;

1.1.21.61. Forceful Browsing;

1.1.21.62. HTTP Denial of Service;

1.1.21.63. HTTP hidden field manipulation;

1.1.21.64. HTTP request smuggling;

1.1.21.65. HTTP Response Splitting;

1.1.21.66. Malicious Robots;

1.1.21.67. Parameter Tampering;

1.1.21.68. Remote File Inclusion Attacks;





- 1.1.21.69. Sensitive Data Leakage (Social Security Numbers, Cardholder Data, PII, HPI);
- 1.1.21.70. Session Hijacking;
- 1.1.21.71. SQL Injection;
- 1.1.21.72. Web Scraping;
- 1.1.21.73. Web server software and operating system attacks;
- 1.1.21.74. Web Services (XML) attacks;
- 1.1.21.75. Deve permitir que possa ser especificado na política os tipos de arquivos que serão bloqueados (File Types);
- 1.1.21.76. A solução deve permitir a inspeção de upload de arquivos para os servidores de aplicação, ou enviar para inspeção através do protocolo ICAP;
- 1.1.21.77. Deve encriptar dados e credenciais na camada de aplicação, sem ter a necessidade de atualizar a aplicação. Essas informações devem ser encriptadas para proteger o login e as credenciais dos usuários e com isso os dados da aplicação;
- 1.1.21.78. Deve proteger informações sensíveis e confidenciais da interceptação por terceiros, através da criptografia de dados quando ainda no browser do usuário. Deve proteger esses dados criptografados de malwares e keyloggers;
- 1.1.21.79. Deve ofuscar o nome de um parâmetro sensível da aplicação em caracteres randômicos. Esse nome de parâmetro deve ser mudado constantemente pela ferramenta para dificultar ataques direcionados;
- 1.1.21.80. A solução deve fornecer relatórios consolidados de ataques com pelo menos os seguintes dados:
- 1.1.21.81. Resumo geral com as políticas ativas, anomalias e estatísticas de tráfego, Ataques DoS, Ataques de Força Bruta, Ataques de Robôs, Violações, URL, Endereços IP, Países, Severidade;
- 1.1.21.82. Deverá permitir o agendamento de relatórios a serem entregues por email;
- 1.1.21.83. Emitir os seguintes relatórios gráficos por:
- 1.1.21.84. Política de segurança;
- 1.1.21.85. Tipos de ataques;
- 1.1.21.86. Violações;



- 1.1.21.87. URL que foram atacadas;
- 1.1.21.88. Endereços IP de origem;
- 1.1.21.89. Localização geográfica dos endereços IPs de origem;
- 1.1.21.90. Severidade;
- 1.1.21.91. Código de resposta;
- 1.1.21.92. Métodos;
- 1.1.21.93. Protocolos;
- 1.1.21.94. Sessão;
- 1.1.21.95. A solução deve ser capaz de proteger GraphQL APIs com pelos menos os seguintes parâmetros: tamanho total, tamanho de cada parâmetro
- 1.1.21.96. A solução deve ser capaz de proteger GraphQL APIs limitando a quantidade de queries dentro de uma requisição HTTP
- 1.1.21.97. A solução deve ser capaz de proteger APIs baseadas em OpenAPI 2.0
- 1.1.21.98. A solução deve ser capaz de proteger APIs baseadas em OpenAPI 3.0
- 1.1.21.99. A solução deve suportar a criação de políticas de proteção com base no modelo OWASP, onde pelo menos devem ser aplicadas políticas de proteção contra o TOP 10 OWASP
- 1.1.21.100. A solução deve emitir relatório com análise cada política de proteção comparado com o TOP 10 OWASP.
- 1.1.21.101. A solução deverá possuir as seguintes formas de detecção de ataques DoS na camada de aplicação:
- 1.1.21.102. Número de requisições por segundo enviados a uma URL específica;
- 1.1.21.103. Número de requisições por segundo enviados de um IP específico;
- 1.1.21.104. Detecção através de código executado no cliente com o objetivo de detectar interação humana ou comportamento de robôs (bots);
- 1.1.21.105. Número máximo de transações por segundo (TPS) de um determinado IP;
- 1.1.21.106. Aumento de um determinado percentual do número de transações por segundo (TPS);
- 1.1.21.107. Aumento do stress do servidor de aplicação;
- 1.1.21.108. Funcionalidades de Balanceamento de Carga
- 1.1.21.109. Deve suportar todas as aplicações comuns de um Switch Layer 7, como:





- 1.1.21.110. Server Load-Balancing;
- 1.1.21.111. Firewall Load-Balancing;
- 1.1.21.112. Proxy Load-Balancing;
- 1.1.21.113. Deve suportar balanceamento apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente;
- 1.1.21.114. Deve permitir o encapsulamento, em camada 3, do tráfego entre a solução e o servidor para tráfego IPv4 e IPv6, quando o balanceamento é realizado apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente;
- 1.1.21.115. Permitir a clonagem de pools, de forma que a solução envie uma cópia do tráfego para um pool adicional, como por exemplo um pool de IDSs ou Sniffers, para fins de análise de tráfego de rede ou mesmo para identificação de padrões de acesso não permitidos ou indicações de atividade maliciosas ou ataques de rede;
- 1.1.21.116. Possuir recursos para balancear servidores com qualquer hardware, sistema operacional e tipo de aplicação;
- 1.1.21.117. A solução deve possuir recurso de ativação de grupo prioritário, no qual o administrador pode especificar a quantidade mínima de servidores que devem estar disponíveis em cada grupo e a prioridade dos grupos.
- 1.1.21.118. Caso o número de servidores disponíveis fique menor do que o estipulado pelo administrador, a solução deve automaticamente distribuir o tráfego para o próximo grupo com maior prioridade não afetando o serviço.
- 1.1.21.119. Caso o número de servidores disponíveis volte ao valor mínimo estipulado pelo administrador, a solução deve automaticamente retirar o grupo com menor prioridade de balanceamento, voltando ao estado original.
- 1.1.21.120. Possuir capacidade de abrir um número reduzido de conexões TCP com o servidor e inserir os HTTP requests gerado pelos clientes nestas conexões, reduzindo a necessidade de estabelecimento de conexões nos servidores e aumentando a performance do serviço;
- 1.1.21.121. Suportar os seguintes métodos de balanceamento:
- 1.1.21.122. Round Robin;
- 1.1.21.123. Least Connections;





- 1.1.21.124. Weighted Percentage (por peso);
- 1.1.21.125. Servidor ou equipamento com resposta mais rápida baseado no tráfego real;
- 1.1.21.126. Weighted Percentage dinâmico (baseado no número de conexões)
- 1.1.21.127. Dinâmico, baseado em parâmetros de um determinado servidor ou equipamento, coletados via SNMP ou WMI;
- 1.1.21.128. A solução deve permitir aplicar criptografia de cookies para a proteção dos cookies utilizados pela aplicação web;
- 1.1.21.129. Possuir recursos para balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência de sessão dos seguintes tipos:
- 1.1.21.130. Por cookie: inserção de um novo cookie na sessão;
- 1.1.21.131. Por cookie: utilização do valor do cookie da aplicação, sem adição de cookie;
- 1.1.21.132. Por endereço IP destino;
- 1.1.21.133. Por endereço IP origem;
- 1.1.21.134. Por sessão SSL;
- 1.1.21.135. Através da análise da URL acessada.;
- 1.1.21.136. Através da análise de qualquer parâmetro no header HTTP;
- 1.1.21.137. Através da análise do MS Terminal Services Session (MSRDP)
- 1.1.21.138. Através da análise do SIP Call ID ou Source IP;
- 1.1.21.139. Através da análise de qualquer informação da porção de dados (camada 7);
- 1.1.21.140. A solução deve utilizar Cache Array Routing Protocol (CARP) no algoritmo de HASH;
- 1.1.21.141. Deve suportar os seguintes métodos de monitoramento dos servidores reais:
- 1.1.21.142. ICMP;
- 1.1.21.143. Conexões TCP e UDP pela respectiva porta no servidor;
- 1.1.21.144. Devem existir monitores predefinidos para, no mínimo, os seguintes protocolos:  
ICMP,  
HTTP, HTTPS, Diameter, FTP, SASP, SMB, RADIUS, MSSQL, NNTP, ORACLE, RPC, LDAP,  
IMAP, SMTP, POP3, SIP, Real Server, SOAP, SNMP e WMI;
- 1.1.21.145. Possuir recursos para balanceamento de carga de servidores SIP para VoIP





(equipamento SIP PROXY);

1.1.21.146. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor Físico ;

1.1.21.147. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor virtual;

1.1.21.148. Possuir recursos para limitar o número de sessões estabelecidas com cada grupo de servidores;

1.1.21.149. Realizar Network Address Translation (NAT);

1.1.21.150. Realizar Proteção contra Denial of Service (DoS);

1.1.21.151. Realizar Proteção contra Syn flood;

1.1.21.152. Realizar Limpeza de cabeçalho HTTP;

1.1.21.153. Deve permitir o controle da resposta ICMP por servidor virtual;

1.1.21.154. Possuir recursos para que a configuração seja baseada em perfis, permitindo uma fácil administração;

1.1.21.155. Possuir capacidade de geração e gestão de perfis hierarquizados, permitindo maior facilidade na administração de políticas similares;

1.1.21.156. Permitir a criação de Virtual Servers com endereço IPv4 e os servidores reais com endereços IPv6;

1.1.21.157. Possuir recursos para executar compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente;

1.1.21.158. Definir qual tipo de compressão será habilitada (gzip1 a gzip9, deflate);

1.1.21.159. Possuir capacidade para definir compressão especificamente para certos tipos de objetos;

1.1.21.160. Permitir a utilização de memória RAM como cache de objetos HTTP, para responder às requisições dos usuários sem utilizar recursos dos servidores;

1.1.21.161. Permitir definir quais tipos de objeto serão armazenados em cache e quais nunca devem ser cacheados;

1.1.21.162. Garantir que o recurso de cache possa ajustar quanta memória será utilizada para armazenar objetos;





- 1.1.21.163. Suporte a otimização do protocolo TCP para ajustes a parâmetros das conexões clientes e servidor;
- 1.1.21.164. Deve possuir relatórios das aplicações, com pelos menos os seguintes gráficos:
- 1.1.21.165. Tempo de resposta da aplicação;
- 1.1.21.166. Latência ;
- 1.1.21.167. Conexões para conjunto de servidores, servidores individuais;
- 1.1.21.168. Por URL;
- 1.1.21.169. A ferramenta de relatórios deve possuir pelo menos os seguintes filtros para a geração dos gráficos:
- 1.1.21.170. Servidores virtuais
- 1.1.21.171. Servidores balanceados
- 1.1.21.172. URLs
- 1.1.21.173. Países de origem, baseados em geolocalização (GEOIP)
- 1.1.21.174. Dispositivos de origem do cliente (user agent)
- 1.1.21.175. Deve possuir framework unificado para configuração da aplicação
- 1.1.21.176. Quando licenciada, a solução deve ter a capacidade de realizar cache transparente das respostas DNS;
- 1.1.21.177. A Solução deve ter suporte a sFlow;
- 1.1.21.178. A solução deve possuir múltiplos domínios de roteamento em IPv4 e IPv6;
- 1.1.21.179. A solução deve permitir que cada domínio de roteamento utilize BGP, OSPF e RIP em IPv4 e IPv6;
- 1.1.21.180. A solução deve suportar Equal Cost Multipath (ECMP);
- 1.1.21.181. A solução deve realizar Bidirectional Forward Detection (BFD);
- 1.1.21.182. A solução deve ter suporte a Stream Control Transmission Protocol (SCTP);
- 1.1.21.183. Deve ter suporte a Transport Layer Security (TLS) Server Name Indication (SNI);
- 1.1.21.184. A solução deve possuir monitor HTTP/HTTPS com autenticação NTLM embutida, que permita verificar se o HTTP/HTTPS está operando assim como a plataforma de autenticação;
- 1.1.21.185. A solução deve ter suporte a TLS 1.2, SHA 2 Cipher e SHA256 hash;
- 1.1.21.186. A solução deve ter suporte a criptografia Perfect Forward Secrecy não apenas para





troca de chaves RSA.

1.1.21.187. A solução deve ser capaz de colocar em fila as requisições TCP que excedam a capacidade de conexões do grupo de servidores ou de um servidor. A solução não deverá descartar as conexões que excedam o número de conexões do servidor ou do grupo de servidores:

1.1.21.188. Deve ser possível configurar o tamanho máximo da fila;

1.1.21.189. Deve ser possível configurar o tempo máximo de permanência na fila;

1.1.21.190. A solução deve realizar Controle de Banda Estático para grupos de aplicações e rede;

1.1.21.191. A solução deve realizar Controle de Banda Dinâmico por aplicação e usuário;

1.1.21.192. A solução deve realizar Controle de Banda baseado em domínio de roteamento;

1.1.21.193. Permitir tráfego por parâmetros de QoS (Quality of Service) ou rate-shaping, com pelo menos 2 (duas) filas para priorização de tráfego baseada na camada de aplicação;

1.1.21.194. Através dessa priorização de tráfego e restrição de largura de banda deverá ser possível permitir um melhor nível de serviço para clientes preferenciais em detrimento dos demais clientes.

1.1.21.195. A solução deve permitir a priorização de tráfego de entrada para determinadas aplicações.

1.1.21.196. A solução deve permitir a criação de túneis IP por domínio de roteamento utilizando GRE, IPIP, EtherIP, PPP;

1.1.21.197. A solução deve permitir a criação de túneis IP transparente utilizando GRE e IPIP;

1.1.21.198. Fornecer recursos para o uso de servidores (reals) no mesmo Virtual Server;

1.1.21.199. Possuir suporte ao protocolo SPDY e HTTP 2.0;

1.1.21.200. O equipamento deve possuir suporte ao espelhamento de conexões FTP, Telnet, HTTP, UDP, SSL.

1.1.21.201. O equipamento deverá permitir a sincronização das configurações:

1.1.21.202. De forma automática; e

1.1.21.203. Manualmente, forçando a sincronização apenas no momento desejado;

1.1.21.204. Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar a distribuição dinâmica de tráfego e aumentar a proteção contra ataques;





1.1.21.205. A solução deve possuir linguagem de programação open-source que permita a manipulação do tráfego de entrada e saída, viabilizando assim a alteração de parâmetros no cabeçalho e no corpo das mensagens.

1.1.21.206. Essa linguagem de programação deve permitir a importação de pacotes, garantindo assim que a agilidade e flexibilidade no compartilhamento dos scripts.

1.1.21.207. Permitir a criação de políticas através de interface gráfica web para manipulação de tráfego através de lógica para pelo menos os seguintes operadores:

1.1.21.208. GEOIP, http-basic-auth, http-cookie, http-header, http-host, http-method, http-referer, http-set-cookie, http-status, http-uri e http-version

1.1.21.209. Deve ser possível tomar as seguintes ações através dessas políticas:

1.1.21.210. Bloqueio de tráfego

1.1.21.211. Reescrita e manipulação de URL

1.1.21.212. Registro de tráfego (log)

1.1.21.213. Adição de informação no cabeçalho HTTP

1.1.21.214. Redirecionamento do tráfego para um membro específico

1.1.21.215. Selecionar uma política específica para Aplicação Web

1.1.21.216. A solução deverá ser capaz de fazer log de todas as sessões, onde os registros deverão conter:

1.1.21.217. Endereço IP de origem;

1.1.21.218. Porta TCP ou UDP de origem;

1.1.21.219. Endereço IP de destino;

1.1.21.220. Porta TCP ou UDP de destino;

1.1.21.221. Protocolo de camada 4 (TCP ou UDP);

1.1.21.222. Data e hora da mensagem;

1.1.21.223. URL acessada;

1.1.21.224. A solução deve possuir políticas de uso de senhas administrativas tais como: nível de complexidade, período de validade e travamento de conta devido a erros múltiplos de login de forma nativa ou no mínimo integrado a uma base Active Directory.

1.1.21.225. A solução deve suportar controle de versão da política de configuração de forma a



permitir fazer roll back de políticas aplicadas.

1.1.21.226. Funcionalidades para alta disponibilidade entre ambientes de Datacenter

1.1.21.227. Fornecer recurso de agregação de portas baseado no protocolo LACP;

1.1.21.228. Deve possuir suporte a LACP em modo passivo e ativo;

1.1.21.229. Fornecer recurso para suportar até 8 portas em um mesmo conjunto agregado;

1.1.21.230. Deve possuir suporte a Spanning-Tree(802.1D), Fast Spanning-Tree (802.1w, 802.1t) e Multi Spanning-Tree (802.1s);

1.1.21.231. Fornecer recurso para o transporte de múltiplas VLAN por uma única porta (ou por um conjunto agregado de portas) utilizando o protocolo 802.1q;

1.1.21.232. Possuir suporte a IPv6;

1.1.21.233. A solução deve suportar múltiplas tabelas de rotas independentes;

1.1.21.234. A solução deve possuir suporte a múltiplos domínios de roteamento em IPv4 e IPv6;

1.1.21.235. Possuir ferramenta online web gratuita na qual seja possível carregar as configurações e receber diagnóstico da solução com informações sobre atualizações, melhores práticas, estado da solução e informações preventivas.

1.1.21.236. A solução deve operar em, no mínimo, a seguintes formas:

1.1.21.237. DNS autoritativo;

1.1.21.238. DNS secundário;

1.1.21.239. DNS resolver;

1.1.21.240. DNS cache;

1.1.21.241. Balanceamento de DNS servers;

1.1.21.242. DNSSec;

1.1.21.243. A solução deve ser capaz de realizar transferência de zonas para múltiplos servidores DNS Primários responsáveis por diferentes zonas.

1.1.21.244. Deve possuir funcionalidade de DNS cache, realizando cache transparente, caching resolver e validação de caching resolver.

1.1.21.245. Capacidade de uso de chave criptográfica TSIG para comunicação segura entre servidores DNS, obedecendo no mínimo os padrões: HMAC MD5, HMAC SHA-1 ou HMAC SHA 256;





1.1.21.246. A solução deve realizar o offload dos servidores de DNS, funcionando como o DNS secundário;

1.1.21.247. A solução deve servir as respostas as requisições onde o DNS é o autoritativo a partir da memória RAM;

1.1.21.248. A solução deve possuir proteções contra ataques DNS, no mínimo:

1.1.21.249. Inspeção de protocolo;

1.1.21.250. Validação de protocolo;

1.1.21.251. UDP flood;

1.1.21.252. Pacotes malformados;

1.1.21.253. Ataque teardrop;

1.1.21.254. Ataque ICMP;

1.1.21.255. Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar a distribuição dinâmica de tráfego e aumentar a proteção contra ataques;

1.1.21.256. A solução deve ser capaz de realizar balanceamento dos servidores DNS;

1.1.21.257. A solução deve ser capaz de realizar filtragem de pacotes;

1.1.21.258. A solução deve prover segurança do protocolo DNS, protegendo contra ataques de negação de serviço, NXDOMAIN e reflexão de DNS.

1.1.21.259. A solução deve prover segurança do protocolo DNS, protegendo contra ataques de Cache Poisoning.

1.1.21.260. A solução deve realizar stateful inspection;

1.1.21.261. A solução deve possuir base de Geolocalização IP;

1.1.21.262. A solução deve implementar DNS64;

1.1.21.263. A solução deve suportar pelo menos os seguintes tipos de requisição DNS: SOA, A, AAAA, CNAME, DNAME, HINFO, MX, NS, PTR, SRV, TXT

1.1.21.264. Deve ser capaz de gerar estatísticas sobre consultas de DNS por: Aplicação, nome da query, tipo da query, endereço IP do cliente;

1.1.21.265. Deve ser possível configurar a solução de modo inline a estrutura de DNS existente e transparente sem requerer grandes mudanças na infraestrutura;

1.1.21.266. Deve prover as respostas a queries DNS da própria RAM CACHE;





- 1.1.21.267. A solução deve ser capaz de realizar IP Anycast;
- 1.1.21.268. A solução deve ser capaz de realizar DNSSec, independente da estrutura dos servidores DNS em uso;
- 1.1.21.269. A solução de alta disponibilidade não deve depender de BGP ou outro protocolo de roteamento;
- 1.1.21.270. A solução de alta disponibilidade será realizada baseada em respostas a requisições DNS. A resposta a requisições DNS devem conter apenas endereços que estejam disponíveis no momento, e balanceadas por usuário, de acordo com as políticas definidas;
- 1.1.21.271. A solução deverá aceitar resolução de nomes baseada em topologia, onde requisições de DNS são respondidas baseado no país, continente, ou endereço IP de onde veio a requisição;
- 1.1.21.272. Deve ser possível ajustar quantos endereços são enviados em uma única resposta;
- 1.1.21.273. Suporte a monitoração de estado de saúde de servidores, serviços e links de conexão a provedor de serviço, garantindo a disponibilidade do serviço oferecido entre datacenters;
- 1.1.21.274. Deve possuir suporte a monitoração de pelo menos 15 diferentes aplicações, incluindo SAP, Oracle, MySQL e LDAP.
- 1.1.21.275. Suportar pelo menos os seguintes algoritmos de balanceamento global: 1.1.21.276. Round Robin;
- 1.1.21.277. Global Availability;
- 1.1.21.278. Ratio;
- 1.1.21.279. LDNS Persist;
- 1.1.21.280. Geografia;
- 1.1.21.281. Disponibilidade da Aplicação;
- 1.1.21.282. Capacidade do Virtual Server;
- 1.1.21.283. Least Connections;
- 1.1.21.284. Pacotes por segundo;
- 1.1.21.285. Round trip time;
- 1.1.21.286. Hops;
- 1.1.21.287. Packet Completion Rate;
- 1.1.21.288. QoS definido pelo usuário;





- 1.1.21.289. Kilobytes per Second;
- 1.1.21.290. Implementar persistência da conexão do usuário entre aplicações ou data centers;
- 1.1.21.291. A solução deverá suportar o controle de grupos de aplicações, e permitir que um usuário seja redirecionado para outro datacenter quando houver falha em qualquer das aplicações de um mesmo grupo;
- 1.1.21.292. A solução deverá permitir que as políticas sejam configuradas individualmente por aplicação sendo balanceada;
- 1.1.21.293. A solução deverá permitir que a contingência seja automática, mas que o retorno seja manual;
- 1.1.21.294. A solução deve ser capaz de lidar com clientes IPv6 quando o site atende apenas com IPv4 (requests AAAA ou A6);
- 1.1.21.295. Possuir suporte a IPv6 no balanceamento global entre datacenters.
- 1.1.21.296. Ter capacidade de tratar informações das camadas L4-L7 (FTP, SMTP, URL, HTTP Header, TCP e UDP) para a tomada de decisão de encaminhamento a servidor real, em IPv4 e IPv6.
- 1.1.21.297. Deverá possuir a funcionalidade de resposta rápida a queries DNS, permitindo respostas mais rápidas para zonas que seja autoritativo.
- 1.1.21.298. A solução deve possuir suporte a Response Policy Zones (RPZ), mecanismo de firewall usado por DNS recursivo para permitir o tratamento customizado da resolução de nomes. Portanto a solução deve ser capaz de filtrar queries DNS para domínios considerados maliciosos e retornar respostas customizadas.
- 1.1.21.299. A solução deve possuir linguagem de programação open-source que permita a manipulação do tráfego de entrada e saída, viabilizando assim a alteração de parâmetros no cabeçalho e no corpo das mensagens.
- 1.1.21.300. Essa linguagem de programação deve permitir a importação de pacotes, garantindo assim que a agilidade e flexibilidade no compartilhamento dos scripts.
- 1.1.21.301. Deve estender a funcionalidade de programabilidade com Node.js, provendo um ambiente para rodar JavaScript independente de web browser.

**1.1.28. ITEM 28 – INSTALAÇÃO FIREWALL DE APLICAÇÃO WEB – WAF –**





## DATACENTER

- 1.1.28.1. Instalação e Configuração de Firewall de Aplicação Web – Datacenter dos itens 20 e 21;
- 1.1.28.2. A instalação deve ser feita conforme item 6 deste TR.

### **1.1.34. ITEM 34 – SERVIÇO DE MONITORAMENTO E SUPORTE TÉCNICO 24X7 DE FIREWALL DE APLICAÇÃO WEB – DATACENTER – 36 MESES**

- 1.1.34.1. Monitoramento e Suporte Técnico 24X7 de Firewall de Aplicação Web dos itens 20 e 21;
- 1.1.34.2. O serviço deve ser prestado conforme item 6.3 deste TR.

### **1.1.35. ITEM 35 - SERVIÇO DE SOC SECURITY OPERATIONS CENTER -24X7 COM SIEM PACO TES DE 200 EPS -36 MESES**

#### **1.1.35.1. SERVIÇO DE MONITORAÇÃO E NOTIFICAÇÃO DE INCIDENTES DE SEGURANÇA**

1.1.35.1.1. Os recursos destinados à plena utilização e atendimento aos serviços requeridos pela CONTRATANTE deverão ser e estar hospedados em infraestrutura de DATACENTER que possua certificação Uptime Tier III ou compatível, a ser disponibilizada exclusivamente pela LICITANTE vencedora e por conseguida CONTRATADA. Todas as exigências mínimas contidas nos itens abaixo são indispensáveis e o não atendimento a qualquer um desses itens é motivo suficiente para a imediata desclassificação da LICITANTE.

1.1.35.1.2. O serviço deve contemplar dois ou mais Centros de Operações de Segurança (SOC), operando em regime 24x7x365 (vinte e quatro horas por dia, sete dias por semana, todos os dias do ano);

1.1.35.1.3. A CONTRATADA deve prover níveis de segurança elevados, utilizando no SOC ferramentas para garantir a segurança dos dados manipulados, contemplando, no mínimo, os seguintes controles de segurança física e lógica:

1.1.35.1.3.1. Solução de proteção de endpoints;

1.1.35.1.3.2. Controle de acesso físico ao SOC, com a utilização de pelo menos 02 (dois) mecanismos de autenticação, sendo, no mínimo, um deles por biometria;

1.1.35.1.3.3. Monitoramento por sistema interno de TV (CFTV), armazenando as imagens dos últimos 30 (trinta) dias;





1.1.35.1.3.4. Todos os funcionários da CONTRATADA envolvidos na operação ou que possuam acesso às informações do CONTRATANTE devem assinar termo de responsabilidade e sigilo;

1.1.35.1.4. A CONTRATADA deve disponibilizar toda a infraestrutura necessária para o monitoramento dos alertas de segurança realizado por seus analistas, em regime 24 X 7 (24 horas por dia, 7 dias da semana);

1.1.35.1.5. A CONTRATADA deve realizar as ações necessárias para identificação de incidentes de segurança por meio dos dados e alertas monitorados na Solução Integrada de SOC, que podem comprometer a segurança dos serviços e ativos do CONTRATANTE. A CONTRATADA deve analisar eventos detectados, classificar e categorizar conforme definição do CONTRATANTE. Identificar, registrar, escalar e notificar os incidentes de segurança ao CONTRATANTE para tratamento;

1.1.35.1.6. A CONTRATADA é responsável pelas atividades de camada 1 do SOC, que para o modelo definido corresponde minimamente às atividades relacionadas abaixo:

1.1.35.1.6.1. Definição de linha base (baseline) de forma a entender o comportamento normal do ambiente monitorado, ajustando métricas e limiares de detecção, com o objetivo de reduzir o número de falsos positivos e aumentar a precisão da detecção

1.1.35.1.6.2. Monitoração de alertas de segurança, onde o analista deve decidir se uma análise é necessária. A detecção consiste em avaliar os alertas de segurança dos sensores buscando indicadores de comportamentos maliciosos que ultrapassem os limiares estabelecidos no baseline. A lógica de detecção deve ser ajustada e desenvolvida, podendo passar a utilizar múltiplos eventos e diferentes fontes de dados. Os alertas devem indicar minimamente:

1.1.35.1.6.2.1. Ataques de força bruta com e sem sucesso;

1.1.35.1.6.2.2. Falhas de autenticação que indiquem suspeita de roubo de identidade;

1.1.35.1.6.2.3. Infecção de equipamentos por vírus;

1.1.35.1.6.2.4. Comprometimento de ativos da rede;

1.1.35.1.6.2.5. Realização de ações suspeitas por parte de usuários privilegiados;

1.1.35.1.6.2.6. Alertas de operação de serviços, como interrupções e falhas;

1.1.35.1.6.2.7. Ataques de negação de serviço;

1.1.35.1.6.2.8. Ataques comuns em aplicações WEB, como XSS e SQL injection; Atividades de botnets;





1.1.35.1.6.2.9. Exploração de vulnerabilidades;

1.1.35.1.7. Detecção por análise de logs, onde o analista realiza pesquisas, revisões e análises estatísticas no histórico de log armazenado na Solução Integrada de SOC, com o objetivo de identificar comportamentos e evidências que indiquem atividades maliciosas ou novas ameaças.

1.1.35.1.8. Análise de eventos, onde o analista deve pesquisar informações adicionais que podem estar relacionadas ao evento em análise, que forneçam algum valor investigativo para identificar comportamentos anômalos ou maliciosos. A análise realizada nessa etapa é preliminar, tendo o objetivo de confirmar a ocorrência de um evento de segurança, eliminando falsos positivos confirmados. O resultado da análise pode ser uma das seguintes categorias:

1.1.35.1.8.1. Evento confirmado: os sensores detectaram corretamente uma ameaça válida. Os incidentes confirmados devem ser escalados para a etapa de mitigação da gestão de incidentes;

1.1.35.1.8.2. Falso positivo: ocorre quando o sistema detecta incorretamente uma ameaça ou não existe risco no evento detectado, sendo eventos alertados como maliciosos, mas não são;

1.1.35.1.8.3. Eventos autorizados: são ameaças detectadas corretamente, mas que são aprovadas pela política de segurança, como por exemplo, a análise de vulnerabilidades;

1.1.35.1.8.4. Indeterminado: quando não existe evidência suficiente para confirmar o evento de segurança;

1.1.35.1.9. Registro de análise, todo evento detectado que for selecionado para análise, deve ser registrado no Sistema de Ticket ofertado, incluindo as atividades de investigação. O resultado da análise pode ser a definição de um falso positivo, encerrando o tíquete, ou a confirmação de um incidente de segurança, escalando o tíquete para tratamento. O tíquete deve conter as seguintes informações:

1.1.35.1.9.1. Identificador do ticket;

1.1.35.1.9.2. Sensor que detectou o evento;

1.1.35.1.9.3. Identificador do evento gerado no sensor;

1.1.35.1.9.4. Limiar de detecção utilizado para enviar o evento para análise;

1.1.35.1.9.5. Log do evento detectado;

1.1.35.1.9.6. Origem e categoria do ataque;

1.1.35.1.9.7. Data e hora;

1.1.35.1.10. Triagem e Categorização de eventos, os tíquetes registrados devem ser priorizados

 



por categorias, unificando os eventos potenciais de incidentes com as características em comum, que podem receber tratamento padronizado. Os eventos confirmados, classificados como incidente, devem ter seu tíquete escalado para os analistas do CONTRATANTE;

1.1.35.1.11. Elaboração de relatórios. A CONTRATADA deverá disponibilizar relatórios em formato pdf, referentes aos indicadores monitorados com periodicidade mínima mensal, ou sob demanda, podendo incluir:

1.1.35.1.11.1. Classificação dos eventos de segurança;

1.1.35.1.11.2. Total de eventos avaliados;

1.1.35.1.11.3. Total de eventos escalados;

1.1.35.1.11.4. TOP aplicações mais impactadas, TOP origens dos eventos de segurança;

1.1.35.1.11.5. TOP endereços de destino das ameaças;

1.1.35.1.11.6. TOP URLs e suas categorias;

1.1.35.1.11.7. TOP atacantes, vulnerabilidades, ameaças, alarmes, violações de auditoria;

1.1.35.1.11.8. Principais tipos de ataques;

1.1.35.1.11.9. Descrição dos casos de uso utilizados para avaliar os alertas de segurança;

1.1.35.1.11.10. Novas informações de inteligência configuradas na ferramenta: como as novas regras de monitoramento, dashboards, assinaturas instaladas, etc;

1.1.35.1.12. O Sistema de Ticket ofertado deverá ser utilizado para registrar e escalar eventos de segurança, de modo a permitir o registro, envio de notificações e alertas entre as equipes do CONTRATANTE e da própria CONTRATADA;

1.1.35.1.13. O CONTRATANTE é responsável por avaliar os incidentes escalados após o processo de triagem inicial. Caso o incidente seja confirmado, o CONTRATANTE executará os seus processos e procedimentos internos para executar as medidas de contenção e correção, incluindo configurações nos sensores de segurança ou outros ativos. O CONTRATANTE registrará as ações realizadas no tíquete correspondente ao incidente, permitindo que a CONTRATADA esteja ciente do fechamento do mesmo;

1.1.35.1.14. Os analistas do CONTRATANTE responsáveis pelos tíquetes escalados devem possuir acesso total as informações do incidente relacionado;

1.1.35.1.15. Os analistas do CONTRATANTE devem poder contatar os analistas da CONTRATADA, por telefone ou via Sistema de Ticket, para consulta de informações em caso de





qualquer dúvida sobre os eventos escalados e demais procedimentos para tratamento dos incidentes. As solicitações e respostas de informações adicionais sobre os incidentes, como logs e evidências, devem ser anexadas ao tíquete registrado na ferramenta;

1.1.35.1.16. O CONTRATANTE é responsável por fornecer informações de negócio adequadas, seguindo a regra do privilégio mínimo e necessidade de conhecer, para melhoria da atividade de monitoramento da CONTRATADA;

1.1.35.1.17. O CONTRATANTE pode solicitar, a qualquer momento, a customização dos indicadores e informações sobre incidentes e eventos apresentados nos relatórios. A CONTRATADA deve avaliar os requisitos técnicos necessários e operacionalizar. As solicitações devem ser registradas e realizadas por meio dos canais de suporte da CONTRATADA;

1.1.35.1.18. Por padrão, a CONTRATADA não deve possuir nenhum tipo de acesso aos ativos, sensores e ferramentas de proteção do CONTRATANTE. Em casos específicos e por tempo determinado, caso autorizado pela área de segurança do CONTRATANTE, pode ser fornecido acesso de leitura de registros do IPS, dados de sessão de rede (flow) e outras ferramentas de segurança para auxiliar em pesquisas pontuais de eventos de segurança. Não será fornecido nenhum tipo de acesso a dados ou sistemas do CONTRATANTE, além dos estritamente necessários para o serviço de monitoramento que serão armazenados na ferramenta de inteligência;

1.1.35.1.19. A CONTRATADA deve prover informação específica sobre ameaças, gerada através de um processo (com coleta, validação, correlação, avaliação e interpretação de conhecimento baseado em evidências), que colocam em perigo ativos de informação ou de tecnologia do CONTRATANTE. Tal inteligência pode ser usada para embasar decisões sobre a resposta a tal ameaça ou risco, permitindo melhorar as táticas de detecção de ataques e configuração dos sensores de segurança. O processo deve resultar ainda em conhecimento utilizado para criação de novos indicadores e auxiliar na detecção de ataques futuros, possibilitando a identificação de ameaças específicas ao ambiente do CONTRATANTE;

## **1.1.35.2. CARACTERÍSTICAS E REQUISITOS INDISPENSÁVEIS PARA OS SERVIÇOS E RECURSOS FORNECIDOS PELO SECURITY OPERATIONS CENTER (SOC):**

### **1.1.35.2.1. CORRELACIONAMENTO DE EVENTOS DE SEGURANÇA DA INFORMAÇÃO**





1.1.35.2.1.1. Todo o gerenciamento dos componentes e funções administrativas devem ser feitas através de uma única interface web, acessível por navegador, sem a necessidade de instalação de aplicação adicionais;

1.1.35.2.1.2. A solução deverá ser fornecida para instalação e uso no idioma Português Brasil e Inglês;

1.1.35.2.1.3. A solução deverá ter o pleno funcionamento independentemente de conexão (física ou lógica) com o fabricante;

1.1.35.2.1.4. A solução deve sincronizar o horário de seus componentes utilizando o serviço NTP;

1.1.35.2.1.5. A solução deve ser gerenciada centralmente (configurações, controle e atualizações), através de interface web única, sem necessidades de intervenção nos equipamentos onde está instalado;

1.1.35.2.1.6. A solução deve ser licenciada com a capacidade de coletar, processar e correlacionar 200 (duzentos) eventos por segundo de forma sustentada. Deve-se considerar os eventos com tamanho médio de 700 bytes;

1.1.35.2.1.7. A solução deve permitir a recepção de eventos que excedam temporariamente os limites contratados, processando o volume excedente assim que volume for normalizado. Mantendo a operação com situações de picos temporários, sem incorrer na perda de eventos e sem incorrer em qualquer cobrança adicional por excesso ou bloqueio da solução;

1.1.35.2.1.8. A comunicação entre os componentes da solução deverá ser feita de forma criptografada, garantindo a autenticidade, confidencialidade e integridade dos dados;

1.1.35.2.1.9. Para o acesso à interface web de administração, deve permitir o uso de certificado digital emitido por autoridade certificada interna da organização ou por autoridade certificadora reconhecida pelos navegadores;

1.1.35.2.1.10. Ter suporte a monitoração por SNMPv2c e SNMPv3;

1.1.35.2.1.11. A administração da solução deve usar uma única conta para cada usuário administrador (mesma conta, mesma senha), independente da funcionalidade gerenciada;

1.1.35.2.1.12. A coleta, normalização e o correlacionamento dos eventos provenientes dos dispositivos monitorados devem ser realizadas próximos ao tempo real;

1.1.35.2.1.13. Os eventos devem ser normalizados e categorizados em um padrão único que será usado pela solução;





1.1.35.2.1.14. Deve permitir a definição de metadados customizados/personalizados, para extrair dados existentes na linha de log (raw), usando recursos como expressões regulares ou algum recurso gráfico para essa extração;

1.1.35.2.1.15. Propriedades customizadas devem poder ser usadas em regras de correlação online e em regras de correlação histórica;

1.1.35.2.1.16. Permitir a agregação de eventos semelhantes;

1.1.35.2.1.17. Deve atribuir métrica de prioridade para os eventos e para os alertas/incidentes;

1.1.35.2.1.18. Gerar alertas/incidentes com base nas regras definidas previamente;

1.1.35.2.1.19. Verificar conformidade com as políticas, controles e normas internas (customizadas) e regulamentações externas (ex. ISO 27001);

1.1.35.2.1.20. Deve permitir armazenar os eventos, inclusive os normalizados, de forma compactada;

1.1.35.2.1.21. Apresentar painéis gráficos (dashboards) com indicativos de situações relacionados à segurança, compliance, aplicações e monitoração do próprio sistema;

1.1.35.2.1.22. Os painéis gráficos (dashboards) devem ser customizáveis, por usuário;

1.1.35.2.1.23. Permitir a análise de eventos baseados em contexto, tais como, usuários, localização geográfica, bem como qualquer outro metadado contido no evento;

1.1.35.2.1.24. Enviar notificações relacionadas a um incidente/alerta por e-mail, trap snmp e syslog;

1.1.35.2.1.25. A solução deverá ter, no mínimo, as seguintes formas de coleta de eventos: Syslog (UDP, TCP), Syslog criptografado com TLS, JDBC, SNMP (v1, v2 e v3), Microsoft Event Log, MQ Series client, Arquivos de Log em formato de texto, Kafka, AWS Cloudwatch, Checkpoint OPSEC/LEA, CISCO NSEL e Juniper NSM Protocol;

1.1.35.2.1.26. Deve permitir a configuração de ofuscação de qualquer parte dos dados recebidos, assim que normalizados;

1.1.35.2.1.27. A ofuscação de dados deve ser configurada com chaves de criptografia;

1.1.35.2.1.28. Possuir a capacidade de automatizar a resposta a incidentes, através da execução de scripts, como ação customizada dentro das regras de correlação;

1.1.35.2.1.29. Tratar eventos em formato "comprimido" (zip, gz, tar.gz), sem a necessidade da





descompressão manual;

1.1.35.2.1.30. Deverá fazer a agregação de eventos, mostrando a contagem de eventos, quando o mesmo evento ocorrer dentro de um período curto. A opção de realizar ou não a agregação de eventos deve ser configurável, por dispositivo integrado;

1.1.35.2.1.31. Deve manter o evento bruto ("raw") e seus metadados para o armazenamento e consulta futura;

1.1.35.2.1.32. Deve ser capaz de agregar informações sobre localização geográfica dos endereços IP envolvidos no evento, para que a mesma seja usada no correlacionamento;

1.1.35.2.1.33. A solução deve suportar, nativamente, pelo menos as seguintes fontes de logs: Windows, Linux, IBM/AIX, IBM/RACF, HP/UX, Solaris, Oracle Database, IBM/DB2, MS SQL Server, Firewalls (Checkpoint, Cisco/ASA, Juniper, Fortinet e Palo Alto e SonicWall), Network IPS (Sourcefire, IBM/ISS, HP Tipping Point, Snort e McAfee);

1.1.35.2.1.34. A solução deve suportar "overlap de IP", isto é, rotular os eventos para que seja possível gerenciar eventos de fontes de log que estejam em redes diferentes, mas possuem o mesmo endereçamento IP;

1.1.35.2.1.35. Deve exibir perfil visual do tráfego em tempo real, e normalizada de forma agregada. Deve incluir informações de bytes, pacotes e protocolos;

1.1.35.2.1.36. Usar mecanismo de correlação para a detecção de ataques de negação de serviço (DoS) e de negação de serviço distribuído (DDoS) a partir dos flows de rede;

1.1.35.2.1.37. Deve possuir mecanismo para não sofrer as consequências da monitoração de flows de rede em uma situação de DDoS;

1.1.35.2.1.38. Deve suportar o recebimento dos seguintes protocolos de flow: Netflow (versão 5 e 9), IPFIX, J Flow, sFlow (versões 2, 4 e 5) e Packeteer;

1.1.35.2.1.39. Monitorar a rede e identificar padrão de tráfego que possa ser uma ameaça, bem como detectar tráfego de rede de aplicativos como compartilhamento de arquivos, P2P e jogos;

1.1.35.2.1.40. Deve ser capaz de apresentar informações de fluxo de rede por período de tempo pré-definido;

1.1.35.2.1.41. Deve ser capaz de montar visualizações de fluxo de rede baseados em comunicações provenientes ou destinadas à internet agrupado por regiões geográficas;





1.1.35.2.1.42. Deve correlacionar logs e flows em conjunto, gerando incidentes de segurança;

1.1.35.2.1.43. Deve possuir regras de correlação específicas para regulações/conformidades, com suporte no mínimo a: ISO 27001 e GDPR/LGPD;

1.1.35.2.1.44. Deve possuir repositório do fabricante da solução que ofereça novas regras de correlação especializada em segurança para atualização e ampliação da capacidade de detecção de incidentes, sem custo adicional;

1.1.35.2.1.45. Deve permitir a criação de regras que identifiquem mudanças de comportamento, como surto ou ausência de eventos/tráfego, quando comparados a outros períodos similares (ex. mesmo período do dia, mesmo dia da semana);

1.1.35.2.1.46. Capacidade de fazer o correlacionamento entre eventos e fluxos de rede, NetFlow, J-Flow, S-Flow e IPFIX, sem a necessidade de ferramentas de terceiros ou qualquer componente adicional ao licenciamento da solução;

1.1.35.2.1.47. Possuir pelo menos os seguintes tipos de correlação:

1.1.35.2.1.44.1. Correlação por regras;

1.1.35.2.1.44.2. Extrapolação de um limite (threshold);

1.1.35.2.1.44.3. Correlação por anomalia e padrão de comportamento;

1.1.35.2.1.48. Como resultado das regras, deve ser capaz de executar ações automáticas, no mínimo: enviar e-mail, enviar mensagem para o usuário conectado no console, criar um incidente no sistema de workflow interno, enviar traps SNMP e popular lista (watch list);

1.1.35.2.1.49. Disponibilizar pelo menos uma base de inteligência em ameaças com informações de riscos globais, com updates diários, integrada às regras de correlação para detecção de incidentes;

1.1.35.2.1.50. Qualquer metadado dos eventos pode ser usado em uma regra de correlação;

1.1.35.2.1.51. A correlação histórica deve permitir a escolha do período a ser analisado, atendendo no mínimo a correlação compreendo a análise de 1 dia, 7 dias e 30 dias;

1.1.35.2.1.52. Mecanismo para ajuste fino de regras de correlação, exibindo de forma gráfica as regras de correlação que são mais acionadas por eventos (que geram mais alertas) e seus elementos relacionados. Facilitando o refinamento da solução com vistas à redução de falso positivo e melhoria da performance;

1.1.35.2.1.53. Identificação de ações que comprometam dados cobertos pelas regulações LGPD



(Lei Geral de Proteção a Dados) ou GDPR (General Data Protection Regulation);

1.1.35.2.1.54. Comunicação dos equipamentos internos com sites conhecidos por serem controladores de botnet;

1.1.35.2.1.55. Deve permitir o uso de algoritmo para garantia de integridade dos eventos armazenados, utilizando no mínimo os algoritmos: MD2, MOS, SHA-256, SHA-384 e SHA-512;

1.1.35.2.1.56. Deve permitir o uso dos algoritmos para garantia de integridade, do item anterior, com código de autenticação da mensagem (HMAC);

1.1.35.2.1.57. Permitir a remoção de dados das listas (watchlist) de forma manual, automática através de regras de correlação, por API ReST e pela expiração do tempo de vida da informação;

1.1.35.2.1.58. A solução deve implementar auto monitoração, para detectar comandos que possam modificar arquivos de logs, tentativas de logins por força bruta, edição e remoção de arquivos sensíveis ou críticos da solução e o uso de contas compartilhadas de administradores da solução;

1.1.35.2.1.59. Possuir capacidade de integração com bases Microsoft Active Directory, LDAP, TACACS e RADIUS para autenticação de usuários;

1.1.35.2.1.60. Deve permitir a integração com Single Sign-On que suporte o protocolo SAML 2.0;

1.1.35.2.1.61. Permitir pesquisa nos eventos históricos, a partir de metadados, fornecendo capacidade de "drill down", ou seja, o refinamento da pesquisa a partir da seleção de elementos no resultado, para efetuar nova pesquisa;

1.1.35.2.1.62. Capacidade de criação de novos painéis gráficos (dashboards) e alteração dos existentes;

1.1.35.2.1.63. Permitir a criação de novos modelos de relatórios e alteração dos relatórios nativos da solução sem a necessidade de uso de linguagens de programação, através da interface web;

1.1.35.2.1.64. Permitir agendar a geração de relatórios de forma periódica e notificar/enviar automaticamente os relatórios gerados para os destinatários dos mesmos;

1.1.35.2.1.65. Deve possuir templates de relatórios para as principais normas de conformidade. Sendo exigido, no mínimo, o atendimento a ISO/27001;

1.1.35.2.1.66. Permitir a manipulação dos incidentes identificados pela solução usando a API ReST, permitindo adicionar anotações, identificar os detalhes do incidente e encerrar o incidente usando esse acesso;



1.1.35.2.1.67. Deve permitir a geração de relatórios, contendo múltiplas informações num mesmo relatório, como dados de segurança e rede;

1.1.35.2.1.68. Deve permitir a criação de relatórios relacionados a: incidentes, logs, flows de rede, vulnerabilidades;

1.1.35.2.1.69. Deve gerar relatórios de eventos, alertas/incidentes em nível técnico e gerencial os quais devem ter a possibilidade de serem gerados em PDF, HTML, XLS;

1.1.35.2.1.70. Deve possuir módulo capaz de extrair os dados de usuário e ações executadas dos eventos coletados para geração de score de risco;

1.1.35.2.1.71. Deve ser capaz de importar dados de usuário em bases LDAP, CSV e Windows AD para identificação da pessoa associada a conta do sistema monitorado, deve ser capaz de coletar e associar no mínimo: nome completo, departamento, contas associadas, e-mail e cargo.

## ANEXO II - PLATAFORMA DE MONITORAMENTO

1. A Plataforma de Monitoramento deverá permitir a monitoração dos firewalls, a partir de um servidor central, possibilitando a geração de notificações específicas para cada equipe, através de acesso WEB à aplicação de gerenciamento com as seguintes características:

2. A interface de gerenciamento deverá ser em modo WEB acessada através de navegador.

3. Deverá ser compatível com, pelo menos, um dos seguintes navegadores: Google Chrome, Mozilla Firefox ou Internet Explorer.

4. Permitir que as informações gerenciadas, coletadas em diversos pontos de captura, sejam consolidadas em uma única visão em um console gráfico central.

5. Possuir a capacidade de reiniciar serviços de monitoração automaticamente após a ocorrência de "queda" e alertar em sequência o retorno do equipamento que está sendo gerenciado.

6. Deverá ter capacidade de monitoração dos equipamentos ofertados neste edital em, pelo menos, os seguintes itens:

6.1. Modelo do equipamento;

6.2. Utilização de CPU;

6.3. Uso de memória RAM;



*[Handwritten signature]*



- 6.4. Espaço livre em disco;
- 6.5. Versão do sistema operacional;
- 6.6. Status ou data de expiração do licenciamento;
- 6.7. Temperatura de operação do equipamento;
- 6.8. Status da (s) fonte (s) de alimentação;
- 6.9. Número de conexões ou sessões concorrentes;
- 6.10. Lista de interfaces de rede, contemplando, também:
  - 6.10.1. Status das interfaces;
  - 6.10.2. Throughput das interfaces;
  - 6.10.3. Status da funcionalidade de alta disponibilidade;
7. Gatilhos e alertas:
  - 7.1. A plataforma deve permitir a construção para a detecção de eventos (gatilhos) de acordo com a necessidade de gerenciamento dos sistemas, gerando os alertas necessários. Como exemplo, ela deve permitir a criação de gatilhos quando limites forem excedidos. Os alertas devem ser configuráveis para criação de SLAs. Os alertas devem ser visualizados também pela interface gráfica.
  - 7.2. O envio de E-mail e SMS devem ser configurados por tipo de alerta em cada recurso monitorado, permitindo, por exemplo, que em diferentes interfaces de um mesmo equipamento existam gatilhos e formas de envios diferentes.
  - 7.3. Prover o envio de alarmes para a console de gerenciamento de aplicações e E-mails e SMS para os Administradores quando os recursos monitorados atingirem os seus respectivos gatilhos.
  - 7.4. Para o mesmo item podem ser gerados vários gatilhos com criticidade diferentes, permitindo assim, um melhor controle do tipo de problema. monitorados;
9. Deve suportar o monitoramento através do protocolo SNMP nas versões 1, 2c e 3 e SNMP Traps;
10. Análise, relatórios e comparação:
  - 10.1. Armazenar informações para posterior análise, que possa permitir comparações para acertos nos equipamentos.
  - 10.2. A solução deverá possuir uma interface interna para geração de relatórios.
  - 10.3. A solução deve possuir interface WEB para geração e visualização de relatórios.
  - 10.4. A interface WEB deve possibilitar o envio de relatórios por E-mail manualmente ou mesmo pré



agendar a geração e o envio em uma data ou horários especificados.

10.5. A solução deve possibilitar a exportação dos relatórios em pelo menos dois dos seguintes formatos:

10.5.1. PDF.

10.5.2. HTML.

10.5.3. csv.

10.6. Todos os relatórios devem ter a flexibilidade de exibir informações em tempo real e também dados históricos, coletados em períodos anteriores.

10.7. A solução deve permitir a publicação automática de relatórios no formato HTML em um servidor WEB, permitindo uma análise sobre a situação dos servidores monitorados, com as seguintes características:

10.7.1. Apresentação dos nomes dos equipamentos no relatório.

10.7.2. Apresentação das informações gerenciadas por equipamento.

10.7.3. Exibição por grupo de equipamentos previamente estabelecidos.

10.8. Opções de periodicidade especificada pelo usuário: diária, semanal, mensal, trimestral, anual ou intervalo de data.

11. Apresentação em modo gráfico:

11.1. Dependência entre objetos monitorados: permitir que sejam cadastradas dependências entre os objetos monitorados, inclusive no nível de subitem de monitoramento, permitindo analisar o impacto de uma parada perante os demais objetos monitorados;