COMISSÃO PERMANENTE DE LICITAÇÃO CPL_TCE

Equipe de Pregão

EDITAL

Processo Eletrônico nº 5705/2020 – TCE/AP

MODALIDADE: PREGÃO Nº 01/2021 – Forma Eletrônica **PARA REGISTRO DE PREÇO**
OBJETO: Contratação de empresa especializada para o fornecimento de Solução integrada de segurança, composta por um cluster de Gerenciamento Unificado de Ameaças (Firewall UTM) e seu Gerenciamento de Logs e Relatórios de Segurança; Solução em Firewall de Aplicações WEB (WAF - Web Application Firewall); Solução de software para gerenciamento de logs e eventos de segurança (SIEM - Security Information and Event Management), além de suporte técnico e serviços especializados.

DADOS GERAIS DA DISPUTA

LOCAL: Portal de Compras do Governo Federal - endereço eletrônico: www.gov.br/compras - (Sala virtual);

UASG: 927045

Apresentação de propostas: até DIA: 16/03/2021 - 8:59h;

Abertura da Sessão: 16/03/2021 - 9h;

Critério de disputa: Disputa aberto/fechado

Todas as referências de tempo no Edital, no aviso e durante a sessão pública seguirão o horário de Brasília–DF

Critério de Julgamento: MENOR PREÇO POR LOTE.

Impugnações e Esclarecimentos: até dia 10/03/2021, pelo e-mail cpl@tce.ap.gov.br.

1. PREÂMBULO

A Presidência do Tribunal de Contas do Estado do Amapá, **por intermédio** do (a) **Pregoeiro(a),** designado pela Portaria n.º 301/2020–PRESI/TCE/AP, de 24 de Julho de 2020, leva ao conhecimento dos interessados que, na forma da **Lei n° 10.520, de 17 de julho de 2002**, realizará licitação, na modalidade **Pregão – na forma eletrônica**, do tipo **menor preço POR LOTE**, constante do objeto, mediante as condições estabelecidas neste **edital** e seus **anexos.**

2. DA LEGISLAÇÃO

2.1. O **Edital** da presente licitação pública reger-se-á, principalmente, pelos comandos legais seguintes:

2.1.1. **Lei nº 10.520, de 17 de julho de 2002**;

2.1.2. Decreto Federal nº 10.024/2019 - Regulamento do Pregão Eletrônico;

2.1.3. Decreto Estadual 3.182/2016 – Regulamento do Registro de Preço;

2.1.4. Lei Complementar Federal 123/06(ME/EPP);

2.1.5. Lei Complementar Estadual 108/2018(ME/EPP/MEI);

2.1.6. Com aplicação subsidiária da Lei nº 8.666, de 21.06.1993, e alterações posteriores;

2.1.7. Demais exigências deste edital e seus anexos.

3. DO OBJETO

3.1. A presente licitação tem como objeto a **contratação, por registro de preços, de empresa especializada para o fornecimento de Solução integrada de segurança, composta por um cluster de Gerenciamento Unificado de Ameaças (Firewall UTM) e seu Gerenciamento de Logs e Relatórios de Segurança; Solução em Firewall de Aplicações WEB (WAF - Web Application Firewall); Solução de software para gerenciamento de logs e eventos de segurança (SIEM - Security Information and Event Management), além de suporte técnico e serviços especializados,** conforme especificações e quantitativos constantes do Anexo I deste edital.

3.2. Em caso de discordância existente entre as especificações deste objeto descritas no Comprasnet e as especificações constantes deste Edital, prevalecerão as últimas.

3.3. Critério de julgamento se dará pelo MENOR PREÇO POR LOTE.

3.4. O valor estimado (caráter sigiloso).

4. DA PARTICIPAÇÃO NA LICITAÇÃO

4.1 Poderão participar deste Pregão quaisquer licitantes que:

4.1.1. Estiverem previamente credenciados no Sistema de Cadastramento Unificado de Fornecedores – Sicaf e no sítio www.gov.br/compras**;**

4.1.2. Para ter acesso ao sistema eletrônico, os interessados em participar deste Pregão deverão dispor de chave de identificação e senha pessoal.

4.1.3. O uso da senha de acesso pela **licitante** é de sua responsabilidade exclusiva, incluindo qualquer transação por ela efetuada diretamente, ou por seu representante, não cabendo ao provedor do sistema ou ao TCE-AP responsabilidade por eventuais danos decorrentes do uso indevido da senha, ainda que por terceiros comprovem possuir os documentos de habilitação exigidos neste Edital.

4.2. Não poderão concorrer neste Pregão:

4.2.1. Consórcios de empresas, qualquer que seja sua forma de constituição;

4.2.2. Empresas que estejam declaradas inidôneas para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos da punição;

4.2.3. Empresas que estejam impedidas de contratar com o Estado do Amapá e o TCE/AP;

4.2.4. Empresas que estejam sob falência, em recuperação judicial ou extrajudicial, concurso de credores, concordata ou insolvência, em processo de dissolução ou liquidação.

4.2.5. Pessoas alcançadas pelo art. 9º, da Lei 8.666/93.

4.2.6. Empresário cujo estatuto ou contrato social não seja pertinente e compatível com o objeto deste Pregão;

5. DA PROPOSTA E DA HABILITAÇÃO

5.1. A licitante deverá encaminhar proposta, **concomitantemente** com os documentos de habilitação exigidos neste Edital, exclusivamente por meio do sistema eletrônico, EM CAMPO PRÓPRIO, **até** a data e horário marcados para abertura da sessão pública, quando então encerrar-se-á automaticamente a fase de recebimento de propostas e dos documentos de habilitação.

5.2. A licitante deverá consignar, na forma expressa no sistema eletrônico, o **valor GLOBAL da proposta**, para cada lote, constando os valores unitários, já considerados e inclusos todos os tributos, fretes, tarifas e demais despesas decorrentes da execução do objeto, incluindo o prazo de validade de 60 dias – contados a partir da data de abertura da sessão.

5.3. A licitante deverá declarar, em campo próprio do sistema eletrônico, que cumpre plenamente os requisitos de habilitação e que sua proposta está em conformidade com as exigências do Edital.

5.4. A licitante deverá declarar, em campo próprio do Sistema, sob pena de inabilitação, que não emprega menores de dezoito anos em trabalho noturno, perigoso ou insalubre, nem menores de dezesseis anos em qualquer trabalho, salvo na condição de aprendiz, a partir dos quatorze anos.

5.5. A licitante enquadrada como microempresa ou empresa de pequeno porte deverá declarar, em campo próprio do Sistema, que atende aos requisitos do art. 3º da LC nº 123/2006, para fazer jus aos benefícios previstos.

5.6. A **declaração falsa** relativa ao cumprimento dos requisitos de habilitação, à conformidade da proposta ou ao enquadramento como microempresa ou empresa de pequeno porte sujeitará a licitante às sanções previstas neste Edital.

5.7. As propostas ficarão disponíveis no sistema eletrônico:

5.7.1. Qualquer elemento que possa identificar a licitante importa desclassificação da proposta, sem prejuízo das sanções previstas nesse Edital.

5.7.2. Até a abertura da sessão pública, a licitante poderá retirar ou substituir a proposta e os documentos de habilitação anteriormente encaminhados.

5.7.3. O(A) pregoeiro(a) avaliará a conformidade das propostas e após informará, **via chat**, aos licitantes o início da oferta de lances.

5.8. A proposta deverá cumprir os requisitos estabelecidos no Termo de Referência (Anexo I), sob pena de desclassificação:

5.9. Após a análise das propostas, serão desclassificadas, com base no **artigo 48, incisos I e II da Lei n.º 8.666/93,** as propostas que:

5.9.1. Apresentarem preços excessivos ou com valor global superior ao limite estabelecido ou com preços manifestamente inexequíveis, assim considerados aqueles que não venham a ter demonstrada sua viabilidade através de documentação que comprove que os custos dos insumos são coerentes com os de mercado e que os coeficientes de produtividade são compatíveis com a execução do objeto;

5.9.2. Não atenderem às exigências contidas neste Pregão.

5.9.3. A desclassificação da proposta será fundamentada e registrada no sistema, acompanhado em tempo real por todos os participantes, conforme o parágrafo único do art. 28 do Decreto nº 10.024/2019.

6. DA ABERTURA DA SESSÃO PÚBLICA

6.1. A abertura da sessão pública deste Pregão, conduzida pelo(a) Pregoeiro(a), ocorrerá na data e na hora indicadas nos dados gerais deste Edital, no sítio www.gov.br/compras.

6.2. Durante a sessão pública, a comunicação entre o Pregoeiro e as licitantes ocorrerá exclusivamente via *chat*, em campo próprio do Sistema eletrônico.

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

7. DA CONFORMIDADE E CLASSIFICAÇÃO DAS PROPOSTAS

7.1. O(A) Pregoeiro(a) verificará a conformidade das propostas apresentadas e desclassificará, motivadamente, aquelas que não estejam atendendo os requisitos mínimos estabelecidos neste Edital.

7.2. O sistema ordenará automaticamente as propostas classificadas pelo(a) pregoeiro(a).

7.3. Somente as licitantes com propostas classificadas participarão da fase de lances.

7.4. Terminada a classificação das propostas o (a) Pregoeiro (a) informará aos licitantes, via chat, o início da fase competitiva.

8. DA FORMULAÇÃO DE LANCES

8.1. Aberta o **início da fase competitiva** os licitantes encaminharão os lances exclusivamente por meio do sistema eletrônico

8.1.1. Os licitantes serão imediatamente informados do recebimento do lance e do valor consignado no registro, mantendo-se em **sigilo** a identificação da ofertante.

8.2. O licitante poderá oferecer lances sucessivos e somente quando o valor for inferior ou maior for o percentual de desconto ao último lance por ele ofertado e registrado pelo sistema.

8.3. As licitantes serão informadas, em tempo real, do valor do menor lance registrado.

8.4. Não serão aceitos dois ou mais lances iguais e prevalecerá aquele que for recebido e registrado primeiro.

8.5. Os lances apresentados e levados em consideração para efeito de julgamento serão de exclusiva e total responsabilidade da licitante, não lhe cabendo o direito de pleitear qualquer alteração.

8.6. Durante a fase de lances, o(a) Pregoeiro(a) poderá excluir, justificadamente, lance cujo valor seja manifestamente inexequível. Caso o licitante entenda como correto poderá apresentar novamente o mesmo lance;

8.7. Se ocorrer a desconexão do Pregoeiro no decorrer da etapa de lances, e o sistema eletrônico permanecer acessível às licitantes, os lances continuarão sendo recebidos, sem prejuízo dos atos realizados.

8.8. No caso de a desconexão do Pregoeiro persistir por tempo superior a 10 (dez) minutos, a sessão pública do Pregão será suspensa e reiniciada somente decorridas 24 (vinte e quatro) horas após a comunicação expressa do fato aos participantes no sítio www.gov.br/compras.

9. DO MODO DE DISPUTA

9.1. Neste Pregão o modo de disputa adotado é o **aberto/fechado**, assim definido no art. 33º do Decreto n.º 10.024/2019.

9.1.2 Na etapa posterior à disputa de lances abertos será iniciada uma fase para lance único fechado, com a participação das propostas até o limite de 10% da menor ou quando não houver no mínimo três, o sistema classificará até o limite de três para participarem da fase competitiva fechada.

10. DO DIREITO DE PREFERÊNCIA DA ME/EPP E DOS CRITÉRIOS DE DESEMPATE

10.1. Terminada todos os lances, havendo proposta de Microempresa (ME) ou Empresa de Pequeno Porte (EPP) que seja igual ou até 5% (cinco por cento) superior a proposta mais bem classificada, esta empresa poderá no prazo **de 5 minutos** apresentar uma última oferta, obrigatoriamente inferior à proposta do primeiro colocado; nos termos do art. 44 e 45 da Lei Complementar nº 123/2006.

10.2. Caso a licitante que se enquadre no direito de preferência melhor classificada **opte por não ofertar lance inferior** o sistema, de maneira automática, **convocará as ME/EPP remanescentes**, na ordem classificatória, para o exercício do direito de desempate.

10.3. Não havendo proposta, decaíra - neste momento – o direito previsto na Lei Complementar nº 123/2006, art. 44 e 45.

11. DA NEGOCIAÇÃO

11.1. Encerrada a etapa de lances, o (a) Pregoeiro (a) deverá encaminhar, pelo sistema eletrônico, contraproposta à licitante que tenha apresentado o melhor preço, sendo que esta negociação poderá ser acompanhada pelos demais licitantes.

11.1.1. É vedado qualquer negociação que não se submeta a este item.

11.2. A licitante melhor classificada encaminhará a proposta readequada, atendendo o último lance ofertado após a negociação, em arquivo único, via sistema COMPRASNET, até **2 horas** após sua convocação, via sistema.

11.2.1. A proposta readequada deverá obedecer ao Modelo de Proposta constante na proposta original e de acordo com o Termo de Referência.

11.2.2. Este procedimento poderá repetir-se ao final da etapa da habilitação, também no prazo de 2 (duas) horas, conforme estabelecido no § 2º, do art. 43 deste mesmo decreto.

12. DO JULGAMENTO DA PROPOSTA

12.1. Findada a negociação, o (a) **Pregoeiro (a) examinará a proposta classificada em primeiro lugar** quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado ou estimativa de preço, para contratação.

12.1.1. O (A) pregoeiro (a) poderá convocar a equipe técnica da área fim, para orientar a sua decisão.

12.2. A proposta readequada, encaminhada via sistema pelo licitante não poderá conter:

12.2.1. Valor incompatível com os preços de mercado, exceto quando houver comprovação da viabilidade de execução para este valor.

12.2.2. Valor superior ao estimado ou inexequíveis.

12.2.3. Não corrigir ou justificar falhas apontadas pelo Pregoeiro no momento de sua convocação.

12.3. Se a proposta não for aceitável ou se a licitante não atender às exigências de habilitação, o Pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a seleção da proposta que melhor atenda a este Edital e verificará se os documentos de habilitação do licitante estão em conformidade com as disposições deste Edital.

12.4. A licitante que abandonar o certame e assim deixar de enviar a documentação exigida neste Edital será desclassificada e sujeitar-se-á as sanções previstas na lei e no edital deste instrumento convocatório.

12.5. O (A) Pregoeiro (a) constatando o atendimento a todas as exigências contidas declarará a **melhor oferta e segue para análise da habilitação**.

13. DAS AMOSTRAS

13.1. Não serão solicitadas amostras nesta licitação.

14. DA HABILITAÇÃO

14.1. Será verificado no primeiro momento da habilitação se o licitante declarado como melhor oferta cumpre as condições de participação do certame, para que então seja analisado os documentos habilitatórios;

14.2. Os documentos de habilitação serão verificados por meio do SICAF e o licitante também poderá optar por encaminhar a documentação via sistema, concomitantemente a proposta – conforme estabelecido no item 5.

14.3. A **licitante** interessada em participar deste **Pregão** deverá apresentar os seguintes Documentos:

14.3.1. **<u>Relativos à Habilitação Jurídica:</u>**

14.3.1.1. Registro comercial, no caso de empresa individual; **ou,**

14.3.1.2. Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, em se tratando de sociedades comerciais e, no caso de **sociedades por ações**, acompanhado de documentos de eleição de seus administradores, acompanhados de todas as alterações ou da consolidação respectiva; ou

14.3.1.3. Inscrição do ato constitutivo, no caso de sociedades civis, acompanhada de prova de diretoria em exercício; e

14.3.1.4. Decreto de autorização, em se tratando de empresa ou sociedade estrangeira em funcionamento no País, e ato de registro ou autorização para funcionamento expedido pelo Órgão competente, quando a atividade assim o exigir.

14.3.2. <u>Relativos à Regularidade Fiscal e Trabalhista:</u>

14.3.2.1. Prova de regularidade para com a **Fazenda Federal** relativa aos Tributos Federais e quanto à Dívida Ativa da União (certidão conjunta);

14.3.2.2. Prova de regularidade para com a **Fazenda Municipal (ISS-mobiliário)** do domicílio ou sede da licitante, ou outra equivalente, na forma da lei;

14.3.2.3. Prova de regularidade relativa ao **Fundo de Garantia por Tempo de Serviço** (**FGTS**), demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei;

14.3.2.4. Certidão Negativa de Débitos Trabalhistas - CNDT.

14.3.3. <u>Relativos à Qualificação Econômico-Financeira:</u>

14.3.3.1. Certidão negativa de falência, expedida pelo distribuidor da sede da pessoa jurídica, ou de execução patrimonial, expedida no domicílio da pessoa física.

14.3.4. <u>Qualificação Técnica:</u>

14.3.4.1. Apresentar atestado para a qualificação técnica operacional e profissional, previstas no item 5 do Termo de Referência (Anexo I).

14.3.5. <u>Cumprimento de requisitos constitucionais:</u>

14.3.5.1. Declaração (modelo anexo VI) da **licitante** de que não possui em seu quadro de pessoal empregado (s) com menos de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e de 16 (dezesseis) anos em qualquer trabalho, salvo na condição de aprendiz, nos termos do inciso **XXXIII do art. 7º** da **Constituição Federal de 1988 (Lei nº 9.854/99).**

14.4. Tratando-se de ME/EPP, em caso de restrição quanto às regularidades fiscais e trabalhista, será assegurado o prazo de 5 (cinco) dias úteis prorrogáveis por igual período, a critério da administração, para sua regularização.

14.4.1. O prazo será contado a partir da declaração do resultado da fase de habilitação.

14.4.2. A não regularização implicará na decadência do direito à contratação, sem prejuízo das sanções que couber e, ainda, facultará ao (a) Pregoeiro (a) a convocação das licitantes remanescentes, na ordem classificatória.

14.5. O(A) Pregoeiro(a) constatando o atendimento a todas as exigências contidas neste Edital declarará o **vencedor do certame**.

15. DO RECURSO

15.1. Declarado o vencedor, qualquer licitante poderá, durante o prazo de 60 **(sessenta) minutos** concedido na sessão pública, em campo próprio do sistema, manifestar sua intenção de recorrer.

15.2. Havendo manifestação, caberá ao (à) Pregoeiro (a) examinar a intenção de recurso, aceitando-a ou rejeitando-a motivadamente, em campo próprio do sistema.

15.2.1. O (A) Pregoeiro (a) não poderá rejeitar o recurso em análise de mérito, assim, apenas pela total falta de motivação é que o recurso não será aceito;

15.3. Caso a intenção de recorrer seja aceita a licitante deverá registrar as razões do recurso, em campo próprio do sistema, no prazo de 3 dias; ficando os demais licitantes intimados para, se desejarem, apresentar suas contrarrazões, também no prazo de três dias, contado da data final do prazo do recorrente, assegurada vista imediata dos elementos indispensáveis à defesa dos seus interesses.

15.4. O pregoeiro terá 5 (cinco) dias para proceder a análise de reconsideração ou fazer subir, devidamente instruído, à autoridade superior, a qual poderá reconsiderar sua decisão, no prazo de 5 (cinco) dias úteis, contado do recebimento do recurso pelo Pregoeiro, conforme art. 109 da Lei nº 8.666/1993.

15.5. A ausência de manifestação imediata e motivada do licitante quanto à intenção de recorrer, nos termos do disposto no caput, importará na decadência desse direito, e o pregoeiro estará autorizado a adjudicar o objeto ao licitante declarado vencedor.

16. DA ADJUDICAÇÃO E HOMOLOGAÇÃO

16.1. O objeto deste Pregão será adjudicado pelo (a) Pregoeiro (a)**, inexistindo interposição de recurso,** seguindo para **homologação pelo Presidente**.

16.2. Caso haja recurso, os itens recorridos serão **adjudicados e homologados** pelo Presidente do Tribunal de Contas do Estado do Amapá.

17. DOS SERVIÇOS

17.1. Conforme consta no Termo de Referência (Anexo I).

18. DA FORMALIZAÇÃO E ASSINATURA DA ATA DE REGISTRO DE PREÇO

18.1. Depois de homologado o resultado deste Pregão, o Órgão Gerenciador solicitará ao primeiro fornecedor classificado e, se for o caso, aos demais classificados que aceitarem fornecer pelo preço do primeiro, obedecida à ordem de classificação e os quantitativos propostos, a formalização da correspondente Ata de Registro de Preços.

18.2. O licitante vencedor terá o prazo de 5(cinco) dias úteis para assinar a ata de registro de preço. Será permitido uma única prorrogação por igual período mediante justificativa.

19. DA ASSINATURA DO CONTRATO

19.1. A Administração do Tribunal de Contas do Estado do Amapá convocará oficialmente a licitante vencedora, durante a validade da sua proposta para, **no prazo máximo de 05 (cinco) dias úteis, assinar o contrato**, sob pena de decair o direito ao fornecimento, sem prejuízo das sanções previstas no art. 07 da Lei n° 10.520/02 e art. 81 da Lei nº 8.666/93.

19.2. O prazo da convocação poderá ser prorrogado uma vez, por igual período, quando solicitado pela **licitante vencedora** durante o seu transcurso, desde que ocorra motivo justificado e aceito pela Administração.

19.3. A recusa injustificada da **licitante vencedora** em aceitar ou retirar a nota de empenho, dentro do prazo estabelecido pela Administração, caracteriza o descumprimento total da obrigação assumida, sujeitando-a as penalidades legalmente estabelecidas.

20. DOS ENCARGOS DO TRIBUNAL CONTAS DO ESTADO DO AMAPÁ E DA LICITANTE VENCEDORA

20.1. As obrigações da Contratante e da Contratada estão as estabelecidas nos itens 14 e 15 do Termo de Referência (Anexo I), respectivamente, e na minuta contratual.

21. DAS OBRIGAÇÕES SOCIAIS, COMERCIAIS E FISCAIS.

21.1. Assumir a responsabilidade por todos os encargos previdenciários e obrigações sociais previstos na legislação social e trabalhista em vigor, obrigando-se a saldá**-**los na época própria, **vez que os seus empregados não manterão nenhum vínculo empregatício com o Tribunal de Contas do Estado do Amapá;**

21.2. Assumir, também, a responsabilidade por todas as providências e obrigações estabelecidas na legislação específica de acidentes de trabalho, quando, em ocorrência da espécie, forem vítimas os seus empregados quando da execução dos **serviços** ou em conexão com ele, ainda que acontecido em dependência do **Tribunal de Contas do Estado do Amapá;**

21.3. Assumir todos os encargos de possível demanda trabalhista, civil ou penal, relacionados ao fornecimento dos **serviços**, originariamente ou vinculada por prevenção, conexão ou contingência;

21.4. Assumir, ainda, a responsabilidade pelos **encargos fiscais** e **comerciais** resultantes da adjudicação deste **Pregão.**

21.5. A inadimplência da licitante, com referência aos encargos estabelecidos na condição anterior, não transfere a responsabilidade por seu pagamento à Administração do Tribunal de Contas do Estado do Amapá, nem poderá onerar o objeto deste Pregão, razão pela qual a licitante vencedora renuncia expressamente a qualquer vínculo de solidariedade, ativa ou passiva, com o Tribunal de Contas do Estado do Amapá.

22. DO RECEBIMENTO DOS SERVIÇOS

22.1. Os critérios de atestação e recebimento do objeto está previsto no item 8 do Termo de Referência e na minuta contratual.

23. DO ACOMPANHAMENTO E DA FISCALIZAÇÃO

23.1. Os critérios de fiscalização estão previstos no item 7 do Termo de Referência e na minuta contratual.

24. DO PAGAMENTO

24.1. Os prazos e condições de pagamento estão previstos no item 10 do Termo de Referência (Anexo I) e na minuta contratual.

25. DO AUMENTO OU SUPRESSÃO

25.1. No interesse da **Administração do Tribunal de Contas do Estado do Amapá**, o valor inicial atualizado da **Nota de Empenho** poderá ser aumentado ou suprimido até o limite de 25% (vinte e cinco por cento), conforme disposto no **Artigo 65, parágrafos 1º e 2º, da Lei nº 8.666/93.**

25.2. A licitante vencedora fica obrigada, a aceitar, nas mesmas condições licitadas, os acréscimos ou supressões que se fizerem necessária; e nenhum acréscimo ou supressão poderá exceder o limite estabelecido nesta condição, exceto as supressões resultantes de acordo entre as partes.

26. DAS SANÇÕES ADMINISTRATIVAS

26.1. DAS SANÇÕES ADMINISTRATIVAS

26.1.1. Com fundamento no artigo 7º da Lei nº 10.520/2002, ficará impedida de licitar e contratar com o Estado do Amapá, pelo prazo de até 5 (cinco) anos, garantida a ampla defesa, sem prejuízo da rescisão unilateral do contrato e da aplicação de multa previstas no Termo de Referência sobre o valor total da contratação, a CONTRATADA que:

26.1.2. Apresentar documentação falsa;

26.1.3. Fraudar a execução do contrato;

26.1.4. Comportar-se de modo inidôneo;

26.1.5. Reputar-se-ão inidôneos atos tais como os descritos nos artigos 92, parágrafo único, 96 e 97, parágrafo único, da Lei nº 8.666/1993.

26.1.6. Cometer fraude fiscal; ou

26.1.7. Fizer declaração falsa.

26.2. Com fundamento nos artigos 86 e 87, inciso IV, da Lei nº 8.666, de 1993; poderá ser sancionada, isoladamente, ou juntamente com as multas definidas nos itens abaixo, com as seguintes sanções:

26.2.1. Advertência;

26.2.2. Multa de 0,3 (zero virgula três) % até o limite de 10% para atrasos injustificados na execução do contrato;

26.2.3. Declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a CONTRATADA ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso anterior.

27. DO PREGÃO

27.1 A critério da Administração do **Tribunal de Contas do Estado do Amapá**, este **Pregão** poderá:

27.1.1. Ser anulado, se houver ilegalidade de ofício ou por provocação de terceiros, mediante parecer escrito e devidamente fundamentado; ou

27.1.2. Ser revogado, a juízo da Administração do **Tribunal de Contas do Estado do Amapá**, se for considerado inoportuno ou inconveniente ao interesse público, decorrente de fato superveniente devidamente comprovado, pertinente e suficiente para justificar tal conduta; ou

27.2. Será observado, ainda, quanto ao procedimento deste Pregão:

27.2.1. A anulação do procedimento licitatório por motivo de ilegalidade não gera obrigação de indenizar, ressalvado o disposto no parágrafo único do **art. 59 da Lei n.º 8.666/93;**

27.2.2. A nulidade do procedimento licitatório induz à da nota de empenho, ressalvado, ainda, o dispositivo citado na alínea anterior; e

27.2.3. No caso de desfazimento do processo licitatório, fica assegurado o contraditório e a ampla defesa.

27.2.4. As normas disciplinadoras da presente licitação, serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde

que não comprometam o interesse da Administração, a finalidade e a segurança da contratação.

28. DAS CONSIDERAÇÕES FINAIS

28.1. Da sessão pública do Pregão divulgar-se-á Ata no sistema eletrônico.

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

28.3. No julgamento das propostas e da habilitação, o Pregoeiro poderá sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante despacho fundamentado, registrado em ata e acessível a todos, atribuindo-lhes validade e eficácia para fins de habilitação e classificação.

29. DOS ANEXOS

29.1. São partes integrantes deste edital os seguintes anexos:

ANEXO I	- Termo de Referência
ANEXO II –	- Minuta da Ata de Registro de Preços
ANEXO II –	- Minuta de Contrato

30. DO FORO

30.1. Fica eleito, de comum acordo entre as partes, o Foro da Comarca de Macapá - AP, para dirimir quaisquer litígios oriundos da licitação e do contrato decorrente, com expressa renúncia a outro qualquer, por mais privilegiado que seja.

Macapá-AP, 23 de fevereiro de 2021.

Marta Marcione Pelaes Suares

Pregoeira TCE-AP

TERMO DE REFERÊNCIA
SOLUÇÕES EM SEGURANÇA DA INFORMAÇÃO

1. DO OBJETO

O objeto da presente licitação é o registro de preços para contratação de empresa especializada para o fornecimento de:

- **Solução integrada de segurança, composta por um cluster de Gerenciamento Unificado de Ameaças (Firewall UTM) e seu Gerenciamento de Logs e Relatórios de Segurança;**
- **Solução em Firewall de Aplicações WEB (WAF - Web Application Firewall);**
- **Solução de software para gerenciamento de logs e eventos de segurança (SIEM - Security Information and Event Management).**

Além de suporte técnico e serviços especializados, de acordo com as especificações, quantitativos e observações constantes deste Termo de Referência.

2. MODALIDADE

2.1. Pregão eletrônico no Sistema de Registro de Preço

3. DAS JUSTIFICATIVAS

No ano de 2013 o TCE-AP realizou a contratação de solução integrada de segurança, compreendendo o fornecimento de um cluster Firewall UTM (Fortigate 100D) e de uma solução para armazenamento de logs e produção de relatório (FortiAnalyzer), além dos serviços de instalação e suporte do fabricante pelo período de 36 meses. No decorrer do ano de 2014 os equipamentos foram disponibilizados na rede corporativa do TCE-AP. Considerando a não renovação da licença à época, a mudança dos requisitos no período, a natureza contínua da prestação dos serviços, e as limitações determinadas pelo inciso II do Art. 57 da lei 8.666/93, torna-se necessária nova contratação.

Justifica-se esta contratação pela necessidade de prestação continuada de serviços de segurança da informação, mas sobretudo da ATUALIZAÇÃO de tecnologia, capazes de regular o tráfego de rede no TCE-AP, impedir a transmissão e recepção de tráfego nocivo, implementar recursos de criptografia para tunelamento em redes inseguras de comunicação (VPN), identificar, prevenir e bloquear tentativas de intrusão, realizar serviços de filtro de conteúdo web, monitorar e regular as solicitações feitas a aplicações web, fazer a gestão das vulnerabilidades encontradas em sistemas e recursos de TI e monitorar eventos que possam afetar a segurança computacional da instituição.

Observaram-se ainda avanços na tecnologia utilizada para explorar vulnerabilidades, e que não podiam ser previstas a época da confecção do termo de referência da última contratação, e para qual os produtos fornecidos não fornecem, nos dias de hoje, proteção adequada a este Tribunal de Contas.

Destes pode-se salientar os ataques de “dia zero”, nome utilizado na indústria de segurança da informação para ataques utilizados por meio da exploração de uma vulnerabilidade anteriormente desconhecida que afeta de maneira adversa programas, dados, computadores e redes. Códigos maliciosos que exploram tais vulnerabilidades não podem ser detectados pelo método tradicional de assinatura utilizado pela solução ora em uso. Desta forma, são necessárias outras formas de detecção, como o uso de métodos heurísticos de análise, emulação de código e virtualização

Há ainda que se destacar as medidas regulatórias estabelecidas nos últimos anos que necessitam de ferramentas atuais e adequadas para garantir conformidade (compliance). Como é o caso da GDPR e a mais recente LGPD, que conhecidamente soluções atuais de segurança conseguem contemplar.

É justificada, portanto, a substituição dos atuais equipamentos que compõem a solução de segurança por uma nova solução ou ainda a manutenção da solução de gerenciamento de ameaças (Firewall UTM), atualmente em uso, com a adição de novas funcionalidades em face das novas tecnologias que trarão benefícios ao TCE-AP, tais como: ferramentas de conformidade regulatória, elevar a capacidade de prevenção de ataques, permitir a avaliação das vulnerabilidades a que os ativos de TI estão sujeitas, possibilitando a eliminação antes que sejam exploradas, permitir a monitoração e que permita proteger as chamadas de sistema a aplicações disponibilizadas em servidores web, mesmo criptografadas, a análise avançada de ameaças evasivas e persistentes e análise de tráfego de rede dentro do ambiente de servidores, não apenas no perímetro com as redes externas e com a internet.

Da mesma forma a aquisição de uma solução de WAF (Web Application Firewall) se deve a necessidade de proteção de acesso ao site do TCE-AP, tal como a toda e qualquer aplicação com acesso público na Internet. Trata-se, portanto, de recurso capaz de evitar e mitigar ataques de hackers e botnets. A solução também auxiliará na melhoria de gestão e desempenho de acesso aos sites protegidos.

A infraestrutura de tecnologia da informação e comunicação do TCE-AP, composta de ativos de rede, enlaces ópticos de comunicação, sistemas de virtualização e de armazenamento, entre outros, que dão suporte a todos os sistemas de TI utilizados pelos usuários, tornou-se complexa devido a sua abrangência e variedade de soluções e fornecedores. Embora todos os sistemas gerem logs, é custoso e, de certo modo ineficiente, obter uma visão completa do que acontece em toda a infraestrutura disponível, no que se refere à análise e apresentação de informações dos dispositivos de segurança de rede, softwares de controle de acesso, gerenciamento de vulnerabilidades, ferramentas de conformidade, logs de sistema operacional, banco de dados e aplicações e principalmente dados de ameaças externas.

Há de considerar que, sempre que é requerido auditorias de cruzamento de dados de logs entre diferentes recursos de TI, é necessário realizar uma busca manual nos logs dos principais sistemas, o que reflete na dificuldade de entregar informações consolidadas.

Daí vem a necessidade de adquirir uma ferramenta que reúna dados de eventos de segurança dos sistemas de segurança, sistemas operacionais, aplicativos e outros componentes de software, que possa analisar grandes volumes de dados, identificar ataques, que ofereça uma análise histórica dos eventos de segurança, também coletando e correlacionando os eventos, permitindo consultas mais complexas ao repositório.

Uma solução de gerenciamento de logs e eventos de segurança (SIEM) irá oferecer a catalização de registros de todos os eventos de segurança dos ativos de informação da infraestrutura de TIC do TCE-AP. A ferramenta poderá, ainda, manter uma análise histórica dos eventos de segurança, coletando e correlacionando eventos.
Por último, a solução SIEM auxiliará na garantia de conformidade com as regulamentações relativas à infraestrutura de TIC, exigidas ao TCE-AP. Da mesma forma na redução do tempo gasto para rastrear informações de acesso a sistemas e serviços.

4. DAS QUANTIDADES

Lote	Item	Equipamento	Registro de Preço	Previsão de Contratação Inicial
1	1	Solução em cluster de gerenciamento unificado de ameaças (Firewall UTM) com suporte e garantia do fabricante pelo período de 36 (trinta e seis) meses.	2	1
	2	Gerenciamento, logs e relatoria do cluster de Firewall UTM.	2	1
	3	Treinamento oficial da solução integrada de segurança.	6	3
	4	Instalação e configuração da solução integrada de segurança.	1	1
2	1	Solução em Firewall de Aplicações WEB (WAF), com suporte e garantia do fabricante pelo período de 36 (trinta e seis) meses.	2	1
	2	Capacidade adicional para solução em Firewall de Aplicações WEB.	3	0

	3	Treinamento oficial da solução WAF.	6	3
	4	Instalação e configuração da solução em WAF.	1	1
3	1	Solução de gerenciamento de logs e eventos de segurança (SIEM), com licença perpétua, suporte e atualização para 36 meses de uso.	1	0
	2	Capacidade adicional para software de gerenciamento de logs e eventos de segurança (SIEM), com licença perpétua, suporte e atualização para o primeiro ano de uso.	3	0
	3	Suporte anual para software de gerenciamento de logs e eventos de segurança (SIEM), para módulo principal, descrito no item 01, não incluindo os primeiros 36 meses de uso.	3	0
	4	Treinamento oficial para solução de SIEM.	6	0
	5	Instalação e configuração da solução de SIEM.	1	0

5. DA QUALIFICAÇÃO TÉCNICA

5.1. Apresentar Declaração e/ou Certidão comprovando de que a LICITANTE é fabricante ou distribuidora ou representante credenciada dos equipamentos e serviços objeto deste pregão e, no caso das duas últimas hipóteses que a LICITANTE está autorizada a fornecer, instalar e a prestar assistência técnica e manutenção;

5.2. É obrigatório às licitantes, apresentar atestado(s) ou certidão(ões) de capacidade técnico-operacional comprobatórios de que a empresa proponente tenha executado ou esteja executando, serviços de características técnicas semelhantes às do objeto do presente Edital;

5.3. Os Atestado(s) de Capacidade Técnica-Operacional deverá(ão) ser emitido(s) por entidade da Administração Federal, Estadual ou Municipal, direta ou indireta e/ou empresa privada que comprove ter a empresa licitante executado serviços de características técnicas semelhantes ao objeto desta contratação nos termos da Lei, comprovando:

5.3.1. Experiência na prestação de serviços de administração de solução de Gerenciamento Unificado de Ameaças - UTM e solução de proteção para aplicações WEB, baseado em nuvem. (Web Application Firewall, cloud based);

5.3.2. Experiência na prestação de serviços de administração de solução de anti-malware para estações de trabalho em ambiente computacional com, no mínimo, 250 (duzentos e cinquenta) estações de trabalho;

5.3.3. Experiência na prestação de serviços de administração de solução de anti-malware para ambiente de datacenter utilizando plataforma de virtualização VMware ESXi com, no mínimo, 200 (cem) servidores de rede;

5.3.4. Experiência na prestação de serviços de administração de solução de segurança para proteção de gateway de e-mail, contemplando proteção anti-malware e anti-spam em ambiente computacional com, no mínimo, 250 (duzentos e cinquenta) caixas postais;

5.3.5. Experiência na prestação de serviços de implantação de solução de Gerenciamento e Correlação de Eventos de Segurança da Informação - SIEM, em ambientes com, no mínimo, 200 (duzentos) ativos;

5.3.6. Experiência na prestação de serviços de testes de invasão para exploração de vulnerabilidades de segurança da informação, em conformidade com boas práticas internacionais;

5.4. Entende-se por similar, soluções ou produtos (equipamentos ou softwares) com funcionalidades equivalentes, escalabilidade compatível e porte corporativo;

5.5. Deverão constar do(s) atestado(s) de capacidade técnicaoperacional em destaque, os seguintes dados: identificação do emitente, especificação do fornecimento/serviço executado, prazo de vigência do contrato, local e data de expedição, data de início e término, quando for o caso, do contrato;

5.6. Será permitido o somatório de atestado(s) de capacidade técnica-operacional para efeito de comprovação de experiência na prestação dos serviços de características técnicas semelhantes ao objeto desta contratação;

5.7. A CONTRATANTE poderá diligenciar a pessoa jurídica indicada no Atestado de Capacidade Técnica-Operacional, visando validar ou esclarecer informações sobre o serviço prestado;

6. ESPECIFICAÇÕES TÉCNICAS

6.1. LOTE 01 – ITEM 01 – SOLUÇÃO EM CLUSTER DE GERENCIAMENTO UNIFICADO DE AMEAÇAS (FIREWALL UTM).

6.1.1. Os equipamentos que irão compor o cluster deverão ter, no mínimo, os seguintes requisitos técnicos:

6.1.1.1. Conformidade;

6.1.1.2. O Fabricante deve comprovar participação no MAPP da Microsoft;

6.1.1.3. A tecnologia deve possuir pelo menos uma certificação da ICSA Labs, ICSA Firewall ou Antivirus;

6.1.1.4. O fabricante da solução deverá ser avaliado pela NSS Labs (Network Security Services) no desempenho do Next Generation Firewall Comparative Analysis mais recente, estando no “Security Value Map” acima de 90 % (noventa por cento) ou ser certificado como NGFW pelo laboratorio NetsecOpen;

6.1.1.5. No momento da entrega dos equipamentos a proponente vencedora deverá fornecer declaração do(s) fabricante(s), em papel timbrado com firma reconhecida, dos produtos ofertados, declarando que a proponente possui credenciamento do mesmo para a implantação e suporte técnico de seus produtos;

6.1.1.6. Deve ser homologado pela ANATEL;

6.1.2. Características gerais

6.1.2.1. A solução deve consistir em appliances formando um cluster alta disponibilidade, e de proteção de rede com funcionalidades de proteção de próxima geração;

6.1.2.2. Por funcionalidades de proteção de rede e próxima geração entende-se: reconhecimento e controle granular de aplicações, prevenção de ameaças, identificação de usuários, IPS e Firewall;

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

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

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

6.1.3. Requisitos de performance

6.1.3.1. Throughput de pelo menos 1.7 Gbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação e prevenção de ameaças avançadas habilitados simultaneamente;

6.1.3.2. O Throughput é considerado como a quantidade de tráfego que um único equipamento consegue redirecionar. Não há soma entre o tráfego de entrada e de saída das interfaces;

6.1.3.3. Suportar pelo menos 2.000.000 (dois milhões) conexões ou sessões simultâneas;
6.1.3.4. Suportar pelo menos 70.000 (setenta mil) novas conexões ou sessões por segundo;
6.1.3.5. Armazenamento interno em HDD ou SSD de pelo menos 200GB;
6.1.3.6. Possuir 1 interface de rede dedicada ao gerenciamento;
6.1.3.7. Possuir 1 interface de rede dedicada para acesso via console;
6.1.3.8. Suportar até 10 (dez) instâncias (contextos) virtuais de firewall;
6.1.3.9. Gbps de IPSec/AES-128 VPN Throughput;

6.1.4. Funcionalidades de rede

6.1.4.1. Suportar IPV4 e IPV6;
6.1.4.2. Suportar VLAN 802.1.q
6.1.4.3. Suportar Agregação de links 802.3x;
6.1.4.4. Implementar DHCP e DHCPv6;
6.1.4.5. Implementar DHCP Relay e DHCP Server;
6.1.4.6. Implementar NTP;
6.1.4.7. Roteamento estático e dinâmico em IPv4 e dinâmico IPv6;
6.1.4.8. Roteamento RIP v1/v1, OSPF v2, OSPF v3 ou BGP v4;
6.1.4.9. Suportar OSPF graceful restart;
6.1.4.10. Suportar SNMP v2c ou SNMP v3;
6.1.4.11. Suporte a, no mínimo, 1024 VLAN Tags 802.1q;
6.1.4.12. Agregação de links 802.3x;
6.1.4.13. Implementar Policy based routing ou policy based forwarding;
6.1.4.14. Roteamento multicast (PIM-SM);
6.1.4.15. Deve suportar os seguintes tipos de NAT: Nat dinâmico (Manyto-1), Nat estático (1-to-1), Tradução de porta (PAT), NAT de Origem, NAT de Destino e suportar NAT de Origem e NAT de Destino simultaneamente;
6.1.4.16. Enviar logs para sistemas de monitoração externos, simultaneamente;
6.1.4.17. Prover mecanismo de prevenção a ataques de falsificação de endereços (IP Spoofing) através da especificação da interface de rede pela qual uma comunicação deverá se originar;

6.1.5. Requisitos mínimos de hardware

6.1.5.1. 02 interfaces SFP+ de 10 GbE ativas/licenciadas. Os gbics para cada interface devem ser fornecidos junto com o equipamento;
6.1.5.2. 12 portas 1 GbE, sendo que destas no mínimo 6 portas devem ser de 1 GbE (Ethernet RJ45). Caso as outras interfaces sejam ópticas, os gbics para cada interface devem ser fornecidos junto com os equipamentos e se essas interfaces forem de velocidades diferentes de 1Gbps elas devem permitir que sejam configuradas para trabalhar na velocidade de 1Gbps;
6.1.5.3. 01 interface de 1 GbE dedicada para gerenciamento e 01 para console;
6.1.5.4. 01 interface dedicada para sincronismo de estados da solução de alta disponibilidade;

6.1.5.5. Deve ser fornecido com todas as suas portas de comunicação, interfaces e afins habilitadas, operacionais e prontas para operação, sem custos adicionais;

6.1.5.6. 200GB de armazenamento interno em disco de estado sólido

6.1.5.7. Sistema de ventilação de dupla abordagem;

6.1.5.8. 2 (duas) fontes de alimentação independentes, redundantes, com alimentação nominal 100~120AC e 210~230AC e frequência 50 ou 60 Hz.

6.1.5.9. Deve possibilitar a visualização da utilização dos recursos de CPU, memória, armazenamento interno e atividade de rede na sua interface de gerência e/ou em sistema de gerência centralizado;

6.1.5.10. O equipamento deve ser fornecido com a capacidade máxima de memória e processamento;

6.1.6. Requisitos de Software e Funcionalidades

6.1.6.1. A Contratada deverá fornecer licenças com validade de 60 (sessenta) meses, tal exigência é comum no mercado pois é disponível em sites de fabricantes de equipamentos o período exigido como tempo de garantia, nos serviços dos itens “a” ao “f” que compõem a solução de firewall:

6.1.6.1.1. Antivírus e antispyware;

6.1.6.1.2. Serviço de prevenção contra intrusão (IPS – Intrusion Prevetion System);

6.1.6.1.3. Controle de aplicações (application control);

6.1.6.1.4. Serviço de filtragem de conteúdo;

6.1.6.1.5. Serviço de suporte técnico na modalidade de 24x7 (24 horas/dia e 7 dias/semana);

6.1.6.1.6. Atualizações e upgrades de softwares e firmwares.

6.1.6.2. O licenciamento deve prover a atualização automática e em tempo real dos filtros de conteúdo WEB, através da categorização contínua de novos sites da internet, dos mecanismos de prevenção a intrusão e recursos de segurança contra novos vírus, spywares, vulnerabilidades de softwares e códigos maliciosos;

6.1.6.3. Deve implementar decriptografia e inspeção de tráfego SSL. Esta funcionalidade já deve estar licenciada por pelo menos 60 (sessenta) meses;

6.1.6.4. Deve possuir a capacidade de identificação de ataques como: ataques direcionados, Zero Day, exploração de vulnerabilidades, indicadores de ofuscação e indicadores de comprometimentos automáticos, mesmo que necessite de licenciamento específico para esta finalidade;

6.1.6.5. Deve permitir acesso ao equipamento via CLI (console), SSH e interface web HTTPS;

6.1.6.6. Deve possuir funcionalidade de backup/restore da configuração e políticas de segurança;

6.1.7. Requisitos de filtro de conteúdo web

6.1.7.1. Controle de políticas por aplicações, grupos de aplicações e categorias de aplicações;

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

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

6.1.7.4. Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários prédefinidos automaticamente;

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

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

6.1.7.5.2. Reconhecer pelo menos 2.900 (duas mil e novecentas) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

6.1.7.6. A checagem de assinaturas deve determinar se uma aplicação está utilizando a porta padrão ou não;

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

6.1.7.8. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo;

6.1.7.9. A decodificação de protocolo deve também identificar comportamentos específicos dentro da aplicação;

6.1.7.10. Atualizar a base de assinaturas de aplicações automaticamente;

6.1.7.11. Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;

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

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

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

6.1.7.15. Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;

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

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

6.1.7.16.2. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;
6.1.7.16.3. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs atráves da integração com serviços de diretório, autenticação via Active Directory e base de dados local;
6.1.7.16.4. Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;
6.1.7.16.5. Deve bloquear acesso a sites com conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, mesmo que a opção “Safe Search” esteja desabilitada no navegador do usuário;
6.1.7.16.6. Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs;
6.1.7.16.7. Suportar a criação de categorias de URLs customizadas;
6.1.7.16.8. Suportar a exclusão de URLs do bloqueio, por categoria;
6.1.7.16.9. Permitir a customização de página de bloqueio;
6.1.7.17. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, sem a necessidade de instalar nenhum cliente nos servidores Active Directory ou em outra máquina da rede;
6.1.7.18. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via Radius ou syslog, para a identificação de endereços IP e usuários;
6.1.7.19. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no Firewall (Captive Portal);

6.1.8. Requisitos de prevenção de ameaças
6.1.8.1. Os dispositivos de proteção devem possuir módulo de IPS e suportar os módulos de: Antivírus e Anti-Malware integrados no próprio equipamento;
6.1.8.2. Deve incluir assinaturas de prevenção de intrusão (IPS) e suporte ao bloqueio de arquivos maliciosos (Antivírus e AntiMalware);
6.1.8.3. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Malware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
6.1.8.4. Deve suportar granularidade nas políticas de Antivírus e Antimalware, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
6.1.8.5. Deverá possuir os seguintes mecanismos de inspeção de IPS:
6.1.8.5.1. Análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;
6.1.8.6. Detectar e bloquear a origem de portscans;
6.1.8.7. Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;

6.1.8.8. Possuir assinaturas para bloqueio de ataques de buffer overflow;
6.1.8.9. Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;
6.1.8.10. Suportar bloqueio de arquivos por tipo;
6.1.8.11. Identificar e bloquear comunicação com botnets;
6.1.8.12. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:
6.1.8.12.1. O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;
6.1.8.13. Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware;
6.1.8.14. Os eventos devem identificar o país de onde partiu a ameaça;
6.1.8.15. Suportar rastreamento de vírus em arquivos pdf;
6.1.8.16. Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);
6.1.8.17. Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/Países seja bloqueado;
6.1.8.18. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
6.1.8.19. Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing), através da especificação da interface de rede pela qual uma comunicação deve se originar baseado na topologia, não sendo aceito soluções que utilizem tabela de roteamento para esta proteção;

6.1.9. Requisitos de prevenção de ameaças avançadas
6.1.9.1. A solução deverá prover as funcionalidades de inspeção e prevenção de tráfego de entrada de malwares não conhecidos e do tipo APT, com filtro de ameaças avançadas e análise de execução em tempo real e inspeção com prevenção de tráfego de saída de callbacks (comunicação do malware com o servidor de comando e controle);
6.1.9.2. Implementar, identificar e bloquear malwares de dia zero em anexos de e-mail e URL's conhecidas;
6.1.9.3. A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows 7 (32 e 64 bits), Windows 8, Windows 8.1 e Windows 10 (64 bits), assim como Office 2003, 2010 e 2013;
6.1.9.4. Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endereço IP;
6.1.9.5. Implementar a emulação, detecção e bloqueio de qualquer malware e/ou código malicioso detectado como desconhecido. A solução deve permitir a análise e bloqueio dos seguintes tipos de arquivos caso tenham malware desconhecido: cab, csv, doc, docx, docm, dot, dotm, dotx, exe, hwp, jar, pdf, pif, ppam, pps, ppsm, ppsx, potx, potm, ppt, pptm, pptx, rar, rtf, seven-z, sldm, sldx, swf, tar, tgz, xlam, xls, xlsx, xlt, xltx, xlsm, xltm, xll, xlsb, zip;
6.1.9.6. Prover informações para que a solução de relatórios possa apresentar via interface gráfica as seguintes informações:
6.1.9.6.1. Sumário executivo;

6.1.9.6.2. Relatório de máquinas infectadas;
6.1.9.6.3. Atividades do malware durante a execução de arquivo, nos ambientes controlados em todas as versões de sistemas operacionais requisitados neste projeto;
6.1.9.7. A solução deve permitir a criação de whitelists baseado no MD5 do arquivo;
6.1.9.8. Para melhor administração da solução, a solução deve possibilitar as seguintes visualizações a nível de monitoração:
6.1.9.8.1. Número de arquivos emulados;
6.1.9.9. A solução de possuir os indicadores abaixo referente ao último dia, última semana ou últimos 30 dias:
6.1.9.9.1. Arquivos scaneados;
6.1.9.9.2. Arquivos maliciosos;

6.1.10. Requisitos de controle de qualidade de serviço (QoS)

6.1.10.1. Suportar a criação de políticas de QoS por:
6.1.10.1.1. Endereço de origem, endereço de destino e por porta;
6.1.10.2. QoS deve possibilitar a definição de classes por:
6.1.10.2.1. Banda garantida, banda máxima e fila de prioridade;
6.1.10.3. Disponibilizar estatísticas RealTime para classes de QoS;

6.1.11. Requisitos de VPN

6.1.11.1. Suportar VPN Site-to-Site e Client-to-Site;
6.1.11.2. Suportar IPSec VPN;
6.1.11.3. Suportar SSL VPN;
6.1.11.4. A VPN IPSEc deve suportar: 3DES, Autenticação MD5 e SHA1, Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Algoritmo Internet Key Exchange (IKE), AES 128 e 256 (Advanced Encryption Standard) e autenticação via certificado IKE PKI;
6.1.11.5. A VPN SSL deve suportar:
6.1.11.5.1. Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
6.1.11.5.2. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
6.1.11.5.3. Atribuição de endereço IP nos clientes remotos de VPN;
6.1.11.5.4. Atribuição de DNS nos clientes remotos de VPN;
6.1.11.5.5. Dever permitir criar políticas para tráfego dos clientes remotos conectados na VPN SSL;
6.1.11.5.6. Suportar autenticação via AD/LDAP, certificado digital e base de usuários local;
6.1.11.5.7. Suportar leitura e verificação de CRL (certificate revocation list);
6.1.11.5.8. O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows 7, Windows 8 e MacOS X;

6.2. **LOTE 01 – ITEM 02 – GERENCIAMENTO, LOGS E RELATORIA DO CLUSTER DE FIREWALL UTM.** Os recursos que irão compor o item deverão ter, no mínimo, os seguintes requisitos técnicos:

6.2.1. A solução deve possuir integração 100% compatível com o ITEM 01 do LOTE 01;
6.2.2. A solução de gerenciamento deverá ser entregue como appliance virtual e deve ser compatível/ homologado para VMware ESXi versão 5.5 e superior, alocado no ambiente da CONTRATADA. Não será aceito solução em nuvem.
6.2.3. A solução ofertada poderá ser composta por um ou mais componentes (software, appliance, etc), desde que sejam do mesmo fabricante, totalmente interoperáveis entre si, gerenciados através de uma interface única e em número de licenças suficientes.
6.2.4. Caso a solução possua licenças relacionadas a armazenamento, deve ser ofertada uma licença de capacidade não inferior a 100GB/dia;
6.2.5. Deve possuir solução de gerenciamento e administração centralizado;
6.2.6. Suportar criação de regras que fiquem ativas em horário definido;
6.2.7. Suportar criação de regras com data de expiração;
6.2.8. Suportar backup das configurações e rollback de configuração para a última configuração salva;
6.2.9. Suportar validação de regras antes da aplicação;
6.2.10. Suportar validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
6.2.11. A solução deve possuir processo automático, formal para o acompanhamento, aprovação e alterações de política de segurança;
6.2.12. A solução deve suportar notificação por e-mail acerca das instalações de políticas;
6.2.13. Deve permitir a customização de dashboards da solução de gerenciamento;
6.2.14. A solução deverá prover funcionalidade para apoiar nos processos internos de gerência de mudanças e gerência de configuração;
6.2.15. A solução deve possibilitar o funcionamento em modo de auditoria provendo a possibilidade de auditar todas as mudanças de políticas com relatório detalhado de cada alteração efetuada;
6.2.16. A solução deve permitir um fluxo de aprovação da alteração efetuada para possibilitar que somente alterações gerencialmente aprovadas poderão ser efetivamente aplicadas;
6.2.17. A solução deverá prover um relatório detalhado da alteração para que seja possível uma revisão da alteração antes da aprovação;
6.2.18. Permitir criações de políticas de acesso de usuários autenticados no Active Directory, de forma que reconheça os usuários de forma transparente;
6.2.19. Permitir o download de assinaturas, atualizações e firmwares para distribuição centralizada aos dispositivos de segurança integrados a mesma;
6.2.20. Deve fornecer uma interface gráfica para criação das regras citadas no item anterior;
6.2.21. Deve possuir painéis de eventos em tempo real com possibilidade de configuração das atualizações e frequências;

6.2.22. Deve permitir a criação de objetos e políticas compartilhadas;
6.2.23. Deve suportar configuração em alta disponibilidade para fins de redundância;
6.2.24. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança;
6.2.25. O gerenciamento da solução deve suportar acesso via SSH, cliente e WEB (HTTPS);
6.2.26. O gerenciamento deve permitir/possuir monitoração de logs, ferramentas de investigação de logs e acesso concorrente de administradores;
6.2.27. Deve possibilitar a integração com outras soluções de SIEM de mercado desde que não sejam software livre;
6.2.28. Suportar geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;
6.2.29. Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-Malware), etc;
6.2.30. Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus, Anti- Malware), e URLs que passaram pela solução;
6.2.31. Deve ser possível exportar os logs em CSV;
6.2.32. Deve possibilitar a geração de relatórios no formato PDF;
6.2.33. Possibilitar rotação do log;
6.2.34. Suportar geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:
6.2.34.1. Resumo gráfico de aplicações utilizadas;
6.2.34.2. Principais aplicações por utilização de largura de banda;
6.2.34.3. Principais aplicações por taxa de transferência de bytes;
6.2.34.4. Principais hosts por número de ameaças identificadas;
6.2.34.5. Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti- Malware), de rede vinculadas a este tráfego;
6.2.35. Deve permitir a criação de relatórios personalizados;
6.2.36. Suportar enviar os relatórios de forma automática via e-mail em PDF ou HTML;
6.2.37. Deve consolidar logs e relatórios de todos os dispositivos administrados; Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura;
6.2.38. Deverá possuir mecanismo de Drill-Down para navegação e análise dos logs em tempo real;
6.2.39. Nas opções de Drill-Down, deve ser possível identificar o usuário que fez determinado acesso;
6.2.40. Os itens subnivelados a seguir, caso necessitem de licença adicional, devem estar disponíveis na entrega com no mínimo 1 ano de licenciamento incluso:
6.2.40.1. Suportar gerar relatórios de aderência às políticas de negócio;
6.2.40.2. Suportar gerar alertas não aderentes às políticas de negócio;
6.2.40.3. Permitir a integração e avaliação de todos os equipamentos de proteção de rede do ITEM 01, LOTE 01, na gerência com os seguintes padrões e instrumentos regulatórios:
6.2.40.3.1. ISO27002;

6.2.40.3.2. GDPR;
6.2.40.3.3. LGPD;
6.2.40.4. Simular o impacto de segurança das alterações de configuração antes da instalação de acordo com a aderência aos padrões e instrumentos regulatórios apresentados no item anterior;
6.2.40.5. Permtir a customização do padrão/instrumento regulatório da própria instituição;
6.2.40.6. Pemitir notificação instantânea sobre mudanças de política de segurança que impactam negativamente a segurança;
6.2.40.7. Monitar constantemente o status de conformidade da solução aos padrões e instrumentos regulatórios informados;
6.2.40.8. Possuir status de segurança com atualização automática a cada alteração de configuração;
6.2.40.9. Possuir alertas de políticas e as potenciais violações de conformidade;
6.2.40.10. Gerar relatórios regulamentares com base nas configurações de segurança em tempo real;
6.2.41. Permitir que os relatórios possam ser salvos, enviados e impressos;
6.2.42. Deve permitir a criação de filtros com base em qualquer característica do evento, tais como a origem e o IP destino, serviço, tipo de evento, severidade do evento, nome do ataque, o país de origem e destino, etc;
6.2.43. A solução deve prover, no mínimo, as seguintes funcionalidades para análise avançada dos incidentes:
6.2.43.1. Visualizar quantidade de tráfego utilizado de aplicações e navegação;
6.2.43.2. Gráficos com principais eventos de segurança de acordo com a funcionalidade selecionada;
6.2.44. A solução deve ser capaz de detectar ataques de tentativa de login e senha;
6.2.45. Deve suportar a geração de relatório gerencial para apresentar aos executivos os eventos de ataque de forma completamente visual, utilizando, para tanto, gráficos, consumo de banda utilizado pelos ataques e quantidade de eventos gerados e protegidos;
6.2.46. A solução deve permitir gerenciar mudanças com segurança automatizada;
6.2.47. A solução deve permitir o controle de alterações de forma visual e através de relatórios;
6.2.48. Permitir a visualização de gráficos e mapa de ameaças;
6.2.49. Possuir mecanismo para que logs antigos sejam removidos automaticamente;
6.2.50. Possuir a capacidade de personalização de gráficos;
6.2.51. Deve permitir a criação de dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino;
6.2.52. Deve possuir a capacidade de visualizar na interface gráfica da solução de relatórios informações do sistema como licenças, memória, disco, uso de CPU, taxa de logs por segundo recebidos, total de logs diários recebidos, alertas gerados entre outros;
6.2.53. Deve disponibilizar a geração de pelo menos os seguintes tipos de relatórios:

6.2.53.1. Máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas e categorias Web mais acessadas;

6.2.54. Deve permitir a integração com sistemas terceiros através de API;

6.3. **LOTE 01 – ITEM 03 – TREINAMENTO OFICIAL DA SOLUÇÃO INTEGRADA DE SEGURANÇA.** As condições que irão delinear a entrega do serviço item deverão ter, no mínimo, os seguintes requisitos:

6.3.1. A CONTRATADA deverá fornecer inscrição para REINAMENTO OFICIAL na solução integrada de segurança, cujo escopo deve cobrir os equipamentos e softwares ofertados no LOTE 01, ITENS 01 e 02;

6.3.2. O TREINAMENTO OFICIAL poderá ser dividido em módulos de cursos complementares entre si;

6.3.3. Cada treinamento deverá prever a capacitação para 1 turma com até 6 pessoas, a serem nomeadas pela CONTRATANTE;

6.3.4. O treinamento poderá ser fornecido na modalidade online (EAD), in-loco em centro autorizado de treinamento do fabricante, ou na modalidade in-company, em Macapá/AP e em local de providência e responsabilidade da CONTRATADA;

6.3.5. Os treinamentos deverão ser iniciados até 40 (quarenta) dias após assinatura do Contrato.

6.3.6. A CONTRATADA deverá apresentar, em até 20 (vinte) dias após assinatura do Contrato, um Plano de Treinamento que será avaliado e aprovado pela equipe técnica da CONTRATANTE;

6.3.7. O Plano citado no item anterior deverá apresentar o programa de cada treinamento com conteúdo, carga horária, duração em dias, modalidade e avaliações de aprendizagem;

6.3.8. O Treinamento deverá ser oficial do fabricante em cada uma das ferramentas, contemplando módulos, com conteúdo teórico e prático, com programas mínimos que abordem toda a instalação, configuração, e implementação de 100% dos recursos e funcionalidades;

6.3.9. O treinamento oficial do fabricante deverá prover todas as ferramentas necessárias para atender aos requisitos citados na alínea anterior;

6.3.10. Só será admitido a entrada em funcionamento de componentes da solução sem que tenha havido o respectivo treinamento caso seja de interesse expresso por parte da CONTRATANTE, não tornando o mesmo indispensável sob nenhum aspecto ou condição.

6.3.11. O instrutor que irá ministrar o treinamento deverá ser certificado pelo fabricante da solução;

6.3.12. A CONTRATADA arcará com todas as despesas relativas aos seus profissionais e técnicos envolvidos nas atividades do treinamento;

6.3.13. Caso o treinamento seja fornecido na modalidade EAD, a CONTRATADA deverá inscrever os participantes informados pela CONTRATANTE na primeira turma disponível após a assinatura do contrato ou em data definida pela DAINF-TCE/AP, de acordo com o calendário de turmas disponíveis;

6.3.14. Caso o treinamento seja fornecido na modalidade in-loco ou incompany, a CONTRATADA deverá definir o período do treinamento, incluindo a carga horária diária em comum acordo com a CONTRATANTE logo após a assinatura do contrato de forma independente dos prazos de entrega dos equipamentos e softwares deste termo de referência;

6.3.15. Nos casos das modalidades in-loco ou in-company A CONTRATADA deverá prover toda a estrutura acessória para os treinamentos, incluindo coffee-break;

6.3.16. O treinamento deverá incluir laboratório virtual para a simulação das configurações e testes;

6.3.17. O Conteúdo do treinamento deverá ser de natureza teórica e prática, devendo abranger todas as funcionalidades, componentes e softwares, em seus aspectos mais relevantes e, em especial, envolvendo aqueles relacionados à solução implantada no ambiente computacional do TCE/AP, contendo:

6.3.17.1. Instalação e configuração inicial;

6.3.17.2. Conceitos e configuração das funcionalidades de firewall, controle de aplicações, filtro de conteúdo, proteção contra malwares e análise em nuvem (sandbox), APT, IPS, DPL;

6.3.17.3. Firewall policy;

6.3.17.4. Decryption;

6.3.17.5. VPN:

6.3.17.6. Client-to-LAN;

6.3.17.7. LAN-to-LAN;

6.3.17.8. IPSec;

6.3.17.9. VPN SSL;

6.3.17.10. Roteamento estático e dinâmico;

6.3.17.11. NAT;

6.3.17.12. Logs & Reporting;

6.3.17.13. Integração com serviços de diretório (SSO);

6.3.17.14. Monitoramento e gestão da ferramenta com vistas às atividades de rotina.

6.3.18. A CONTRADA poderá fornecer materiais didáticos em formatos digitais;

6.3.19. A CONTRATADA deverá emitir certificados de conclusão do treinamento. Deverá constar no certificado a data de início e fim, carga horária, nome do instrutor, nome do treinamento e nome do participante;

6.4. **LOTE 01 – ITEM 04 – INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO INTEGRADA DE SEGURANÇA.** A entrega do serviço deverá cumprir os seguintes requisitos:

6.4.1. Requisitos Gerais

6.4.1.1. Iniciar a execução das atividades de entrega, instalação e configuração dos equipamentos e softwares da solução integrada de segurança de acordo com os prazos definidos em cronograma, contados a partir da emissão de Ordem de Serviço - OS pela CONTRATANTE;

6.4.1.2. No 3o (terceiro) dia após a emissão da Ordem de Serviço, deverá ser realizada reunião presencial na SEDE do TCE-AP, em Macapá/AP, com o objetivo de

apresentar sua metodologia de trabalho, planejamento e coordenação das atividades de entrega da solução integrada de segurança;

6.4.1.3. A CONTRATADA deverá apresentar um Plano de Implantação, em até 15 (quinze) dias da emissão da Ordem de Serviço pelo CONTRATANTE, contendo a documentação detalhada das atividades de entrega, instalação, configuração e testes dos equipamentos e softwares que compõem a solução integrada de segurança;

6.4.1.4. A CONTRATADA deverá inventariar todas configurações atualmente aplicadas no ambiente do CONTRATANTE, bem como migrar todas as políticas, regras de exceção e aplicar todas as demais configurações de proteção e serviços de NGFW utilizados pelo órgão. Revisões e correções poderão ser sugeridas para melhor implementação;

6.4.1.5. O processo de instalação, atualização ou migração da solução deverá ser acompanhado pela equipe técnica indicada pela CONTRATANTE;

6.4.1.6. Para garantir que a instalação, atualização ou migração não afetará o ambiente da CONTRATANTE, os procedimentos e atividades deverão ser realizados por técnicos qualificados pelo fabricante nos produtos envolvidos, comprovado no ato de entrega do PLANO DE IMPLANTAÇÃO;

6.4.1.7. O Plano de Implantação deverá dispor também sobre o cronograma de execução, previsão de recursos humanos e materiais, pessoas envolvidas e atividades a serem desenvolvidas pela CONTRATADA e indicar os principais riscos e forma de mitigação, contendo também os seguintes itens:

6.4.1.7.1. Detalhar os procedimentos para entrega, retirada das embalagens e conferência dos equipamentos, softwares e acessórios entregues;

6.4.1.7.2. Detalhar informações sobre as etapas de instalação física dos equipamentos, incluindo: distribuição dos equipamentos pelos racks, movimentação de equipamentos existentes, conexões elétricas e lógicas necessárias, definição de nomes dos equipamentos e endereçamento de gerência IP;

6.4.1.7.3. Documentar regras e configurações atuais aplicadas aos ativos de segurança existentes no CONTRATANTE e planejar a aplicação destas regras e configurações nos equipamentos e softwares da solução integrada de segurança, eliminado as regras inativas ou desnecessárias, mediante aprovação do CONTRATANTE;

6.4.1.7.4. Indicar de forma detalhada as condições de rollback de cada mudança no ambiente do TCE-AP;

6.4.1.7.5. Elaborar atividades de teste de operação da solução e planos de testes para os diversos componentes da solução que comprovem o funcionamento das regras e configurações aplicadas, bem como dos recursos de tolerância a falhas dos equipamentos e softwares da solução integrada de segurança;

6.4.1.7.6. Planejamento para atualização da solução atual ou migração de todas políticas, regras de exceção e todas as demais configurações de proteção atuais para a nova solução;

6.4.2. Requisitos de entrega

6.4.2.1. Entregar todos os equipamentos, licenças de softwares e acessórios no prazo máximo de até 45 (quarenta e cinco) dias, a contar da data de emissão da Ordem de Serviço pela CONTRATANTE

6.4.2.2. Entregar os equipamentos novos e de 1º uso juntamente com todos os itens acessórios de hardware e de software necessários à perfeita instalação e funcionamento, incluindo cabos, conectores, interfaces, suportes, drivers de controle e programas de configuração, conforme especificações constantes deste Termo de Referência;

6.4.2.3. Entregar os equipamentos devidamente protegidos e embalados, originais e lacrados, os quais devem evitar danos de transporte e manuseio;

6.4.2.4. Desembalar os equipamentos após a entrega nas dependências do CONTRATANTE;

6.4.2.5. Entregar os equipamentos e softwares, a suas expensas, bem como instalar e realizar todos os testes necessários à verificação do perfeito funcionamento dos produtos fornecidos;

6.4.2.6. Entregar todos os documentos comprobatórios de garantia indicados neste Termo de Referência;

6.4.2.7. Entregar toda a documentação técnica em meio eletrônico, completa e atualizada, contendo os manuais e guias de utilização;

6.4.2.8. Instalar os equipamentos e softwares nas datas e horários definidos no Plano de Implantação, sob supervisão da equipe técnica da CONTRATANTE;

6.4.2.9. Aceitar que as atividades de instalação e configuração dos equipamentos e softwares da solução integrada de segurança deverão ocorrer localmente nas dependências do TCE-AP, devendo ser realizada em horários que não coincidam com o expediente do CONTRATANTE. O TCE-AP poderá autorizar a realização de atividades durante o horário de expediente se, ao seu exclusivo critério, entender que não oferece risco ao funcionamento de sua rede de computadores e serviços em produção;

6.4.2.10. Aceitar que o processo de entrega, instalação e configuração dos equipamentos e softwares da solução integrada de segurança da solução deverá ser acompanhado pela equipe técnica indicada pelo CONTRATANTE;

6.4.2.11. Aceitar que caso a implantação de qualquer elemento da solução integrada de segurança cause interferência na correta operação da rede de dados do TCE-AP, a CONTRATADA deverá alocar profissionais com qualificação suficiente para corrigir o problema ou retornar o ambiente à condição anterior à implantação;

6.4.2.12. A execução dos serviços de entrega, instalação e configuração dos equipamentos e softwares da solução integrada de segurança deverão contemplar, no mínimo, os seguintes itens:

6.4.2.12.1. Instalação física e ativação dos equipamentos da solução;

6.4.2.12.2. Realizar a integração dos equipamentos da solução a rede LAN existente no TCE-AP, sem interrupção no funcionamento normal dos serviços de TI. Caso exista a necessidade de interrupção de qualquer equipamento ou serviço em

produção para a integração dos equipamentos, o prazo para realização e a duração da janela de manutenção deverão ser acordados com o TCE-AP;

6.4.2.12.3. Instalar e configurar todas as funcionalidades exigidas na especificação técnica da solução, bem como quaisquer outras disponíveis adicionalmente nos diversos componentes da solução mediante solicitação da equipe do TCE-AP;

6.4.2.12.4. Realizar testes de operação da solução que comprovem o funcionamento dos recursos de tolerância a falhas das soluções de segurança;

6.4.2.12.5. Atualizar o plano de implantação com todas as informações que represente a topologia física e lógica, a configuração final e as regras aplicadas aos equipamentos e softwares da solução integrada de segurança;

6.4.2.13. Receber cópia de documento Termo de Recebimento Provisório (TRP) após entrega dos equipamentos, softwares, acessórios, Plano de Implantação e demais documentações da solução, conforme descrito no cronograma do ANEXO II. A finalização da entrega deverá ser formalizada mediante comunicação escrita da CONTRATADA ao CONTRATANTE. O recebimento provisório realizar-se-á no prazo máximo de 15 (quinze) dias corridos, contados da comunicação da empresa, desde que não haja pendências a cargo da CONTRATADA;

6.4.2.14. Concluir no prazo de 45 (quarenta e cinco) dias corridos, contados a partir da emissão do Termo de Recebimento Provisório, os serviços de instalação e configuração dos equipamentos e softwares da solução integrada de segurança, realizando todas as atividades programadas para esta etapa;

6.4.2.15. Receber cópia do Termo de Recebimento Definitivo (TRD), após a formalização por escrito da CONTRATADA referente à conclusão das atividades de entrega, instalação e configuração dos equipamentos e softwares da solução integrada de segurança. O recebimento definitivo realizar-se-á no prazo máximo de 10 (dez) dias corridos, contados da comunicação da empresa, desde que não haja pendências a cargo da CONTRATADA;

6.4.2.16. Realizar, por 30 (trinta) dias corridos após a emissão do Termo de Recebimento Definitivo (TRD), operação assistida da solução de segurança, esclarecendo dúvidas e realizando ajustes na configuração visando à melhor utilização dos recursos oferecidos nos equipamentos que compõe a solução;

6.4.2.17. O período de operação assistida da solução de segurança poderá ser executado remotamente, 3 (três) horas por dia, no período entre 08h e 18h;

6.4.2.18. O período de operação assistida faz parte dos serviços de instalação e configuração, não representando ônus adicional para o CONTRATANTE;

6.4.3. Repasse de conhecimento

6.4.3.1. A CONTRATADA deverá realizar a repasse de conhecimento para a equipe técnica da CONTRATANTE por meio de documentação e apresentação estruturada sobre todo o processo de instalação e configuração das tecnologias da solução integrada;

6.4.3.2. O repasse de conhecimento deverá iniciar imediatamente ao passo que antecede a emissão do Termo de Recebimento Provisório;

6.4.3.3. A transferência de conhecimento deverá abordar, no mínimo, as seguintes funcionalidades da solução:

6.4.3.3.1. Gerenciamento Unificado de Ameaças;

6.4.3.3.2. Filtro de Conteúdo;

6.4.3.3.3. Balanceamento de Carga;

6.4.3.3.4. Prevenção de Intrusão;

6.4.3.3.5. Ataques avançados;

6.4.3.3.6. Segurança para ambiente virtual;

6.4.3.3.7. Gerenciamento e elaboração de relatórios da solução;

6.4.3.4. O repasse de conhecimento deverá ser realizada em Macapá/AP, cabendo a CONTRATADA providenciar as instalações para este fim. A transferência de conhecimento poderá ser realizada na sede do CONTRATANTE caso manifeste interesse;

6.4.3.5. O repasse conhecimento deverá ser de natureza teórica e prática, devendo abranger os equipamentos e softwares fornecidos em seus aspectos relacionados à solução implantada no ambiente computacional do Tribunal de Contas, contendo, no mínimo:

6.4.3.5.1. Orientação sobre a topologia lógica da solução implantada, mostrando a interligação dos componentes físicos da solução, informando as interconexões realizadas com a infraestrutura existente no CONTRATANTE;

6.4.3.5.2. Descrição do hardware e software de cada equipamento;

6.4.3.5.3. Configuração e administração dos equipamentos;

6.4.3.5.4. Descrição geral da plataforma de gerência;

6.4.3.5.5. Diagnóstico de problemas;

6.4.3.5.6. Configuração de alarmes, eventos e rotinas para os serviços de monitoramento;

6.4.3.5.7. Gerência de desempenho e segurança;

6.4.3.5.8. Manipulação de objetos MIB, SNMP e RMON para monitoração;

6.4.3.5.9. Resolução de problemas “troubleshooting”;

6.4.3.5.10. Relatórios;

6.4.3.6. Um plano de repasse conhecimento deverá ser previamente aprovado pela CONTRATANTE, e eventuais mudanças de conteúdo poderão ser solicitadas;

6.4.3.7. O cronograma efetivo do repasse de conhecimento será definido em conjunto com o CONTRATANTE, na primeira reunião de planejamento;

6.4.3.8. Caso a transferência de conhecimento não seja satisfatória com relação à profundidade do conteúdo apresentado ou domínio dos temas por parte do instrutor, a CONTRATADA deverá complementar, sem ônus adicional, o repasse dos pontos considerados pela CONTRATANTE como insatisfatórios;

6.4.3.9. A transferência de conhecimento deverá ser realizada por técnicos qualificados e certificados pelos fabricantes dos equipamentos e softwares da solução ofertada;

6.5. **LOTE 02 – ITEM 01 – SOLUÇÃO EM PROTEÇÃO PARA APLICAÇÕES WEB (WAF) -** Os recursos que irão compor a solução deverão ter, no mínimo, os seguintes requisitos técnicos:

6.5.1. Características gerais

6.5.1.1. Devido aos modelos comerciais dos mais importantes fabricantes serem diferentes, o fornecedor da solução poderá ofertar ao menos uma das formas de citadas a seguir, ou combinação delas, devidamente descrito na proposta comercial, desde que atenda os volumes e quantitativos esperados; 5.5.1.2. A solução deve suportar uma taxa de transmissão de no mínimo 20 Mbps.

6.5.1.2. A solução deve suportar, inicialmente, 5 FQDNs, onde cada FQDN representa uma aplicação web;

6.5.1.3. A solução deve suportar tráfego agregado (upstream+downstream) de no mínimo 210 GB/dia;

6.5.1.4. A solução de Firewall de Aplicação Web (WAF) deverá ser fornecida na forma de appliance virtual. Devem estar inclusas todas as licenças e garantias necessárias para sua instalação, configuração e operação;

6.5.1.5. A solução deve possibilitar a integração com Solução SIEM de no mínimo 5 fabricantes;

6.5.1.6. Deve ser fornecido em appliance virtual compatível com no mínimo os seguintes hypervisors:

6.5.1.7. VMware ESX/ESXi 5.0/5.1/5.5/6.0;

6.5.1.8. Microsoft Hyper-V 2008 R2/2012/2012 R2/2016;

6.5.1.9. Deve suportar instalação em ambiente de alta disponibilidade:

6.5.1.10. Ser capaz de operar em modo Ativo/Standby;

6.5.1.10.1. Ser capaz de operar em modo Ativo/Ativo, mantendo o status das conexões. Aceita-se como Ativo/Ativo a utilização de dois endereços Virtuais, onde cada endereço fica ativo em um elemento e standby no outro;

6.5.1.10.2. Assegurar que a operação da solução de 02 (dois) ou mais appliances, quando implementada em ambiente redundante, suporte sincronismo de sessão entre os dois membros. A falha do equipamento principal não deverá causar a interrupção das sessões balanceadas;

6.5.1.10.3. Fornecer todos os recursos possíveis de redundância sem nenhuma despesa com licenças adicionais;

6.5.1.10.4. A solução deve possuir escalabilidade, podendo incrementar sua capacidade de processamento através de licenças;

6.5.1.11. A solução deverá possuir sistema operacional certificado ICSA Labs podendo assim ser instalado na borda de rede antes de qualquer equipamento de segurança, como por exemplo Firewall;

6.5.1.12. A solução, quando habilitado para mais de uma função deverá permitir a definição da importância da mesma, determinando quanta CPU e memória será alocada para cada uma;

6.5.1.13. Deve possuir recursos para gerenciamento:

6.5.1.14. Permitir configuração de endereçamento IP estático ou dinâmico (DHCP/BOOTP) para o gerenciamento;

6.5.1.14.1. Implementar o SNTP (Simple Network Time Protocol) ou NTP (Network Time Protocol);
6.5.1.14.2. Permitir acesso in-band via SSH;
6.5.1.14.3. Manter internamente múltiplos arquivos de configurações do sistema;
6.5.1.14.4. Utilizar SCP ou HTTPS como mecanismo de transferência de arquivos de configuração e Sistema Operacional;
6.5.1.14.5. Interface por linha de comando (CLI – Command Line Interface) que possibilite a configuração dos equipamentos;
6.5.1.14.6. Possuir auto-complementação de comandos na CLI;
6.5.1.14.7. Possuir um comando, via CLI, que mostre o tráfego de utilização das interfaces (bps e pps);
6.5.1.14.8. Reinicialização do equipamento por comando na CLI;
6.5.1.14.9. Possuir, no mínimo, Três níveis de usuários na GUI – SuperUsuário, Usuário com permissões reduzidas, e usuário Somente Leitura;
6.5.1.14.10. Os usuários de gerência deverão poder ser autenticados em bases remotas. No mínimo RADIUS, LDAP e TACACS+ deverão ser suportados;
6.5.1.14.11. Deverá ser possível receber da base RADIUS, LDAP e TACACS+ o nível de acesso (Grupo ou Permissões);
6.5.1.15. Possuir interface gráfica via Web:
6.5.1.15.1. A interface gráfica deverá permitir a atualização do sistema operacional e/ou a instalação de patches ou Hotfixes sem o uso da linha de comando;
6.5.1.15.2. A interface gráfica deverá permitir a configuração de qual partição o appliance deverá dar o boot;
6.5.1.15.3. A interface gráfica deverá permitir a reinicialização do equipamento;
6.5.1.16. Suportar a rollback de configuração e imagem;
6.5.1.17. Possuir e fornecer geração de mensagens de syslog para eventos relevantes ao sistema;
6.5.1.18. Possuir configuração de múltiplos syslog servers para os quais o equipamento irá enviar as mensagens de syslog;
6.5.1.19. Possuir armazenamento de mensagens de syslog em dispositivo interno ao equipamento;
6.5.1.20. Possuir recurso de gerência via SNMP e implementar SNMPv1, SNMPv2c e SNMPV3;
6.5.1.21. Possuir traps SNMP;
6.5.1.22. Possui suporte a monitoração utilizando RMON através de pelo menos 4 grupos: statistics, history, alarms e events
6.5.1.23. Implementar Debugging: CLI via console e SSH;

6.5.2. Funcionalidades de Segurança Web

6.5.2.1. O equipamento oferecido deverá proteger a infra-estrutura web de ataques contra a camada de aplicação (Camada 7);
6.5.2.2. Deve possuir tecnologia para mitigação de DDoS em camada 7 baseado em análise comportamental, usando o aprendizado;

6.5.2.3. Não deve haver a necessidade de intervenção de usuário para configurar thresholds DoS pois esses valores devem ser autoajustáveis e adpatativos de acordo com mudanças;

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

6.5.2.5. A solução deve suportar o uso de firewall camada 3-4 junto com firewall camada 7 no mesmo equipamento/appliance para evitar problemas com o aumento da latência;

6.5.2.6. O equipamento oferecido deverá possuir a certificação ICSA para Firewall de Aplicação (Web Application Firewall);

6.5.2.7. Permitir a utilização de um modelo positivo de segurança para proteger contra ataques conhecidos aos protocolos HTTP e HTTPS e às aplicações web acessíveis através destes;

6.5.2.8. Possuir política de segurança de aplicações web pré-configurada na solução;

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

6.5.2.10. Permitir a criação de políticas diferenciadas por aplicação;

6.5.2.11. Permite configurar de forma granular, por aplicação protegida, restrições de métodos HTTP permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de cookies;

6.5.2.12. A solução de permitir integrações de produtos:

6.5.2.12.1. Permitir a integração com soluções de análise de vulnerabilidades (Scanner) de terceiros como por exemplo: Trustwave App Scanner (Cenzic), White Hat Sentinel, IBM AppScan, Qualys, Quotium Seeker, HP Webinspect;

6.5.2.12.2. Permitir a integração com Firewall de Database de outros fabricantes;

6.5.2.12.3. Deve se integrar com outras soluções de segurança e análise de logs de outros fabricantes;

6.5.2.13. A solução deve permitir a inspeção de upload de arquivos para os servidores de aplicação. Essa inspeção pode ser feita via integração ICAP. Deve ser possível integrar com diferentes softwares de Antivírus;

6.5.2.14. Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar e aumentar a proteção contra ataques recentes;

6.5.2.15. Deve possuir tecnologia de detecção de anomalias baseado nos IDs dos dispositivos, permitindo a detecção de DoS, ataques de força bruta e ataques de sequestro de sessão. Deve ser possível filtar relatórios por IDs de dispositivos;

6.5.2.16. A solução deve permitir incluir em blacklist os endereços IPs que repetidamente falharem a desafios no browser. Portanto o sistema não precisa utilizar recursos para mitigar trafego enviado por esses endereços Ips. Ao entrar em Blacklist o sistema automaticamente bloqueia os pacotes enviados por esse endereço por um período de tempo;

6.5.2.17. A solução deve suportar e fazer a proteção do tráfego em cima de protocolo WebSocket;

6.5.2.18. A solução deve possibilitar o uso de multiplas formas de logging remoto ao mesmo tempo para a mesma aplicação. Portanto dever ser possível por exemplo logar os requests válidos num servidor de SIEM e os requests inválidos em outro servidor de SIEM de outra marca e modelo;

6.5.2.19. A solução deverá possuir funcionalidade de proteção positiva e segura contra ataques, como:

6.5.2.19.1. Acesso por Força Bruta;

6.5.2.19.2. Ameaças Web AJAX/JSON;

6.5.2.19.3. DoS e DDoS camada 7;

6.5.2.19.4. Buffer Overflow;

6.5.2.19.5. Cross Site Request Forgery (CSRF);

6.5.2.19.6. Cross-Site Scripting (XSS);

6.5.2.19.7. SQL Injection;

6.5.2.19.8. Parameter tampering;

6.5.2.19.9. Cookie poisoning;

6.5.2.19.10. HTTP Request Smuggling;

6.5.2.19.11. Manipulação de campos escondidos;

6.5.2.19.12. Manipulação de cookies;

6.5.2.19.13. Roubo de sessão através de manipulação de cookies;

6.5.2.19.14. Sequestro de sessão;

6.5.2.19.15. Força bruta no browser

6.5.2.19.16. XML bombs/DoS;

6.5.2.19.17. Checagem de consistência de formulários;

6.5.2.19.18. Checagem do cabeçalho do “user-agent” para identificar clientes inválidos;

6.5.2.20. A solução deve suportar o uso de páginas de login AJAX/JSON tanto com configuração manual como descoberta automatica;

6.5.2.21. Deverá ser capaz de identificar e bloquear ataques através de:

6.5.2.21.1. Assinaturas, com atualização periódica da base pelo fabricante;

6.5.2.21.2. As assinaturas devem ser atualizadas durante o período do contrato sem que seja necessário nenhum custo a mais por parte da CONTRATANTE na aquisição de novas licenças ou subscrições. Deve fazer parte da solução de WAF ofertada;

6.5.2.21.3. Regras de verificação personalizadas – política de segurança configurada;

6.5.2.22. Prevenir contra vazamento de dados sensíveis (mensagens de erro HTTP, códigos das aplicações, entre outros) dos servidores de aplicação, retirando os dados ou mascarando a informação nas páginas enviadas aos usuários;

6.5.2.23. Permitir a customização da resposta de bloqueio;

6.5.2.24. Permitir a liberação temporária ou definitiva (white-list) de endereços IP bloqueados por terem originados ataques detectados pela solução;

6.5.2.25. Deve permitir limitar o número de conexões e requisições por IP de origem para cada endereço IP Virtual;

6.5.2.26. Deve permitir adicionar, automaticamente e manualmente, em uma lista de bloqueio, os endereços IP de origem que ultrapassarem o limite estabelecido, por um período de tempo determinado através de configuração;

6.5.2.27. Deve permitir criar lista de exceção (white list) por endereço IP específico ou faixa de sub-rede;
6.5.2.28. A solução deve suportar o modelo de segurança positiva definido pelo OWASP, pelo menos o que consta no TOP 10;
6.5.2.29. Permitir o uso do parâmetro HTTP X-Forwarded-For como parte da política de controle;
6.5.2.30. Deverá implantar, no mínimo, as seguintes funcionalidades:
6.5.2.30.1. Proteção contra Buffer Overflow;
6.5.2.30.2. Checagem de URL;
6.5.2.30.3. Checagem de métodos HTTP utilizados (GET, POST, HEAD, OPTIONS, PUT, TRACE, DELETE, CONNECT);
6.5.2.30.4. Proteção contra envios de comandos SQL escondidos nas requisições enviadas a bases de dados (SQL Injection);
6.5.2.30.5. Proteção contra Cross-site Scripting;
6.5.2.30.6. Funcionalidade de Cookie Encryption;
6.5.2.30.7. Checagem de consistência de formulários;
6.5.2.30.8. Checagem do cabeçalho “user-agent” para identificar clientes inválidos;
6.5.2.31. Deve ser possível verificar o endereço de origem do pacote IP no cabeçalho IP e no parâmetro X-forwarded-for (XFF);
6.5.2.32. Deve suportar a criação de políticas por geo-localização, permitindo que o tráfego de determinado(s) País/Países seja(m) bloqueado(s);
6.5.2.33. Possuir mecanismo de aprendizado automático 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), cookies, arquivos XML e elementos XML;
6.5.2.34. Deve possuir uma funcionalidade de criação automática de políticas, onde a política de segurança é criada e atualizada automaticamente baseando-se no tráfego real observado à aplicação;
6.5.2.35. O perfil aprendido de forma automatizada pode ser ajustado, editado ou bloqueado;
6.5.2.36. Deve possuir proteção baseada em assinaturas para prover proteção contra ataques conhecidos. Deve ser possível desabilitar algumas assinaturas específicas em determinados parâmetros, como uma exceção à regra geral;
6.5.2.37. As atualizações de assinaturas deverão passar por um período configurável de testes, ondes nenhuma requisição que viole a assinatura será bloqueada, apenas informada no relatório. Este processo deve ser automatizado, não sendo necessário criar regras específicas a cada atualização de assinatura;
6.5.2.38. O equipamento oferecido deverá permitir o bloqueio de ataques DoS na camada 7, possuindo também a opção de apenas registrar o ataque, sem tomar nenhuma ação de bloqueio;
6.5.2.39. Deve possuir as seguintes formas de detecção de ataques DoS na camada de aplicação:
6.5.2.39.1. Número de requisições por segundo enviados a uma URL específica;
6.5.2.39.2. Número de requisições por segundo enviados de um IP específico;

6.5.2.39.3. Detecção através de código executado no cliente com o objetivo de detectar interação humana ou comportamento de robôs (bots);
6.5.2.39.4. Número máximo de transações por segundo (TPS) de um determinado IP;
6.5.2.39.5. Aumento de um determinado percentual do número de transações por segundo (TPS);
6.5.2.39.6. Aumento do stress do servidor de aplicação;
6.5.2.40. Deve permitir o bloqueio de robôs (bots) que acessam a aplicação através de detecção automática, não dependendo de cadastros manuais. Robôs conhecidos do mercado, como Google, Yahoo e Microsoft Bing deverão ser liberados por padrão;
6.5.2.41. Deve permitir o cadastro de robôs que podem acessar a aplicação;
6.5.2.42. Possuir política de segurança de aplicações pré-configuradas no equipamento para pelo menos as seguintes aplicações:
6.5.2.42.1. Microsoft ActiveSync v1.0, v2.0;
6.5.2.42.2. Microsoft OWA in Exchange 2003, 2007, 2010;
6.5.2.42.3. Microsoft SharePoint 2003, 2007, 2010;
6.5.2.42.4. Oracle 10g Portal;
6.5.2.42.5. Oracle Application 11i;
6.5.2.42.6. Oracle PeopleSoft Portal;
6.5.2.42.7. SAP NetWeaver;
6.5.2.43. O equipamento oferecido deverá implementar proteção ao JSON (JavaScript Object Notation);
6.5.2.44. Possuir firewall XML integrado – suporte a filtro e validação de funções XML específicas da aplicação;
6.5.2.44.1. Implementar a segurança de web services, através dos seguintes métodos:
6.5.2.44.2. Criptografar/Decriptografar partes das mensagens SOAP;
6.5.2.44.3. Assinar digitalmente partes das mensagens SOAP;
6.5.2.45. Verificação de partes das mensagens SOAP;
6.5.2.45.1. Deverá proteger o protocolo FTP com pelo menos os seguintes métodos:
6.5.2.45.2. Determinar os comandos FTP permitidos;
6.5.2.45.3. Requests FTP anônimos;
6.5.2.46. Checar compliance com o protocolo FTP;
6.5.2.46.1. Proteger contra-ataques de força bruta nos logins;
6.5.2.47. Deverá proteger o protocolo SMTP com pelo menos os seguintes métodos:
6.5.2.47.1. A comunicação deve ser aderente a RFC 2821;
6.5.2.47.2. Limitar o número de mensagens;
6.5.2.47.3. Validar registro SPF do DNS;
6.5.2.47.4. Determinar quais métodos SMTP podem ser utilizados;
6.5.2.48. Deverá proteger contra atraques CSRF (Cross-Site Request Forgery), podendo ser possível especificar quais URLs serão examinadas;
6.5.2.49. Deverá possuir controle de fluxo por aplicação permitindo definir o fluxo de acesso de uma URL para outra da mesma aplicação. Dessa forma qualquer tentativa de acesso a um determido site que não siga o fluxo passando pelas URLs pré-definidas deverá ser bloqueado como uma tentativa de acesso ilegal;

6.5.2.50. A solução deve fornecer relatórios consolidados de ataques com pelo menos os seguintes dados: 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 e PCI Compliance;
6.5.2.51. Deverá permitir o agendamento de relatórios a serem entregues por email;
6.5.2.52. Fornecer diferentes tipos de gráficos de alertas;
6.5.2.53. Deverá exportar as requisições que contém os ataques, pelo menos nos formatos PDF e binário;
6.5.2.54. Deve possuir relatório em tempo real sobre ataques DoS L7, atualizado automaticamente;
6.5.2.55. A solução deve mostrar o impacto de ataques DoS L7 na performance e memória do servidor;
6.5.2.56. Os logs devem indicar o momento de início e final de um ataque DoS L7;
6.5.2.57. Possuir método de mitigação de DoS L7 baseado em:
6.5.2.57.1. CAPTCHA;
6.5.2.57.2. Descarte de todas as requisições de um determinado IP e/ou país suspeito;
6.5.2.57.3. Geolocalização, incluindo a prevenção com CAPTCHA para países suspeitos que ultrapassarem os thresholds;
6.5.2.57.4. Defesa proativa contra Bot, através da injeção de um desafio JavaScript para detectar se é um usuário legítimo ou robô;
6.5.2.58. A solução deve permitir que ao detectar um falso positivo, o administrador aceite a requisição e atualize a política automaticamente;
6.5.2.59. A solução deve classificar o nível de violação de uma requisição, possuindo pelo menos 5 níveis, onde o nível 5 é referente a violação mais grave e, portanto, deve ter prioridade;
6.5.2.60. A solução deve possuir proteção de DDoS L7 baseado em análise comportamental, sem precisar de nenhuma configuração manual;
6.5.2.61. Suportar os protocolos HTTP/1.0, HTTP/1.1 e HTTP/2.0;
6.5.2.62. Suportar codificação HTML "application/x-www-form-urlencoded";
6.5.2.63. Suportar Cookies v0 e v1;
6.5.2.64. Suportar codificação fragmentada (chunked encoding) em requisições e respostas;
6.5.2.65. Suportar compressão de requisições e respostas;
6.5.2.66. Suportar validação de protocolo, como:
6.5.2.66.1. Possibilidade de restringir uso de métodos;
6.5.2.66.2. Possibilidade de restringir protocolos e versões de protocolos;
6.5.2.66.3. Strict (per-RFC) Request Validation;
6.5.2.66.4. Validar caracteres URL-encoded;
6.5.2.66.5. Validação de codificação fora de padrão %uXXYY;
6.5.2.67. Suportar restrições de HTML, como:
6.5.2.67.1. Tamanho do nome de parâmetros;
6.5.2.67.2. Tamanho dos valores de parâmetros;
6.5.2.67.3. Combinação de tamanho de parâmetros (nome e valores);
6.5.2.68. Suportar POST no upload de arquivo;
6.5.2.69. Permitir configurar ou oferecer restrições para tamanho individual de arquivo;

6.5.2.70. Permitir customizar a lógica na inspeção de upload de arquivos;
6.5.2.71. Suporte para os métodos Basic, Digest e NTLM para autenticação;
6.5.2.72. Suporte para autenticação por back end tipo LDAP e Microsoft Active Directory;
6.5.2.73. Capacidade de filtrar cabeçalhos, corpo e status de respostas;
6.5.2.74. Suportar as seguintes técnicas de detecção:
6.5.2.74.1. URL-decoding;
6.5.2.74.2. Terminação Null Byte String;
6.5.2.74.3. Paths auto-referenciados;
6.5.2.74.4. Case de caracteres misturados;
6.5.2.74.5. Uso excessivo de espaços em branco;
6.5.2.74.6. Remoção de comentários;
6.5.2.74.7. Decodificação de entidades HTML;
6.5.2.74.8. Caracteres de escape;
6.5.2.75. Possuir registro de logs com as seguintes características:
6.5.2.75.1. Em cada registro de log de acesso deve ser inserido um identificador de transação HTTP que deve ser único, envolvendo o par requisição/resposta;
6.5.2.75.2. Os registros de log de acesso e eventos devem ser armazenados em arquivo ou em banco de dados que permita a exportação ou em outro formato aberto como CSV ou TXT, podendo ainda serem armazenados localmente ou carregados (upload) em servidor de log via FTP ou SCP ou armazenados em servidor externo de banco de dados;
6.5.2.75.3. Permitir configurar a retenção dos logs por tempo e volume;
6.5.2.75.4. Ter capacidade para detecção, remoção ou codificação de dados sensíveis do log;
6.5.2.76. A solução deverá gerar relatórios com as seguintes características:
6.5.2.76.1. Permitir a filtragem por data ou hora, endereço IP e tipo de incidente;
6.5.2.76.2. Permitir a geração de relatórios sob demanda ou préprogramados periodicamente (diário e semanal);
6.5.2.76.3. Permitir a geração de relatórios em formatos PDF/A (versão aberta) e HTML;
6.5.2.77. Possuir as seguintes características de gerenciamento:
6.5.2.77.1. Facilidade para liberação de regras aprendidas automaticamente que estejam gerando grande quantidade de falso positivo;
6.5.2.77.2. Facilidade para transformar um ataque detectado e considerado falso positivo como regra do firewall;
6.5.2.77.3. Facilidade para aplicar diferentes regras para diversas aplicações;
6.5.2.77.4. Capacidade para customizar regras de negação de serviço;
6.5.2.77.5. Capacidade para combinar detecção e prevenção na construção das regras;
6.5.2.77.6. Capacidade para desfazer a aplicação de uma regra;
6.5.2.77.7. Possuir mecanismos que garantam a capacidade de gerenciamento do equipamento sob condições de alto tráfego;
6.5.2.77.8. Permitir o gerenciamento da configuração com autenticação dos usuários e as autorizações baseadas em perfis (roles);
6.5.2.77.9. Capacidade de gerenciamento remoto dos equipamentos;
6.5.2.78. Apresentar logs e relatórios administrativos com as seguintes características:

6.5.2.78.1. Capacidade para identificar e notificar falhas do sistema ou perda de performance;
6.5.2.78.2. Capacidade de agregação de informações para simplificar a revisão das atividades do dispositivo;
6.5.2.78.3. Capacidade para gerar estatísticas de serviço e sistema;
6.5.2.79. Possuir suporte a XML para proteção de WebServices, em conformidade com a especificação WS-I básico; e com capacidade de restringir métodos do WebService via definição em WSDL;
6.5.2.80. Suportar funções de camuflagem (cloaking);
6.5.2.81. Proteger a aplicação Web contra robôs sofisticados através da combinação de desafios enviados ao browser do usuário e tecnicas avançadas de análise comportamental;
6.5.2.82. A solução deve ecnriptar dados e credenciais na camada de aplicação, sem ter a necessidade de atualizar a aplicação;
6.5.2.83. Essas informações devem ser encriptadas para proteger o login e as credenciais dos usuários e com isso os dados da aplicação;
6.5.2.84. Deve aprender automaticamente o comportamento da aplicação e combinar o comportamento heurístico do tráfego com o stress do servidor de aplicação para determinar uma condição de DDoS;
6.5.2.85. Ao detectar uma condição de DDoS, assinaturas dinâmicas devem ser automaticamente criadas e implementadas em tempo real para proteção da aplicação;
6.5.2.86. Deve possuir uma proteção proativa contra ataques automatizados por robôs e outras ferramentas de ataque;
6.5.2.87. Deve proteger informações sensíveis e confidenciais da interceptação por terceiros, através da criptografia de dados quando ainda no browser do usuário;
6.5.2.88. Deve proteger esses dados criptografados de malwares e keyloggers;
6.5.2.89. Deve possuir proteção contra ataques DDoS, através da análise de comportamento de tráfego usando técnicas de análise de dados e Machine Learning;
6.5.2.90. Através da análise contínua de carga e monitoração de saúde de servidores, deve ser possível identificar anomalias e mitiga-las;
6.5.2.91. Deve ajudar a previnir contra ataques de Credential Stuffing, onde bases de credenciais expostas na Internet são usados para tentativa de acesso de outras aplicações Web.

6.5.3. Funcionalidades de Balanceamento de Carga

6.5.3.1. Deve suportar todas as aplicações comuns de um Switch Layer 7, como:
6.5.3.1.1. Server Load-Balancing;
6.5.3.1.2. Firewall Load-Balancing;
6.5.3.1.3. Proxy Load-Balancing;
6.5.3.2. Deve suportar balanceamento apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente;

6.5.3.3. 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;

6.5.3.4. 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;

6.5.3.5. Possuir recursos para balancear servidores com qualquer hardware, sistema operacional e tipo de aplicação;

6.5.3.6. 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;

6.5.3.7. 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;

6.5.3.8. 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;

6.5.3.9. 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;

6.5.3.10. Suportar os seguintes métodos de balanceamento:

6.5.3.10.1. Round Robin;

6.5.3.10.2. Least Connections;

6.5.3.10.3. Weighted Percentage (por peso);

6.5.3.10.4. Servidor ou equipamento com resposta mais rápida baseado no tráfego real;

6.5.3.10.5. Weighted Percentage dinâmico (baseado no número de conexões);

6.5.3.10.6. Dinâmico, baseado em parâmetros de um determinado servidor ou equipamento, coletados via SNMP ou WMI;

6.5.3.11. A solução deve permitir aplicar criptografia de cookies para a poteção dos cookies utilizados pela aplicação web;

6.5.3.12. Possuir recursos para balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência de sessão dos seguintes tipos:

6.5.3.12.1. Por cookie: inserção de um novo cookie na sessão;

6.5.3.12.2. Por cookie: utilização do valor do cookie da aplicação, sem adição de cookie;

6.5.3.12.3. Por endereço IP destino;

6.5.3.12.4. Por endereço IP origem;

6.5.3.12.5. Por sessão SSL;

6.5.3.12.6. Através da análise da URL acessada;

6.5.3.12.7. Através da análise de qualquer parâmetro no header HTTP;

6.5.3.12.8. Através da análise do MS Terminal Services Session (MSRDP);

6.5.3.12.9. Através da análise do SIP Call ID ou Source IP;

6.5.3.12.10. Através da análise de qualquer informação da porção de dados (camada 7);

6.5.3.13. A solução deve utilizar Cache Array Routing Protocol (CARP) no algoritmo de HASH;

6.5.3.14. Deve suportar os seguintes métodos de monitoramento dos servidores reais:

6.5.3.14.1. ICMP;

6.5.3.14.2. Conexões TCP e UDP pela respectiva porta no servidor;

6.5.3.14.3. 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;

6.5.3.15. Possuir recursos para balanceamento de carga de servidores SIP para VoIP (equipamento SIP PROXY);

6.5.3.16. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor físico;

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

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

6.5.3.19. Realizar Network Address Translation (NAT);

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

6.5.3.21. Realizar Proteção contra Syn flood;

6.5.3.22. Realizar Limpeza de cabeçalho HTTP;

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

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

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

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

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

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

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

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

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

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

6.5.3.33. Suporte a otimização do protocolo TCP para ajustes a parâmetros das conexões clientes e servidor;

6.5.3.34. Deve possuir relatórios das aplicações, com pelos menos os seguintes gráficos:
6.5.3.34.1. Tempo de resposta da aplicação;
6.5.3.34.2. Latência;
6.5.3.34.3. Conexões para conjunto de servidores, servidores individuais;
6.5.3.34.4. Por URL;
6.5.3.35. A ferramenta de relatórios deve possuir pelo menos os seguintes filtros para a geração dos gráficos:
6.5.3.35.1. Servidores virtuais;
6.5.3.35.2. Servidores balanceados;
6.5.3.35.3. URLs;
6.5.3.35.4. Países de origem, baseados em geolocalização (GEOIP);
6.5.3.35.5. Dispositivos de origem do cliente (user agent);
6.5.3.36. Deve possuir framework unificado para configuração da aplicação;
6.5.3.37. A solução deve ter a capacidade de realizar cache transparente das respostas DNS;
6.5.3.38. A Solução deve ter suporte a sFlow;
6.5.3.39. A solução deve possuir múltiplos domínios de roteamento em IPv4 e IPv6;
6.5.3.40. A solução deve permitir que cada domínio de roteamento utilize BGP, OSPF e RIP em IPv4 e IPv6;
6.5.3.41. A solução deve suportar Equal Cost Multipath (ECMP);
6.5.3.42. A solução deve realizar Bidirectional Forward Detection (BFD);
6.5.3.43. A solução deve ter suporte a Stream Control Transmission Protocol (SCTP);
6.5.3.44. Deve ter suporte a Transport Layer Security (TLS) Server Name Indication (SNI);
6.5.3.45. 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;
6.5.3.46. A solução deve ter suporte a TLS 1.2, SHA 2 Cipher e SHA256 hash;
6.5.3.47. A solução deve ter suporte a criptografia Perfect Forward Secrecy não apenas para troca de chaves RSA;
6.5.3.48. 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:
6.5.3.48.1. Deve ser possível configurar o tamanho máximo da fila;
6.5.3.48.2. Deve ser possível configurar o tempo máximo de permanência na fila;
6.5.3.49. A solução deve realizar Controle de Banda Estático para grupos de aplicações e rede;
6.5.3.50. A solução deve realizar Controle de Banda Dinâmico por aplicação e usuário;
6.5.3.51. A solução deve realizar Controle de Banda baseado em domínio de roteamento;
6.5.3.52. Permitir tráfego por parâmetros de QoS (Quality of Service) ou rateshaping, com pelo menos 2 (duas) filas para priorização de tráfego baseada na camada de aplicação;

6.5.3.53. 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;
6.5.3.54. A solução deve permitir a priorização de tráfego de entrada para determinadas aplicações;
6.5.3.55. A solução deve permitir a criação de túneis IP por domíno de roteamento utilizando GRE, IPIP, EtherIP, PPP;
6.5.3.56. A solução deve permitir a criação de túneis IP transparente utilizando GRE e IPIP;
6.5.3.57. Fornecer recursos para o uso de servidores (reals) no mesmo Virtual Server;
6.5.3.58. Possuir suporte ao protocolo SPDY e HTTP 2.0;
6.5.3.59. O equipamento deve possuir suporte ao espelhamento de conexões FTP, Telnet, HTTP, UDP, SSL;
6.5.3.60. O equipamento deverá permitir a sincronização das configurações de forma automática e manualmente, forçando a sincronização apenas no momento desejado;
6.5.3.61. Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar a distribuição dinâmica de tráfego e aumentar a proteção contra ataques;
6.5.3.62. 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;
6.5.3.63. Essa linguagem de programação deve permitir a importação de pacotes, garantindo assim que a agilidade e flexibilidade no compartilhamento dos scripts;
6.5.3.64. Permitir a criação de políticas através de interface gráfica web para manipulação de tráfego através de lógica para pelo menos os seguintes operadores: GEOIP, http-basic-auth, http-cookie, httpheader, http-host, http-method, http-referer, http-set-cookie, httpstatus, http-uri e http-version;
6.5.3.65. Deve ser possível tomar as seguintes ações através dessas políticas:
6.5.3.65.1. Bloqueio de tráfego;
6.5.3.65.2. Reescrita e manipulação de URL;
6.5.3.65.3. Registro de tráfego (log);
6.5.3.65.4. Adição de informação no cabeçalho HTTP;
6.5.3.65.5. Redirecionamento do tráfego para um membro específico;
6.5.3.65.6. Selecionar uma política específica para Aplicação Web;
6.5.3.66. A solução deverá ser capaz de fazer log de todas as sessões, onde os registros deverão conter no mínimo:
6.5.3.66.1. Endereço IP de origem;
6.5.3.66.2. Porta TCP ou UDP de origem;
6.5.3.66.3. Endereço IP de destino;
6.5.3.66.4. Porta TCP ou UDP de destino;
6.5.3.66.5. Protocolo de camada 4 (TCP ou UDP);
6.5.3.66.6. Data e hora da mensagem;
6.5.3.66.7. URL acessada;

6.5.3.67. 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;

6.5.3.68. A solução deve suportar controle de versão da política de configuração de forma a permitir fazer roll back de políticas aplicadas;

6.6. **LOTE 02 – ITEM 02 – CAPACIDADE (PACOTE) ADICIONAL PARA SOLUÇÃO EM FIREWALL DE APLICAÇÕES WEB.** As condições que irão delinear a entrega do item deverão ter, no mínimo, os seguintes requisitos:

6.6.1. O pacote de capacidade adicional deverá entregar um upgrade de licença válida, no mínimo, pelo tempo restante de licenciamento da solução em WAF instalada no TCE-AP;

6.6.2. A capacidade adicional deverá entregar suporte a uma taxa de transmissão de no mínimo 1,5 x 20 Mbps.

6.6.3. A capacidade adicional deverá entregar suporte de no mínimo 2x 5 FQDNs, onde cada FQDN representa uma aplicação web;

6.6.4. A capacidade adicional deverá entregar suporte a no mínimo 1,5 x 210 GB /dia de tráfego agregado;

6.7. LOTE 02 – ITEM 03 – TREINAMENTO OFICIAL DA SOLUÇÃO EM WAF. As condições que irão delinear a entrega do serviço item deverão ter, no mínimo, os seguintes requisitos:

6.7.1. A CONTRATADA deverá fornecer inscrição para TREINAMENTO OFICIAL na solução integrada de segurança, cujo escopo deve cobrir os equipamentos e softwares ofertados no LOTE 01, ITENS 01 e 02;

6.7.2. O TREINAMENTO OFICIAL poderá ser dividido em módulos de cursos complementares entre si;

6.7.3. Cada treinamento deverá prever a capacitação para 1 turma com até 6 pessoas, a serem nomeadas pela CONTRATANTE;

6.7.4. O treinamento poderá ser fornecido na modalidade online (EAD), in-loco em centro autorizado de treinamento do fabricante, ou na modalidade in-company em Macapá/AP e em local de providência e responsabilidade da CONTRATADA;

6.7.5. Os treinamentos deverão ser iniciados até 40 (quarenta) dias após assinatura do Contrato.

6.7.6. A CONTRATADA deverá apresentar, em até 20 (vinte) dias após assinatura do Contrato, um Plano de Treinamento que será avaliado e aprovado pela equipe técnica da CONTRATANTE;

6.7.7. O Plano citado no item anterior deverá apresentar o programa de cada treinamento com conteúdo, carga horária, duração em dias, modalidade e avaliações de aprendizagem;

6.7.8. O Treinamento deverá ser oficial do fabricante em cada uma das ferramentas, contemplando módulos, com conteúdo teórico e prático, com programas mínimos que abordem toda a instalação, configuração, e implementação de 100% dos recursos e funcionalidades;

6.7.9. O treinamento oficial do fabricante deverá prover todas as ferramentas necessárias para atender aos requisitos citados na alínea anterior;
6.7.10. Só será admitido a entrada em funcionamento de componentes da solução sem que tenha havido o respectivo treinamento caso seja de interesse expresso por parte da CONTRATANTE, não tornando o mesmo indispensável sob nenhum aspecto ou condição.
6.7.11. O instrutor que irá ministrar o treinamento deverá ser certificado pelo fabricante da solução;
6.7.12. A CONTRATADA arcará com todas as despesas relativas aos seus profissionais e técnicos envolvidos nas atividades do treinamento;
6.7.13. Caso o treinamento seja fornecido na modalidade EAD, a CONTRATADA deverá inscrever os participantes informados pela CONTRATANTE na primeira turma disponível após a assinatura do contrato ou em data definida pela DAINF-TCE/AP, de acordo com o calendário de turmas disponíveis;
6.7.14. Caso o treinamento seja fornecido na modalidade in-loco ou incompany, a CONTRATADA deverá definir o período do treinamento, incluindo a carga horária diária em comum acordo com a CONTRATANTE logo após a assinatura do contrato de forma independente dos prazos de entrega dos equipamentos e softwares deste termo de referência;
6.7.15. Nos casos das modalidades in-loco ou in-company A CONTRATADA deverá prover toda a estrutura acessória para os treinamentos, incluindo coffee-break;
6.7.16. O treinamento deverá incluir laboratório virtual para a simulação das configurações e testes;
6.7.17. O Conteúdo do treinamento deverá ser de natureza teórica e prática, devendo abranger todas as funcionalidades, componentes e softwares, em seus aspectos mais relevantes e, em especial, envolvendo aqueles relacionados à solução implantada no ambiente computacional do TCE/AP, contendo:
6.7.17.1. Instalação e configuração inicial;
6.7.17.2. Conceitos e configuração de todos os recursos presentes na Solução em WAF, dentre os quais a exemplo:
6.7.17.2.1. Proteções de ataques à aplicações;
6.7.17.2.2. ACLs
6.7.17.2.3. Proteções DDoS;
6.7.17.2.4. Balanceamento e falhas;
6.7.17.2.5. CDN;
6.7.17.2.6. Deployment;
6.7.17.2.7. Dashboards;
6.7.17.2.8. Análise e gerencia de falsos positivos;
6.7.17.2.9. Gerenciamento e relatórios;
6.7.17.2.10. Monitoramento;
6.7.17.2.11. Autenticação;
6.7.18. A CONTRADA poderá fornecer materiais didáticos em formatos digitais;

6.7.19. A CONTRATADA deverá emitir certificados de conclusão do treinamento. Deverá constar no certificado a data de início e fim, carga horária, nome do instrutor, nome do treinamento e nome do participante;

6.8. **LOTE 02 – ITEM 04 – INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO EM WAF.** A entrega do serviço deverá cumprir os seguintes requisitos:

6.8.1. Requisitos Gerais

6.8.1.1. Iniciar a execução das atividades de entrega, instalação e configuração dos equipamentos e softwares da Solução em WAF de acordo com os prazos definidos em cronograma, contados a partir da emissão de Ordem de Serviço - OS pela CONTRATANTE;

6.8.1.2. No 3o (terceiro) dia após a emissão da Ordem de Serviço, deverá ser realizada reunião presencial na SEDE do TCE-AP, em Macapá/AP, com o objetivo de apresentar sua metodologia de trabalho, planejamento e coordenação das atividades de entrega da Solução em WAF;

6.8.1.3. A CONTRATADA deverá apresentar um Plano de Implantação, em até 15 (quinze) dias da emissão da Ordem de Serviço pelo CONTRATANTE, contendo a documentação detalhada das atividades de entrega, instalação, configuração e testes dos equipamentos e softwares que compõem a Solução em WAF;

6.8.1.4. O processo de instalação e configuração da Solução em WAF deverá ser acompanhado pela equipe técnica indicada pela CONTRATANTE;

6.8.1.5. Para garantir que a instalação não afetará o ambiente da CONTRATANTE, os procedimentos e atividades deverão ser realizados por técnicos qualificados pelo fabricante nos produtos envolvidos, comprovado no ato de entrega do PLANO DE IMPLANTAÇÃO;

6.8.1.6. O Plano de Implantação deverá dispor também sobre o cronograma de execução, previsão de recursos humanos e materiais, pessoas envolvidas e atividades a serem desenvolvidas pela CONTRATADA e indicar os principais riscos e forma de mitigação, contendo também os seguintes itens:

6.8.1.6.1. Detalhar os procedimentos para entrega, retirada das embalagens e conferência dos equipamentos, softwares e acessórios entregues;

6.8.1.6.2. Detalhar informações sobre as etapas de instalação física dos equipamentos, incluindo: distribuição dos equipamentos pelos racks, movimentação de equipamentos existentes, conexões elétricas e lógicas necessárias, definição de nomes dos equipamentos e endereçamento de gerência IP;

6.8.1.6.3. Indicar de forma detalhada as condições de rollback de cada mudança no ambiente do TCE-AP;

6.8.1.6.4. Elaborar atividades de teste de operação da solução e planos de testes para os diversos componentes da Solução em WAF que comprovem o funcionamento das configurações aplicadas;

6.8.2. Requisitos de entrega

6.8.2.1. Entregar todos os equipamentos, licenças de softwares e acessórios no prazo máximo de até 45 (quarenta e cinco) dias, a contar da data de emissão da Ordem de Serviço pela CONTRATANTE

6.8.2.2. Entregar os equipamentos novos e de 1º uso juntamente com todos os itens acessórios de hardware e de software necessários à perfeita instalação e funcionamento, incluindo cabos, conectores, interfaces, suportes, drivers de controle e programas de configuração, conforme especificações constantes deste Termo de Referência;

6.8.2.3. Entregar os equipamentos devidamente protegidos e embalados, originais e lacrados, os quais devem evitar danos de transporte e manuseio;

6.8.2.4. Desembalar os equipamentos após a entrega nas dependências do CONTRATANTE;

6.8.2.5. Entregar os equipamentos e softwares, a suas expensas, bem como instalar e realizar todos os testes necessários à verificação do perfeito funcionamento dos produtos fornecidos;

6.8.2.6. Entregar todos os documentos comprobatórios de garantia indicados neste Termo de Referência;

6.8.2.7. Entregar toda a documentação técnica em meio eletrônico, completa e atualizada, contendo os manuais e guias de utilização;

6.8.2.8. Instalar os equipamentos e softwares nas datas e horários definidos no Plano de Implantação, sob supervisão da equipe técnica da CONTRATANTE;

6.8.2.9. Aceitar que as atividades de instalação e configuração dos equipamentos e softwares da Solução em WAF deverão ocorrer localmente nas dependências do TCE-AP, devendo ser realizada em horários que não coincidam com o expediente do CONTRATANTE. O TCE-AP poderá autorizar a realização de atividades durante o horário de expediente se, ao seu exclusivo critério, entender que não oferece risco ao funcionamento de sua rede de computadores e serviços em produção;

6.8.2.10. Aceitar que o processo de entrega, instalação e configuração dos equipamentos e softwares da Solução em WAF deverá ser acompanhado pela equipe técnica indicada pelo CONTRATANTE;

6.8.2.11. Aceitar que caso a implantação de qualquer elemento da Solução em WAF cause interferência na correta operação da rede de dados do TCE-AP, a CONTRATADA deverá alocar profissionais com qualificação suficiente para corrigir o problema ou retornar o ambiente à condição anterior à implantação;

6.8.2.12. A execução dos serviços de entrega, instalação e configuração dos equipamentos e softwares da Solução em WAF deverão contemplar, no mínimo, os seguintes itens:

6.8.2.12.1. Instalação física e ativação dos equipamentos da solução;

6.8.2.12.2. Realizar a integração dos equipamentos da solução a rede LAN existente no TCE-AP, sem interrupção no funcionamento normal dos serviços de TI. Caso exista a necessidade de interrupção de qualquer equipamento ou serviço em produção para a integração dos equipamentos, o prazo para realização e a duração da janela de manutenção deverão ser acordados com o TCE-AP;

6.8.2.12.3. Instalar e configurar todas as funcionalidades exigidas na especificação técnica da solução, bem como quaisquer outras disponíveis adicionalmente nos diversos componentes da solução mediante solicitação da equipe do TCE-AP;

6.8.2.12.4. Realizar testes de operação da solução que comprovem o funcionamento dos recursos;

6.8.2.12.5. Atualizar o plano de implantação com todas as informações que represente a topologia física e lógica, a configuração final e as regras aplicadas aos equipamentos e softwares da Solução em WAF;

6.8.2.13. Receber cópia do Termo de Recebimento Provisório (TRP) após entrega dos equipamentos, softwares, acessórios, Plano de Implantação e demais documentações da solução, conforme descrito no cronograma do ANEXO II. A finalização da entrega deverá ser formalizada mediante comunicação escrita da CONTRATADA ao CONTRATANTE. O recebimento provisório realizar-se-á no prazo máximo de 15 (quinze) dias corridos, contados da comunicação da empresa, desde que não haja pendências a cargo da CONTRATADA;

6.8.2.14. Concluir no prazo de 45 (quarenta e cinco) dias corridos, contados a partir da emissão do Termo de Recebimento Provisório, os serviços de instalação e configuração dos equipamentos e softwares da Solução em WAF, realizando todas as atividades programadas para esta etapa;

6.8.2.15. Receber cópia do Termo de Recebimento Definitivo (TRD), após a formalização por escrito da CONTRATADA referente à conclusão das atividades de entrega, instalação e configuração dos equipamentos e softwares da Solução em WAF. O recebimento definitivo realizar-se-á no prazo máximo de 10 (dez) dias corridos, contados da comunicação da empresa, desde que não haja pendências a cargo da CONTRATADA;

6.8.2.16. Realizar, por 30 (trinta) dias corridos após a emissão do Termo de Recebimento Definitivo (TRD), operação assistida da solução, esclarecendo dúvidas e realizando ajustes na configuração visando à melhor utilização dos recursos oferecidos nos equipamentos que compõem a solução;

6.8.2.17. O período de operação assistida da Solução em WAF poderá ser executado remotamente, 3 (três) horas por dia, no período entre 08h e 18h;

6.8.2.18. O período de operação assistida faz parte dos serviços de instalação e configuração, não representando ônus adicional para o CONTRATANTE;

6.8.3. Repasse de conhecimento

6.8.3.1. A CONTRATADA deverá realizar a repasse de conhecimento para a equipe técnica da CONTRATANTE por meio de documentação e apresentação estruturada sobre todo o processo de instalação e configuração das tecnologias da Solução em WAF;

6.8.3.2. O repasse de conhecimento deverá iniciar imediatamente ao passo que antecede a emissão do Termo de Recebimento Provisório;

6.8.3.3. A transferência de conhecimento deverá abordar, no mínimo, as seguintes funcionalidades da solução:

6.8.3.3.1. Proteções de ataques à aplicações;
6.8.3.3.2. Serviços de segurança;
6.8.3.3.3. Análise e gerencia de falsos positivos;
6.8.3.3.4. Gerenciamento e relatórios;
6.8.3.3.5. Monitoramento;
6.8.3.3.6. Autenticação;
6.8.3.3.7. CDN;
6.8.3.3.8. DDoS;
6.8.3.3.9. Deployment;
6.8.3.3.10. Gerenciamento e elaboração de relatórios da solução;

6.8.3.4. O repasse de conhecimento deverá ser realizada em Macapá/AP, cabendo a CONTRATADA providenciar as instalações para este fim. A transferência de conhecimento poderá ser realizada na sede do CONTRATANTE caso manifeste interesse;

6.8.3.5. O repasse conhecimento deverá ser de natureza teórica e prática, devendo abranger os equipamentos e softwares fornecidos em seus aspectos relacionados à solução implantada no ambiente computacional do Tribunal de Contas, contendo, no mínimo:

6.8.3.5.1. Orientação sobre a topologia lógica da solução implantada, mostrando a interligação dos componentes físicos da solução, informando as interconexões realizadas com a infraestrutura existente no CONTRATANTE;
6.8.3.5.2. Descrição do hardware e software de cada equipamento;
6.8.3.5.3. Configuração e administração dos equipamentos;
6.8.3.5.4. Descrição geral da plataforma de gerência;
6.8.3.5.5. Diagnóstico de problemas;
6.8.3.5.6. Configuração de alarmes, eventos e rotinas para os serviços de monitoramento;
6.8.3.5.7. Gerência de desempenho e segurança;
6.8.3.5.8. Manipulação de objetos MIB, SNMP e RMON para monitoração;
6.8.3.5.9. Resolução de problemas “troubleshooting”;
6.8.3.5.10. Relatórios;

6.8.3.6. Um plano de repasse conhecimento deverá ser previamente aprovado pela CONTRATANTE, e eventuais mudanças de conteúdo poderão ser solicitadas;

6.8.3.7. O cronograma efetivo do repasse de conhecimento será definido em conjunto com o CONTRATANTE, na primeira reunião de planejamento;

6.8.3.8. Caso a transferência de conhecimento não seja satisfatória com relação à profundidade do conteúdo apresentado ou domínio dos temas por parte do instrutor, a CONTRATADA deverá complementar, sem ônus adicional, o repasse dos pontos considerados pela CONTRATANTE como insatisfatórios;

6.8.3.9. A transferência de conhecimento deverá ser realizada por técnicos qualificados e certificados pelos fabricantes dos equipamentos e softwares da solução ofertada;

6.9. LOTE 03 – ITEM 01 – SOLUÇÃO DE GERENCIAMENTO DE LOGS E VENTOS DE SEGURANÇA (SIEM), COM LICENÇA PERPÉTUA, SUPORTE E ATUALIZAÇÃO PARA 36 MESES DE USO. As condições que irão delinear a entrega do item deverão ter, no mínimo, os seguintes requisitos:

6.9.1. Características Gerais:

6.9.1.1. O solicitado é uma solução completa de SIEM (Security Information and Event Management), que deve implementar todos os requisitos previstos neste Termo de Referência.

6.9.1.2. A proposta deverá contemplar todas as licenças de software, sistemas operacionais, bancos de dados, subscrições ou qualquer outro tipo de licenciamento necessário para seu completo funcionamento, de acordo com as características e prazos estipulados;

6.9.1.3. A infraestrutura de virtualização será fornecida pela contratante;

6.9.1.4. A solução ofertada poderá ser composta por um ou mais softwares, desde que sejam do mesmo fabricante, totalmente interoperáveis entre si, gerenciados através de uma interface única e em número de licenças suficientes para atender aos volumes de dados e/ou quantidades de eventos solicitados.

6.9.1.5. Todos os itens do lote deverão ser fornecidos/prestados pela mesma empresa;

6.9.1.6. Devido aos modelos de licenciamento dos mais importantes fabricantes serem diferentes, o fornecedor da solução poderá ofertar ao menos uma das formas de licenciamento citadas a seguir, ou combinação delas, devidamente descrito na proposta comercial, desde que atenda os volumes de dados e eventos esperados:

6.9.1.6.1. Por volume de dados recebidos e tratados, partindo de 30 GBytes/dia e sem limite de ativos geradores de eventos;

6.9.1.6.2. Por quantidade de eventos recebidos e tratados por segundo em tempo real, partindo de 1000 EPS (Eventos por Segundo) medidos pela quantidade instantânea (rajada) ou 15000 FPM (Flows por minuto);

6.9.1.6.3. Por quantidade de eventos recebidos e tratados por segundo, partindo de 600 EPS (Eventos por segundo) medidos pela média diária, sem limite de Flows por minuto;

6.9.1.6.4. As licenças de software deverão ser registradas junto ao fabricante da solução em nome da contratante;

6.9.1.7. O primeiro ano de suporte deverá estar incluso no valor deste item;

6.9.1.8. O tipo de licenciamento é licença perpétua para instalação onpremises, com possibilidade de atualização enquanto durar o contrato de suporte;

6.9.1.9. Deverá ser ofertada a última versão estável de todos os softwares;

6.9.1.10. Poderão ser considerados servidores para armazenamento de logs e tratamento de eventos em separado.

6.9.2. Requisitos de Software e Funcionalidades

6.9.2.1. Todos os componentes da solução devem permitir sua instalação em ambiente virtual, servidores físicos de propósito genérico ou em appliance virtual especializado;

6.9.2.2. Deverá permitir o controle de acesso dos usuários à solução por meio de autenticação em serviço de diretório como Microsoft Active Directory e LDAP;

6.9.2.3. A comunicação entre os componentes da solução deve ser feita através de criptografia, garantindo a autenticidade, confidencialidade e integridade dos dados, utilizando o protocolo TCP/IP;

6.9.2.4. Juntamente com a subscrição de atualização dos componentes da solução pelo período do contrato de suporte, a contratada deverá prover acesso à biblioteca de casos de uso do fabricante, que contenha conteúdo para download que inclua pacotes especializados de dashboards e coletores desenvolvidos pelo fabricante;

6.9.2.5. A solução deverá implementar o protocolo IPv6;

6.9.2.6. A solução deverá ser capaz de coletar, aplicar parsing, normalizar e categorizar os eventos dos dispositivos monitorados em tempo próximo ao real (near-real-time);

6.9.2.7. Será considerada nesse Termo de Referência a seguinte definição para conector: software desenvolvido e suportado pelo fabricante da solução que tem como função básica fazer a interface com o dispositivo monitorado, recebendo ou buscando eventos relevantes que serão inseridos na solução, contendo obrigatoriamente documentação de todos coletores nativos com informações detalhadas de configurações de cada ativo suportado;

6.9.2.8. A coleta de eventos de dispositivos (ativos geradores de eventos) não suportados nativamente pode ser feita através de conectores customizados. Estes conectores customizados devem utilizar padrões de mercado como o SYSLOG e outros;

6.9.2.9. Ser capaz de coletar, no mínimo, os logs dos sitemas e ativos listado abaixo:

6.9.2.10. Firewalls: Fortigate 100D, Fortigate 400E, Fortigate 501E, PfSense;

6.9.2.11. Roteadores e Switches DATACOM;

6.9.2.12. Roteadores e Switches Cisco;

6.9.2.13. Hypervisors: VMware ESXi e Hyper-V

6.9.2.14. Sistemas Operacionais: Linux, FreeBSD, OpenBSD e Windows Server (2008, 2012 e 2016);

6.9.2.15. Antivírus Kaspersky;

6.9.2.16. Servidores de Aplicação e WEB: Apache2, Tomcat, JBOSS Wildfly e IIS;

6.9.2.17. Containers: DOCKER e OpenVZ;

6.9.2.18. VPN SSL e IPSEC;

6.9.2.19. Para coleta de logs deve suportar, no mínimo, os seguintes métodos:

6.9.2.19.1. Syslog (UDP, TCP e TLS);

6.9.2.19.2. FTP;

6.9.2.19.3. MySQL;

6.9.2.19.4. MS SQL;

6.9.2.19.5. Oracle;

6.9.2.19.6. API;

6.9.2.19.7. JSON;

6.9.2.19.8. CEF

6.9.2.20. Suportar o modo de criptografia em todos os conectores;

6.9.2.21. A solução deve ser capaz de normalizar e categorizar os eventos em um padrão único;

6.9.2.22. O coletor da solução deverá ser capaz de armazenar os dados localmente (cache) em caso de indisponibilidade da comunicação com os destinos dos eventos;

6.9.2.23. O envio dos dados em cache deve ocorrer imediatamente após a disponibilização do destino do evento;

6.9.2.24. A solução deve ser capaz de enviar o evento bruto (raw) para o armazenamento e consulta futura;

6.9.2.25. A solução deve ser capaz de inserir nos eventos normalizados metadados sobre georreferência dos mesmos;

6.9.2.26. Tanto os eventos de segurança quanto os de conformidade devem ser normalizados para um único padrão de eventos utilizados pela solução;

6.9.2.27. A solução deve permitir múltiplos perfis de configuração;

6.9.2.28. A solução deverá realizar no conector a agregação de eventos semelhantes que ocorram dentro de um limite de tempo e quantidade de eventos específicos, devendo permitir agregar os eventos cuja única diferença seja o horário de ocorrência;

6.9.2.29. Possuir a funcionalidade de atualização, gerenciamento e configuração centralizados de todos os conectores distribuídos da solução;

6.9.2.30. Permitir a categorização manual de eventos (já normalizados) que não se encaixem em nenhuma categoria existente, cuja nova categoria poderá ser aplicada nos eventos futuros de mesma característica;

6.9.2.31. Deverá armazenar no mínimo os seguintes dados: eventos, alertas, e toda informação pertinente à solução, tais como configuração, usuários, trilhas de auditoria e informações de depuração;

6.9.2.32. Ser capaz de armazenar logs por tempo determinado e personalizado, conforme necessidade do órgão;

6.9.2.33. Ter a capacidade de definir políticas diferentes de retenção dos dados on-line por tecnologia, conectores, dispositivos e compliance, ou seja, poderão ser definidos tempos de retenção diferentes para cada tipo de dados mantidos no banco de dados da solução, disponíveis para consulta imediata;

6.9.2.34. De forma a permitir seu uso em auditorias e processos forenses, não deveráser possível a seleção, alteração e exclusão de eventos individuais, exceto por contas de usuário com perfil adequado a esta tarefa;

6.9.2.35. Permitir o expurgo dos dados de forma automática de acordo com a personalização do prazo de retenção que precede o expurgo;

6.9.2.36. Deverá permitir a utilização de volumes de armazenamento locais e externos. Deverá permitir a segregação de tipos de eventos diferentes em grupos lógicos de armazenamento diferentes, com políticas de retenção diferentes, de forma a permitir a otimização de performance;

6.9.2.37. Deverá permitir exportar eventos para formato pdf e csv;

6.9.2.38. Deverá permitir que o usuário defina quais campos do evento serão exportados;

6.9.2.39. Deverá implementar funcionalidade de ajuda (helper) para facilitar a criação de queries;
6.9.2.40. Deverá implementar assistente gráfico para criação de queries;
6.9.2.41. Deverá implementar indexação baseada em campo e palavrachave para acelerar buscas;
6.9.2.42. Deverá implementar alertas por syslog, SNMP e e-mail;
6.9.2.43. Deverá permitir visualização em tempo real de eventos que atendam ao critério de seleção definido pelo usuário;
6.9.2.44. Possuir relatórios pré-configurados (templates) separados em categorias;
6.9.2.45. Deverá suportar pelo menos os formatosde relatórios: pdf e csv;
6.9.2.46. Permitir o agendamento de geração de relatórios e o envio dos mesmos por e-mail;
6.9.2.47. Possuir ferramenta ou interface gráfica para desenho de modelos de relatórios ou dashboards personalizados;
6.9.2.48. Apresentar painéis de controles gráficos (dashboards) que mostrem o status do ambiente, dos logs de eventos, além de apresentar resultados de consultas tempestivas, quando se fizerem necessárias;
6.9.2.49. Deverá implementar tecnologia de pesquisa que permita encontrar as informações armazenadas na solução a partir de uma única interface de pesquisa;
6.9.2.50. Apresentar relatórios de eventos, alertas e incidentes em nível técnico (analítico, drill down) e gerencial (sintético / dashboards);
6.9.2.51. Permitir pesquisa nos eventos, e a partir de um dado evento ou conjunto de eventos, mostrar de forma gráfica seus relacionamentos e permitir o drill-down (detalhamento) até o nível dos dados brutos (raw), para efetiva investigação de incidentes, identificação de causa raiz e análise forense;
6.9.2.52. Armazenar os eventos e os alertas, inclusive os normalizados, de forma indexada;
6.9.2.53. Deverá permitir que os campos de logs de dispositivos diferentes estejam presentes no mesmo resultado, bem como deverá ser possível a seleção dos campos que estarão presentes no resultado;
6.9.2.54. Deverá ser fornecido com solução de gerenciamento central com as seguintes características mínimas:
6.9.2.54.1. Deverá implementar, de forma centralizada, a configuração de políticas e a monitoração de todos os conectores e da solução de centralização de eventos;
6.9.2.54.2. Deverá permitir a implementação de atualização e distribuição de novas políticas de segurança pelos elementos/componentes gerenciados;
6.9.2.54.3. Deverá possuir regras de monitoração pré-configuradas, as quais podem ser editadas ou apagadas;
6.9.2.54.4. Deverá interagir diretamente com a biblioteca de casos de uso do fabricante da solução para download e atualizações de conteúdo;
6.9.2.54.5. Deverá possuir interface WEB acessível por HTTPS e CLI por SSH, com suporte ao padrão UTF-8;
6.9.2.54.6. Deverá possuir tela de monitoração com as seguintes características:

6.9.2.54.6.1. Tabela com percentuais e gráfico de pizza do status dos elementos/componentes monitorados agregados por tipo, mostrando o número de elementos em cada estado, bem como o número total de nós;

6.9.2.54.6.2. Listagem de todos os elementos/componentes que estão reportando problemas;

6.9.2.54.6.3. Permitir a visualização do sumário de monitoração por tipo de produto;

6.9.2.55. Deverá possuir tela de gerenciamento de configuração para gerenciar e criar configurações, sincronizar a configuração entre componentes/elementos e automatizar a configuração inicial dos mesmos;

6.9.2.56. Deverá permitir o backup e a restauração da configuração da solução de gerenciamento, assim como a configuração de usuários e grupo de usuários;

6.9.2.57. Deverá ser possível visualizar o consumo de licenças da solução;

6.9.2.58. Deverá permitir a visualização das taxas em eventos por segundo (EPS), flows por minuto (FPM) ou volume de dados diário (conforme a métrica adotada pela solução) de entrada e de saída de cada conector;

6.9.2.59. Deverá permitir a visualização dos dispositivos gerenciados por localização, host e tipo;

6.9.2.60. Permitir adição, visualização, edição e exclusão da localização de dispositivos;

6.9.2.61. Permitir a adição de atributos de um dispositivo, visualização e remoção de dispositivos, visualização de todos os dispositivos de uma localidade e varredura (scan) de dispositivos para detecção de novos conectores;

6.9.2.62. Deverá permitir a apresentação de árvore hierárquica de dispositivos;

6.9.2.63. Deverá apresentar para cada dispositivo: nome ou endereço IP, versão do agente (se aplicável), status de problemas encontrados no dispositivo, modelo, tipo e versão;

6.9.2.64. Deverá implementar as seguintes ações nos elementos/componentes de centralização de logs: reboot, shutdown, upgrade remoto, editar ou remover a configuração, configurar um ou múltiplos elementos/componentes;

6.9.2.65. Deverá implementar o gerenciamento deconectores: adição, edição de conectores, atualização de parâmetros, gerenciar os destinos e failover de logs de múltiplos conectores, envio de comandos e edição de conectores customizados;

6.9.2.66. Deverá ser fornecido com os seguintes modelos para o desenvolvimento de conectores customizados: arquivo, banco de dados por ID, múltiplos bancos de dados, expressão regular para arquivo, expressão regular para pasta de arquivos, SNMP, banco de dados por tempo e arquivo xml. Caso não existam estes modelos específicos, a solução deverá possibilitar a criação de interpretadores (parsers) customizados, para o desenvolvimento de conectores customizados;

6.9.2.67. Deverá permitir o gerenciamento dos eventos arquivados;

6.9.2.68. Deverá permitir o gerenciamento de peers de centralizadores de logs;

6.9.2.69. Deverá permitir que a configuração dos elementos/componentes seja criada diretamente na solução de gerenciamento, importada de um elemento ativo e enviada a múltiplos elementos gerenciados;
6.9.2.70. Deverá permitir a configuração de usuários e grupos de usuários, seus dispositivos associados e os respectivos privilégios (administrador, relatórios, pesquisas, operação, gerenciamento);
6.9.2.71. Deverá implementar dashboards com funcionalidade de drill down para visualização do status dos dispositivos monitorados;
6.9.2.72. Deverá implementar visão de topologia que apresente graficamente, a relação entre os dispositivos de origem dos eventos, os conectores e os destinos, com a visualização do status, tipo de dispositivo, número de dispositivos de cada tipo, dispositivos ativos e inativos;
6.9.2.73. O correlacionador deve ser capaz de receber eventos dos agentes, coletores e de outros correlacionadores;
6.9.2.74. O correlacionador deve efetuar a análise dos eventos em near realtime (tempo próximo ao real);
6.9.2.75. Deve permitir ao administrador a criação de novas regras e a edição das existentes;
6.9.2.76. O correlacionador deve identificar anomalias baseadas em eventos e análise de dados históricos conforme período a ser definido;
6.9.2.77. O correlacionador deve possuir a capacidade de detectar automaticamente padrões de ataques especializados que acontecem ao longo do tempo e que não foram previstos ou observados anteriormente;
6.9.2.78. O correlacionador deve permitir a correlação de eventos e alertas com dados existentes em listas (watchlist). Deve permitir também a criação de novas listas e a personalização das existentes;
6.9.2.79. O correlacionador deve ter a capacidade de fazer a correlação entre eventos oriundos de:
6.9.2.79.1. Agentes (ou solução similar) ou coletores de outros correlacionadores;
6.9.2.79.2. Diferentes ativos do mesmo tipo (por exemplo, Firewall A e Firewall B);
6.9.2.79.3. Ativos de diferentes tipos (por exemplo, Firewall A e IPS B e Proxy C);
6.9.2.79.4. Ativos e Banco de Dados (por exemplo, catraca e consultas (queries) a banco de dados);
6.9.2.80. O correlacionador deve ser capaz de inserir os alertas gerados no próprio fluxo de correlação ou no fluxo de eventos. Deve permitir a correlação de tais alertas/eventos, derivados de alertas, com novos eventos e/ou regras, no intuito de detectar padrões mais complexos de ameaças ou violações de conformidade;
6.9.2.81. O correlacionador deve priorizar os eventos e alertas com base, pelo menos, nos seguintes critérios:
6.9.2.81.1. Severidade do evento;
6.9.2.81.2. Criticidade do ativo;
6.9.2.81.3. Existência de vulnerabilidade no ativo;
6.9.2.82. Possuir a funcionalidade de geração de incidentes em módulos de tratamento interno;

6.9.2.83. Possuir a funcionalidade de definição de prioridade para os eventos, alertas e incidentes;
6.9.2.84. Como resultado da aplicação de regras, o correlacionador deve ser capaz de executar ações automáticas como: enviar e-mail, enviar mensagem para o usuário conectado ao console, executar comandos e abrir caso na ferramenta de incidentes interna;
6.9.2.85. O correlacionador deve armazenar os eventos, alertas e incidentes na base de dados da solução;
6.9.2.86. A solução deve possuir um mecanismo de correlação avançada para processar e comparar informações de logs de diferentes fontes e fluxos de rede;
6.9.2.87. A solução deve incluir regras pré-programadas (out-of-the-box) tanto para normalização de logs quanto para correlação de eventos, bem como permitir que se escrevam / definam regras próprias / personalizadas;
6.9.2.88. Fornecer a funcionalidade de geração de alertas (sonoros e/ou visuais) para incidentes de alta criticidade detectados na correlação de eventos;
6.9.2.89. A solução deve notificar e associar comportamentos anômalos baseados em múltiplos eventos que ocorrerem em um determinado período de tempo;
6.9.2.90. A correlação de eventos deve possuir uma linha de base (baseline) comportamental da rede, definido por suas regras de correlações, fornecendo alertas sempre que ocorrer algum evento fora do comportamento normal;
6.9.2.91. A solução deve possuir a capacidade de prover contextualização de dados de alertas de fontes diversas (ativos de rede e/ou segurança, servidores, aplicações, etc.) em um único console, otimizando com isso a capacidade e prazos de análise no processo de resposta a incidentes de segurança;
6.9.2.92. A solução deve possibilitar o envio de notificações ou alertas baseados no fator de importância e criticidade do ativo/dispositivo definidos pela contratada;
6.9.2.93. Permitir a instalação de certificado digital para prover o acesso seguro, e configurar o repositório de certificados confiáveis;
6.9.2.94. Manter seu próprio log de auditoria;
6.9.2.95. Ter a funcionalidade de visualização de eventos e alertas de segurança em tempo real;
6.9.2.96. Permitir testar as regras com eventos reais capturados anteriormente e mantidos na base de dados da solução;
6.9.2.97. Permitir a inserção manual de anotações em alertas;
6.9.2.98. A solução deve ser capaz de notificar os administradores, ou usuários cadastrados, caso algum dispositivo monitorado pare de enviar eventos;
6.9.2.99. Deve permitir a visualização de eventos e alertas de segurança em tempo próximo ao real, sem necessidade de refazer consultas no banco de dados e/ou storage para atualização das visualizações (atualização da visualização de eventos e alertas de segurança em contexto de memória);
6.9.2.100. Deverá se integrar com a ferramenta de incidentes externos, permitindo que o SIEM abra casos na ferramenta externa diretamente e automaticamente;
6.9.2.101. Deve permitir o registro de ações tomadas e planejadas.

6.10. **LOTE 03 – ITEM 02 – CAPACIDADE ADICIONAL PARA SOFTWARE DE GERENCIAMENTO DE LOGS E EVENTOS DE SEGURANÇA (SIEM), COM LICENÇA PERPÉTUA, SUPORTE E ATUALIZAÇÃO PARA O PRIMEIRO ANO DE USO.** As condições que irão delinear a entrega do item deverão ter, no mínimo, os seguintes requisitos:

6.10.1. Entende-se como Capacidade Adicional: pacotes de licenciamento de software para ampliação da capacidade da solução de software ofertada no ITEM 01;
6.10.2. Cada pacote adicional previsto neste ITEM 02 devem contemplar, no mínimo, de acordo com o tipo de licenciamento proposto para o ITEM 01 do LOTE em referência;
6.10.3. Por volume de dados recebidos e tratados: 12,5 GBytes/dia de logs. 4.3.2.2 Por quantidade de eventos recebidos e tratados por segundo: 500 EPS (Eventos por segundo) medidos pelo máximo instantâneo (rajada) ou 6800 FPM (Flows por minuto);
6.10.4. Por quantidade de eventos recebidos e tratados por segundo: 300 EPS (Eventos por segundo) medidos pela média diária;
6.10.5. O primeiro ano de suporte deverá estar incluso no valor deste item;
6.10.6. O tipo de licenciamento é licença perpétua para instalação onpremises, com possibilidade de atualização enquanto durar o contrato de suporte;
6.10.7. Deverá ser ofertado a última versão estável de todos os softwares;

6.11. **LOTE 03 – ITEM 03 – SUPORTE ANUAL PARA SOFTWARE DE GERENCIAMENTO DE LOGS E EVENTOS DE SEGURANÇA (SIEM), PARA MÓDULO PRINCIPAL DESCRITO NO ITEM 01, NÃO INCLUINDO OS PRIMEIROS 36 MESES DE USO.** As condições que irão delinear a entrega do item deverão ter, no mínimo, os seguintes requisitos:
6.11.1. Subscrição de suporte, oferecida pelo fabricante, suficientes para suportar todos os softwares que compuserem a solução ofertada;
6.11.2. Deverá contemplar todos os softwares oferecidos no item 01, em módulos anuais;
6.11.3. Poderão ser adquiridos pacotes para até 3 anos de suporte, subsequentes e ininterruptos, não incluído o primeiro ano de uso;
6.11.4. Os serviços de suporte, com exceção das atividades realizadas até a homologação do produto, poderão ser feitos por telefone, email, Webex ou outro meio tecnológico acordado entre as partes;
6.11.5. Deverá permitir a atualização do produto, seja para novas versões, seja para instalação de patches de atualizações e segurança;
6.11.6. Em dias úteis a contratada deverá atender aos chamados para suporte em, no máximo, 8h, e a solução definitiva ou de contorno deverá ocorrer em, no máximo, 72h;

6.12. **LOTE 03 – ITEM 04 – TREINAMENTO OFICIAL PARA SOLUÇÃO DE SIEM.** As condições que irão delinear a entrega do item deverão ter, no mínimo, os seguintes requisitos:

6.12.1. A CONTRATADA deverá fornecer inscrição para TREINAMENTO OFICIAL na solução de SIEM, cujo escopo deve cobrir os softwares ofertados no LOTE 03, ITEM 01;

6.12.2. O TREINAMENTO OFICIAL poderá ser dividido em módulos de cursos complementares entre si;

6.12.3. Cada treinamento deverá prever a capacitação para 1 turma com até 6 pessoas, a serem nomeadas pela CONTRATANTE;

6.12.4. O treinamento poderá ser fornecido na modalidade online (EAD), in-loco em centro autorizado de treinamento do fabricante, ou na modalidade in-company em Macapá/AP e em local de providência e responsabilidade da CONTRATADA;

6.12.5. Os treinamentos deverão ser iniciados até 40 (quarenta) dias após assinatura do Contrato.

6.12.6. A CONTRATADA deverá apresentar, em até 20 (vinte) dias após assinatura do Contrato, um Plano de Treinamento que será avaliado e aprovado pela equipe técnica da CONTRATANTE;

6.12.7. O Plano citado no item anterior deverá apresentar o programa de cada treinamento com conteúdo, carga horária, duração em dias, modalidade e avaliações de aprendizagem;

6.12.8. O Treinamento deverá ser oficial do fabricante em cada uma das ferramentas, contemplando módulos, com conteúdo teórico e prático, com programas mínimos que abordem toda a instalação, configuração, e implementação de 100% dos recursos e funcionalidades;

6.12.9. O treinamento oficial do fabricante deverá prover todas as ferramentas necessárias para atender aos requisitos citados na alínea anterior;

6.12.10. Só será admitido a entrada em funcionamento de componentes da solução sem que tenha havido o respectivo treinamento caso seja de interesse expresso por parte da CONTRATANTE, não tornando o mesmo indispensável sob nenhum aspecto ou condição.

6.12.11. O instrutor que irá ministrar o treinamento deverá ser certificado pelo fabricante da solução;

6.12.12. A CONTRATADA arcará com todas as despesas relativas aos seus profissionais e técnicos envolvidos nas atividades do treinamento;

6.12.13. Caso o treinamento seja fornecido na modalidade EAD, a CONTRATADA deverá inscrever os participantes informados pela CONTRATANTE na primeira turma disponível após a assinatura do contrato ou em data definida pela DAINF-TCE/AP, de acordo com o calendário de turmas disponíveis;

6.12.14. Caso o treinamento seja fornecido na modalidade in-loco ou incompany, a CONTRATADA deverá definir o período do treinamento, incluindo a carga horária diária em comum acordo com a CONTRATANTE logo após a assinatura do contrato de forma independente dos prazos de entrega dos equipamentos e softwares deste termo de referência;

6.12.15. Nos casos das modalidades in-loco ou in-company A CONTRATADA deverá prover toda a estrutura acessória para os treinamentos, incluindo coffee-break;

6.12.16. O treinamento deverá incluir laboratório virtual para a simulação das configurações e testes;

6.12.17. O Conteúdo do treinamento deverá ser de natureza teórica e prática, devendo abranger todas as funcionalidades, componentes e softwares, em seus aspectos mais relevantes e, em especial, envolvendo aqueles relacionados à solução implantada no ambiente computacional do TCE/AP, contendo:

6.12.17.1. Instalação e configuração inicial;

6.12.17.2. Conceitos e apresentação das funcionalidades;

6.12.17.3. Análise de ataques;

6.12.17.4. Verificação de políticas e conformidades (compliance);

6.12.17.5. Administração de logs;

6.12.17.6. Coleta e processamento de Eventos;

6.12.17.7. Coleta e processamento de Flow;

6.12.17.8. Administração de ativos;

6.12.17.9. Scanners;

6.12.17.10. Reporting;

6.12.17.11. Integração com serviços de diretório (SSO);

6.12.17.12. Monitoramento e gestão da ferramenta com vistas às atividades de rotina.

6.12.18. A CONTRADA poderá fornecer materiais didáticos em formatos digitais;

6.12.19. A CONTRATADA deverá emitir certificados de conclusão do treinamento. Deverá constar no certificado a data de início e fim, carga horária, nome do instrutor, nome do treinamento e nome do participante;

6.13. **LOTE 03 – ITEM 05 – INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO DE SIEM.** As condições que irão delinear a entrega do item deverão ter, no mínimo, os seguintes requisitos:

6.13.1. Instalar e configurar os sistemas operacionais, bancos de dados e softwares da solução, de forma presencial, na sede do TCE-AP;

6.13.2. Configurar, no mínimo 20 (vinte) fontes de dados, incluindo seus coletores, a serem escolhidos pela contratada, dentro de sua base de ativos;

6.13.3. Repassar os conhecimentos básicos para incluir novas fontes de dados, configurar coletores, criar relatórios e modelos, criar filtros de pesquisa, fazer backups, criar dashboards, gerenciar usuários e utilizar os principais recursos da solução;

6.13.4. Apresentar plano de instalação e configuração, que deverá contemplar todos os tipos de ativos em produção na rede da contratante;

6.13.5. Requisitos Gerais

6.13.5.1. Iniciar a execução das atividades de entrega, instalação e configuração dos equipamentos e softwares da Solução em SIEM de acordo com os prazos

definidos em cronograma, contados a partir da emissão de Ordem de Serviço - OS pela CONTRATANTE;

6.13.5.2. No 3o (terceiro) dia após a emissão da Ordem de Serviço, deverá ser realizada reunião presencial na SEDE do TCE-AP, em Macapá/AP, com o objetivo de apresentar sua metodologia de trabalho, planejamento e coordenação das atividades de entrega da Solução em SIEM;

6.13.5.3. A CONTRATADA deverá apresentar um Plano de Implantação, em até 15 (quinze) dias da emissão da Ordem de Serviço pelo CONTRATANTE, contendo a documentação detalhada das atividades de entrega, instalação, configuração e testes dos equipamentos e softwares que compõem a Solução em SIEM;

6.13.5.4. O processo de instalação e configuração da Solução de SIEM deverá ser acompanhado pela equipe técnica indicada pela CONTRATANTE;

6.13.5.5. Para garantir que a instalação não afetará o ambiente da CONTRATANTE, os procedimentos e atividades deverão ser realizados por técnicos qualificados pelo fabricante nos produtos envolvidos, comprovado no ato de entrega do PLANO DE IMPLANTAÇÃO;

6.13.5.6. O Plano de Implantação deverá dispor também sobre o cronograma de execução, previsão de recursos humanos e materiais, pessoas envolvidas e atividades a serem desenvolvidas pela CONTRATADA e indicar os principais riscos e forma de mitigação, contendo também os seguintes itens:

6.13.5.6.1. Detalhar os procedimentos para entrega, licenciamento, cópias de software, documentação, etc.;

6.13.5.6.2. Detalhar informações sobre as etapas de instalação dos softwares, incluindo: provisionamento de infraestrutura processamento, storage e network), tal como requisitos de conexões lógicas e demais necessários;

6.13.5.6.3. Indicar de forma detalhada as condições de rollback de cada mudança no ambiente do TCE-AP;

6.13.5.6.4. Elaborar atividades de teste de operação da solução e planos de testes para os diversos componentes da Solução em SIEM que comprovem o funcionamento das configurações aplicadas;

6.13.6. Requisitos de entrega

6.13.6.1. Entregar todos os equipamentos, licenças de softwares e acessórios no prazo máximo de até 45 (quarenta e cinco) dias, a contar da data de emissão da Ordem de Serviço pela CONTRATANTE

6.13.6.2. Entregar todos os recursos, fisicos ou digitais pertinentes e necessários à perfeita instalação e funcionamento da solução em SIEM, conforme especificações constantes deste Termo de Referência;

6.13.6.3. Entregar os equipamentos e softwares, a suas expensas, bem como instalar e realizar todos os testes necessários à verificação do perfeito funcionamento dos produtos fornecidos;

6.13.6.4. Entregar todos os documentos comprobatórios de garantia indicados neste Termo de Referência;

6.13.6.5. Entregar toda a documentação técnica em meio eletrônico, completa e atualizada, contendo os manuais e guias de utilização;

6.13.6.6. Instalar os equipamentos e softwares nas datas e horários definidos no Plano de Implantação, sob supervisão da equipe técnica da CONTRATANTE;

6.13.6.7. Aceitar que as atividades de instalação e configuração dos equipamentos e softwares da Solução em SIEM deverão ocorrer localmente nas dependências do TCE-AP, devendo ser realizada em horários que não coincidam com o expediente do CONTRATANTE. O TCE-AP poderá autorizar a realização de atividades durante o horário de expediente se, ao seu exclusivo critério, entender que não oferece risco ao funcionamento de sua rede de computadores e serviços em produção;

6.13.6.8. Aceitar que o processo de entrega, instalação e configuração dos equipamentos e softwares da Solução em SIEM deverá ser acompanhado pela equipe técnica indicada pelo CONTRATANTE;

6.13.6.9. Aceitar que caso a implantação de qualquer elemento da Solução em SIEM cause interferência na correta operação da rede de dados do TCE-AP, a CONTRATADA deverá alocar profissionais com qualificação suficiente para corrigir o problema ou retornar o ambiente à condição anterior à implantação;

6.13.6.10. A execução dos serviços de entrega, instalação e configuração dos equipamentos e softwares da Solução em SIEM deverão contemplar, no mínimo, os seguintes itens:

6.13.6.10.1. Instalação completa da solução;

6.13.6.10.2. Realizar a integração dos equipamentos da solução a rede LAN existente no TCE-AP, sem interrupção no funcionamento normal dos serviços de TI. Caso exista a necessidade de interrupção de qualquer equipamento ou serviço em produção para a integração dos equipamentos, o prazo para realização e a duração da janela de manutenção deverão ser acordados com o TCE-AP;

6.13.6.10.3. Instalar e configurar todas as funcionalidades exigidas na especificação técnica da solução, bem como quaisquer outras disponíveis adicionalmente nos diversos componentes da solução mediante solicitação da equipe do TCE-AP;

6.13.6.10.4. Realizar testes de operação da solução que comprovem o funcionamento dos recursos;

6.13.6.10.5. Atualizar o plano de implantação com todas as informações que represente a topologia física e lógica, a configuração final e as regras aplicadas aos equipamentos e softwares da Solução em SIEM;

6.13.6.11. Receber cópia do Termo de Recebimento Provisório (TRP) após entrega dos equipamentos, softwares, acessórios, Plano de Implantação e demais documentações da solução, conforme descrito no cronograma do ANEXO II. A finalização da entrega deverá ser formalizada mediante comunicação escrita da CONTRATADA ao CONTRATANTE. O recebimento provisório realizar-se-á no prazo máximo de 15 (quinze) dias corridos, contados da comunicação da empresa, desde que não haja pendências a cargo da CONTRATADA;

6.13.6.12. Concluir no prazo de 45 (quarenta e cinco) dias corridos, contados a partir da emissão do Termo de Recebimento Provisório, os serviços de instalação e

configuração dos equipamentos e softwares da Solução em SIEM, realizando todas as atividades programadas para esta etapa;

6.13.6.13. Receber cópia do Termo de Recebimento Definitivo (TRD), após a formalização por escrito da CONTRATADA referente à conclusão das atividades de entrega, instalação e configuração dos equipamentos e softwares da Solução em SIEM. O recebimento definitivo realizar-se-á no prazo máximo de 10 (dez) dias corridos, contados da comunicação da empresa, desde que não haja pendências a cargo da CONTRATADA;

6.13.6.14. Realizar, por 30 (trinta) dias corridos após a emissão do Termo de Recebimento Definitivo (TRD), operação assistida da solução, esclarecendo dúvidas e realizando ajustes na configuração visando à melhor utilização dos recursos oferecidos nos equipamentos que compõem a solução;

6.13.6.15. O período de operação assistida da Solução em SIEM poderá ser executado remotamente, 3 (três) horas por dia, no período entre 08h e 18h;

6.13.6.16. O período de operação assistida faz parte dos serviços de instalação e configuração, não representando ônus adicional para o CONTRATANTE;

6.13.7. Repasse de conhecimento

6.13.7.1. A CONTRATADA deverá realizar a repasse de conhecimento para a equipe técnica da CONTRATANTE por meio de documentação e apresentação estruturada sobre todo o processo de instalação e configuração das tecnologias da Solução em SIEM;

6.13.7.2. O repasse de conhecimento deverá iniciar imediatamente ao passo que antecede a emissão do Termo de Recebimento Provisório;

6.13.7.3. A transferência de conhecimento deverá abordar, no mínimo, as seguintes funcionalidades da solução:

6.13.7.4. Instalação e configuração inicial;

6.13.7.5. Conceitos e apresentação das funcionalidades;

6.13.7.6. Análise de ataques;

6.13.7.7. Verificação de políticas e conformidades (compliance);

6.13.7.8. Administração de logs;

6.13.7.9. Coleta e processamento de Eventos;

6.13.7.10. Coleta e processamento de Flow;

6.13.7.11. Administração de ativos;

6.13.7.12. Scanners;

6.13.7.13. Dashboards;

6.13.7.14. Reporting;

6.13.7.15. Integração com serviços de diretório (SSO);

6.13.7.16. Monitoramento e gestão da ferramenta com vistas às atividades de rotina.

6.13.7.17. O repasse de conhecimento deverá ser realizada em Macapá/AP, cabendo a CONTRATADA providenciar as instalações para este fim. A transferência de conhecimento poderá ser realizada na sede do CONTRATANTE caso manifeste interesse;

6.13.7.18. O repasse conhecimento deverá ser de natureza teórica e prática, devendo abranger os equipamentos e softwares fornecidos em seus aspectos

relacionados à solução implantada no ambiente computacional do Tribunal de Contas, contendo, no mínimo:

6.13.7.18.1. Orientação sobre a topologia lógica da solução implantada, demostrando a interligação dos componentes da solução (arquitetura), informando as interconexões realizadas com a infraestrutura existente no CONTRATANTE;

6.13.7.18.2. Configuração e administração da Solução em SIEM;

6.13.7.18.3. Descrição geral da plataforma de gerência;

6.13.7.18.4. Diagnóstico de problemas;

6.13.7.18.5. Configuração de alarmes, eventos e rotinas para os serviços de monitoramento;

6.13.7.18.6. Gerência de desempenho;

6.13.7.18.7. Manipulação de objetos MIB, SNMP e RMON para monitoração;

6.13.7.18.8. Resolução de problemas “troubleshooting”;

6.13.7.18.9. Relatórios;

6.13.7.19. Um plano de repasse conhecimento deverá ser previamente aprovado pela CONTRATANTE, e eventuais mudanças de conteúdo poderão ser solicitadas;

6.13.7.20. O cronograma efetivo do repasse de conhecimento será definido em conjunto com o CONTRATANTE, na primeira reunião de planejamento;

6.13.7.21. Caso a transferência de conhecimento não seja satisfatória com relação à profundidade do conteúdo apresentado ou domínio dos temas por parte do instrutor, a CONTRATADA deverá complementar, sem ônus adicional, o repasse dos pontos considerados pela CONTRATANTE como insatisfatórios;

6.13.7.22. A transferência de conhecimento deverá ser realizada por técnicos qualificados e certificados pelos fabricantes dos equipamentos e softwares da solução ofertada;

7. DO ACOMPANHAMENTO E DA FISCALIZAÇÃO

7.1. A execução dos serviços será fiscalizada e acompanhada por servidor designado pela administração, com competências pertinentes ao objeto contratado;

7.2. As decisões e providências que ultrapassarem a competência do Fiscal de Contrato, deverão ser solicitadas ao Diretor Administrativo do Tribunal de Contas do Estado do Amapá, em tempo hábil, para a adoção das medidas convenientes;

7.3. A licitante vencedora deverá indicar preposto, aceito pela Administração do Tribunal de Contas do Estado do Amapá, para representá-la sempre que for necessário;

8. DA ATESTAÇÃO E DO RECEBIMENTO DOS PRODUTOS E SERVIÇOS.

8.1. A atestação das Notas Fiscais referente aos equipamentos e materiais, tal como à execução dos serviços especificados, caberá ao Fiscal de Contrato designado pela Administração do Tribunal de Contas do Estado do Amapá;

8.2. O recebimento definitivo dos serviços será efetuado pelo Fiscal de Contrato, mediante termo circunstanciado, assinado pelas partes, após o decurso do prazo máximo de até 5(cinco) dias, necessário à observação, ou à vistoria que comprove a adequação do objeto aos termos contratuais, observado o disposto no art. 69 da Lei nº 8.666/93;

8.3. Os serviços somente serão considerados concluídas e em condições de serem recebidas, após cumpridas todas as obrigações assumidas pela licitante vencedora e atestada sua conclusão pela DIRETORIA DA AREA DE INFORMATICA DO TCE/AP;

9. PROPRIEDADE, SIGILO E RESTRIÇÕES

9.1. Na execução dos serviços, a empresa contratada cumprirá todos os padrões de segurança e regras de uso e de controle de acesso às instalações do TCE-AP. A empresa contratada se compromete a manter sigilo acerca das informações obtidas e geradas no decorrer de todo o contrato;

9.2. Durante a execução dos serviços, a Contratada deverá observar as Políticas de Controle de Acesso definidas pelo TCE-AP;

10. PAGAMENTO

10.1. O pagamento será efetuado através de Ordem Bancária, mediante depósito na conta-corrente da Contratada, no prazo de até 10 (dez) dias úteis após a assinatura do Termo de Recebimento Definitivo (TRD), com a formalização por escrito da CONTRATADA referente à conclusão das atividades de entrega, sejam de treinamentos ou instalação e configuração dos equipamentos e softwares, em consonância com todos as especificações dos LOTES/ITEMS pertinentes;

10.2. O pagamento deverá ser acompanhado da respectiva Nota Fiscal/Fatura, emitida em, no mínimo, 2 (duas) vias, de acordo com a Nota de Empenho, a qual será conferida e atestada pelo servidor ou comissão responsável pelo recebimento, observado o estabelecido no art. 5º da Lei 8.666/93, e desde que não ocorra fator impeditivo provocado pela Contratada;

10.3. No caso do valor do contrato, representado pela Nota de Empenho, não ultrapassar o limite de que trata o inciso II do art. 24, da Lei nº 8.666/93, o pagamento deverá ser efetuado no prazo de até 5 (cinco) dias úteis, nas condições referidas no item;

10.4. Nenhum pagamento será efetuado à Contratada enquanto pendente de liquidação qualquer obrigação financeira que lhe for imposta, em virtude de penalidade ou inadimplência, sem que isso gere direito ao pleito de reajustamento dos preços ou correção monetária;

11. DA GARANTIA

11.1. Fornecer serviços de manutenção e suporte técnico pelo período de 36 (trinta e seis) meses, contados da data de emissão do Termo de aceite de recebimento dos produtos, contemplando o suporte técnico para os produtos especificados no LOTE 01, itens 01 e 02; LOTE 02 item 01; e LOTE 03, item 01;

11.2. Abertura de chamados para suporte on-line sem limitação;

11.3. Para a abertura dos chamados, deverá ser fornecido um canal de atendimento (site de internet, e-mail e/ou ligação), sem custos para a CONTRATANTE para consultas dos chamados em aberto, abertura de novos chamados técnicos, envio de arquivos para análise por parte do suporte, orientação quanto a dúvidas e informações sobre as tecnologias envolvidas;

11.4. Deve contemplar suporte on-line do Fabricante pelo período vigente, com no mínimo, as seguintes características:

11.4.1. O suporte do fabricante deve ter um sistema de abertura de chamados para acompanhamento – funcionando 24 horas por dia e 7 dias por semana. Para atendimento telefônico, deve operar preferencialmente em língua Portuguesa, ou obrigatoriamente com a língua Inglesa, e pelo menos em regime 8x5.

11.4.2. Deve assegurar a utilização de novas versões de software da solução sem ônus a Licitante, sempre que esta estiver disponível a qualquer cliente;

11.4.3. Deve permitir o acesso à base de conhecimento da solução;

11.5. Da garantia dos ITEM 01, LOTE 01 e LOTE 02, espera-se:

11.5.1. A garantia deverá ser de 36 meses.

11.5.2. 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 do TCE-AP, para cada caso particular. Caso o TCE-AP 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;

11.6. A garantia terá seu prazo contabilizado a contar a partir da data de entrega dos produtos e homologação dos serviços;

12. EXECUÇÃO DO CONTRATO

12.1. As licitantes vencedoras deverão fornecer o serviço dentro do prazo proposto e aceito pelo Tribunal de Contas do estado do Amapá no certame licitatório, de acordo com o descrito neste termo de referência;

12.2. Todos os produtos e serviços deverão ser possuir garantia especificada na proposta, e deverá considerar no mínimo 03 meses para serviços e 06 meses para materiais e 12 meses para equipamentos;

12.3. Em caso de substituição de qualquer componente da solução, este deverá ser realizado no prazo máximo de 24 (doze) horas, após a notificação pelo TCE/AP;

12.4. O horário de realização de serviços fica estipulado: de segunda à sexta-feira, das 7:30 às 18:00, excluindo-se feriados coincidentes. Os serviços deverão ser acompanhados por representantes do Setor de Patrimônio, dos Serviços Gerais e pela Fiscalização dos Contratos;

12.5. Para todo fornecimento de serviços, um cronograma executivo deverá ser apresentado pela empresa contratada ainda na fase de mobilização. Este cronograma servirá como instrumento para determinar o cumprimento dos prazos;

13. PRAZOS

13.1. Os prazos pertinentes ao objeto deste termo de referência deverão cumpridos conforme relação:

13.1.1. Lote 01, Itens 01 e 02: **28 dias**;

13.1.2. Lote 01, Item 03: **60 dias**;

13.1.3. Lote 01, Item 04**: 45 dias**;

13.1.4. Lote 02, Item 01: **28 dias**;

13.1.5. Lote 02, Item 02: **21 dias**;

13.1.6. Lote 02, Item 03: **60 dias**;

13.1.7. Lote 02, Item 04: **45 dias**;

13.1.8. Lote 03, Item 01: **21 dias**;

13.1.9. Lote 03, Item 02 e 03: **21 dias**;

13.1.10. Lote 03, Item 04: **60 dias**;

13.1.11. Lote 04, Item 05: **45 dias**;

13.2. Estes prazos admitem prorrogação, mantidas as condições iniciais do contrato e assegurada a manutenção do equilíbrio econômico-financeiro, desde que configurada uma das condições previstas nos incisos do parágrafo 1º, Art. 57 da lei 8.666/93;

14. OBRIGAÇÕES DO TRIBUNAL DE CONTAS (CONTRATANTE);

14.1. Será responsabilidade do Tribunal de Contas, representado pelos seus dirigentes e servidores prepostos ou representantes, para os efeitos deste TERMO DE REFERÊNCIA:

14.1.1. Verificar os equipamentos instalados, e, quando atenderem ao objeto do contrato, aprová-los;

14.1.2. Liquidar o empenho e efetuar os pagamentos das faturas à empresa vencedora do certame licitatório dentro dos prazos preestabelecidos em contrato;

14.1.3. Prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATADA;

14.1.4. Permitir acesso dos empregados da empresa contratada nas suas dependências para a entrega do equipamento e para as devidas instalações;

14.1.5. Prestar as informações e os esclarecimentos pertinentes que venham a ser solicitados pelo representante da empresa contratada;

14.1.6. Comunicar oficialmente à empresa contratada quaisquer falhas ocorridas;
14.1.7. Lavrar e entregar à empresa contratada o Termo de Recebimento, bem como atestar a Nota Fiscal no prazo estipulado;
14.1.8. Efetuar o pagamento no prazo previsto neste Termo de Referência;
14.1.9. Fornecer demais informações à empresa contratada para a perfeita execução do objeto;
14.1.10. Realizar a Fiscalização do objeto para a perfeita execução do objeto.

15. OBRIGAÇÕES DA CONTRATADA

15.1. Fornecer, ao executar os serviços, materiais de alta qualidade e de primeiro uso;
15.2. Os materiais deverão apresentar total conformidade com todas as especificações e requisitos detalhados neste termo de referência;
15.3. Manter a compatibilidade com o padrão e qualidade de materiais já instalados nas dependências do TCE-AP;
15.4. Ser responsável, em relação aos seus empregados, por todas as despesas decorrentes da execução dos serviços, tais como: salários, seguros de acidente, taxas, impostos e contribuições, indenizações, vale-refeição, vale-transporte e outras que porventura venham a ser criadas e exigidas pelo Governo;
15.5. Manter os seus empregados sujeitos às normas disciplinares do Tribunal de Contas do Estado do Amapá, porém, sem qualquer vínculo empregatício com o órgão;
15.6. Manter, ainda, os seus empregados identificados, quando em trabalho, devendo substituir imediatamente qualquer um deles que seja considerado inconveniente à boa ordem e às normas disciplinares do Tribunal de Contas do Estado do Estado do Amapá;
15.7. Responder pelos danos causados diretamente à Administração do Tribunal de Contas do Estado do Amapá ou a terceiros, decorrentes de sua culpa ou dolo, quando da execução dos serviços, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento pelo Tribunal de Contas do Estado do Amapá;
15.8. Responder, também, por quaisquer danos causados diretamente aos bens de propriedade do Tribunal de Contas do Estado do Amapá, quando esses tenham sido ocasionados por seus empregados durante a execução dos serviços;
15.9. Arcar com despesa decorrente de qualquer infração, seja qual for, desde que praticada por seus empregados na execução dos serviços ou no recinto do Tribunal de Contas do Estado do Amapá;
15.10. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, as etapas dos serviços em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais utilizados, no prazo máximo de 5 (cinco) dias ou no prazo para tanto estabelecido pela fiscalização;
15.11. Permitir, aos técnicos do Tribunal de Contas do Estado do Amapá e àqueles a quem o Tribunal formalmente indicar, acesso às suas instalações e a todos os locais onde estiverem sendo estocados materiais relacionados com o objeto;

15.12. Responsabilizar-se pelas despesas decorrentes da rejeição de componentes, materiais e serviços pela Fiscalização do Tribunal de Contas do Estado do Amapá e pelos atrasos acarretados por esta rejeição;
15.13. Responsabilizar-se por todo transporte necessário à execução dos serviços, bem como por ensaios, testes ou provas necessários, inclusive os mal executados;
15.14. Providenciar, às suas expensas, atestado de similaridade de desempenho dos materiais apresentados, junto a instituições ou fundações capacitadas para este fim, quando do uso de similar ao descrito nas Especificações Técnicas, sempre que a fiscalização do Tribunal de Contas do Estado do Amapá julgar necessário;
15.15. Responsabilizar-se pela perfeita execução e completo acabamento dos serviços, obrigando-se a prestar assistência técnica e administrativa necessária para assegurar andamento conveniente dos trabalhos;
15.16. Submeter à aprovação da Fiscalização do Tribunal de Contas do Estado do Amapá, o(s) nome(s) e o(s) dado(s) demonstrativo(s) da respectiva capacidade técnica do responsável técnico que, porventura, venha a substituir o originalmente indicado;
15.17. Executar os serviços e comprovar, após instalação, o funcionamento e entrega através de relatório de atividade técnica específico;
15.18. Comunicar à Divisão de Dados e Redes, qualquer anormalidade verificada na instalação e prestar os devidos esclarecimentos sempre que solicitados;
15.19. Cumprir, às suas próprias expensas, todas as cláusulas contratuais que definam suas obrigações;

16. GARANTIA DO CONTRATO

16.1. Para se garantir o fiel cumprimento de todas as cláusulas e condições do contrato, a LICITANTE deverá optar por uma das modalidades de garantia previstas nos incisos de I a III, do parágrafo primeiro, do art. 56, da Lei nº 8.666/93.

17. VIGÊNCIA DO CONTRATO

17.1. O contrato terá prazo de execução de **12(doze) meses** prorrogáveis por até **48(quarenta e oito) meses** nos termos do Art. 57, inciso IV da Lei 8666/93 e suas alterações;

Elaborado por:

_____

(assinado digitalmente)
MAYK CAMPELO PINHEIRO
Chefe da Divisão de Dados e Redes

Revisado por:

_____

(assinado digitalmente)
MARCUS PINHEIRO DE SANTANA
Diretor da Área de Informática

ANEXO I do TR – PLANILHA DE PREÇOS

LOTE 1					
ITEM	**DESCRIÇÃO**	**QTD**	**Descrever os nomes dos produtos que compõe a solução**	**Preço Unitário (R$)**	**Preço Total (R$)**
1	Solução em cluster de gerenciamento unificado de ameaças (Firewall UTM) com suporte e garantia do fabricante pelo período de 36 (trinta e seis) meses.	2			
2	Gerenciamento, logs e relatoria do cluster de Firewall UTM.	2			
3	Treinamento oficial da solução integrada de segurança.	6			
4	Instalação e configuração da solução integrada de segurança	1			
VALOR TOTAL DO LOTE 01					

LOTE 2

LOTE 2					
ITEM	**DESCRIÇÃO**	**QTD**	**Descrever os nomes dos produtos que compõe a solução**	**Preço Unitário (R$)**	**Preço Total (R$)**
1	Solução em Firewall de Aplicações WEB (WAF), com suporte e garantia do fabricante pelo período de 36 (trinta e seis) meses.	1			
2	Capacidade adicional para solução em Firewall de Aplicações WEB.	3			
3	Treinamento oficial da solução WAF	6			
4	Instalação e configuração da solução em WAF	1			
VALOR TOTAL DO LOTE 02					

LOTE 3

LOTE 3					
ITEM	**DESCRIÇÃO**	**QTD**	**Descrever os nomes dos produtos que compõe a solução**	**Preço Unitário (R$)**	**Preço Total (R$)**

1	Solução de gerenciamento de logs e eventos de segurança (SIEM), com licença perpétua, suporte e atualização para 36 meses de uso.	1			
2	Capacidade adicional para software de gerenciamento de logs e eventos de segurança (SIEM), com licença perpétua, suporte e atualização para o primeiro ano de uso.	3			
3	Suporte anual para software de gerenciamento de logs e eventos de segurança (SIEM), para módulo principal, descrito no item 01, não incluindo os primeiros 36 meses de uso.	3			
4	Treinamento oficial para solução de SIEM.	6			
5	Instalação e configuração da solução de SIEM	1			
VALOR TOTAL DO LOTE 03					

OBSERVAÇÕES

1. É obrigatório as empresas licitantes preencherem integralmente esta planilha de preço.

2. Os custos relativos ao serviço de garantia dos equipamentos e softwares que compõe a solução já devem estar incluídos no preço dos próprios itens.

3. A CONTRATADA deverá emitir Nota Fiscal/Fatura relativa aos valores dos equipamentos e softwares da solução e garantia por 36 (trinta e seis) meses, serviços de instalação e configuração e serviço de transferência de conhecimento após receber cópia do Termo de Recebimento Definitivo previsto no Cronograma (ANEXO II).

4. **Mesmo considerando que a vencedora do certame será a empresa que apresentar o menor preço do lote, não será adquirido isoladamente item para o qual a licitante vencedora não apresentou o menor preço.**

ANEXO II do TR - CRONOGRAMA DE IMPLANTAÇÃO

Prazo Máximo (em dias corridos)	Cronograma de Atividades da Prestação dos Serviços	Responsável
D	Data de emissão de Ordem de Serviço – OS dos equipamentos, softwares e serviços da solução pelo CONTRATANTE.	TCE-AP
D+3	Reunião de Planejamento.	TCE-AP e CONTRATADA
D+15	Entregar o Plano de Implantação contendo o planejamento das atividades para as etapas de entrega, instalação, configuração e testes dos equipamentos e softwares que compõe a solução.	CONTRATADA
D+15	Comprovar que os técnicos que executarão as atividades são certificados pelos fabricantes dos componentes da solução.	CONTRATADA
	Aprovar o Plano de Implantação para as etapas de entrega, instalação, configuração e testes dos equipamentos e softwares que compõe a solução.	TCE-AP
D+45	Concluir a entrega dos equipamentos, softwares e acessórios, juntamente com toda a documentação técnica em meio eletrônico, completa e atualizada, contendo os manuais e guias de utilização e os demais documentos.	CONTRATADA
	Emitir o Termo de Recebimento Provisório (TRP) após a entrega dos equipamentos, softwares, Plano de Implantação aprovado e demais documentações da solução. A entrega deverá ser formalizada mediante comunicação escrita da CONTRATADA ao CONTRATANTE. O recebimento provisório realizar-se-á no prazo máximo de 15 (quinze) dias corridos, contados da comunicação da empresa, desde que não haja pendências a cargo da CONTRATADA.	TCE-AP
Data de Emissão do TRP+45	Concluir, a partir da data de emissão do Termo de Recebimento Provisório (TRP), os serviços de instalação e configuração dos equipamentos e softwares da solução integrada de segurança, realizando todas as atividades programadas para esta etapa.	CONTRATADA

	Emitir o Termo de Recebimento Definitivo (TRD) após a finalização dos serviços de instalação e configuração, acompanhado da documentação técnica detalhada de todos os procedimentos executados, desde que não haja pendências a cargo da CONTRATADA.	TCE-AP
Data de Emissão do TRP+30	Realizar o acompanhamento (operação assistida) da operação inicial da solução integrada de segurança, esclarecendo dúvidas e realizando ajustes na configuração visando à melhor utilização dos recursos oferecidos nos equipamentos que compõe a solução	CONTRATADA

ANEXO II – PREGÃO ELETRÔNICO 01/2021-TCE/AP

MINUTA ATA DE REGISTRO DE PREÇOS N° __/2021

VALIDADE: ATÉ XX DE XXXXXXX DE 202X(12 meses)

ATA DE REGISTRO DE PREÇOS QUE, ENTRE SI, CELEBRAM, DE UM LADO XXXXXX E DE OUTRO O XXXXX., NA FORMA ABAIXO

Aos ___ dias do mês de _____ do ano 2021, o TRIBUNAL DE CONTAS DO ESTADO DO AMAPÁ - TCE/AP, pessoa jurídica de direito público, criado pela Lei nº xxxxx de xx.xx.xx, , com sede a Av FAB, 900 - Centro, inscrito no CNPJ sob o nº 0xxxxxxxxxxxxxxxxx, neste ato representado pelo seu PRESIDENTE, xxxxxxxxxxxxxxxxxxxxx CI xx CPFxxx, doravante denominado CONTRATANTE, e de outro lado a Empresa abaixo descrita(s), em face da classificação das propostas de preços – no **Pregão Eletrônico para formação da Ata de Registro de Preços** – (Empresa) , tendo como fundamento a Ata de julgamento e classificação das propostas de preços, resolve(m) registrar os preços para Serviços de Agenciamento de Viagens, conforme o Termo de Homologação do dia xx de xxxxxx de 2021, que passam a fazer parte desta Ata de Registro de Preços, tendo sido a empresa xxxxxx CNPJ/MF xxxx, sediada na Rua xxxxx, CEP xxxx classificada em primeiro lugar, com os respectivos itens e preços , conforme planilha anexa. A Ata de Registro de Preços tem validade de 12 (doze) meses a partir de sua assinatura.

1. CLÁUSULA PRIMEIRA – DO OBJETO

1.1 O objeto da presente **ATA DE REGISTRO DE PREÇOS** para contratação por registro de preços, de empresa especializada para o **fornecimento de Solução integrada de segurança, composta por um cluster de Gerenciamento Unificado de Ameaças** (Firewall UTM) e seu Gerenciamento de Logs e Relatórios de Segurança; Solução em Firewall de Aplicações WEB (WAF - Web Application Firewall); Solução de software para gerenciamento de logs e eventos de segurança (SIEM - Security Information and Event Management), além de suporte técnico e serviços especializados, previamente definidos através do Procedimento Licitatório e constantes no Anexo I – Termo de Referência do Edital de PREGÃO N. 01 /2021e dos anexos

1.2 A **gestão e controle das contratações oriundas desta ata ficará a cargo da DARAD/Gestão de Contratos**, em conjunto com a Diretoria da Área de Informática-DAINF.

1.3 QUANTIDADE REGISTRADA

LOTE 01
Empresa classificada em 1º lugar: XXXXXXXXXXXXXXX
CNPJ nº xx.xxx.xxx/xxxx-xx
Endereço:
Telefone/email:
Representante Legal:
Objeto:

LOTE 1					
ITEM	**DESCRIÇÃO**	**QTD**	**Descrever os nomes dos produtos que compõe a solução**	**Preço Unitário (R$)**	**Preço Total (R$)**
1	Solução em cluster de gerenciamento unificado de ameaças (Firewall UTM) com suporte e garantia do fabricante pelo período de 36 (trinta e seis) meses.	2			
2	Gerenciamento, logs e relatoria do cluster de Firewall UTM.	2			
3	Treinamento oficial da solução integrada de segurança.	6			
4	Instalação e configuração da solução integrada de segurança	1			
VALOR TOTAL DO LOTE 01					

LOTE 2

Empresa classificada em 1º lugar: XXXXXXXXXXXXXXX
CNPJ nº xx.xxx.xxx/xxxx-xx
Endereço:
Telefone/email:
Representante Legal:
Objeto:

LOTE 2					
ITEM	**DESCRIÇÃO**	**QTD**	**Descrever os nomes dos produtos que compõe a solução**	**Preço Unitário (R$)**	**Preço Total (R$)**
1	Solução em Firewall de Aplicações WEB (WAF), com suporte e garantia do fabricante pelo período de 36 (trinta e seis) meses.	1			
2	Capacidade adicional para solução em Firewall de Aplicações WEB.	3			
3	Treinamento oficial da solução WAF	6			

4	Instalação e configuração da solução em WAF	1			
VALOR TOTAL DO LOTE 02					

LOTE 3

Empresa classificada em 1º lugar: XXXXXXXXXXXXXXX
CNPJ nº xx.xxx.xxx/xxxx-xx
Endereço:
Telefone/email:
Representante Legal:
Objeto:

LOTE 3					
ITEM	**DESCRIÇÃO**	**QTD**	**Descrever os nomes dos produtos que compõe a solução**	**Preço Unitário (R$)**	**Preço Total (R$)**
1	Solução de gerenciamento de logs e eventos de segurança (SIEM), com licença perpétua, suporte e atualização para 36 meses de uso.	1			
2	Capacidade adicional para software de gerenciamento de logs e eventos de segurança (SIEM), com licença perpétua, suporte e atualização para o primeiro ano de uso.	3			
3	Suporte anual para software de gerenciamento de logs e eventos de segurança (SIEM), para módulo principal, descrito no item 01, não incluindo os primeiros 36 meses de uso.	3			
4	Treinamento oficial para solução de SIEM.	6			
5	Instalação e configuração da solução de SIEM	1			
VALOR TOTAL DO LOTE 03					

2. CLÁUSULA SEGUNDA - DA VALIDADE DOS PREÇOS REGISTRADOS

2.1 A presente Ata de Registro de Preços terá a validade de 12 (doze) meses, a partir da sua assinatura final.

2.2 Durante o prazo de validade desta o Tribunal de Contas do Estado do Amapá, Gestor do Registro fica obrigado a firmar as contratações que dela poderão advir, facultando-se a realização de licitação específica para a aquisição pretendida, sendo assegurado ao beneficiário do registro preferência de fornecimento em igualdade de condições.

3. CLÁUSULA TERCEIRA - DA UTILIZAÇÃO DA ATA DE REGISTRO DE PREÇOS

3.1 A presente Ata de Registro de Preços poderá ser usada (carona) por órgãos usuários, desde que autorizados pelo TCE/AP, nos termos do Decreto Estadual nº 3.182/2016.

3.2 Em cada fornecimento decorrente desta Ata serão observadas, quanto ao preço, às cláusulas e condições constantes do Edital, que a precedeu e integra o presente instrumento de compromisso.

3.3 O TCE/AP permitirá adesões para o dobro do quantitativo registrado em cada lote, limitados a 100%(cem por cento) para cada órgão solicitante, nos termos constante no art. 24 do Decreto Estadual nº 3.182/2016.

3.4 A **gestão e controle referente a possíveis adesões (carona), a outros órgãos da administração, ficará sob a responsabilidade da Comissão Permanente de Licitação-CPL, que instruirá à Presidência visando às devidas autorizações, dentro dos limites legais autorizáveis.**

3.5 As solicitações deverão vir acompanhadas de termo de justificativa de vantagem para a adesão à Ata

4. CLÁUSULA QUARTA - DO LOCAL E INÍCIO DA EXECUÇÃO

4.1 A prestação de serviços **estabelecidos na primeira cláusula – do objeto,** serão entregues conforme dispõe o termo de referência:

4.1.1 No Prédio Sede do TCE-AP, sito à Avenida FAB, nº 900, Bairro Central e prédio anexo, Avenida Mendonça Furtado, Centro, conforme o caso.

4.1.2 Quando da execução do serviço será iniciada na data da emissão da ordem de serviço, para instalar, testar, configurar e dar treinamento de uso dos equipamentos em todos os setores e localidades.

4.1.3 Nos órgãos ou entidades que aderirem à Ata de Registro de Preços, conforme seu cadastro, oportunamente registrado nos procedimentos anteriores a adesão.

5. CLÁUSULA QUINTA – DO CANCELAMENTO DA ATA

5.1 O Proponente terá sua Ata de Registro de Preços, parcial ou totalmente cancelada por intermédio de processo administrativo específico, assegurado o contraditório e ampla defesa, ou:

5.1.1 A pedido, quando:

a) Comprovar estar impossibilitado de cumprir as exigências da Ata, por ocorrência de casos fortuitos ou de força maior;

b) O seu preço registrado se tornar, comprovadamente, inexequível em função da elevação dos preços de mercado, dos insumos que compõem o custo dos serviços, e se a comunicação ocorrer antes do pedido de fornecimento.

5.1.2 Por iniciativa do Órgão Gerenciador, quando:

a) O fornecedor não aceitar reduzir o preço registrado, na hipótese deste se tornar superior àqueles praticados no mercado;
b) Perder qualquer condição de habilitação exigida no processo licitatório;
c) Por razões de interesse público, devidamente, motivadas e justificadas;
d) Não cumprir as obrigações decorrentes da Ata de Registro de Preços;
e) Não responder a convocação ou se recusar entregar, no prazo estabelecido, os pedidos/serviços decorrentes da Ata de Registro de Preços; e

5.2 A Ata de Registro de Preços decorrente desta licitação também será cancelada automaticamente:

5.2.1 Por decurso do prazo de vigência;
5.2.2 Quando atingir 100% do valor registrado;
5.2.3 Quando não restarem fornecedores registrados.

6. DA REVISÃO DOS PREÇOS REGISTRADOS

6.1 O preço registrado poderá ser revisto em decorrência de eventual variação daqueles praticados no mercado, ou de fato que altere o custo dos serviços ou bens registrados, cabendo ao órgão gerenciador promover as negociações junto aos possíveis fornecedores cadastrados.

7. CLÁUSULA SEXTA - DAS DISPOSIÇÕES FINAIS

7.1 Integram esta Ata, o Edital do Pregão no 01/2021 e seus Anexos, e a(s) proposta(s) da(s) empresa(s) classificada(s) em 1º lugar, no(s) item(ns) acima mencionado(s).

7.2 Fica eleito o foro judiciário da Comarca de Macapá/AP para dirimir quaisquer questões decorrentes da utilização da presente ATA. Os casos omissos serão resolvidos de acordo com as Leis Nº 8.666 de 1993 e alterações posteriores, Lei 10.520/2002, e do Decreto Estadual nº 3182/2016 (Regulamento do Registro de Preço), e demais normas aplicáveis.

Estando as partes de pleno acordo, firmam o presente Instrumento em xx (xxxx) vias de igual forma e teor, na presença de 02 (duas) testemunhas abaixo assinadas.

Macapá-AP, xx de xxxxx de 2021.

Presidente do TCE/AP
RG: nº xxxxxxxxx / xx ,
CPF: xxx.xxx.xxx-xx

Empresa xxxxxxxx
Representante Legal
Xxxxxxxxxxx
CPF xxxxxxxxxxxxxx

TESTEMUNHAS:

1 _____

CPF _____

2.

_____

CPF _____

* Publicação DOE.

ANEXO III – PREGÃO ELETRÔNICO 01/2021-TCE/AP

Minuta DE CONTRATO

CONTRATO DE PRESTAÇÃO DE SERVIÇOS Nº XXXX/2021 - TCE/AP QUE ENTRE SI CELEBRAM O TRIBUNAL DE CONTAS DO ESTADO DO AMAPÁ E A EMPRESA xxxxxxxxxxxxxx, PARA OS FINS NELE DECLARADOS.

Pelo presente instrumento e nos melhores termos de direito, a(o) **TRIBUNAL DE CONTAS DO ESTADO DO AMAPÁ - TCE/AP,** com sede nesta Capital, sito à Av. XXXXXX, nº. XXX, bairro Central, representada pela(o) sua(eu) Presidente, Conselheiro xxxxx**,** brasileiro**,** xxx, residente e domiciliado a xxx – xx, portador da Cédula de Identidade nº. xxxx e do CPF nº. xx, doravante denominado **CONTRATANTE** e a Empresa _____, CNPJ/MF nº. _____, estabelecida no _____, doravante denominada **CONTRATADA,** neste ato representada legalmente pelo Sr. (a) _____, brasileiro (a), RG nº. _____, CPF nº. _____, residente e domiciliado (a) na _____, – Macapá/AP, tendo em vista o que consta no Processo eletrônico nº ..... e em observância às disposições da Lei nº 8.666, de 21 de junho de 1993, resolvem celebrar o presente Termo de Contrato, decorrente do Pregão nº 01/2021, mediante as cláusulas e condições a seguir enunciadas.

1. **CLAUSULA PRIMEIRA – DO OBJETO**
   - **1.1.** O presente contrato tem como objeto a **contratação, por registro de preços, de empresa especializada para o fornecimento de Solução integrada de segurança, composta por um cluster de Gerenciamento Unificado de Ameaças (Firewall UTM) e seu Gerenciamento de Logs e Relatórios de Segurança; Solução em Firewall de Aplicações WEB (WAF - Web Application Firewall); Solução de software para gerenciamento de logs e eventos de segurança (SIEM - Security Information and Event Management), além de suporte técnico e serviços especializados** deste Tribunal, conforme os anexos do Edital do Pregão Eletrônico nº 01/2021-TCE-AP.
   - **1.2.** Compõem este contrato, além da mão de obra, o fornecimento de todos os insumos e materiais e o emprego dos equipamentos necessários à execução dos serviços, conforme disposto no **Termo de Referência** do Pregão Eletrônico 01/2021.

     Obs: Descrever os itens contratados constante na planilha.

2. **CLÁUSULA SEGUNDA – DO REGIME DE EXECUÇÃO**
   - **2.1.** A forma de execução indireta, em regime de empreitada por preço unitário, com fundamento previsto no artigo 6º, VIII, c/c art. 10, II, alínea “b” da Lei nº 8.666/93.
   - **2.2.** Cabe à contratada responder por qualquer serviço específico quando executado por terceiros.

3. **CLÁUSULA TERCEIRA – DOS VALOR DO CONTRATO E DAS CONDIÇÕES DE PAGAMENTO**

3.1 O valor global do presente Termo de Contrato é de R$ XXX**.**

3.1. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução contratual, 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.

4. CLÁUSULA QUARTA – REAJUSTE E ALTERAÇÕES

4.1. Dos reajustes:

a) O valor da Remuneração dos serviços e materiais poderá ser reajustado pela Administração, por apostila, após completados 12 (doze) meses (se for o caso), contados da data da proposta, com base no Índice Nacional de Preços ao Consumidor Amplo – IPCA ou naquele que o vier a substituir.

4.1.a.1. Fórmula de cálculo:

$$Pr = P + (P \times V)$$

Onde,

Pr = preço reajustado, ou novo preço;

P = preço atual (antes do reajuste);

V = variação percentual obtida na forma do item 4.1, a, de modo que (P x V) significa o acréscimo ou decréscimo de preço decorrente do reajuste.

4.2. Das alterações:

a) Os preços são fixos e irreajustáveis no prazo de um ano contado da data limite para a apresentação das propostas.

b) Eventuais alterações contratuais reger-se-ão pela disciplina do art. 65 da Lei nº 8.666, de 1993.

c) A CONTRATADA é obrigada 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.

d) As supressões resultantes de acordo celebrado entre as partes contratantes poderão exceder o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

5. CLÁUSULA QUINTA – DOS RECURSOS ORÇAMENTÁRIOS

5.1. As despesas para atender a esta licitação estão programadas em dotação orçamentária própria, prevista no orçamento deste Tribunal para o exercício de 2021 ou 2021, conforme Nota de Empenho – NE nº _____, na classificação abaixo:

a) Fonte:

b) Programa de Trabalho:

c) Elemento de Despesa:

6. CLÁUSULA SEXTA – DOS PRAZOS

6.1. Prazo de execução: 12 (doze) meses, prorrogáveis por até 48(quarenta e oito) meses conforme estabelecido no Termo de Referência.

6.2. Prazo de recebimento

a) **Provisório:** EM ATÉ 15 DIAS corridos, pelo fiscal do contrato, contados após o término da instalação dos equipamentos, pelo responsável de fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes neste termo de referência e na proposta;

b) **Definitivo:** EM ATÉ 45 DIAS CORRIDOS, contados do recebimento provisório,

após a verificação da qualidade e quantidade do serviço executado e materiais empregados, com a consequente aceitação mediante termo circunstanciado.

6.3. Prazo de vigência deste Termo de Contrato:

a) O prazo de vigência deste Termo de Contrato tem início a partir da data da assinatura da Ordem de Serviço.

6.4. Em caso de conflito: entre os prazos estipulado no Termo de Referência e vigente neste contrato será considerado aquele de maior prazo.

7. CLÁUSULA SÉTIMA – DAS OBRIGAÇÕES DAS PARTES

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

7.2. DA LICITANTE VENCEDORA:

7.2.a.1 Fornecer, ao executar os serviços, materiais de alta qualidade e de primeiro uso;

7.2.a.2 Os materiais deverão apresentar total conformidade com todas as especificações e requisitos detalhados neste termo de referência;

7.2.a.3 Manter a compatibilidade com o padrão e qualidade de materiais já instalados nas dependências do TCE-AP;

7.2.a.3 Ser responsável, em relação aos seus empregados, por todas as despesas decorrentes da execução dos serviços, tais como: salários, seguros de acidente, taxas, impostos e contribuições, indenizações, vale-refeição, vale-transporte e outras que porventura venham a ser criadas e exigidas pelo Governo;

7.2.a.4 Manter os seus empregados sujeitos às normas disciplinares do Tribunal de Contas do Estado do Amapá, porém, sem qualquer vínculo empregatício com o órgão;

7.2.a.4 Manter, ainda, os seus empregados identificados, quando em trabalho, devendo substituir imediatamente qualquer um deles que seja considerado inconveniente à boa ordem e às normas disciplinares do Tribunal de Contas do Estado do Estado do Amapá;

7.2.a.5 Responder pelos danos causados diretamente à Administração do Tribunal de Contas do Estado do Amapá ou a terceiros, decorrentes de sua culpa ou dolo, quando da execução dos serviços, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento pelo Tribunal de Contas do Estado do Amapá;

7.2.a.6 Responder, também, por quaisquer danos causados diretamente aos bens de propriedade do Tribunal de Contas do Estado do Amapá, quando esses tenham sido ocasionados por seus empregados durante a execução dos serviços;

7.2.a.7 Arcar com despesa decorrente de qualquer infração, seja qual for, desde que praticada por seus empregados na execução dos serviços ou no recinto do Tribunal de Contas do Estado do Amapá;

7.2.a.8 Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, as etapas dos serviços em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais utilizados, no prazo máximo de 5 (cinco) dias ou no prazo para tanto estabelecido pela fiscalização;

7.2.a. 9 Permitir, aos técnicos do Tribunal de Contas do Estado do Amapá e àqueles a quem o Tribunal formalmente indicar, acesso às suas instalações e a todos os locais onde estiverem sendo estocados materiais relacionados com o objeto;

7.2.a.10 Responsabilizar-se pelas despesas decorrentes da rejeição de componentes, materiais e serviços pela Fiscalização do Tribunal de Contas do Estado do Amapá e pelos atrasos acarretados por esta rejeição;

7.2.a.11 Responsabilizar-se por todo transporte necessário à execução dos serviços, bem como por ensaios, testes ou provas necessários, inclusive os mal executados;

7.2.a.12 Providenciar, às suas expensas, atestado de similaridade de desempenho dos materiais apresentados, junto a instituições ou fundações capacitadas para este fim, quando do uso de similar ao descrito nas Especificações Técnicas, sempre que a fiscalização do Tribunal de Contas do Estado do Amapá julgar necessário;

7.2.a.13 Responsabilizar-se pela perfeita execução e completo acabamento dos serviços, obrigando-se a prestar assistência técnica e administrativa necessária para assegurar andamento conveniente dos trabalhos;

7.2.a.14 Submeter à aprovação da Fiscalização do Tribunal de Contas do Estado do Amapá, o(s) nome(s) e o(s) dado(s) demonstrativo(s) da respectiva capacidade técnica do responsável técnico que, porventura, venha a substituir o originalmente indicado;

7.2.a.15 Executar os serviços e comprovar, após instalação, o funcionamento e entrega através de relatório de atividade técnica específico;

7.2.a.16 Comunicar à Divisão de Dados e Redes, qualquer anormalidade verificada na instalação e prestar os devidos esclarecimentos sempre que solicitados;

7.7.a.17 Cumprir, às suas próprias expensas, todas as cláusulas contratuais que definam suas obrigações;

7.3. DO TCE-AP

7.3.a.1. Será responsabilidade do Tribunal de Contas, representado pelos seus dirigentes e servidores prepostos ou representantes, para os efeitos deste TERMO DE REFERÊNCIA:

7.3.a.2 Verificar os equipamentos instalados, e, quando atenderem ao objeto do contrato, aprová-los;

7.3.a.3 Liquidar o empenho e efetuar os pagamentos das faturas à empresa vencedora do certame licitatório dentro dos prazos preestabelecidos em contrato;

7.3.a.4 Prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATADA;

7.3.a.5 Permitir acesso dos empregados da empresa contratada nas suas dependências para a entrega do equipamento e para as devidas instalações;

7.3.a.6 Prestar as informações e os esclarecimentos pertinentes que venham a ser solicitados pelo representante da empresa contratada;

7.3.a.7 Comunicar oficialmente à empresa contratada quaisquer falhas ocorridas;

7.3.a.8 Lavrar e entregar à empresa contratada o Termo de Recebimento, bem como atestar a Nota Fiscal no prazo estipulado;

7.3.a.9 Efetuar o pagamento no prazo previsto neste Termo de Referência;

7.3.a.10 Fornecer demais informações à empresa contratada para a perfeita execução do objeto;

7.3.a.11 Realizar a Fiscalização do objeto para a perfeita execução do objeto.

8. CLÁUSULA OITAVA - DO ACOMPANHAMENTO E DA FISCALIZAÇÃO

8.1 A execução dos serviços será fiscalizada e acompanhada por servidor designado pela administração, com competências pertinentes ao objeto contratado;

8.2. As decisões e providências que ultrapassarem a competência do Fiscal de Contrato, deverão ser solicitadas ao Diretor Administrativo do Tribunal de Contas do Estado do Amapá, em tempo hábil, para a adoção das medidas convenientes;

8.3. A licitante vencedora deverá indicar preposto, aceito pela Administração do Tribunal de Contas do Estado do Amapá, para representá-la sempre que for necessário;

9. CLÁUSULA NONA – DO PAGAMENTO

9.1 O pagamento será efetuado através de Ordem Bancária, mediante depósito na contracorrente da Contratada, no prazo de até 10 (dez) dias úteis após a assinatura do Termo de Recebimento Definitivo (TRD), com a formalização por escrito da CONTRATADA referente à conclusão das atividades de entrega, sejam de treinamentos ou instalação e configuração dos equipamentos e softwares, em consonância com todos as especificações dos LOTES/ITEMS pertinentes;

9.2. O pagamento deverá ser acompanhado da respectiva Nota Fiscal/Fatura, emitida em, no mínimo, 2 (duas) vias, de acordo com a Nota de Empenho, a qual será conferida e atestada pelo servidor ou comissão responsável pelo recebimento, observado o estabelecido no art. 5º da Lei 8.666/93, e desde que não ocorra fator impeditivo provocado pela Contratada;

9.3. No caso do valor do contrato, representado pela Nota de Empenho, não ultrapassar o limite de que trata o inciso II do art. 24, da Lei nº 8.666/93, o pagamento deverá ser efetuado no prazo de até 5 (cinco) dias úteis, nas condições referidas no item;

9.4. Nenhum pagamento será efetuado à Contratada enquanto pendente de liquidação qualquer obrigação financeira que lhe for imposta, em virtude de penalidade ou inadimplência, sem que isso gere direito ao pleito de reajustamento dos preços ou correção monetária;

10. CLÁUSULA DÉCIMA – DA GARANTIA DO CONTRATO

10.1. Para se garantir o fiel cumprimento de todas as cláusulas e condições do contrato, a LICITANTE deverá optar por uma das modalidades de garantia previstas nos incisos de I a III, do parágrafo primeiro, do art. 56, da Lei nº 8.666/93.

11. CLÁUSULA DÉCIMA PRIMEIRA - DAS SANÇÕES ADMINISTRATIVAS

11.1. Com fundamento no artigo 7º da Lei nº 10.520/2002, ficará impedida de licitar e contratar com a União e será descredenciada do SICAF, pelo prazo de até 5 (cinco) anos, garantida a ampla defesa, sem prejuízo da rescisão unilateral do contrato e da aplicação de multa previstas no Termo de Referência sobre o valor total da contratação, a CONTRATADA que:

a) Apresentar documentação falsa;

b) Fraudar a execução do contrato;

c) Comportar-se de modo inidôneo;

d) Reputar-se-ão inidôneos atos tais como os descritos nos artigos 92, parágrafo único, 96 e 97, parágrafo único, da Lei nº 8.666/1993.

e) Cometer fraude fiscal; ou

f) Fizer declaração falsa.

11.2. Com fundamento nos artigos 86 e 87, incisos I a IV, da Lei nº 8.666, de 1993; e no art. 7º da Lei nº 10.520, de 17/07/2002, nos casos de retardamento, de falha na execução do contrato, inexecução parcial ou de inexecução total do objeto, garantida a ampla defesa, a CONTRATADA poderá ser sancionada, isoladamente, ou juntamente com as multas definidas nos itens abaixo, com as seguintes sanções:

a) Advertência;

b) Suspensão temporária de participação em licitação e impedimento de contratar

com a Administração do Tribunal de Contas do Estado do Amapá (TCE-AP) por prazo não superior a dois anos;

c) Declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a CONTRATADA ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso anterior;

d) Impedimento de licitar e contratar com a União e descredenciamento no SICAF, ou nos sistemas de cadastramento de fornecedores a que se refere o inciso XIV do art. 4º da Lei nº 10.520/2002, pelo prazo de até cinco anos.

11.3. Multa compensatória de 10% (dez por cento) sobre o valor global do respectivo item.

12. CLÁUSULA DÉCIMA SEGUNDA – HABILITAÇÃO

12.1. A contratada deverá manter até o final do cumprimento de suas obrigações, todas as condições e habilitações exigidas no edital.

13. CLÁUSULA DÉCIMA TERCEIRA – VEDAÇÕES

13.1. É vedado à CONTRATADA:

a) Caucionar ou utilizar este Termo de Contrato para qualquer operação financeira;

b) Interromper a execução contratual sob alegação de inadimplemento por parte da CONTRATANTE, salvo nos casos previstos em lei.

14. CLÁUSULA DÉCIMA QUARTA – DA RESCISÃO

14.1. O presente Termo de Contrato poderá ser rescindido nas hipóteses previstas no art. 78 da Lei nº 8.666, de 1993, com as consequências indicadas no art. 80 da mesma Lei, sem prejuízo das sanções aplicáveis.

14.2. É admissível a fusão, cisão ou incorporação da contratada com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato.

14.3. Os casos de rescisão contratual serão formalmente motivados, assegurando-se à CONTRATADA o direito à prévia e ampla defesa.

14.4. A CONTRATADA reconhece os direitos da CONTRATANTE em caso de rescisão administrativa prevista no art. 77 da Lei nº 8.666, de 1993.

15. CLÁUSULA DÉCIMA QUINTA – DA FUNDAMENTAÇÃO LEGAL E DA VINCULAÇÃO AO EDITAL

15.1. O presente contrato fundamenta-se no Decreto nº 10.024/2019 e nas Leis n.º 10.520/2002 e n.º 8.666/1993 e vincula-se ao Edital e Anexos do Pregão Eletrônico n.º 08/2021, constante do processo nº 11.857/2018, bem como à proposta do CONTRATADO.

16. CLÁUSULA DÉCIMA SEXTA – DOS CASOS OMISSOS.

16.1. Os casos omissos serão decididos pela CONTRATANTE, segundo as disposições contidas no Decreto nº 10.024/2019, na Lei nº 8.666, de 1993, na Lei nº 10.520, de 2002 e demais normas federais de licitações e contratos administrativos e, subsidiariamente, segundo as disposições de normas e princípios gerais dos contratos

17. CLÁUSULA DÉCIMA SÉTIMA – PUBLICAÇÃO

17.1. Incumbirá à CONTRATANTE providenciar a publicação deste instrumento, por extrato, no Diário Oficial Eletrônico do TCE, no prazo previsto no art. 61 da Lei nº 8.666, de 1993.

18. CLÁUSULA DÉCIMA OITAVA – DOS DOCUMENTOS INTEGRANTES

18.1. Fazem parte integrante deste contrato, independentemente de transcrição, os documentos abaixo relacionados:

a) Proposta Escrita;

b) Termo de Referência, e;

c) Edital do Pregão, na Forma Eletrônico nº 01/2021-CPL/TCE

19. CLÁUSULA DÉCIMA NONA – DO FORO

19.1. As partes elegem o Foro da Cidade de Macapá-AP para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não possam ser compostos pela conciliação, conforme art. 55, §2º da Lei nº 8.666/93.

19.2. Para firmeza e validade do pactuado, o presente Termo de Contrato foi lavrado em 02 (duas) vias de igual teor, que, depois de lido e achado em ordem, vai assinado pelos contraentes.

....., ... de de 2021

_____

Responsável legal da CONTRATANTE

_____

Responsável legal da CONTRATADA

TESTEMUNHAS: