

TERMO DE CONSULTA

1. OBJETO E CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Objeto

1.1.1. Aquisição de solução de WAF – Web Application Firewall (Firewall de Aplicações Web), com recursos para monitorar, filtrar, bloquear pacotes de dados e ataques cibernéticos, incluindo os serviços de instalação, configuração, operação assistida, migração e capacitação técnica para 4 (quatro) profissionais, suporte, manutenção com substituição de peças e atualização de versão da solução, pelo período de 60 (sessenta) meses nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste Termo de Consulta e seus Anexos.

Itens	Descritivo	Unidade de medida	Quantidade
1	Aquisição de solução de WAF com licenciamentos necessários conforme descrito no Anexo I-B – Especificação Técnica	Unidade	4
2	Serviços de instalação e configuração	Prestação de Serviço	1
3	Serviço de Operação Assistida	Prestação de Serviço	1
4	Serviço de migração	Prestação de Serviço	1
5	Serviço de Capacitação para 4 alunos	Turma	1
6	Serviço de Suporte, manutenção e atualização de versão por 60 meses	Prestação de Serviço	Durante o contrato.

Tabela 1 – Objeto

1.2. Caracterização do objeto

1.1.2. O objeto da presente contratação é caracterizado como comum, por apresentar padrões de desempenho e qualidade objetivamente definidos por meio de especificações usuais de mercado. Em razão dessa característica, a licitação será conduzida na modalidade pregão, na forma eletrônica, nos termos do art. 4º, inciso IV, e art. 6º, § 2º, do Regulamento Interno de Licitações e Contratos – RILC, respeitadas as rotinas estabelecidas na Lei nº 13.303/2016 quanto aos procedimentos operacionais necessários, a partir da abertura da sessão pública até a homologação do certame, devido ao uso do portal de compras do Estado de Minas Gerais.

1.1.3. Esta especificação técnica faz parte do processo de prospecção destinado a atender às necessidades da PRODEMGE e em função disto é uma especificação sujeita a críticas e sugestões de melhoria pelo mercado.

1.1.4. **Solicitamos às PROPONENTES o envio da seguinte documentação:**

- Mesmo que não atendam a todos os requisitos, que preencham o formulário definido no Anexo I-A e informem quais requisitos na especificação técnica (Anexo I-B) não são atendidos pela solução proposta e quais as alternativas propostas para o atendimento.
- Documento com a especificação técnica detalhada das soluções ofertadas e seus componentes principais.
- Documento com a ementa da capacitação técnica proposta.

1.1.5. Após o envio dos formulários estaremos à disposição para nos reunirmos com os PROPONENTES com o objetivo de avaliarmos as soluções apresentadas, além das críticas e sugestões que foram encaminhadas.

1.3. Lotes exclusivos para microempresas e empresas de pequeno porte

1.2.1. A participação na presente licitação é aberta a todos (sem exclusividade ou reserva de lotes para Microempresas, Empresas de Pequeno Porte e equiparados aos benefícios do Decreto nº 47.437, de 26 de junho de 2018, e Lei Complementar nº 123, de 14 de dezembro de 2006).

1.4. Prazo de vigência do contrato e prorrogações / ou substituição do contrato por OCS.

1.4.1. O prazo de vigência deste contrato será determinado conforme a tabela a seguir, na forma do artigo 137 do Regulamento Interno de Licitações e Contratos da **PRODEMGE**.

Item	Descrição	Prazo de Entrega	Vigência	Início da vigência	Natureza
1	Solução de WAF incluindo licenciamento	30 dias úteis	60 meses	Assinatura do contrato	Investimento
2	Serviço de Instalação e configuração	10 dias úteis	N/A	Após o aceite provisório da entrega do equipamento	Serviço por escopo definido
3	Serviço de Migração	40 dias úteis (aproximadamente 205 aplicações)	Até a homologação final do cliente	Após a instalação e configuração	Serviço por escopo definido
4	Serviço de Operação Assistida	25 dias úteis	45 dias	Dia útil seguinte após finalizada a migração homologada pelo cliente	Serviço por escopo definido
5	Serviço de capacitação técnica compreendendo arquitetura, gerenciamento, operação, monitoramento, boas práticas de segurança e manutenção, com turma de até 4 (quatro) alunos.	40 dias úteis	N/A	Após a instalação e configuração, devendo ser concluída antes do fim da operação assistida	Serviços por escopo
6	Serviços de suporte técnico continuado,	Imediatamente após aceite definitivo dos serviços de	60 meses	Imediatamente após aceite definitivo dos	Serviços continuados

	incluindo atendimento, diagnósticos, substituição de peças, atualização de firmware e versões de software, garantindo a disponibilidade e continuidade operacional do ambiente.	instalação e configuração.		serviços de instalação e configuração	
--	---	----------------------------	--	---------------------------------------	--

Tabela 2 – Prazos

*O prazo de vigência total do contrato será fixado pela soma do período destinado à entrega e instalação do bem (solução de WAF) com o período destinado à prestação dos serviços associados (instalação, configuração, operação assistida, suporte, manutenção e atualização de versões), observado que este último não poderá exceder a 10 (dez) anos, incluídas as prorrogações, contados da data do recebimento definitivo do objeto.

1.4.2. O prazo de vigência dos serviços associados (Suporte, Manutenção e atualização de versões) poderá ser prorrogado para até 10 (dez) anos, no interesse das partes, mediante a assinatura de Termo Aditivo, respeitado o disposto nos artigos 140 e 141 do *Regulamento Interno de Licitações e Contratos – RILC*

1.4.3. Os serviços associados (suporte, manutenção e atualização de versões) são de natureza continuada e essenciais para garantir, de forma permanente, a disponibilidade, segurança e integridade da solução de WAF ao longo de sua vida útil. Esses serviços visam evitar interrupções que possam comprometer a continuidade dos serviços finalísticos da **PRODEMGE** e o descumprimento dos níveis de serviço acordados com seus clientes.

1.4.4. O prazo de vigência do contrato inicia-se na data da última assinatura digital aposta no instrumento, caso não esteja estabelecido o termo inicial de vigência no próprio contrato.

1.5. Documentos complementares

1.5.1. Os seguintes anexos integram este Termo de Consulta:

- Anexo I-A – Tabela de Precificação;
- Anexo I-B – Especificação Técnica da solução de WAF;
- Anexo I-C - Serviços de Instalação e configuração;
- Anexo I-D - Serviços de Migração;
- Anexo I-E - Serviços de Operação Assistida;
- Anexo I-F – Serviços de Capacitação;
- Anexo I-G - Serviços de Suporte Técnico e atualização de versão;
- Anexo I-H - Laudo técnico de recebimento dos Equipamentos;
- Anexo I-I - Laudo técnico de Execução de Serviços de instalação e configuração, migração e operação assistida.
- Anexo I-J - Ordem de Serviço de Capacitação
- Anexo I-K - Laudo técnico da Capacitação.

Anexo I-L - Laudo Técnico dos Serviços Associados
Anexo I-M - Apuração de Níveis de Serviços
Anexo I-N - Relatório de Apuração de Níveis de Serviços
Anexo I-O – Laudo Técnico de Inconformidades;

1. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO E ESPECIFICAÇÃO DO PRODUTO

1.1. A descrição da solução como um todo encontra-se detalhada na Especificação Técnica, anexo I-B deste Termo de Consulta;

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1. Motivação da contratação

2.1.1. Não se aplica nesta consulta pública.

2.2. Relação entre a necessidade da contratação e os respectivos volumes e características do objeto

2.2.1. Não se aplica nesta consulta pública.

2.3. Benefícios diretos e indiretos que resultarão da contratação.

2.3.1. Não se aplica nesta consulta pública.

3. REQUISITOS DA CONTRATAÇÃO

3.1. Participação de consórcios

3.1.1. Não é admitida a contratação de pessoas jurídicas reunidas em consórcio.

3.2. Subcontratação

3.2.1. É admitida a subcontratação parcial do objeto, nas seguintes condições:

3.2.1.1. É vedada a subcontratação completa ou da parcela principal do objeto da contratação, a qual consiste no fornecimento da solução de WAF.

3.2.1.2. Os serviços de instalação, configuração, migração, operação assistida, suporte e capacitação poderão ser subcontratados desde que executados pelo fabricante da solução ofertada ou por empresa por ele homologada, permanecendo a CONTRATADA responsável perante a CONTRATANTE pelo cumprimento de todas as obrigações contratuais.

3.3. Critérios de sustentabilidade ambiental, social e econômica

3.3.1. Não se aplica nesta consulta pública.

3.4. Indicação de marcas ou modelos (art. 114, I, do RILC)

3.4.1. Não se aplica nesta consulta pública.

3.5. Da vedação de utilização de marca/produto na execução do serviço (art. 114, IV, do RILC)

3.5.1. Não se aplica nesta consulta pública.

3.6. Exigência de carta de solidariedade

3.6.1. Em caso de licitante revendedor ou distribuidor, será exigida carta de solidariedade emitida pelo fabricante, que assegure a execução do contrato.

3.7. Garantia de execução

3.7.1. Não haverá exigência de garantia da contratação prevista no art. 131 do RILC.

3.8. Requisitos legais

3.8.1. O presente processo de contratação deve estar aderente à [Constituição Federal](#), à [Lei nº 13.303/2016](#) (Estatuto Jurídico das Estatais), o *Regulamento Interno de Licitações e Contratos – RILC*, [Lei nº 13.709, de 14 de agosto de 2018](#) (Lei Geral de Proteção de Dados Pessoais – LGPD) e a outras legislações aplicáveis.

3.9. Requisitos de Segurança e Privacidade

3.9.1. A solução deverá atender aos princípios e procedimentos elencados na Política de Segurança da Informação da **PRODEMGE**, as políticas podem ser acessadas através dos links:

a) <https://www.PRODEMGE.gov.br/privacidade-de-dados>;

b) <https://www.PRODEMGE.gov.br/governanca/politicas>.

3.10. Alteração subjetiva

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

4. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E REGIME DE EXECUÇÃO

4.1. Forma de seleção e critério de julgamento da proposta

4.1.1. O fornecedor será selecionado por meio da realização de pregão, sob a forma eletrônica, com adoção do critério de julgamento pelo menor preço.

4.2. Modo de disputa

4.2.1. Será adotado o modo de disputa “aberto”, em que os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

4.3. Intervalo entre lances

4.3.1. Não se aplica nesta consulta pública.

4.4. Regime de execução

4.4.1. O regime de execução será empreitada por preço global.

4.5. Critérios da aceitabilidade da proposta

4.5.1. Para aceitação da melhor proposta, será considerado:

4.5.1.1. Atendimento aos requisitos técnicos definidos no anexo I-B Especificação Técnica;

4.5.1.2. Compatibilidade com os valores unitários e global estimados do lote único;

4.5.1.3. Preenchimento e entrega, junto com a proposta técnica e comercial, do anexo I-A (tabela de precificação) com os preços segmentados por item do objeto, em Reais, com todos os impostos, taxas e despesas inclusos.

4.6. Análise de amostra

4.6.1. Não se aplica nesta consulta pública.

4.7. Prova de Conceito (POC)

4.7.1. Não se aplica nesta consulta pública.

5. HABILITAÇÃO

5.1. Requisitos de habilitação

5.1.1. Para esta consulta pública, não será exigida a apresentação de comprovação. Esta seção tem como objetivo apenas esclarecer os requisitos que a PROPONENTE deverá atender, caso venha a ocorrer o processo de aquisição.

5.1.2. Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos:

5.2. Habilitação jurídica

5.2.1. Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

5.2.2. Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada – EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

5.2.3. Microempreendedor Individual – MEI: Certificado da Condição de Microempreendedor Individual – CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio <https://www.gov.br/empresas-e-negocios/pt-br/empreendedor>;

5.2.4. Sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

5.2.5. Sociedade empresária estrangeira: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77/2020;

5.2.6. Filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz;

5.2.7. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

5.3. Habilitação fiscal, social e trabalhista

5.3.1. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

5.3.2. Prova de inscrição no cadastro de contribuintes municipal, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

5.3.3. Prova de regularidade fiscal perante a Fazenda Estadual de Minas Gerais;

5.3.4. Prova de regularidade relativa à Seguridade Social e ao FGTS, que demonstre cumprimento dos encargos sociais instituídos por lei;

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

5.3.6. Declaração de cumprimento do disposto no inciso XXXIII do art. 7º da Constituição Federal;

5.3.7. Caso o fornecedor seja considerado isento dos tributos relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei;

5.3.8. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar nº 123/2006, estará dispensado da prova de inscrição no cadastro de contribuintes municipal.

5.4. Capacidade Econômico-Financeira

5.4.1. Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor;

5.4.2. Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis do último exercício social, comprovando índices de Liquidez Geral (LG), Liquidez Corrente (LC) e Solvência Geral (SG) superiores a 1 (um);

5.4.2.1. Caso a empresa licitante apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido para fins de habilitação patrimônio líquido de até 10% do valor da proposta apresentada;

5.4.2.2. Os documentos referidos acima deverão ser exigidos com base no limite definido pela Receita Federal do Brasil para transmissão da Escrituração Contábil Digital – ECD ao Sped;

5.4.3. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura;

5.4.4. O atendimento dos índices econômicos previstos neste item deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo fornecedor.

5.5. Qualificação técnica

5.5.1. Não se aplica nesta consulta pública.

5.6. Qualificação técnico-operacional

5.6.1. Comprovação de aptidão para execução de objeto de complexidade tecnológica e operacional equivalente ou superior ao desta contratação, ou com o item pertinente, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado, ou regularmente emitido (s) pelo conselho profissional competente, quando for o caso.

5.6.2. Para fins da comprovação de que trata o item anterior, os atestados deverão possuir as seguintes características mínimas:

5.6.2.1. Comprovação Atestado de Capacidade Técnica comprovando o fornecimento de no mínimo, de uma solução de WAF com características compatíveis ou equivalentes ao objeto deste Termo de Consulta fornecidos por pessoa jurídica de direito público ou privado, comprovando a aptidão do licitante em fornecer o objeto licitado, atestando, inclusive, o bom desempenho e cumprimento a contento das obrigações contratuais;

5.6.2.2. Apresentação de Atestado(s) de Capacidade Técnica, emitido(s) por pessoa jurídica de direito público ou privado, que comprove(m) a aptidão da licitante para a prestação de serviços compatíveis com o objeto da contratação, contemplando, no mínimo, atividades de instalação, configuração, migração e operação assistida da plataforma. O(s) atestado(s) deverá(ão) evidenciar, ainda, o adequado desempenho na execução dos serviços e o cumprimento satisfatório das obrigações contratuais assumidas;

5.6.2.3. Todos os atestados apresentados na documentação de habilitação deverão conter, obrigatoriamente, a especificação das entregas realizadas, o nome, cargo e a empresa do declarante;

5.6.2.4. Todos os documentos emitidos em idioma diferente do português ou inglês, deverão ser acompanhados de traduções, simples ou juramentadas.

5.6.2.5. A empresa licitante deverá possuir credencial de parceria com o fabricante da solução que comprova oficialmente que a licitante possui as qualificações técnicas necessárias para prestar os

serviços de suporte técnico, bem como possui relação comercial com o fabricante, estando assim autorizada a fornecer os produtos e serviços citados neste documento.

5.6.2.6. Não será admitida a apresentação de atestado de capacidade técnica emitido por empresa ou empresas do mesmo grupo econômico em favor da licitante participante, no caso desta também pertencer ao grupo econômico

5.6.3. Será admitida, para fins de comprovação de quantitativo mínimo do serviço, a apresentação e o somatório de diferentes atestados de serviços executados de forma concomitante, pois essa situação equivale, para fins de comprovação de capacidade técnico-operacional, a uma única contratação.

5.6.4. Os atestados de capacidade técnica podem ser apresentados em nome da matriz ou da filial da empresa licitante.

5.6.5. O licitante disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela **PRODEMGE**, cópia do contrato que deu suporte à contratação, endereço atual do contratante e local em que foram prestados os serviços, entre outros documentos.

5.6.6. Os atestados deverão referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificada no contrato social vigente.

5.6.7. Em caso de apresentação por licitante de atestado de desempenho anterior emitido em favor de consórcio do qual tenha feito parte, se o atestado ou o contrato de constituição do consórcio não identificar a atividade desempenhada por cada consorciado individualmente, serão adotados os seguintes critérios na avaliação de sua qualificação técnica:

5.6.7.1. Se o atestado tiver sido emitido em favor de consórcio homogêneo, as experiências atestadas deverão ser reconhecidas para cada empresa consorciada na proporção quantitativa de sua participação no consórcio;

5.6.7.2. Se o atestado tiver sido emitido em favor de consórcio heterogêneo, as experiências atestadas deverão ser reconhecidas para cada consorciado de acordo com os respectivos campos de atuação.

5.7. Qualificação técnico-profissional

5.7.1. Não se aplica nesta consulta pública.

5.8. Vistoria

5.8.1. Não há necessidade de realização de avaliação prévia do local de prestação dos serviços.

5.9. Habilitação de subcontratadas

5.9.1. O CONTRATADO deverá apresentar à PRODEMGE atestados de capacidade técnica do subcontratado, relativos à parcela do objeto cuja subcontratação tenha sido expressamente autorizada em tópico próprio desse

Termo de Consulta, os quais serão avaliados e juntados aos autos do processo, nos termos do § 1º do art. 78 da Lei Federal nº 13.303, de 2016.

6. MODELO DE EXECUÇÃO DO OBJETO

6.1. Prazos de entrega.

6.1.1. O objeto do contrato será entregue nos seguintes prazos e condições:

Item	Descrição	Prazo de Entrega	Início da vigência
1	Solução de WAF incluindo licenciamento	30 dias úteis	Assinatura do contrato
2	Serviço de Instalação e configuração	10 dias úteis	Após o aceite provisório da entrega do equipamento
3	Serviço de Migração	40 dias úteis (aproximadamente 205 aplicações)	Após a instalação e configuração
4	Serviço de Operação Assistida	25 dias úteis	Dia útil seguinte após finalizada a migração homologada pelo cliente
5	Capacitação	40 dias úteis	Após a instalação e configuração, devendo ser concluída antes do fim da operação assistida
6	Serviços de suporte técnico continuado, incluindo atendimento, diagnósticos, substituição de peças, atualização de firmware e versões de software embarcado, garantindo a disponibilidade e continuidade operacional do ambiente.	Imediatamente após aceite definitivo dos serviços de instalação e configuração	Imediatamente após aceite definitivo dos serviços de instalação e configuração

Tabela 3 – Prazos de Entrega

6.1.2. Caso não seja possível a entrega/execução na data assinalada, o contratado deverá comunicar, por escrito, as razões respectivas, com antecedência mínima de 5 (cinco) dias, para análise de qualquer pleito de prorrogação de prazo, ressalvadas as hipóteses de caso fortuito ou força maior.

6.1.3. Para análise do pleito, a solicitação deverá conter, no mínimo:

6.1.3.1. Motivo do não cumprimento do prazo, devidamente comprovado, acompanhado da previsão do novo prazo de entrega;

6.1.3.2. Documentos que relatem e justifiquem a ocorrência do descumprimento de prazo, tais como: carta do fabricante/fornecedor, *Invoice*, laudo técnico de terceiros, boletim de ocorrência de sinistro, ou outro documento equivalente;

6.1.3.3. Evidências dos esforços realizados para mitigação de danos, com demonstração das medidas adotadas para minimizar o impacto negativo decorrente do atraso na entrega da solução.

6.1.4. A solicitação de prorrogação de prazo será analisada pela **PRODEMGE** de acordo com os princípios de razoabilidade e proporcionalidade, informando-se o **CONTRATADO** da decisão proferida.

6.1.5. Em caso de indeferimento da prorrogação do prazo de entrega, e caso não cumpra o prazo inicial, o fornecedor ficará sujeito às penalidades previstas para atraso na entrega estabelecidas neste Termo de Consulta.

6.1.6. A responsabilidade de entregar e fazer é exclusivamente do **CONTRATADO**, independente das suas relações comerciais com terceiros ou seus fornecedores, não sendo justificativa do seu inadimplemento no atendimento dos prazos estabelecidos no contrato.

6.1.7. O período de interrupção da execução contratual decorrente de evento (s) caracterizado (s) como caso fortuito ou força maior, desde que verificado (s) e aceito (s) pela **PRODEMGE**, acarretará a suspensão da contagem do prazo contratual.

6.1.8. Na contagem de prazos estabelecida em dias, excluir-se-á o dia do começo, e incluir-se-á o do vencimento, e considerar-se-ão os dias consecutivos, exceto quando for explicitamente disposto em contrário.

6.1.9. A contagem de prazos estabelecida em meses e anos expiram no dia de igual número do início, ou no imediato, se faltar exata correspondência.

6.2. Local e horário de entrega

6.2.1. Os bens deverão ser entregues nas dependências da PRODEMGE, localizada na Rua da Bahia, 2277 – CEP 30.160-019, Bairro Savassi Belo Horizonte/MG.

6.2.2. As entregas deverão ser realizadas em horário comercial, de 2ª a 6ª feira, com agendamento prévio de 3 (três) dias úteis, com a Gerência de Gestão de Ativos, através do e-mail: gga@prodemge.gov.br

6.3. Condições de entrega

6.3.1. Os itens deverão ser entregues em embalagens apropriadas e não violadas e estar acompanhados da nota fiscal, que deverá conter, além dos itens obrigatórios pela legislação vigente, o número da ordem de fornecimento e informações como descrição, marca, modelo e a quantidade correspondente a cada item.

6.3.2. Não serão recebidos materiais que apresentarem, nas embalagens, sinais de violação e/ou variação na estrutura, umidade, inadequação em relação ao conteúdo.

6.3.3. O armazenamento e o transporte dos itens deverão atender às especificações técnicas de cada produto.

6.3.4. Toda a logística de transporte será de responsabilidade da contratada, incluindo a coleta, o manuseio, o descarregamento e o deslocamento dos equipamentos até o local definitivo de instalação no datacenter, sem qualquer ônus adicional para a contratante.

6.3.5. A fim de comprovar a qualidade dos itens, caso haja queixa técnica ou suspeita de alguma irregularidade, a **PRODEMGE** poderá solicitar, a qualquer momento, amostras para análise.

6.4. Condições da prestação dos serviços

6.4.1. As condições para a execução dos serviços de instalação e configuração; serviços associados, tais como suporte, manutenção e atualização de versões; migração; operação assistida; e capacitação encontram-se detalhadas nos anexos I-C a I-G deste Termo de Consulta.

6.5. Manutenção de sigilo e confidencialidade

6.5.1. O **CONTRATADO** assinará o Termo de Sigilo e Confidencialidade para manter completo e absoluto sigilo sobre quaisquer dados, informações, documentos, especificações técnicas ou comerciais, inovações e aperfeiçoamentos que vierem a ser debatidos, desenvolvidos e/ou fornecidos por qualquer uma delas à outra em razão deste contrato, não podendo, sob qualquer pretexto, divulgar, revelar, reproduzir, utilizar ou deles dar conhecimento a terceiros sem a prévia e expressa concordância da outra Parte ou da Entidade envolvida.

6.5.2. O Termo de Sigilo e Confidencialidade prevalecerá durante toda a vigência deste contrato e por cinco anos a contar de seu término.

6.5.3. Toda e qualquer informação relativa ao contrato e aos frutos provenientes deste somente poderá ser divulgada com a anuência expressa das partes signatárias do presente contrato.

6.5.4. A divulgação de informação de forma indevida ou sem as necessárias autorizações, conforme reza o Termo de Sigilo e Confidencialidade, dá direito de reparação moral ou material, por via judicial, à parte que se julgar prejudicada.

7. MODELO DE GESTÃO DO CONTRATO

7.1. Regras gerais

7.1.1. O equipamento, acessórios, placas e softwares embarcados deverão ser entregues dentro do prazo estabelecido na Tabela 3 – Prazo Entrega deste Termo de Consulta.

7.2.

7.2.1. O contrato deverá ser executado fielmente pelas partes, de acordo com suas cláusulas, *Regulamento Interno de Licitações e Contratos da PRODEMGE – RILC* e Lei nº 13.303/2016, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

7.2.2. As comunicações entre a **PRODEMGE** e o **CONTRATADO** devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim, que deverá ser anexada em processo administrativo de fiscalização contratual.

7.2.3. A **PRODEMGE** poderá convocar o preposto/representante da empresa para adoção de providências que devam ser cumpridas de imediato.

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

7.3. Preposto/representante

7.3.1. A **CONTRATADA** designará formalmente o preposto/representante da empresa, antes do início da execução contratual, indicando no instrumento os poderes e deveres em relação à execução do objeto **CONTRATADO**.

7.3.2. A **PRODEMGE** poderá recusar, desde que justificadamente, a indicação ou a manutenção do preposto/representante da empresa, hipótese em que o **CONTRATADO** designará outro para o exercício da atividade.

7.4. Reunião Inicial

7.4.1. Após a assinatura do Contrato, o gestor do contrato deve convocar o representante da contratada para esclarecimentos relativos a questões operacionais, administrativas e de gerenciamento do contrato.

7.4.2. A reunião será realizada em até 5 (cinco) dias úteis da assinatura do Contrato, podendo ser prorrogada a critério da PRODEMGE.

7.4.3. A pauta desta reunião observará, pelo menos:

- a) Confirmação do repasse dos conhecimentos necessários;
- b) Confirmação da alocação dos recursos necessários;
- c) Esclarecimentos relativos a questões operacionais, administrativos e de gerenciamento do contrato;
- d) Regras de acesso físico às dependências (uniforme, crachá, horário etc.) e/ou lógico aos sistemas (links, acesso remoto, ambiente de desenvolvimento e de testes etc.);
- e) Acordo com clientes de negócio (classificação das informações, autorização para perfis de acesso, procedimentos de segurança etc.);
- f) Processos de identificação e senha de acesso;
- g) Outras questões que se fizerem necessárias.

7.4.4. A ata deverá conter o registro de todas as ocorrências da reunião e a assinatura com aprovação de todos os envolvidos no que for deliberado.

7.5. Rotinas de fiscalização

7.5.1. A execução do contrato deverá ser acompanhada e fiscalizada pela Equipe de Fiscalização do Contrato – EFC.

7.6. Fiscalização técnica

7.6.1. O fiscal técnico do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a **PRODEMGE**.

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

7.6.3. Identificada qualquer inexactidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção.

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

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

7.6.6. O fiscal técnico do contrato deve avaliar a execução do objeto através do Acordo de Níveis de Serviço - ANS, conforme previsto neste Termo de Consulta para aferição da qualidade da prestação dos serviços, devendo haver o redimensionamento no pagamento com base nos indicadores estabelecidos.

7.6.7. A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade do **CONTRATADO**, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica corresponsabilidade da **PRODEMGE** ou de seus agentes, gestores e fiscais, de conformidade com a legislação aplicável.

7.7. Gestor do contrato

7.7.1. O gestor do contrato coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da **PRODEMGE**.

7.7.2. Compete ao Gestor do Contrato a responsabilidade final pelas decisões relativas à prorrogação, modificação, reequilíbrio financeiro, pagamento, imposição de penalidades e extinção dos contratos.

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

7.7.4. O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela Gerência de Contratos – GCT.

7.7.5. O gestor do contrato deverá elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da **PRODEMGE**.

7.7.6. O Gestor de contratos deverá analisar os pedidos de prorrogação de prazos de entrega ou de execução de serviços, mediante avaliação das razões expostas pelo **CONTRATADO**, em especial:

7.7.7. Quanto à viabilidade técnica da concessão ou não da prorrogação do prazo requerido

7.7.8. Avaliação de eventuais prejuízos causados a **PRODEMGE** em razão do atraso e do prazo de prorrogação a ser concedido, quando for o caso.

7.7.9. Avaliação dos fatos supervenientes que justifiquem a prorrogação de prazos de execução.

8. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

8.1. Recebimento do objeto

8.1.1. Os appliances (solução de WAF) serão **recebidos provisoriamente**, de forma sumária, no ato da entrega, juntamente com a respectiva Nota Fiscal, pelo fiscal técnico do contrato, para posterior verificação de sua conformidade com as especificações constantes do Termo de Referência e da proposta vencedora.

8.1.2. O fiscal técnico do contrato deverá remeter a nota fiscal acompanhada do termo de recebimento provisório da solução de WAF às áreas de contabilidade e apoio logístico, observados os procedimentos aplicáveis ao recebimento de bens de capital (CAPEX).

8.1.3. Os appliances (solução de WAF) poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos no prazo de 5(cinco) dias úteis, a contar da notificação formal da **PRODEMGE**, às suas custas, sem prejuízo da aplicação dos níveis mínimos de serviços e das penalidades cabíveis.

8.1.4. O **recebimento definitivo** ocorrerá no prazo de até 5(cinco) dias úteis contados da emissão do Laudo técnico de Execução de Serviços de instalação e configuração, (Anexo I-I), condicionando-se à verificação da conformidade dos bens (solução de WAF) com as especificações constantes do Termo de Referência e da proposta, bem como ao atendimento aos critérios de aceitação, tais como prazo de entrega, quantidade, requisitos técnicos, testes de funcionamento e demais exigências contratuais. Cumpridas essas condições, o Gestor do Contrato emitirá o termo de recebimento definitivo.

8.1.5. O Gestor do contrato deverá remeter o termo de recebimento definitivo da solução de WAF às áreas de contabilidade e apoio logístico, observados os procedimentos aplicáveis ao recebimento de bens de capital (CAPEX).

8.1.6. Os serviços de Instalação e Configuração, Migração, Operação Assistida e Capacitação serão recebidos definitivamente pelo Gestor do contrato no prazo de 5 (cinco) dias úteis, contados da data de sua conclusão, condicionado à verificação do cumprimento integral das exigências contratuais.

8.1.6.1. O Gestor do contrato deverá remeter o termo de recebimento definitivo dos serviços de (instalação e configuração, Migração, Operação Assistida, Capacitação/Treinamento) para Gerência de Contratos – GCT, à qual competirá comunicar ao fornecedor para emissão da NOTA FISCAL, com o valor exato apurado pela fiscalização, relativo à parcela a ser paga.

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

8.1.8. Todos os serviços associados serão recebidos por meio do ateste, servindo como declaração da regular execução do serviço, bem como do atendimento aos acordos de nível de serviço, observadas eventuais glosas aplicáveis.

8.1.9. Para fins de recebimento de todos os serviços associados, ao término de cada período de faturamento, o Fiscal Técnico do Contrato deverá apurar os resultados da execução do objeto, analisando, se for o caso, o desempenho e a qualidade da prestação dos serviços, conforme os indicadores previstos, o que poderá implicar redimensionamento dos valores a serem pagos ao **CONTRATADO**. O resultado deverá ser registrado em relatório e encaminhado à Gerência de Contratos – GCT.

8.1.10. Havendo controvérsia quanto à execução do objeto, seja em relação à dimensão, qualidade ou quantidade, deverá ser comunicada ao **CONTRATADO** para emissão de nota fiscal ou fatura referente à parcela incontroversa, para efeito de pagamento.

8.1.11. O prazo para solução, pelo **CONTRATADO**, de inconsistências na execução do objeto ou para o saneamento de irregularidades na nota fiscal ou fatura, identificadas pela **PRODEMGE** durante a análise prévia ao pagamento, não será computado para efeito de contagem do prazo de recebimento definitivo.

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

8.1.13. A **CONTRATADA** ficará obrigada a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verifiquem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados, podendo a fiscalização reter o ateste da última e/ou única medição de serviços até a plena regularização das pendências.

8.2. Níveis mínimos de serviço exigidos

8.2.1. A avaliação da execução do objeto utilizará o Acordo de Níveis de Serviço - ANS, conforme previsto no Anexo I-M, para aferição da qualidade da prestação dos serviços.

8.3. Condições de pagamento

8.3.1. O pagamento está condicionado ao recebimento definitivo ou ateste de execução dos serviços, e deverá ser efetuado mediante a apresentação, pelo **CONTRATADO**, de Nota Fiscal/Fatura ou documento equivalente contendo o detalhamento do objeto executado.

8.3.2. As Notas Fiscais/Faturas de serviços deverão ser encaminhadas até o dia 25 (vinte e cinco) de cada mês, para o endereço de correio eletrônico gct@prodemge.gov.br.

8.3.3. A primeira Nota Fiscal/Fatura relativa aos serviços continuados, (suporte, manutenção e atualização de versões), deverá ser emitida após o decurso de 30 (trinta) dias a contar do recebimento definitivo dos bens

appliances, devendo as Notas Fiscais/Faturas subsequentes serem emitidas a partir da data final do período de adimplemento de cada parcela.

8.3.4. As Notas Fiscais/Faturas encaminhadas em desacordo com as condições elencadas no item acima conferem à PRODEMGE o direito de solicitar o cancelamento delas.

8.3.5. As Notas Fiscais (DANFE) que acompanham o fornecimento de bens (Appliances) deverão, também, ser enviadas para o endereço de correio eletrônico gct@prodemge.gov.br.

8.3.6. Para fins de pagamento, a Gerência de Contratos – GCT, deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:

8.3.6.1. Identificação completa do fornecedor/beneficiário (nome, endereço, CNPJ ou CPF, matrícula, inscrição estadual e inscrição municipal);

8.3.6.2. Identificação completa da **PRODEMGE** (nome, endereço, CNPJ, inscrição estadual e inscrição municipal);

8.3.6.3. Descrição clara da natureza do fornecimento do produto ou do serviço prestado, do número do contrato e o mês/período da prestação de serviços.

8.3.6.4. Informações bancárias necessárias para viabilizar o pagamento;

8.3.6.5. Ausência de rasuras que ponham em dúvida sua autenticidade;

8.3.6.6. O prazo de validade;

8.3.6.7. A data da emissão;

8.3.6.8. O período respectivo de execução do contrato;

8.3.6.9. O valor a pagar; e

8.3.6.10. Eventual destaque do valor de retenções tributárias cabíveis.

8.3.7. Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça o pagamento, esta ficará sobrestada até que o **CONTRATADO** providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus à **PRODEMGE**.

8.3.8. Caso o **CONTRATADO** opte por efetuar o faturamento por meio de CNPJ (matriz ou filial) distinto do constante do contrato, deverá comprovar a regularidade fiscal tanto do estabelecimento **CONTRATADO** como do estabelecimento que efetivamente executar o objeto, por ocasião dos pagamentos.

8.3.9. A Gerência de Contratos – GCT, deverá realizar consulta ao CAGEF, ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 65, II, do RILC para:

8.3.9.1. Verificar a manutenção das condições de habilitação exigidas no edital;

8.3.9.2. Identificar possível razão que impeça a participação em licitação ou de contratar com o Poder Público, bem como ocorrências impeditivas indiretas.

8.3.10. Constatando-se, junto ao CAGEF, a situação de irregularidade do **CONTRATADO**, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da **PRODEMGE**.

8.3.11. A falta de regularização ou a improcedência da defesa apresentada não constituem justificativa para a retenção de pagamento de objeto efetivamente executado. Em vez disso, tais situações ensejarão a abertura de processo administrativo contra a empresa, o qual poderá resultar na aplicação de sanção por descumprimento de cláusula contratual, conforme previsto no contrato.

8.3.12. A **PRODEMGE**, observados os princípios do contraditório e da ampla defesa, poderá deduzir, cautelar ou definitivamente, do montante a pagar ao **CONTRATADO**, os valores correspondentes a multas, ressarcimentos ou indenizações devidas pelo **CONTRATADO**, nos termos deste contrato.

8.4. Prazo de pagamento

8.4.1. O pagamento relativo ao fornecimento de bens (Appliances) e aos serviços prestados, abrangendo Instalação e Configuração, Migração, Operação Assistida e Capacitação, será realizado no prazo máximo de 30 (trinta) dias corridos, contados a partir da emissão do termo de recebimento definitivo, conforme disposto na seção anterior.

8.4.2. O pagamento relativo aos serviços associados de natureza continuada (Suporte, Manutenção, atualização de versões), será realizado no prazo máximo de 30 (trinta) dias corridos, contados da data do recebimento da Nota Fiscal/Fatura no endereço de correio eletrônico gct@PRODEMGE.gov.br.

8.5. Forma de pagamento

8.5.1. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo **CONTRATADO**.

8.5.2. O desconto de títulos ou cobrança bancária somente poderá ser efetuado com a prévia autorização por escrito da **PRODEMGE**.

8.5.3. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

8.5.4. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

8.5.5. O **CONTRATADO** regularmente optante pelo Simples Nacional, nos termos da [Lei Complementar nº 123, de 2006](#), não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime.

No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

8.6. Critérios de reajuste

8.6.1. Os preços são fixos e irrealizáveis no prazo mínimo de 1 (um) ano contado da data limite para a apresentação das propostas.

8.6.2. Após o interregno mínimo de um ano, os preços iniciais podem ser reajustados, mediante a aplicação, pela **PRODEMGE**, do índice de ICTI/IPEA (Índice de Custo da Tecnologia da Informação), exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

8.6.3. Os reajustes deverão ser precedidos de solicitação do **CONTRATADO**

8.6.4. Os efeitos financeiros do reajuste serão devidos a partir da data da solicitação formal do **CONTRATADO**, a qual deverá fazê-lo tempestivamente até a data de prorrogação contratual, sob pena de preclusão do direito

8.6.5. Ocorrerá igualmente a preclusão do direito ao reajuste, caso a solicitação seja formulada depois de extinto o contrato

8.6.6. Nos reajustes subsequentes ao primeiro, o interregno mínimo de 1 (um) ano será contado a partir dos efeitos financeiros do último reajuste.

8.6.7. No caso de atraso ou não divulgação do índice de reajustamento, a **PRODEMGE** pagará ao **CONTRATADO** a importância calculada pela última variação conhecida, quitando a diferença correspondente tão logo seja divulgado o índice definitivo.

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

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

8.6.10. O reajuste será realizado por apostilamento.

8.6.11. O reajuste não interfere no direito das partes de solicitar, a qualquer momento, a manutenção do equilíbrio econômico dos contratos com base no disposto no art. 164 do RILC.

8.6.12. O **CONTRATADO** deverá complementar eventual garantia contratual anteriormente prestada, de modo que se mantenha a proporção inicial em relação ao valor **CONTRATADO**.

9. PAPÉIS E RESPONSABILIDADES

9.1. São obrigações da contratante:

9.1.1. Exigir o cumprimento de todas as obrigações assumidas pelo **CONTRATADO**, de acordo com Termo de Referência e demais documentos que pautaram a contratação.

9.1.2. Receber o objeto no prazo e condições estabelecidas neste Termo de Consulta.

9.1.3. Notificar o **CONTRATADO**, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto fornecido, para que seja por ele substituído, reparado ou corrigido, no total ou em parte, às suas expensas.

9.1.4. Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pelo **CONTRATADO**.

9.1.5. Comunicar o **CONTRATADO** para emissão de Nota Fiscal relativa à parcela incontroversa da execução do objeto, para efeito de pagamento, quando houver controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade.

9.1.6. Efetuar o pagamento ao **CONTRATADO** do valor correspondente à execução do objeto, no prazo, forma e condições estabelecidos neste Termo de Consulta.

9.1.7. Aplicar ao **CONTRATADO** as sanções previstas na Lei e em Termo de Referência.

9.1.8. Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente Contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste.

9.1.9. A **PRODEMGE** não responderá por quaisquer compromissos assumidos pelo **CONTRATADO** com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato do **CONTRATADO**, de seus empregados, prepostos ou subordinados.

9.2. São obrigações do contratado:

9.2.1. O **CONTRATADO** deve cumprir todas as obrigações constantes deste Termo de Consulta e dos demais documentos que pautaram a contratação, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as demais obrigações constantes deste item:

9.2.1.1. Cumprir os prazos previstos neste Termo de Consulta;

9.2.1.2. Indicar formalmente representante junto à **PRODEMGE**, que deverá responder pela fiel execução do contrato;

9.2.1.3. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

9.2.1.4. Reparar quaisquer danos diretamente causados à Contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução do contrato pela Contratante;

9.2.1.5. Propiciar todos os meios necessários à fiscalização do contrato pela Contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão;

9.2.1.6. Manter, durante toda a execução do contrato, as mesmas condições da habilitação;

9.2.1.7. Quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;

9.2.1.8. Responsabilizar-se pelo cumprimento das obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade a **PRODEMGE**.

9.2.2. Quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato;

9.2.2.1. Ceder os direitos patrimoniais dos artefatos produzidos para a PRODEMGE em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados à **PRODEMGE**;

9.2.2.2. Fazer a transição contratual, com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações, podendo exigir, inclusive, a capacitação dos técnicos do contratante ou da nova empresa que continuará a execução do contrato, quando for o caso;

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

9.2.2.4. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança da **PRODEMGE**

10. SANÇÕES ADMINISTRATIVAS

10.1. Em caso de infrações cometidas pelo **CONTRATADO** na execução do contrato, aplicar-se-ão as disposições do *Manual de Processo Sancionatório em Licitações e Contratos* e do *Regulamento Interno de Licitações e Contratos* da **PRODEMGE**.

10.2. Considera-se infração administrativa, para os fins deste Contrato, o cometimento, pelo **CONTRATADO**, de qualquer das seguintes condutas:

- I. Der causa à inexecução parcial do contrato;
- II. Der causa à inexecução parcial do contrato que acarrete grave dano à **PRODEMGE**, ao funcionamento dos serviços públicos ou ao interesse coletivo;
- III. Der causa à inexecução total do contrato;
- IV. Ensejar retardamento da execução ou da entrega do objeto, sem motivo justificado;

- V. Apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;
- VI. Praticar ato fraudulento na execução do contrato;
- VII. Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
- VIII. Praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

10.3. Constatada a ocorrência de qualquer das infrações descritas no item 11.2, poderão ser aplicadas ao **CONTRATADO** as seguintes sanções:

10.3.1. **Advertência** – aviso formal por escrito, aplicável nos casos de descumprimento contratual de natureza leve, tais como:

- a) Não apresentação de cópia de guias quitadas de INSS, FGTS ou de outros recolhimentos legais, quando solicitado pela **PRODEMGE**;
- b) Descumprimento de prazos acordados para execução do objeto contratual, sem prejuízos para a **PRODEMGE**;
- c) Mora na reexecução do objeto contratual rejeitado pela fiscalização, sem ocorrência de prejuízos para a **PRODEMGE**.

10.3.2. **Multa** – aplicável às faltas de natureza média ou grave, nas seguintes modalidades:

- a) **Moratória** de 0,20% por dia de atraso injustificado, calculada sobre o valor da parcela inadimplida, até o limite de 30 (trinta) dias;
- b) **Moratória** de 0,07% do valor total do contrato por dia de atraso injustificado, até o limite de 2% (dois por cento), pela inobservância do prazo para apresentação, suplementação ou reposição da garantia;
- c) **Compensatória** de 0,05% do valor do contrato, para reincidência de falta já punida com advertência;
- d) **Compensatória** de até 10% da parcela inadimplida, nos casos de inexecução parcial do contrato, inclusive quando:
 - 1. Ocorrer execução deficitária ou defeituosa de parcela do objeto;
 - 2. Ocorrer descumprimento de obrigações acessórias previstas no contrato, edital ou anexos;
 - 3. Houver 2 (dois) descontos consecutivos ou 4 (quatro) alternados, no período de 1 (um) ano, por descumprimento de níveis mínimos de serviço, sem justificativa aceita;
 - 4. Ocorrer descumprimento de níveis mínimos de serviço que resultem na aplicação do desconto máximo sobre o valor faturado;

5. Houver não atendimento imotivado das determinações da fiscalização do contrato;
6. Ocorrer descumprimento de item estabelecido no Termo de Sigilo e Confidencialidade;
7. Houver atraso na entrega ou execução do objeto superior a 30 (trinta) dias, sem prejuízo da aplicação da multa moratória.

e) **Compensatória** de até 20% do valor do contrato, nos casos de inexecução total, inclusive quando:

1. Não houver início da execução do objeto no prazo contratual;
2. O objeto for executado de forma defeituosa e não houver possibilidade de aproveitamento;
3. Houver paralisação definitiva da execução, sem aproveitamento da parcela realizada;
4. Houver atraso superior a 30 (trinta) dias, sem entrega integral do objeto;

f) Para infração de apresentar documentação falsa ou prestar declaração falsa, multa de 10% do valor do Contrato.

g) Para infração de praticar ato fraudulento, comportar-se de modo inidôneo ou praticar outros atos lesivos previstos no art. 5º da Lei nº 12.846, de 1º de agosto de 2013, multa de 20% do valor do Contrato.

10.3.3. **Suspensão** – impedimento temporário de participar de licitações e contratar com a **PRODEMGE**, pelo prazo de 1 (um) a 24 (vinte e quatro) meses, conforme a gravidade da infração, observando-se, entre outros, os seguintes critérios:

- a) Descumprimento do prazo fixado para adoção de medidas corretivas, quando da aplicação da sanção de advertência: Sanção de 1 (um) a 6 (seis) meses;
- b) Não apresentação da documentação ou da garantia, nos termos do instrumento: Sanção - de 1 (um) a 6 (seis) meses;
- c) Atraso na execução do objeto que não cause grave prejuízo à **PRODEMGE**: Sanção - de 1 (um) a 6 (seis) meses.
- d) Quando o licitante deliberadamente não responder às diligências destinadas a esclarecer ou a complementar a instrução do processo administrativo licitatório: Sanção – de 6 (seis) a 12 (doze) meses
- e) Alteração de quantidade ou qualidade prevista no edital ou na proposta que não cause grave prejuízo à **PRODEMGE**: Sanção – de 6 (seis) a 12 (doze) meses
- f) Alteração de quantidade ou qualidade prevista no edital ou na proposta que cause grave prejuízo à **PRODEMGE**: Sanção – de 12 (doze) a 24 (vinte e quatro) meses;

g) Retardamento imotivado na execução de serviço, obra ou fornecimento de bens que implique necessária rescisão contratual: Sanção - de 12 (doze) meses a 24 (vinte e quatro) meses;

h) Paralisação do serviço, obra ou fornecimento de bens sem justo motivo e prévia anuência da **PRODEMGE**: Sanção - de 12 (doze) a 24 (vinte e quatro) meses;

i) Entrega de documentação ou de objeto contratual falsificado ou adulterado, ou cometer no procedimento de contratação de qualquer outro modo, comportar-se de modo inidôneo, ou cometer fraude fiscal: Sanção - de 12 (doze) a 24 (vinte e quatro) meses;

j) Inexecução parcial do contrato: Sanção - de 12 (doze) a 24 (vinte e quatro) meses;

k) Recusa injustificada do adjudicatário em assinar o contrato ou ata de registro de preços, aceitar ou retirar o instrumento equivalente, quando convocado dentro do prazo de validade de sua proposta: Sanção de 12 (doze) a 24 (vinte e quatro) meses;

l) Atraso na execução do objeto que cause grave prejuízo à **PRODEMGE**: Sanção - de 12 (doze) a 24 (vinte e quatro) meses;

m) Inexecução total do contrato: Sanção - 24 (vinte e quatro) meses.

10.4. A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado à **PRODEMGE**.

10.5. Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa.

10.6. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pela **PRODEMGE** ao **CONTRATADO**, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente.

10.7. Antes do ajuizamento, a multa poderá ser recolhida administrativamente no prazo de até 10 (dez) dias úteis, contados do recebimento da comunicação pela autoridade competente.

10.8. A aplicação de sanções será precedida de processo administrativo que assegure o contraditório e a ampla defesa, observado o procedimento previsto no *Manual de Processo Sancionatório em Licitações e Contratos da PRODEMGE*.

10.9. Quando a infração administrativa também for tipificada como ato lesivo na Lei nº 12.846, de 2013, a apuração e o julgamento ocorrerão conjuntamente, nos mesmos autos, observados o rito procedimental e a autoridade competente.

10.10. A dosimetria das sanções observará a natureza e a gravidade da infração, a extensão e relevância da obrigação descumprida, a culpabilidade do **CONTRATADO**, os objetivos da sanção e os princípios da razoabilidade e da proporcionalidade.

11. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

11.1. Não se aplica neste momento de consulta.

12. RECURSOS ORÇAMENTÁRIOS

12.1. Não se aplica neste momento de consulta.

Anexo I-A – Tabela de Precificação

As PROPONENTES deverão preencher a tabela a seguir, detalhando marca e modelo dos appliances, valores unitários de cada item e valores totais de cada item, considerando o quantitativo total de cada item e o valor total por lote.

Os preços devem ser apresentados em Reais (R\$), com todos os impostos, taxas e despesas inclusas.

A CONTRATADA deverá incluir no preço dos serviços todos custos de mão de obra, incluindo encargos e despesas de transporte, traslado e alimentação de sua equipe.

Os cenários abaixo são independentes e destinam-se exclusivamente à prospecção de mercado, não representando definição da quantidade final a ser contratada.

Cenário 1				
Descrição	Unidade	Quantidade	Valor Unitário	Valor Total
Solução de WAF incluindo licenciamento	Unidade	4		
Serviço de Instalação e configuração	Prestação de serviços	1		
Serviço de Migração	Prestação de serviços	1		
Serviço de Operação Assistida	Prestação de serviços	1		
Capacitação para uma turma de 4 alunos.	Prestação de serviços	1		
Serviços de suporte técnico continuado, incluindo atendimento, diagnósticos, substituição de peças, atualização de firmware e versões de software embarcado, garantindo a disponibilidade e continuidade operacional do ambiente por 60 meses	Prestação de serviços 24x7x365	1		
Proposta válida até: dia/mês/ano			Total consolidado	

Anexo I-B – Especificação Técnica da solução de WAF

1. ESPECIFICAÇÃO TÉCNICA DETALHADA DOS ITENS

1.1. CARACTERÍSTICAS ESPECÍFICAS DE CADA APPLIANCE:

- 1.1.1. Possuir a capacidade mínima para tratar 17,5 Gbps processando em camada 4 (L4);
- 1.1.2. Possuir capacidade mínima para tratar 21,25 Gbps processando em camada 7 (L7) sem inspeção de WAF habilitada;
- 1.1.3. Possuir capacidade mínima para tratar 825.000 (oitocentos e vinte e cinco mil) de requisições em L7 com WAF habilitado (capacidade de requisições por segundo já contemplada nos RPS máximos);
- 1.1.4. Possuir capacidade de compressão de 10 (dez) Gbps;
- 1.1.5. Possuir capacidade de manter, no mínimo, 21.250.000 (vinte e um milhões e duzentos e cinquenta mil) de conexões simultâneas na camada 4;
- 1.1.6. Possuir a capacidade de tratar 350.000 (trezentos e cinquenta mil) novas conexões em L4 por segundo;
- 1.1.7. Possuir a capacidade de tratar 20.000.000 (vinte milhões) de SYN Cookies por segundo;
- 1.1.8. Possuir a capacidade de tratar 825.000 (oitocentos e vinte e cinco mil) requisições em camada 7 por segundo;
- 1.1.9. Possuir capacidade de processar 11,25 Gbps de throughput de tráfego SSL bulk (com RSA 2048 bits);
- 1.1.10. Possuir capacidade de processar 20.000 (vinte mil) transações por segundo TLS com RSA 2K;
- 1.1.11. Possuir capacidade de processar 12.500 (doze mil e quinhentas) transações por segundo TLS com ECDHE-ECDSA P-256;
- 1.1.12. Deve possuir no mínimo 02 (duas) portas QSFP+ 40 G / QSFP28 100G;
- 1.1.13. Deve possuir no mínimo 04 (quatro) portas SFP28/SFP+ 25G/10G;
- 1.1.14. Vir acompanhado de seus respectivos módulos, sendo, no mínimo, 04 (quatro) módulos SFP+ 10GBASE-SR;
- 1.1.15. Deve possuir uma interface 1000BASE-T UTP RJ45 dedicada para gerenciamento;
- 1.1.16. Possuir uma interface USB 3.0 para transferência de arquivos;
- 1.1.17. Possuir interface serial para gerenciamento;
- 1.1.18. Não serão aceitos equipamentos servidores e SO genéricos, somente appliance dedicado;
- 1.1.19. Permitir a criação de múltiplas partições administrativas independentes, às quais poderão ser associados servidores virtuais (VIPs) específicos. O balanceamento de carga deverá possibilitar a distribuição dos VIPs entre os appliances do cluster de acordo com a demanda de cada partição, mantendo gerenciamento centralizado das funcionalidades de balanceamento de carga e proteção de aplicações web;
- 1.1.20. Possuir disco interno com tecnologia SSD (1 TB M.2);
- 1.1.21. Possuir fontes internas redundantes (Dual PSU);
- 1.1.22. Possuir altura máxima de 01 (um) RU compatível com rack 19";
- 1.1.23. A solução deve permanecer operante após fim de garantia sem interrupção de tráfego ou funcionalidades, sendo permitida apenas a cessação de atualizações de assinaturas/bases.

2. REQUISITOS GERAIS

- 2.1. Suportar IPv4 e IPv6;
- 2.2. Suportar múltiplas tabelas de roteamento independentes em IPv4 e IPv6;
- 2.3. Suportar VXLAN para integração com o ambiente de virtualização;
- 2.4. Suportar configuração de endereçamento IP estático e dinâmico (DHCP/BOOTP) para o gerenciamento;
- 2.5. Suportar implementação em alta disponibilidade,

- 2.6. Implementar modo ativo/standby;
- 2.7. Suportar modo ativo/ativo para, pelo menos, as funções de balanceamento de servidores. Aceita-se como ativo/ativo a utilização de vários endereços virtuais (múltiplos IPs Virtuais) onde cada endereço fica ativo em um elemento e standby no outro sendo um total de 4 (quatro) caixas;
- 2.8. A solução deverá contemplar a aquisição e implantação de 04 (quatro) appliances, destinados à expansão da infraestrutura de balanceamento de carga e disponibilização de serviços de aplicação da CONTRATANTE.
- 2.9. Os equipamentos deverão suportar arquitetura de alta disponibilidade e distribuição de carga entre os appliances, utilizando mecanismo de agrupamento lógico dos serviços para fins de distribuição, redundância e alta disponibilidade, a exemplo de grupos de tráfego, grupos de failover ou tecnologia funcionalmente equivalente de forma que os equipamentos possam operar de maneira redundante e resiliente. A arquitetura deverá permitir que, para cada grupo de tráfego configurado, um equipamento atue como ativo e outro como contingência (standby/backup), possibilitando a transferência dos serviços para o equipamento redundante em caso de indisponibilidade, falha ou manutenção planejada. Deverá ser possível configurar a relação de redundância de forma bidirecional, permitindo que um equipamento seja responsável pelos serviços de outro e, simultaneamente, que o segundo equipamento seja responsável pelos serviços do primeiro, conforme a distribuição dos respectivos grupos de redundância de tráfego.
- 2.10. A solução deverá permitir a distribuição dos serviços entre os 04 (quatro) appliances, de modo a possibilitar a utilização dos recursos computacionais disponíveis e evitar que um único equipamento concentre a totalidade dos serviços, mantendo, entretanto, a capacidade de contingência e recuperação automática dos serviços em caso de falha de um dos appliances.
- 2.11. Os equipamentos deverão manter a utilização de particionamento lógico, permitindo a criação e administração independente de particionamento lógico administrativo dentro dos appliances. Cada partição deverá possibilitar a segregação lógica de configurações, objetos, políticas e serviços de diferentes ambientes ou aplicações, conforme as necessidades da CONTRATANTE.
- 2.12. Deverá ser mantida a arquitetura baseada em múltiplas interfaces virtuais de entrega de aplicação, permitindo que seja configurado um ou mais interfaces virtuais de entrega de aplicação de forma independente em cada partição lógica, conforme a necessidade dos serviços publicados. As interfaces virtuais de entrega de aplicação deverão permanecer associados às respectivas partições e permitir a aplicação independente de políticas, pools, monitores, perfis e demais objetos necessários à operação dos serviços.
- 2.13. A solução deverá possibilitar que os serviços configurados nas diferentes partições lógicas sejam associados aos respectivos grupos de redundância de tráfego, permitindo sua distribuição e redundância entre os 04 (quatro) appliances sem perda da segregação lógica dos ambientes.
- 2.14. A arquitetura deverá, portanto, preservar os seguintes requisitos:
 - 2.14.1. 04 (quatro) appliances;
 - 2.14.2. Utilização de grupos de redundância de tráfego para distribuição e alta disponibilidade dos serviços;
 - 2.14.3. Possibilidade de configuração ativo/backup de forma bidirecional entre os appliances;
 - 2.14.4. Possibilidade de distribuição dos serviços entre os quatro equipamentos;
 - 2.14.5. Manutenção de partições lógicas independentes;
 - 2.14.6. Manutenção de múltiplas interfaces virtuais de entrega de aplicação, com possibilidade de associação das interfaces virtuais de entrega de aplicação às respectivas partições;
 - 2.14.7. Segregação lógica de configurações, objetos e serviços entre as partições;
 - 2.14.8. Capacidade de transferência dos serviços para o equipamento redundante em caso de falha ou indisponibilidade do equipamento ativo;

- 2.14.9. Preservação da configuração e operação independente dos serviços de cada partição durante a distribuição e failover dos grupos de redundância de tráfego.
- 2.15. Permitir a sincronização das configurações de forma automática e manual, forçando a sincronização quando necessário;
- 2.16. Permitir utilizar qualquer endereçamento IP, inclusive os definidos na RFC 1918, para criação de cluster, heartbeat e sincronização entre os equipamentos;
- 2.17. Fornecer todos os recursos de redundância da solução sem nenhuma despesa com licenças adicionais;
- 2.18. Permitir a expansão do cluster com a inclusão de novos equipamentos, inclusive de modelos ou gerações diferentes, garantindo capacidade igual ou superior à dos nós instalados e total compatibilidade com as funcionalidades de Alta Disponibilidade (HA) e gerenciamento do ambiente.
- 2.19. Possuir interface gráfica via web e interface via CLI por SSH e console para administração, gerenciamento e monitoramento do equipamento;
- 2.20. Implementar o SNTP (Simple Network Time Protocol) ou NTP (Network Time Protocol);
- 2.21. Permitir habilitar e desabilitar acesso administrativo via SSH por qualquer interface do equipamento;
- 2.22. Manter internamente múltiplos arquivos de configurações do sistema;
- 2.23. Utilizar SCP ou HTTPS como mecanismo de transferência de arquivos de configuração e sistema operacional;
- 2.24. Possuir recurso de autocompletar nos comandos na CLI, com ajuda contextual;
- 2.25. Permitir a configuração de múltiplas contas locais de administradores;
- 2.26. Implementar controles de acesso por nível, os quais podem ser atribuídos a usuários ou grupos de usuários para fazer cumprir a separação por perfil de privilégios;
- 2.27. Possuir, no mínimo, três níveis de usuários na GUI: administrador, analista e somente-leitura;
- 2.28. Suportar autenticação e autorização externa de usuários administradores através de RADIUS, LDAP, Active Directory e TACACS+;
- 2.29. A interface gráfica deve permitir a atualização do sistema operacional, atualização de componentes e instalação de patches;
- 2.30. Permitir selecionar pela interface gráfica a versão do sistema operacional para inicialização do equipamento;
- 2.31. Possuir um comando, via CLI, que mostre o tráfego de utilização das interfaces (bps e pps);
- 2.32. Possuir o registro local de eventos relevantes do sistema e suportar o envio via syslog de eventos relevantes ao sistema, com capacidade de configuração de múltiplos servidores de syslog;
- 2.33. Implementar rate limit da taxa logs enviados para servidores externos, com o objetivo de prevenir a sobrecarga e perda de logs por motivos de alta utilização de CPU, memória ou uso de banda;
- 2.34. Implementar SNMPv1, SNMPv2c e SNMPv3;
- 2.35. Implementar traps SNMP;
- 2.36. Possuir MIBs proprietárias do fabricante e permitir a exportação/mapeamento de OIDs customizados para monitoramento.
- 2.37. Possuir suporte a monitoração utilizando RMON através de pelo menos 4 (quatro) grupos: statistics, history, alarms e events
- 2.38. Possuir agente integrado de coleta e exportação de métricas de desempenho e eventos;
- 2.39. Coleta de métricas de desempenho compatível com Prometheus;
- 2.40. Coleta de métricas de desempenho em formato JSON utilizando cliente HTTP;
- 2.41. Exportação de métricas de desempenho compatíveis com, pelo menos, os sistemas AWS CloudWatch e S3, Azure Log Analytics e Application Insights, Elasticsearch, Fluentd, GCP Cloud Monitoring e Logging, Graphite, Kafka e StatsD;

- 2.42. A solução devera possuir capacidade de geração de logs access_log no formato apache combined, de alta capacidade com possibilidade de customização e adição de tags customizadas de syslog para o encaminhamento correto de cada aplicação nos concentradores de logs remoto.
- 2.43. Exportação de métricas de desempenho em formato JSON para um servidor HTTP;
- 2.44. Permitir definir critérios de inclusão e exclusão de coleta e exportação de métricas;
- 2.45. Deve incluir métricas de desempenho relacionadas a servidores virtuais, pool e pool members;
- 2.46. Deve incluir métricas de throughput, conexões, bits, pacotes, disponibilidade;
- 2.47. Deve incluir métricas de requisições, respostas;
- 2.48. Deve incluir métricas de criptografia, incluindo cifras, algoritmos, versão, conexões, bytes criptografados, bytes descriptografados;
- 2.49. Deve incluir métricas de certificados digitais, incluindo data de expiração, issuer e subject;
- 2.50. Deve incluir métricas relacionadas a CPU, memória, discos e interfaces;
- 2.51. Deve incluir métricas de desempenho dos scripts de manipulação de tráfego, incluindo total de execuções, média de ciclos, máximo e mínimo de ciclos e falhas;
- 2.52. Deve incluir informações de inventário (hostname, id, versão, localização, plataforma, chassi, módulos provisionados);
- 2.53. Deve incluir métricas do cluster, incluindo data de sincronização;
- 2.54. Deve incluir informações de data da última configuração aplicada;
- 2.55. Deve possuir documentação pública do fabricante contendo informações de configurações, exemplos de configuração e modelos de mensagens;
- 2.56. Implementar debugging utilizando CLI via console e SSH;
- 2.57. Possuir ferramenta interna nativa de captura de tráfego de rede com informações contextuais da solução inseridas em cada pacote/frame;
- 2.58. Permitir a exportação de informações de diagnóstico, logs, configurações, desempenho para análises externas sem interferência na solução em produção. A análise deve ser feita em ferramenta, disponível sem custo adicional, online via web ou via aplicação para Windows, Linux ou MacOS;
- 2.59. Deve possuir suporte a Link Layer Discovery Protocol (LLDP), com, pelo menos, as informações: Port ID, TTL, Port Description, System Name, System Description, Management Address, Port VLAN ID, Port and Protocol VLAN ID, VLAN Name, Protocol Identity, Link Aggregation, Maximum Frame Size
- 2.60. Suportar exportação de informações de fluxos através sFlow, NetFlow, IPFIX ou outro protocolo similar;
- 2.61. Permitir a implementação de lógicas personalizadas para inspeção e tratamento do tráfego, por meio de regras, políticas, códigos, scripts ou tecnologia funcionalmente equivalente, possibilitando ações como permitir, bloquear, descartar, redirecionar, encaminhar, alterar, substituir e comparar valores ou atributos obtidos da conexão, da sessão, dos cabeçalhos, do conteúdo das mensagens e dos protocolos processados;
- 2.62. Permitir que as regras, políticas, códigos, scripts ou mecanismos equivalentes utilizem listas, tabelas, objetos, repositórios ou outras fontes de dados, internas ou externas, para verificar critérios e subsidiar decisões relacionadas ao estabelecimento, encaminhamento ou tratamento de conexões, sessões e requisições.
- 2.63. Serão aceitas diferentes nomenclaturas, linguagens e formas de implementação, desde que o fabricante ou fornecedor demonstre o atendimento às funcionalidades e aos resultados requeridos.
- 2.64. Implementar roteamento IPv4 e IPv6 estático e dinâmico;
- 2.65. Suportar a criação de múltiplos domínios de roteamento, com tabelas de rotas isoladas, em IPv4 e IPv6, BGP, OSPF e RIP em IPv4 e IPv6;
- 2.66. Permitir que cada domínio de roteamento utilize BGP, OSPF e RIP em IPv4 e IPv6;
- 2.67. Suportar integração via BGP para divulgação de prefixos;

- 2.68. Deve garantir que o retorno do tráfego seja encaminhado para o mesmo host que enviou o tráfego inicialmente para a solução, independente da configuração de rotas do equipamento. Por exemplo, no caso de múltiplos roteadores com acesso à Internet, a solução deve enviar o tráfego de retorno para o cliente sempre para o mesmo roteador que encaminhou o tráfego do cliente inicialmente para a solução;
- 2.69. Suportar Equal Cost Multipath (ECMP);
- 2.70. Implementar Bidirectional Forward Detection (BFD);

3. ENTREGA DE APLICAÇÕES E BALANCEAMENTO DE CARGA

- 3.1. Suportar os protocolos HTTP/1.0, HTTP/1.1, HTTP/2 e HTTP/3, para comunicação com o cliente e comunicação com o servidor;
- 3.2. Implementar a reutilização de conexões entre a solução e os servidores, para diferentes clientes e diferentes requisições;
- 3.3. Suportar os métodos de balanceamento round robin, least connections, weighted (por peso), tempo de resposta mais rápida baseado no tráfego real, baseado em parâmetros dinâmicos coletados via SNMP ou WMI;
- 3.4. Implementar criptografia de cookies;
- 3.5. Implementar persistência com pelo menos os métodos por cookie inserindo um novo cookie na sessão, por cookie utilizando um valor do cookie da aplicação, sem adição de cookie, por endereço IP destino, por endereço IP origem, por sessão SSL, parâmetros da URL acessada, parâmetro no header HTTP, qualquer informação do payload camada 7;
- 3.6. Permitir configuração de grupos de servidores secundários que devem ser utilizados para balanceamento somente quando uma quantidade mínima especificada de servidores estiver disponível no grupo primário. Caso o número de servidores disponíveis fique menor do que o especificado, a solução deve automaticamente distribuir o tráfego para o próximo grupo. Caso o número de servidores disponíveis volte ao valor mínimo, a solução deve automaticamente voltar a utilizar o grupo primário de servidores;
- 3.7. Permitir a replicação do tráfego destinado a servidores virtuais, permitindo habilitar a cópia do tráfego entre o cliente e a solução e entre a solução e o servidor;
- 3.8. Implementar pelo menos monitores de servidores de servidores via ICMP, conexões TCP e UDP pela respectiva porta no servidor e HTTP e HTTPS, incluindo HTTP/2;
- 3.9. Suportar balanceamento de carga de servidores SIP para VoIP;
- 3.10. Permitir limitar o número de conexões estabelecidas com cada servidor real;
- 3.11. Permitir limitar o número de conexões estabelecidas com cada servidor virtual;
- 3.12. Implementar Network Address Translation (NAT) do IP do servidor;
- 3.13. Implementar Network Address Translation (NAT) do IP do cliente;
- 3.14. Implementar proteção contra Denial of Service (DoS) em camada 3, 4 e 7;
- 3.15. Implementar proteção contra SYN floods;
- 3.16. Suportar servidores virtuais com endereço IPv4 e os servidores reais com endereços IPv6;
- 3.17. Suportar multiplexação TCP e reuso de sessão para reaproveitamento e uso eficiente de conexões entre a solução de balanceamento de aplicações e os servidores balanceados;
- 3.18. Suportar Stream Control Transmission Protocol (SCTP);
- 3.19. Implementar aceleração de TLS com instalação do certificado digital na solução, troca de chaves e criptografia dos dados;
- 3.20. Permitir recriptografar a conexão entre a solução e o servidor;
- 3.21. Permitir espelhamento de tráfego de conexões TLS;

- 3.22. Suportar diversas cifras e protocolos SSL/TLS, incluindo TLS 1, 1.1, 1.2, 1.3, Forward Secrecy/Perfect Forward Secrecy, RSA, ECDSA, DHE, ECDHE, AES-128, AES-256, CBC/GCM, Camellia128, Camellia256, SHA, SHA2 (SHA256/384) e ChaCha20-Poly1305;
- 3.23. Em relação ao tráfego TLS, deve suportar:
- 3.24. Autenticação do servidor pelo cliente, apresentando um certificado previamente configurado;
- 3.25. Autenticação do cliente pela solução, através da solicitação e verificação do certificado fornecido pelo cliente;
- 3.26. Autenticação mútua (mTLS), quando ambas as autenticações acima mencionadas ocorrem. Durante a autenticação com mTLS, a solução deve apresentar para o servidor um certificado de cliente com atributos extraídos do certificado original obtido do cliente, preservando a autenticação mútua fim a fim;
- 3.27. Encaminhar ao servidor real via cabeçalho HTTP todo o certificado utilizado pelo cliente para se autenticar;
- 3.28. Encaminhar ao servidor real via cabeçalho HTTP atributos específicos do certificado utilizado pelo cliente;
- 3.29. Suportar os algoritmos para sessões TLS:
- 3.30. SSL session cache Timeout;
- 3.31. Session Ticket;
- 3.32. OCSP (Online Certificate Status Protocol) Stapling;
- 3.33. Dynamic Record Sizing;
- 3.34. ALPN (Application Layer Protocol Negotiation);
- 3.35. Perfect Forward Secrecy;
- 3.36. Suportar múltiplos certificados digitais no mesmo servidor virtual, com identificação via SNI (Server Name Indication);
- 3.37. Suportar importação de certificados digitais e chaves privadas;
- 3.38. Possuir alertas visuais na interface web de certificados com vencimento próximo;
- 3.39. Implementar limpeza de cabeçalho HTTP;
- 3.40. Implementar compressão de conteúdo HTTP, suportar os algoritmos gzip e deflate e permitir definir compressão especificamente para certos tipos de objetos;
- 3.41. Permitir a criação de políticas para classificação de tráfego através de parâmetros da aplicação, incluindo informações de geolocalização IP, cabeçalhos de autenticação HTTP, cookies e operações de cookie, cabeçalhos HTTP, host, método, Referer, Status Code e URI;
- 3.42. Permitir as ações para o tráfego classificado: bloqueio, reescrita e manipulação de URL, adicionar cabeçalho HTTP, redirecionar o tráfego para um servidor específico, escolher uma política de proteção web, logging do tráfego;
- 3.43. Suportar log de todas as sessões e permitir a customização do formato, incluindo endereço IP de origem, Porta TCP e UDP de origem, endereço IP de destino, porta TCP e UDP de destino, protocolo de camada 4 (TCP ou UDP), data e hora da mensagem, URL acessada;
- 3.44. Permitir utilizar diferentes configurações de envio de eventos de uma mesma aplicação, de forma que eventos válidos sejam enviados para um servidor e eventos de violações de segurança sejam enviados para outro servidor;
- 3.45. Permitir exportar eventos de acesso para servidores externos com configuração das informações exportadas;
- 3.46. Permitir a configuração de autenticação e autorização de clientes HTTP, através de base LDAP, RADIUS e certificados digitais;

- 3.47. Implementar integração com ambientes de orquestração de containers para criação dinâmica de serviços de entrega de aplicações e balanceamento de carga na solução, modificando a configuração de forma dinâmica e automática a partir de configurações feitas na plataforma de orquestração;
- 3.48. A plataforma deverá permitir integração nativa ou oficialmente suportada com ambientes Kubernetes, Red Hat OpenShift e VMware Tanzu, possibilitando a criação, atualização e remoção automatizada dos serviços de entrega e proteção de aplicações.
- 3.49. A integração poderá utilizar objetos, APIs e mecanismos suportados pelas respectivas plataformas, tais como Service do tipo LoadBalancer, Ingress, Gateway API, Route, CRD ou tecnologia funcionalmente equivalente, sem vinculação a nomenclatura, controlador, operador, linguagem declarativa ou arquitetura específica de determinado fabricante.
- 3.50. A plataforma deverá receber as alterações do ambiente de orquestração e atualizar automaticamente os pools, endpoints, pods ou nós associados aos serviços publicados. A licitante deverá informar os componentes, licenciamentos e condições necessários para implementação da integração.
- 3.51. Permitir incluir serviços de entrega de aplicações da solução, tais como SSL Offload e proteção de aplicações;
- 3.52. O ADC deverá receber em tempo real as alterações do ambiente e atualizar automaticamente o pool de pods ou nodes disponíveis para o serviço publicado de acordo com a integração realizada;
- 3.53. Suportar o protocolo FTP com, pelo menos, as seguintes características:
- 3.54. Determinar os comandos FTP permitidos;
- 3.55. Requests FTP anônimos;
- 3.56. Validar conformidade com o protocolo FTP;
- 3.57. Proteger contra ataques de força bruta nos logins;
- 3.58. Suportar o protocolo SMTP com, pelo menos, as seguintes características:
- 3.59. Limitar o número de mensagens;
- 3.60. Validar registro SPF do DNS;
- 3.61. Determinar quais métodos SMTP podem ser utilizados;

4. PROTEÇÃO DE APLICAÇÕES NO NÍVEL DE REDE E PROTOCOLO

- 4.1. Permitir implementação no modo que todo o tráfego seja bloqueado com exceções explícitas em regras de permissões e no modo que todo tráfego é permitido com exceções explícitas em regras de bloqueio;
- 4.2. Proteger de ataques DDoS nas camadas de rede e de sessão;
- 4.3. Proteger de ataques DDoS que utilizem SSL;
- 4.4. A solução deve permitir a criação de regras com, no mínimo, os parâmetros:
- 4.5. Endereço IP de destino;
- 4.6. Endereço IP de origem;
- 4.7. Porta de destino;
- 4.8. Porta de origem;
- 4.9. VLAN;
- 4.10. Protocolo;
- 4.11. Ação;
- 4.12. Horário;
- 4.13. Log;
- 4.14. Permitir definir agendamento para ativação da regra;
- 4.15. Permitir criar regras com base em zonas de segurança e por interface ou VLAN;

- 4.16. Implementar a descoberta automática de serviços presentes em objetos monitorados;
- 4.17. Permitir definir, no mínimo, as seguintes ações no tráfego:
- 4.18. Permitir: os pacotes são aceitos e passam pela solução;
- 4.19. Rejeitar: os pacotes são rejeitados e ocorre envio de pacotes de destino inatingível ou similar a origem do tráfego;
- 4.20. Descartar: onde os pacotes são descartados sem o envio de qualquer notificação a origem do tráfego;
- 4.21. Deve ser possível criar regras que sejam aplicadas em diferentes hierarquias, incluindo, no mínimo:
- 4.22. Global, regras válidas para todo o tráfego, independente da interface de ingresso;
- 4.23. Domínio de roteamento, regras válidas para todo o tráfego daquele domínio, independente da interface de ingresso;
- 4.24. Objeto, regras válidas para objetos específicos;
- 4.25. Deve possuir criptografia IPSEC para comunicação entre sites;
- 4.26. Permitir a configuração de alertas que informem automaticamente sobre ataques e anomalia de tráfego, através de limiares baseados no perfil de rede ou através de limites de tráfego atingido;
- 4.27. Permitir a restauração das configurações de proteções originais;
- 4.28. Deve permitir criar lista de exceção de regras por endereço IP específico ou faixa de sub-rede;
- 4.29. Permitir a criação de códigos ou scripts para customizar e aumentar o nível de segurança contra DDoS;
- 4.30. Permitir o consumo de listas externas de IPs para bloqueio com base em destino e origem, com atualização automática e ajuste manual da frequência de atualização;
- 4.31. Permitir o acionamento via API do descarte de conexões (shun) para integração com terceiros, tais como SIEM, IPS, IDS e outros;
- 4.32. Permitir a criação de regras de filtragem através de API REST declarativa;
- 4.33. A documentação da API deve ser pública;
- 4.34. Exibir uma lista de proteções ativas juntamente com estatísticas resumidas sobre as quantidades de tráfego descartado e aceito
- 4.35. Incluir informações estatísticas sobre o tráfego total e o total bloqueado por cada tipo de prevenção;
- 4.36. Implementar proteção contra pacotes inválidos, incluindo verificação para DNS malformed, Bad ICMP Frame, Bad ICMP Checksum, ICMP Frame too Large, Bad IGMP Frame, Bad IP TTL Value, Bad IP Version, Header Length Too Short, Bad Source, Bad IPV6 Hop Count, Bad IPV6 Version, Bad TCP Checksum, Bad TCP Flags, SYN & FIN Set, Bad UDP Checksum, ARP Flood, ICMPv4 Flood, ICMPv6 Flood, IGMP Flood, IGMP Fragment Flood, TCP RST Flood, TCP SYN ACK Flood, TCP SYN Flood, UDP Flood, SIP ACK Method, SIP Malformed, Single Endpoint Flood, Single Endpoint Sweep, LAND Attack, DNS Water-torture e fornecer estatísticas para os pacotes descartados;
- 4.37. Implementar descarte de sessões TCP ociosas se o cliente não enviar uma quantidade de dados dentro de um período configurável;
- 4.38. Limitar o número de consultas DNS por segundo através da configuração de limiares;
- 4.39. Mitigar, no mínimo, os tipos de ataques ICMP/UDP/TCP Flood, TCP Flag Abuse, GET/POST Flood, SYN Flood, UDP Bandwidth Attack, Smurfing, NTP Reflection Attack, TCP/UDP Bandwidth Attack, Fragging Attack, Slowloris, Connection Attack e Fragmentation Attacks;
- 4.40. Possuir recurso de bloqueio automático e temporário de atacantes, devendo ser possível especificar o tempo mínimo para iniciar o bloqueio e o tempo de bloqueio;
- 4.41. Suportar envio de SNMP traps para cada ataque DoS detectado;
- 4.42. Possuir uma ferramenta de teste de pacotes, através da qual deve ser possível realizar testes de pacotes;
- 4.43. Deve possuir a funcionalidade de limiares automático para vetores de DoS

- 4.44. Essa funcionalidade deve valer tanto para proteção geral como também para proteção de serviços específicos.
- 4.45. Os limiares automáticos serão construídos pelo próprio sistema e aplicados aos diversos vetores de ataques selecionados;
- 4.46. Permitir configurar o sistema para detectar e mitigar assinaturas dinâmicas, capaz de detectar possíveis ameaças de DoS baseado no histórico e comportamento do tráfego e mitigar automaticamente essas ameaças;
- 4.47. Suportar integração com serviço de tratamento de DDoS externo através do compartilhamento de informação de vetores e sinalização de ataques em andamento para redirecionamento de tráfego via BGP e limpeza do tráfego em centros de limpezas externos;

5. PROTEÇÃO PARA APLICAÇÕES WEB E API

- 5.1. Possuir tecnologia para mitigação de DDoS em camada 7 a partir de análises comportamentais;
- 5.2. Implementar ajustes automáticos e adaptativos de limiares de DoS;
- 5.3. Permitir a captura automática do tráfego relativo a ataques DoS em camada 7, web scraping e força bruta;
- 5.4. Implementar proteção para aplicações web contra ameaças listadas no OWASP Top 10 2021;
- 5.5. Implementar modelo positivo de segurança de aplicações web;
- 5.6. Implementar modelo negativa de segurança, ou seja, adotar assinatura de ataques, ameaças e exploração de vulnerabilidade, de aplicações web;
- 5.7. Possuir conjuntos de configurações de segurança pré-definidas para configuração rápida de políticas;
- 5.8. Permitir a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes;
- 5.9. Permitir 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;
- 5.10. Permitir desativar a inspeção para URL específicas;
- 5.11. Implementar identificação do usuário da aplicação web, mantendo a identificação até que o usuário tenha deixado o aplicativo;
- 5.12. Permitir a integração com firewall de banco de dados;
- 5.13. Suportar aplicações que utilizam protocolo WebSocket;
- 5.14. Suportar os protocolos HTTP/1.0, HTTP/1.1 e HTTP/2.0, para comunicação com o cliente e comunicação com o servidor, sem a necessidade de downgrade de versão;
- 5.15. Implementar proteção contra:
 - 5.16. Acesso por força bruta;
 - 5.17. DoS e DDoS em camada 7;
 - 5.18. Buffer Overflow;
 - 5.19. Cross Site Request Forgery (CSRF);
 - 5.20. Cross-Site Scripting (XSS);
 - 5.21. Server-Side Request Forgery (SSRF);
 - 5.22. SQL Injection;
 - 5.23. Parameter tampering;
 - 5.24. Cookie poisoning;
 - 5.25. HTTP Request Smuggling;
 - 5.26. Manipulação de campos escondidos (hidden input);
 - 5.27. Manipulação de cookies;
 - 5.28. Roubo de sessão através de manipulação de cookies;
 - 5.29. Sequestro de sessão;

- 5.30. Validação de consistência de formulários;
- 5.31. Validação do cabeçalho do "user-agent" para identificar clientes inválidos;
- 5.32. Permitir especificar quais URLs devem ser utilizadas para proteção contra CSRF (Cross-Site Request Forgery);
- 5.33. Suportar codificação HTML "application/x-www-form-urlencoded";
- 5.34. Suportar HTTP Batched Request com proteções e assinaturas considerando individualmente URLs, cabeçalhos e conteúdo;
- 5.35. Suportar codificação fragmentada (chunked encoding);
- 5.36. Suportar validações de protocolo:
- 5.37. Restrição de métodos;
- 5.38. Restrição de protocolos e versões;
- 5.39. Validação de conformidade com RFCs;
- 5.40. Validação de caracteres URL-encoded;
- 5.41. Validação de codificação fora de padrão %uXXYY.
- 5.42. Suportar validações de HTML com nome de parâmetros, tamanho e tipo dos valores de parâmetros e combinação de nome, tipo e tamanho de parâmetros;
- 5.43. Possuir técnicas de detecção de evasões:
- 5.44. URL-decoding;
- 5.45. Terminação Null Byte String;
- 5.46. Paths autorreferenciados;
- 5.47. Case de caracteres misturados;
- 5.48. Uso excessivo de espaços em branco;
- 5.49. Decodificação de entidades HTML;
- 5.50. Caracteres de escape;
- 5.51. Permitir a inspeção externa de arquivos enviados por usuários (upload) para os servidores de aplicação utilizando Internet Content Adaptation Protocol (ICAP);
- 5.52. Capacidade de filtrar cabeçalhos, corpo e status de respostas;
- 5.53. Permitir o uso do parâmetro HTTP X-Forwarded-For como parte da política de controle;
- 5.54. Implementar validação de URL;
- 5.55. Validação de métodos HTTP utilizados (GET, POST, HEAD, OPTIONS, PUT, TRACE, DELETE, CONNECT) por URL;
- 5.56. Implementar proteção de aplicações web que utilizam chamadas de API, protegendo tanto a aplicação como a API, com a visibilidade que se trata da mesma sessão de usuário;
- 5.57. Suportar aplicações Single-Page Application (SPA);
- 5.58. Permitir a customização da resposta de bloqueio;
- 5.59. Permitir a configuração de lista de exceções temporárias ou permanentes de endereços IP bloqueados;
- 5.60. Permitir adicionar, automaticamente e manualmente, em uma lista de bloqueio, os endereços IP de origem que ultrapassarem limites estabelecido, por um período configurável;
- 5.61. Implementar as proteções:
- 5.62. Proteção contra exposição de informações do ambiente e servidores internos como, sistema operacional e servidor web;
- 5.63. Ocultar qualquer mensagem de erro HTTP dos usuários;
- 5.64. Remover as mensagens de erro às páginas que serão enviadas aos usuários;
- 5.65. Suportar políticas por geolocalização para restrição de acesso a determinados países;

- 5.66. A plataforma deverá disponibilizar recursos que auxiliem a identificação da estrutura e do comportamento esperado das aplicações, bem como a elaboração e a manutenção de suas políticas de segurança.
- 5.67. Esses recursos poderão utilizar análise do tráfego, aprendizagem automatizada, importação de especificações, modelos de aplicação, recomendações assistidas ou outros mecanismos equivalentes, desde que possibilitem identificar os elementos relevantes da aplicação e adequar as políticas de proteção às características observadas.
- 5.68. A forma de implementação não poderá constituir fator de desclassificação quando o fabricante demonstrar, por documentação técnica ou prova de conceito, o atendimento aos resultados de segurança pretendidos.
- 5.69. O perfil aprendido de forma automatizada pode ser ajustado, editado ou bloqueado;
- 5.70. Implementar detecção e mitigação de ameaças e ataques com base em assinaturas de ataques, com atualização periódica e automática da base de assinaturas;
- 5.71. As assinaturas devem ser atualizadas durante o período do contrato, sem custo adicional;
- 5.72. Não serão aceitas soluções que definem assinaturas como sendo uma base de reputação de IP;
- 5.73. A atualização deve ser relacionada apenas as assinaturas, não sendo aceitas soluções que demanda a atualização do sistema operacional para atualização de cada nova versão da base de assinaturas;
- 5.74. Permitir a configuração automática de assinaturas com base em uma lista interna de tecnologias utilizadas pela aplicação;
- 5.75. Permitir desabilitar assinaturas específicas para determinados parâmetros, se comportando como exceção da configuração geral da política;
- 5.76. Permitir configurar um período de adaptação de novas assinaturas, quando nenhuma requisição que viole a assinatura deve ser bloqueada, apenas informada em relatório. Este processo deve ser automático, não sendo necessário a criação de regras específicas a cada atualização de assinatura;
- 5.77. Possuir assinaturas de ataques para conteúdo em JSON e XML;
- 5.78. Possuir proteções contra XML Bomb;
- 5.79. Possuir proteção para WebServices, suportar WS-I Basic Profile, importação de WSDL e aplicação de controles, criptografar e descriptografar partes das mensagens SOAP, assinar digitalmente e verificar de partes das mensagens SOAP;
- 5.80. Possuir integração com soluções externas de análise vulnerabilidade para importação de relatórios e configuração de políticas de segurança, indicando quais vulnerabilidades podem ser resolvidas e quais devem ser resolvidas manualmente externamente;
- 5.81. Implementar detecção de DoS na camada 7, através de análise comportamental, com aprendizado automático do comportamento da aplicação e combinação com nível de carga do servidor;
- 5.82. Permitir apenas registrar o ataque, sem tomar nenhuma ação de bloqueio;
- 5.83. Implementar detecção com base no número de requisições por segundo enviados a uma URL específica;
- 5.84. Implementar detecção com base no número de requisições por segundo enviados de um IP específico;
- 5.85. Implementar detecção com base na validação do cliente através de código executado no navegador para identificação de bots;
- 5.86. Implementar detecção com base no aumento de um determinado percentual do número de transações por segundo (TPS);
- 5.87. Implementar detecção com base no aumento de carga e latência do servidor de aplicação;
- 5.88. Implementar detecção com base no número máximo de transações por segundo de um determinado IP;

- 5.89. Implementar mitigações para ataques DoS, incluindo resolução de CAPTCHA, descarte de todas as requisições de um determinado IP, descarte por geolocalização IP, injeção de um desafio JavaScript para detectar se é um usuário legítimo ou bots;
- 5.90. Implementar mitigação de ataques DDoS através de assinaturas dinâmicas em tempo real para proteção da aplicação;
- 5.91. Implementar detecção e mitigação de ataques de força bruta de usuário/senha em páginas de login, com configuração da quantidade máxima de tentativas e tempo de mitigação;
- 5.92. Identificar ataques com diferentes usuários e mesma origem;
- 5.93. Identificar ataques com diferentes origens e mesmo usuário;
- 5.94. Identificar ataques de forma global, considerando a quantidade de tentativas e implementando contramedidas de forma global para a política;
- 5.95. Implementar mitigação através de listas de bloqueio dinâmica de endereços IPs após validação sem sucesso de desafios e permitir a configuração do tempo de bloqueio;
- 5.96. Implementar mitigação através de listas de bloqueio dinâmica de endereços IPs que ultrapassem um número máximo de violações por minuto e permitir a configuração do tempo de bloqueio;
- 5.97. Implementar detecção e mitigação para proteção contra bots através da combinação de desafios enviados ao navegador do usuário e técnicas avançadas de análise;
- 5.98. Não serão aceitas soluções que utilizam apenas o user-agent para detecção de bots;
- 5.99. Implementar proteção proativa de ataques automatizados por bots e outras ferramentas, como web scrapers.
- 5.100. Possuir atualização automática de definição de bots;
- 5.101. Permitir a configuração de bloqueio e permissão de bots benignos conhecidos, como Google, Yahoo! e Microsoft Bing;
- 5.102. Permitir a criação de definições de bots;
- 5.103. Implementar proteção de APIs através da imposição de regras de endpoint e métodos permitidos;
- 5.104. Permitir a configuração de quotas e rate limits para chamadas em APIs de forma global na política;
- 5.105. Permitir a configuração de quotas e rate limits para chamadas em APIs por endpoint;
- 5.106. Permitir configurar exceções as regras de rate limits para chamadas na API;
- 5.107. Implementar proteção de conteúdo no formato JSON (JavaScript Object Notation);
- 5.108. Suportar proteção de conteúdo de mensagens no formato GraphQL, incluindo assinaturas de ataques, profundidade de query, GraphQL batching, inspeção de conteúdo JSON em mensagens POST e GET;
- 5.109. Suportar importação de especificação de API compatível com OpenAPI v2 e v3, nos formatos YAML ou JSON, com suporte a parâmetros no path e importação de respostas;
- 5.110. Implementar funcionalidade de autenticação e autorização de clientes de API utilizando, pelo menos, os métodos HTTP Basic e OAuth 2.0;
- 5.111. Implementar funcionalidade para prevenir vazamento de informações, dados sensíveis e outros tipos de dados confidenciais, sigilosos ou restrito, através do bloqueio ou remoção dos dados confidenciais;
- 5.112. Implementar funcionalidades para prevenir vazamento de dados sensíveis em mensagens de erro HTTP, códigos das aplicações, entre outros, retirando os dados ou mascarando a informação nas páginas enviadas aos usuários;
- 5.113. Implementar funcionalidade para ocultar erros de aplicação ou infraestrutura do usuário;
- 5.114. Permitir a configuração de fluxo de navegação da aplicação, de forma que um usuário só pode alcançar determinada URL se passar por outras anteriormente;
- 5.115. Permitir a correção de um falso positivo através da aceitação da requisição e atualização da política de forma automática;

- 5.116. Possuir um nível severidade de violação de múltiplos níveis para fácil identificação de violações de maior e menor prioridade;
- 5.117. Implementar um identificador único para cada requisição tratada pela solução;
- 5.118. Permitir o armazenamento local de eventos e exportação para servidores externos;
- 5.119. Permitir configurar a retenção dos eventos por tempo e volume;
- 5.120. Implementar a detecção, remoção ou codificação de dados sensíveis dos eventos como, por exemplo, números de cartão de crédito, CPF e senhas;
- 5.121. Possuir API REST para configuração de servidores virtuais, políticas de segurança, parâmetros, perfis e demais configurações;
- 5.122. Permitir exportar as políticas de segurança para arquivos texto, JSON ou XML;
- 5.123. Possuir integração com esteiras de automação que permita que as configurações sejam realizadas de forma automática e dinâmica, de forma declarativa, por ferramentas de automação e orquestração, permitindo que a solução seja integrada ao ciclo de desenvolvimento;
- 5.124. Suportar integração com funcionalidade de gestão avançada de tráfego automatizado para detecção e mitigação de ataques, abusos e fraudes, com detecção de tráfego gerado por usuários, bots benignos e malignos, através de telemetria de uso coletada da aplicação, sem a utilização de CAPTCHAs ou desafios para o navegador;
- 5.125. Implementar funcionalidade de forma nativa na solução ou possuir integração com serviço em nuvem do mesmo;
- 5.126. Implementar proteção de aplicações web, de dispositivos móveis e APIs;

6. IMPLEMENTAR BASES DE INTELIGÊNCIA DE AMEAÇAS ATUALIZADAS

- 6.1. A solução deve implementar a atualização das bases de inteligência de ameaças para proteção de DoS/DDoS, serviços de DNS, de visibilidade de tráfego e de proteção de aplicações web e API durante a vigência do contrato;
- 6.2. As fontes de inteligência devem ser fornecidas diretamente pelo fabricante da solução ou parceiro homologado através de assinaturas de serviços próprios;
- 6.3. As fontes de inteligência devem ser atualizadas frequentemente pela duração do contrato sem custo adicional;
- 6.4. Deve dispor de bases de inteligência de IP, incluindo IPv4 e IPv6, classificados e categorizados em, pelo menos, as categorias fontes de ataques web, redes e hosts de botnets, scanners de websites, fontes de phishing, servidores proxies, redes e hosts que exploram vulnerabilidades em Windows, redes e hosts de negação de serviço e redes e hosts com baixa reputação;
- 6.5. Permitir que sejam criados filtros utilizando as categorias de IP nas funções de proteção de DDoS e serviços de DNS, de visibilidade de tráfego e de proteção de aplicações web e API;
- 6.6. Permitir utilizar a base de inteligência de IP durante consultas de DNS, permitir ações diferentes configuradas de acordo com a categoria e alterar a resposta antes de ser enviada para o cliente na solução de proteção de DDoS e serviços de DNS;
- 6.7. Permitir utilizar a base de inteligência de IP para classificar e selecionar uma cadeia de serviço na solução de visibilidade de tráfego;
- 6.8. Permitir que sejam criados filtros onde se verifica o endereço de origem no cabeçalho X-Forwarded-For (XFF) com base na classificação de endereços IP na solução de proteção de aplicações web e API;
- 6.9. Dispor de base de inteligência de ameaças relacionados a campanhas e ataques a aplicações web, correlacionando diversas fontes de inteligência e ameaças encontradas diariamente no mundo real;

- 6.10. As regras de proteção e assinaturas derivadas desta base de inteligência devem ser habilitadas automaticamente, sem precisar de um ciclo de aprendizagem na solução;
- 6.11. A base de inteligência deve implementar detecção e mitigação de ataques com baixo índice de falso-positivo;
- 6.12. Este serviço é complementar a atualização de assinaturas de ataques da solução de proteção de aplicações web e API, portanto, as informações disponibilizadas pela base de inteligência não devem ser limitada a apenas indicar qual assinatura do WAF for acionada, devendo disponibilizar informações contextuais incluindo, por exemplo, a capacidade de informar que um agente conhecido de ameaça usou uma exploração específica de vulnerabilidade mais recente (por exemplo, um CVE) em uma tentativa de implantação de uma ameaça como, por exemplo, um software de mineração de criptomoedas;
- 6.13. Devem ser automáticas e frequentes as atualizações de regras, políticas, configurações e demais ajustes que dependem do serviço de inteligência, sem interrupção do serviço, sem necessidade de atualização do sistema operacional e nem reiniciar o equipamento a cada atualização;

7. ORQUESTRAÇÃO DE TRÁFEGO CRIPTOGRAFADO SSL/TLS

- 7.1. Suportar inspeção de tráfego criptografado SSL/TLS de entrada (inbound) e saída (outbound);
- 7.2. Suportar atuação como SSL Forward Proxy e SSL Reverse Proxy;
- 7.3. Suportar os protocolos TLS 1.0, TLS 1.1, TLS 1.2 e TLS 1.3;
- 7.4. Suportar algoritmos criptográficos amplamente utilizados, incluindo RSA, ECDSA, DHE, ECDHE, AES, GCM, CBC e ChaCha20-Poly1305;
- 7.5. Suportar Forward Secrecy e Perfect Forward Secrecy;
- 7.6. Suportar controle e aplicação de políticas de criptografia SSL/TLS, incluindo versões de protocolo e cipher suites;
- 7.7. Suportar descriptografia e recriptografia de tráfego SSL/TLS para inspeção por dispositivos de segurança integrados;
- 7.8. Suportar orquestração de tráfego criptografado entre múltiplas soluções de segurança por meio de security service chaining;
- 7.9. Suportar operação independente de porta TCP para descriptografia SSL/TLS;
- 7.10. Suportar bypass seletivo de tráfego SSL/TLS com base em políticas definidas pelo administrador;
- 7.11. Suportar exceções de descriptografia para tráfego sensível, conforme políticas de segurança e conformidade;
- 7.12. Suportar inspeção baseada em informações do handshake SSL/TLS, incluindo Server Name Indication (SNI);
- 7.13. Suportar geração dinâmica de certificados para interceptação SSL/TLS;
- 7.14. Suportar uso de Autoridade Certificadora (CA) interna para assinaturas de certificados de inspeção;
- 7.15. Suportar importação e gerenciamento de certificados digitais X.509;
- 7.16. Suportar validação de certificados apresentados durante o handshake SSL/TLS;
- 7.17. Suportar integração com infraestrutura de chaves públicas (PKI);
- 7.18. Suportar integração com módulos de segurança de hardware (HSM) para proteção de chaves criptográficas;
- 7.19. Suportar HSMs compatíveis com padrões de mercado;
- 7.20. Suportar armazenamento seguro de chaves privadas e certificados;
- 7.21. Suportar aplicação centralizada de políticas SSL/TLS;
- 7.22. Suportar alta disponibilidade e sincronização de configurações SSL/TLS entre dispositivos;
- 7.23. Suportar registro (logging) de eventos SSL/TLS para auditoria e troubleshooting;
- 7.24. Suportar integração com sistemas externos de monitoramento e análise de eventos de segurança.

8. CONSOLE DE ADMINISTRAÇÃO, MONITORAMENTO E OPERAÇÃO CENTRALIZADA

- 8.1. A plataforma deverá contemplar recurso de gerenciamento centralizado, nativo, integrado ou oficialmente homologado pelos fabricantes dos componentes gerenciados, destinado à administração, configuração, monitoramento, inventário e aplicação coordenada de políticas em múltiplos dispositivos, por meio de uma interface unificada.
- 8.2. A arquitetura ofertada deverá assegurar compatibilidade entre os componentes, suporte técnico para o conjunto da plataforma e funcionamento adequado das atividades de gerenciamento, independentemente da quantidade de fabricantes envolvidos.
- 8.3. A plataforma deverá possuir arquitetura própria e dedicada de gerenciamento, independente da arquitetura funcional dos dispositivos gerenciados, não se limitando a mecanismos de sincronização ou replicação entre os próprios equipamentos, disponibilizando uma camada de gerenciamento dedicada;
- 8.4. A solução de gerenciamento centralizado deve ser obrigatoriamente do mesmo fabricante dos módulos e equipamentos de WAF, balanceamento de carga, cache e aceleração web solicitados;
- 8.5. O gerenciador centralizado deve suportar escalabilidade horizontal para a adição de múltiplos appliances físicos ou instâncias virtuais;
- 8.6. O componente de gerenciamento deverá permitir a administração centralizada ou coordenada das políticas dos equipamentos gerenciados, bem como disponibilizar visão consolidada dos logs de auditoria, eventos de segurança, inventário, relatórios, desempenho e estado operacional dos ativos. Serão aceitas diferentes arquiteturas de armazenamento, processamento e integração, desde que assegurem o atendimento às funcionalidades requeridas.
- 8.7. Caso a comunicação entre os appliances e a plataforma de gerenciamento centralizado seja interrompida, os dispositivos gerenciados devem continuar analisando, filtrando, balanceando e acelerando o tráfego normalmente e sem qualquer interrupção dos serviços;
- 8.8. Toda a transmissão de dados e comunicação entre os componentes distribuídos da solução deve ser criptografada e digitalmente assinada;
- 8.9. A comunicação entre as estações de trabalho dos administradores e o console de administração deve ser estabelecida via protocolos seguros (HTTPS / SSH), com suporte a autenticação de usuários e certificados digitais;
- 8.10. O console de administração deve implementar Controle de Acesso Baseado em Perfis (Role-Based Access Control - RBAC), permitindo a separação granular de funções (ex: Administração Geral, Configuração de Regras, Operação e Somente Leitura/Auditoria);
- 8.11. Possuir, no mínimo, três níveis nativos de privilégios de usuário: Administrador, Usuário com permissões reduzidas/Operador e Usuário Somente Leitura;
- 8.12. Permitir o acesso controlado utilizando uma única conta e senha por administrador, independentemente da funcionalidade ou dispositivo acessado;
- 8.13. Fornecer visualizações, opções de menu e ações diferenciadas na interface conforme o perfil do usuário conectado;
- 8.14. Permitir que múltiplos usuários administradores estejam conectados simultaneamente na interface de administração com permissões de leitura/escrita;
- 8.15. Não serão aceitas restrições de licença que limitem a quantidade de usuários administradores cadastrados ou acessando o console de gerenciamento;
- 8.16. Suportar autenticação centralizada de administradores em bases remotas, no mínimo: Microsoft Active Directory (AD), RADIUS e OpenLDAP;
- 8.17. Permitir a importação automática do nível de acesso, perfil ou grupo de permissões diretamente das bases remotas de autenticação (AD, RADIUS e OpenLDAP);

- 8.18. O gerenciador central deve dispor de interface gráfica via Web (GUI) cross-platform (compatível com navegadores modernos em Windows, Linux e macOS) e interface por linha de comando (CLI) acessível via protocolo seguro SSH e console local;
- 8.19. A interface de linha de comando (CLI) deve possuir recursos de autocompletar comandos, ferramentas de debugging e comandos para exibição em tempo real da utilização de tráfego das interfaces (em bps e/ou pps);
- 8.20. Permitir a execução de operações de reinicialização (reboot) e atualização de firmware, sistema operacional, patches ou hotfixes diretamente pela interface gráfica (GUI) ou por linha de comando (CLI);
- 8.21. Utilizar protocolos seguros SCP, SFTP ou HTTPS para a transferência de arquivos de configuração, atualizações do sistema operacional e exportação de backups;
- 8.22. Realizar backup diário e automatizado de todas as informações armazenadas no componente de administração, incluindo as configurações globais e de todos os módulos gerenciados, com capacidade de transferência automática dos arquivos de backup para servidores remotos via SCP, SFTP ou HTTPS;
- 8.23. Permitir o armazenamento das configurações em memória não volátil, garantindo que em caso de interrupção ou queda no fornecimento de energia, o equipamento restabeleça a operação normalmente na mesma configuração anterior;
- 8.24. Suportar recursos de rollback automatizado de imagem de sistema operacional e de arquivos de configuração;
- 8.25. Permitir a exportação e importação simplificada de regras, perfis e políticas de segurança entre diferentes dispositivos ou instâncias;
- 8.26. A plataforma deverá disponibilizar painéis gráficos ou recursos visualmente equivalentes para apresentação consolidada da disponibilidade, do desempenho, da volumetria de tráfego, do estado operacional dos equipamentos e dos alertas de segurança.
- 8.27. Serão aceitos painéis predefinidos, configuráveis, personalizáveis ou organizados por perfis de acesso, desde que permitam a consulta adequada das informações necessárias à administração e ao monitoramento do ambiente.
- 8.28. A plataforma deverá permitir a geração, consulta e exportação de informações técnicas, operacionais, estatísticas e gerenciais relacionadas aos equipamentos, à disponibilidade, ao desempenho, ao tráfego e aos eventos de segurança.
- 8.29. Os relatórios ou demonstrativos equivalentes poderão ser predefinidos, configuráveis ou gerados a partir de consultas e filtros disponibilizados pela plataforma, desde que possibilitem a obtenção das informações necessárias ao acompanhamento do ambiente.
- 8.30. Deverá ser possível gerar ou disponibilizar essas informações sob demanda ou periodicamente, diretamente pela plataforma ou mediante integração oficialmente suportada pelo fabricante
- 8.31. Permitir a visualização de logs em tempo real, fornecendo visão centralizada e unificada das atividades dos componentes, eventos do sistema e registros de auditoria das alterações realizadas pelos administradores;
- 8.32. Os logs gerados por todos os componentes da solução devem cumprir os seguintes requisitos:
- 8.33. Capacidade de transferência contínua (stream/real-time) para o servidor de gerenciamento central no momento da ocorrência;
- 8.34. Capacidade de armazenamento local temporário nos appliances em caso de falha na comunicação com o servidor central, com posterior sincronização automática;
- 8.35. Capacidade de exportação remota do servidor central para ferramentas de terceiros (ex: SIEM) nos formatos Syslog, SNMP Traps, JSON ou via REST API;
- 8.36. Permitir que os administradores definam com precisão quais tipos de transações, eventos ou violações devem ser registrados e armazenados nos logs;

- 8.37. Implementar mecanismos de ofuscação e mascaramento de dados sensíveis exibidos em alertas, visualizações de logs e relatórios, protegendo dados confidenciais (ex: senhas, números de cartão de crédito e dados pessoais);
- 8.38. A solução deve oferecer capacidade de armazenamento e retenção de logs por um período mínimo de 90 (noventa) dias, considerando uma estimativa diária de 2 GB de dados;
- 8.39. Os dados dos primeiros 30 (trinta) dias devem obrigatoriamente ser armazenados localmente na solução;
- 8.40. Os dados referentes aos 60 (sessenta) dias restantes poderão ser mantidos em armazenamento local ou em repositório externo remoto;
- 8.41. A solução deve disponibilizar interface gráfica com recursos de pesquisa e navegação automatizada sobre todo o histórico de logs armazenado;
- 8.42. Suportar o envio de mensagens Syslog para múltiplos servidores Syslog externos configurados simultaneamente;
- 8.43. Disponibilizar agente SNMP nativo com suporte às MIBs padrão (MIB II, MIB Bridging RFC 1493) e MIBs proprietárias/extensões privadas devidamente documentadas;
- 8.44. Suportar sincronismo de horário via protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol);
- 8.45. Permitir a configuração de endereçamento IP estático e dinâmico (DHCP/BOOTP) nas interfaces de gerenciamento;
- 8.46. Disponibilizar ferramentas integradas para diagnósticos de primeiro nível na interface e CLI, tais como ping, traceroute, logs de eventos e depuração (debug);
- 8.47. O sistema operacional da solução deve disponibilizar nativamente a ferramenta tcpdump (ou equivalente de desempenho igual ou superior) para captura e monitoramento de pacotes em qualquer interface de rede, permitindo o salvamento dos arquivos no formato padrão .pcap (libpcap);
- 8.48. A execução da ferramenta de captura de pacotes (tcpdump) não deve causar degradação ou impacto no desempenho do processamento de tráfego principal (Data Plane) dos appliances.

Anexo I-C - Serviços de Instalação e configuração

1 Serviços de Instalação e Configuração

- 1.1 São de responsabilidade da CONTRATADA os serviços de planejamento, instalação física, instalação lógica e configuração dos equipamentos fornecidos, incluindo sua adequação ao ambiente da PRODEMGE, de forma que a solução esteja plenamente operacional e disponível para utilização pela equipe da PRODEMGE.
- 1.2 Os serviços deverão ser executados por técnico ou profissional devidamente certificado pelo fabricante dos equipamentos ou da solução.
- 1.3 A instalação física deverá compreender, no mínimo, a instalação dos equipamentos nos racks fornecidos pela PRODEMGE, conexão à infraestrutura elétrica e lógica disponibilizada, energização e verificação dos componentes físicos.
- 1.4 A instalação e configuração lógica deverão compreender o ajuste de todos os parâmetros físicos e lógicos necessários ao funcionamento da solução e à sua adequação ao ambiente da PRODEMGE, conforme padrões previamente estabelecidos entre a CONTRATADA e a PRODEMGE.
- 1.5 A CONTRATADA deverá realizar a customização dos equipamentos, incluindo os softwares embarcados necessários para que o sistema operacional e os ativos de rede reconheçam adequadamente os recursos e dispositivos instalados.
- 1.6 A CONTRATADA deverá ativar e disponibilizar todas as funcionalidades previstas nesta especificação e contratadas, de modo que a solução esteja apta para utilização pela PRODEMGE após a conclusão da instalação e configuração.
- 1.7 A CONTRATADA deverá integrar a solução à console de monitoração da PRODEMGE, por meio do protocolo SNMP ou outro mecanismo de monitoração disponibilizado nativamente pela solução, conforme definido pela PRODEMGE.
- 1.8 A CONTRATADA deverá apresentar, em até 10 (dez) dias úteis após a assinatura do contrato, plano de instalação física contendo os requisitos necessários para conexão dos equipamentos às infraestruturas elétrica e lógica da PRODEMGE.
- 1.9 O cronograma para execução das atividades de instalação e configuração deverá ser alinhado entre a CONTRATADA e a PRODEMGE em até 10 (dez) dias úteis após o recebimento provisório dos equipamentos.

- 1.10 A CONTRATADA deverá realizar todos os testes necessários para comprovar o correto funcionamento dos equipamentos e da solução instalada, incluindo os componentes físicos, interfaces de gerenciamento, conectividade e funcionalidades configuradas.
- 1.11 A CONTRATADA deverá elaborar e entregar documentação detalhada contendo os procedimentos de instalação, configuração, parametrização e ajustes realizados no ambiente da PRODEMGE, em meio digital, antes da emissão do atestado de aceite técnico.

Anexo I-D - Serviços de Migração

1 Serviço de Migração das URLs

- 1.1 A PRODEMGE disponibilizará à CONTRATADA, observadas suas políticas de segurança e controle de acesso, as informações, os arquivos exportáveis, os relatórios e o acesso técnico necessário à realização do levantamento do ambiente atual. Caberá à CONTRATADA identificar, coletar, interpretar e documentar as configurações necessárias à migração, utilizando os recursos disponibilizados pela plataforma existente.
- 1.2 São de responsabilidade da CONTRATADA os serviços de planejamento, preparação, configuração, migração, testes e entrada em produção das URLs atualmente protegidas pela solução de WAF existente na PRODEMGE para a nova solução de WAF fornecida no âmbito deste contrato.
- 1.3 A migração deverá contemplar todas as URLs e respectivas aplicações atualmente protegidas pela solução de WAF existente, conforme relação e informações disponibilizadas pela PRODEMGE antes do serviço de migração.
- 1.4 Previamente ao início da migração, a CONTRATADA deverá realizar o levantamento e inventário das configurações existentes na solução atual, contemplando, no mínimo, para cada URL ou aplicação:
 - 1.4.1 URL, domínio e respectivos aliases, quando aplicável;
 - 1.4.2 endereço(s) dos servidores de origem (backend);
 - 1.4.3 portas e protocolos utilizados;
 - 1.4.4 certificados digitais e respectivas configurações, quando aplicável;
 - 1.4.5 políticas de segurança;
 - 1.4.6 regras de proteção;
 - 1.4.7 exceções e liberações específicas;
 - 1.4.8 filtros e listas de controle;
 - 1.4.9 parâmetros de configuração específicos da aplicação; e
 - 1.4.10 demais configurações necessárias ao funcionamento e à proteção da aplicação.
- 1.5 A CONTRATADA deverá elaborar plano de migração das URLs para a nova solução, contemplando, no mínimo:
 - 1.5.1 relação das URLs e aplicações a serem migradas;
 - 1.5.2 levantamento das configurações existentes;
 - 1.5.3 correspondência entre as configurações da solução atual e os recursos disponíveis na nova solução;
 - 1.5.4 identificação de eventuais incompatibilidades ou configurações sem correspondência direta;
 - 1.5.5 estratégia e sequência de migração;
 - 1.5.6 pré-requisitos e dependências;
 - 1.5.7 procedimentos de testes e validação;
 - 1.5.8 estratégia de entrada em produção;
 - 1.5.9 procedimentos de reversão (rollback); e

1.5.10 cronograma das atividades.

1.6 O plano de migração deverá ser submetido à PRODEMGE para análise e aprovação antes do início da migração das URLs para a nova solução.

1.7 A CONTRATADA deverá realizar a configuração das URLs e respectivas aplicações na nova solução de WAF, contemplando todos os parâmetros necessários ao seu funcionamento e à aplicação das políticas de segurança definidas para cada aplicação.

1.8 A migração deverá preservar, sempre que tecnicamente aplicável, as funcionalidades e configurações de segurança existentes na solução atual, incluindo, no mínimo, políticas, regras de proteção, exceções, listas de permissão e bloqueio, filtros e demais configurações específicas das aplicações.

1.9 A migração não poderá resultar na redução do nível de proteção das aplicações atualmente protegidas, salvo quando tecnicamente necessária em razão de incompatibilidade entre as soluções, hipótese em que a CONTRATADA deverá apresentar justificativa técnica e alternativa de proteção à PRODEMGE para aprovação prévia.

1.10 Caso determinada funcionalidade ou configuração existente não possua correspondência direta na nova solução, a CONTRATADA deverá identificar formalmente a situação, apresentar a justificativa técnica e propor alternativa de configuração que possibilite manter, sempre que tecnicamente possível, a funcionalidade ou nível de proteção existente.

1.11 A CONTRATADA deverá realizar testes técnicos e funcionais após a configuração de cada conjunto de URLs migradas, contemplando, no mínimo:

- 1.11.1 resolução e acesso às URLs;
- 1.11.2 comunicação com os servidores de origem;
- 1.11.3 funcionamento dos protocolos e portas configurados;
- 1.11.4 funcionamento dos certificados digitais, quando aplicável;
- 1.11.5 aplicação das políticas de segurança;
- 1.11.6 funcionamento das regras e exceções configuradas;
- 1.11.7 geração de logs e eventos; e
- 1.11.8 funcionamento da aplicação por meio da nova solução de WAF.

1.12 A entrada em produção das URLs migradas deverá ser previamente planejada e realizada em conjunto com a PRODEMGE, de forma a minimizar impactos na disponibilidade e no funcionamento das aplicações.

- 1.13 A CONTRATADA deverá acompanhar o funcionamento das URLs após sua entrada em produção na nova solução, realizando os ajustes e adequações necessários para solucionar eventuais problemas identificados durante a migração ou no período imediatamente posterior à entrada em produção.
- 1.14 Durante a migração e a entrada em produção, a CONTRATADA deverá prestar suporte técnico à equipe da PRODEMGE para identificação e tratamento de eventuais indisponibilidades, falhas de comunicação, bloqueios indevidos, falsos positivos ou outras ocorrências relacionadas à migração.
- 1.15 A CONTRATADA deverá executar, quando necessário e mediante solicitação da PRODEMGE, os procedimentos de reversão para a solução de WAF anterior, caso sejam identificados problemas que impeçam o funcionamento adequado da aplicação, comprometam sua disponibilidade ou reduzam indevidamente seu nível de proteção.
- 1.16 Os procedimentos de reversão deverão ser previamente definidos no plano de migração e deverão permitir o restabelecimento das condições anteriores à migração, sempre que tecnicamente possível.
- 1.17 A migração de uma URL ou aplicação somente será considerada concluída após a realização dos testes previstos, a entrada em produção e a validação de seu funcionamento pelo cliente e pela PRODEMGE. A ausência de validação não poderá ser presumida como aceite.
- 1.18 Eventuais ajustes de configuração identificados durante os testes, a entrada em produção ou o acompanhamento da migração deverão ser realizados pela CONTRATADA sem ônus adicional para a PRODEMGE, desde que relacionados ao escopo originalmente contratado.
- 1.19 Ao término dos serviços de migração, a CONTRATADA deverá entregar documentação técnica contendo, no mínimo:
 - 1.19.1 relação das URLs e aplicações migradas;
 - 1.19.2 configurações aplicadas na nova solução;
 - 1.19.3 políticas e regras de segurança configuradas;
 - 1.19.4 exceções e liberações configuradas;
 - 1.19.5 correspondência entre as configurações da solução anterior e da nova solução;
 - 1.19.6 funcionalidades ou configurações da solução anterior que não puderam ser reproduzidas na nova solução, acompanhadas das respectivas justificativas;
 - 1.19.7 registros dos testes realizados;
 - 1.19.8 ocorrências identificadas durante a migração;
 - 1.19.9 ajustes realizados; e
 - 1.19.10 situação final de cada URL ou aplicação migrada.

- 1.20 A CONTRATADA deverá fornecer à PRODEMGE, ao final da migração, relatório consolidado contendo o status de todas as URLs previstas, identificando as URLs migradas, pendentes, reprovadas e revertidas, quando aplicável.
- 1.21 Todos os serviços necessários à execução da migração, incluindo levantamento, planejamento, configuração, testes, acompanhamento, ajustes, documentação e suporte à entrada em produção, deverão estar incluídos no escopo da contratação.

Anexo I-E - Serviços de Operação Assistida

- 1.1 A CONTRATADA deverá prestar serviço de operação assistida pelo período de 25 (vinte e cinco) dias úteis iniciando no dia útil seguinte após finalizada a migração homologada pelo cliente.
- 1.2 A operação assistida deverá compreender o acompanhamento da solução em funcionamento e a transferência de conhecimento à equipe da PRODEMGE responsável pela operação, administração e manutenção dos equipamentos.
- 1.3 Durante o período de operação assistida, a CONTRATADA deverá prestar o suporte técnico necessário à operacionalidade da solução, orientando a equipe da PRODEMGE quanto aos procedimentos de operação, administração, monitoramento, diagnóstico e solução de problemas relacionados aos equipamentos fornecidos.
- 1.4 A operação assistida deverá contemplar, no mínimo, acompanhamento de eventos e alertas, análise de logs, criação e ajuste de políticas, tratamento de falsos positivos, acompanhamento de bloqueios, troubleshooting, procedimentos de backup e restauração de configurações, atualização de componentes e demais atividades necessárias à operação da solução.
- 1.5 A operação assistida deverá contemplar a transferência de conhecimento de forma prática, permitindo que a equipe da PRODEMGE acompanhe e execute, com orientação da CONTRATADA, as principais atividades necessárias à operação e administração da solução.
- 1.6 Durante o período de operação assistida, a CONTRATADA deverá realizar, sem ônus adicional para a PRODEMGE, as customizações, correções e ajustes finais que se mostrarem necessários em decorrência da instalação, configuração, testes ou utilização da solução.
- 1.7 A CONTRATADA deverá acompanhar o funcionamento da solução durante o período de operação assistida, identificando eventuais inconsistências, falhas de configuração ou necessidades de ajustes e providenciando sua correção.
- 1.8 A operação assistida será realizada preferencialmente de forma presencial nas instalações da PRODEMGE, podendo ser realizada remotamente, mediante definição da PRODEMGE, desde que sejam asseguradas as condições necessárias para a execução integral dos serviços.
- 1.9 Em caráter excepcional, a PRODEMGE poderá solicitar a realização de atividades específicas de operação assistida de forma remota, sem que isso implique ônus adicional.

- 1.10 Ao término da operação assistida, a CONTRATADA deverá entregar relatório contendo, no mínimo, as atividades realizadas, configurações e ajustes efetuados, ocorrências identificadas, respectivas soluções e recomendações para a continuidade da operação pela equipe da PRODEMGE.

Anexo I-F – Serviços de Capacitação

- 1.1 A capacitação técnica deverá contemplar a instalação, configuração, customização, operação, monitoramento e administração da solução ofertada, incluindo seus principais recursos e funcionalidades.
- 1.2 A capacitação deverá ser realizada para turma exclusiva da PRODEMGE, composta por até 4 (quatro) participantes.
- 1.3 Quando houver curso oficial do fabricante que contemple integralmente ou substancialmente os requisitos desta contratação, a CONTRATADA deverá apresentar a respectiva ementa, carga horária e identificação do curso para análise da PRODEMGE.
- 1.4 Serão aceitos cursos oficiais do fabricante ou ministrados por instituição de treinamento por ele autorizada ou credenciada, conforme documentação comprobatória válida na data de realização do curso. Os treinamentos deverão ser conduzidos por instrutores habilitados pelo fabricante, quando essa habilitação estiver prevista em seu programa oficial de capacitação. Poderão ser aceitos cursos não integrantes do catálogo oficial do fabricante, desde que apresentem conteúdo programático e carga horária compatíveis com as funcionalidades da plataforma contratada e sejam ministrados por profissionais que comprovem conhecimento técnico mediante certificação válida do fabricante. A equivalência do curso será previamente avaliada e aprovada pela CONTRATANTE com base no conteúdo programático, na carga horária, na qualificação do instrutor e nos objetivos de aprendizagem.
- 1.5 As capacitações deverão ser ministradas de forma remota, ao vivo, em turma fechada para a PRODEMGE, utilizando solução de videoconferência que permita a participação e interação dos participantes, sendo de responsabilidade da CONTRATADA o fornecimento de toda a infraestrutura necessária para o instrutor.
- 1.6 A capacitação deverá ser realizada em dias úteis, de segunda-feira a sexta-feira, em horário comercial, entre 08:00 e 18:00, em datas previamente acordadas entre a CONTRATADA e a PRODEMGE.
- 1.7 Seja a capacitação realizada de forma remota ou presencial, todos os custos relacionados a material didático, plataforma de capacitação, videoconferência, instrutor, hospedagem, alimentação, passagens e traslado serão de responsabilidade da CONTRATADA.
- 1.8 A CONTRATADA deverá disponibilizar laboratório para realização da capacitação, com acesso pela INTERNET, contendo ambiente compatível com os equipamentos e funcionalidades objeto do treinamento e permitindo a realização de atividades práticas pelos participantes.
- 1.9 A capacitação não poderá utilizar os equipamentos entregues à PRODEMGE no âmbito deste contrato como ambiente de treinamento.

1.10 No caso de capacitação presencial, o local para realização do treinamento será de responsabilidade da CONTRATADA e deverá ser disponibilizado sem ônus adicional para a PRODEMGE.

1. Conteúdo e Metodologia

1.11 O treinamento não poderá ser meramente expositivo, devendo contemplar módulos teóricos e práticos, com utilização de laboratório, exemplos, exercícios e estudos de caso, de modo a capacitar os participantes para a utilização efetiva dos recursos e funcionalidades dos appliances da solução de WAF ofertados.

1.12 O conteúdo programático deverá abranger, no mínimo, os seguintes tópicos:

- 1.21.1 instalação e configuração dos appliances da solução de WAF;
- 1.21.2 customização e parametrização dos equipamentos;
- 1.21.3 acesso, navegação e utilização das interfaces de gerenciamento disponíveis, incluindo, quando aplicável, CLI, GUI e interfaces web;
- 1.21.4 configuração básica e avançada dos recursos e funcionalidades dos appliances da solução de WAF;
- 1.21.5 operação e administração básica e avançada dos equipamentos;
- 1.21.6 gerenciamento e monitoramento dos appliances da solução de WAF e de seus componentes;
- 1.21.7 monitoramento da saúde, desempenho, disponibilidade e utilização dos recursos dos equipamentos;
- 1.21.8 procedimentos de atualização, manutenção e gerenciamento de firmware e demais componentes, quando aplicável;
- 1.21.9 gerenciamento e aplicação das configurações dos equipamentos;
- 1.21.10 identificação, diagnóstico e solução de problemas (troubleshooting), incluindo situações de falha e indisponibilidade;
- 1.21.11 execução de atividades práticas e estudos de caso relacionados às funcionalidades dos equipamentos ofertados.

1.13 A abordagem da capacitação deverá ser predominantemente prática, utilizando exemplos e exercícios que permitam aos participantes executar as atividades apresentadas durante o treinamento.

1.14 A carga horária deverá ser compatível com a carga horária oficial do fabricante, quando existente, de forma a contemplar integralmente o conteúdo programático estabelecido neste Termo de Consulta.

1.15 A capacitação deverá ser realizada conforme cronograma previamente acordado entre a CONTRATADA e a PRODEMGE.

1.16 Os treinamentos das diferentes turmas, quando houver, não poderão ocorrer simultaneamente.

2. Entregáveis e qualificação do instrutor

1.17 A CONTRATADA deverá submeter à PRODEMGE, em até 5 (cinco) dias úteis anteriores à data de realização de cada módulo da capacitação, os seguintes documentos:

1.21.12 Plano da capacitação, contendo, no mínimo, carga horária, cronograma, conteúdo programático, metodologia e 12 (doze) questões para avaliação dos alunos.

1.21.13 As questões deverão ser objetivas, contendo 4 (quatro) alternativas de resposta e apenas 1 (uma) alternativa correta, possuir nível intermediário e contemplar os conteúdos abordados durante o treinamento.

1.21.14 Material didático contendo todos os assuntos abordados na capacitação, disponibilizado em idioma português ou inglês, para análise e aprovação da PRODEMGE.

1.21.15 Instruções e material de apoio do treinamento em mídia eletrônica, em formato HTML ou PDF, ilustrado com imagens, para utilização na divulgação interna pela PRODEMGE.

1.18 A entrega dos materiais deverá ocorrer por meio digital à Gerência de Desenvolvimento de Pessoas da PRODEMGE, através do e-mail capacitar@prodemge.gov.br.

1.19 A PRODEMGE realizará a avaliação do material didático, do plano de capacitação e da qualificação dos instrutores em até 5 (cinco) dias úteis.

1.20 Caso sejam necessários ajustes no material didático, no plano de capacitação ou no conjunto de instrutores, a PRODEMGE solicitará formalmente as adequações à CONTRATADA, que deverá providenciá-las no prazo máximo de 5 (cinco) dias úteis.

1.21 A CONTRATADA deverá apresentar a relação dos profissionais que irão ministrar a capacitação, acompanhada da documentação comprobatória de sua qualificação.

1.22 A comprovação da qualificação deverá ser realizada mediante apresentação de certificação emitida pelo fabricante que demonstre que o instrutor está habilitado para utilização, administração ou ministração de capacitação relacionada aos appliances da solução de WAF ofertados.

3. Direito e uso dos materiais

1.23 Sobre todo o material de capacitação entregue, disponibilizado e utilizado pela CONTRATADA para execução dos serviços de capacitação, incluindo materiais de apoio, apresentações, apostilas, manuais, vídeos de demonstração e outros materiais correlatos, serão concedidos à PRODEMGE os direitos de uso e reprodução, de forma irrestrita, para aplicação em capacitações internas destinadas aos seus funcionários, observadas as limitações legais e os direitos de terceiros eventualmente aplicáveis.

1.24 As aulas poderão ser gravadas pela PRODEMGE para fins de consulta e capacitação interna, desde que observadas as restrições de direitos autorais, propriedade intelectual e proteção de dados eventualmente aplicáveis.

4. Avaliação e Certificação

1.25 Ao final da capacitação, os participantes deverão estar aptos a utilizar e administrar os principais recursos e funcionalidades dos appliances da solução de WAF ofertados, de acordo com o conteúdo programático estabelecido.

1.26 A CONTRATADA deverá aplicar, no último dia da capacitação, avaliação de conhecimento baseada nas questões previamente submetidas à PRODEMGE, com o objetivo de mensurar o aproveitamento dos participantes.

1.27 A CONTRATADA deverá apresentar à PRODEMGE, em até 5 (cinco) dias úteis após o encerramento do treinamento, relatório contendo os resultados da avaliação dos participantes.

1.28 A CONTRATADA deverá emitir, ao final da capacitação, certificado de conclusão para cada participante, contendo, no mínimo, identificação do participante, período de realização, conteúdo programático e carga horária do treinamento.

1.29 Após a realização de cada módulo de capacitação e sua aprovação pela PRODEMGE, será emitido o "Laudo Técnico da Capacitação" (Anexo I-K), atestando a execução da capacitação referente ao módulo.

1.30 Caso a qualidade da execução do treinamento seja comprovadamente considerada insatisfatória pela PRODEMGE, a CONTRATADA deverá realizar novamente a capacitação, sem ônus adicional, no prazo máximo de 10 (dez) dias úteis após a notificação da CONTRATADA.

Anexo I-G - Serviços de Suporte Técnico, manutenção e atualização de versão

1.1. A CONTRATADA deverá prestar serviços de suporte técnico, manutenção corretiva e atualização de software durante 60 (sessenta) meses, contados a partir do aceite definitivo da recepção técnica dos equipamentos, conforme definido neste Termo de Consulta e seus anexos.

1.2. O suporte técnico deverá contemplar o diagnóstico e a identificação de problemas, apoio técnico à utilização, correção de erros, defeitos (bugs), falhas ou mau funcionamento relacionados aos equipamentos, softwares, funcionalidades, recursos e componentes integrantes da solução, inclusive aqueles decorrentes de configurações, customizações e ajustes realizados pela PRODEMGE, desde que compatíveis com as funcionalidades suportadas pelo fabricante.

1.3. A CONTRATADA deverá disponibilizar canais para abertura e acompanhamento de chamados técnicos, contemplando, no mínimo, atendimento por telefone, e-mail, sistema eletrônico de chamados, acesso remoto e atendimento presencial, quando necessário.

1.4. A PRODEMGE poderá registrar quantidade ilimitada de chamados técnicos, durante toda a vigência contratual, sem cobrança adicional.

1.5. O suporte deverá ser prestado em português do Brasil.

1.6. Para chamados classificados como gravidade 1 e 2, conforme os níveis de serviço definidos no Anexo I-M, o atendimento deverá estar disponível em regime 24 x 7, inclusive finais de semana e feriados.

1.7. Para chamados classificados como gravidade 3 e 4, o atendimento deverá estar disponível em regime 8 x 5, em dias úteis, no horário das 08:00 às 18:00 horas.

1.8. Para fins desta especificação, serão considerados feriados oficiais aqueles de âmbito nacional, do Estado de Minas Gerais e do Município de Belo Horizonte.

2. Abertura, acompanhamento e encerramento de chamados

2.1. Na abertura de cada chamado técnico, a CONTRATADA deverá registrar, no mínimo:

- a) código de identificação do chamado;
- b) data e hora de abertura;
- c) descrição do problema ou solicitação;
- d) nível de severidade atribuído;
- e) identificação do solicitante;
- f) identificação do profissional responsável pelo atendimento.

2.2. A CONTRATADA deverá encaminhar à PRODEMGE confirmação da abertura do chamado, contendo as informações registradas no item anterior.

2.3. A severidade atribuída ao chamado poderá ser reclassificada pela CONTRATADA somente mediante justificativa técnica formal, permanecendo assegurado à PRODEMGE o direito de solicitar a revisão da

classificação. A reclassificação não poderá ser utilizada para afastar ou reduzir os prazos de atendimento já aplicáveis ao chamado, salvo quando tecnicamente justificada e aceita pela PRODEMGE.

2.4. O atendimento poderá ser realizado remotamente ou presencialmente, conforme a natureza do problema e os níveis de serviço estabelecidos no Anexo I-M.

2.5. O chamado somente será considerado concluído ou encerrado após o aceite da PRODEMGE, mediante ordem de serviço, e-mail ou sistema eletrônico disponibilizado pela CONTRATADA.

2.6. Ao término de cada atendimento, a CONTRATADA deverá apresentar as informações relativas ao serviço executado, contendo, no mínimo:

- a) código do chamado;
- b) data e hora de conclusão do atendimento;
- c) descrição do problema identificado;
- d) diagnóstico realizado;
- e) procedimentos executados;
- f) solução aplicada ou solução de contorno adotada; e
- g) indicação das providências necessárias para solução definitiva, quando aplicável.

2.7. Quando for adotada solução de contorno, a CONTRATADA deverá manter o chamado em acompanhamento até a implementação da solução definitiva, apresentando, sempre que solicitado pela PRODEMGE, relatório sobre a evolução do atendimento.

3. Atualização de software

3.1. Durante toda a vigência contratual, a CONTRATADA deverá disponibilizar, sem ônus adicional para a PRODEMGE, as atualizações de software, firmware, BIOS, console de gerenciamento e demais softwares fornecidos como parte integrante da solução, incluindo correções, patches, service packs, releases e novas versões disponibilizadas pelo fabricante.

3.2. As atualizações deverão contemplar, quando disponibilizadas pelo fabricante, correções de segurança, correções de erros, aprimoramentos funcionais e demais modificações aplicáveis aos componentes integrantes da solução.

3.3. Para cada atualização disponibilizada, a CONTRATADA deverá fornecer a documentação correspondente, contendo, no mínimo:

- a) identificação e versão da atualização;
- b) descrição das alterações implementadas;
- c) correções realizadas;
- d) eventuais requisitos ou pré-requisitos;
- e) procedimentos para instalação; e
- f) impactos ou recomendações relevantes para sua aplicação.

3.4. A CONTRATADA deverá disponibilizar os arquivos, licenças, autorizações, chaves de instalação e demais elementos necessários para realização das atualizações.

3.5. Caberá exclusivamente à PRODEMGE decidir sobre a instalação das atualizações disponibilizadas, cabendo à CONTRATADA prestar o suporte técnico necessário para sua avaliação e aplicação.

3.6. A CONTRATADA deverá disponibilizar as atualizações por meio eletrônico, mediante download no portal do fabricante ou da própria CONTRATADA, ou por outro meio tecnicamente adequado.

3.7. A CONTRATADA deverá manter atualizados os manuais e demais documentos técnicos correspondentes aos produtos e componentes de software fornecidos.

4. Suporte técnico especializado

4.1. O suporte técnico deverá contemplar, sem ônus adicional:

- a) identificação e diagnóstico de falhas;
- b) correção de erros e defeitos de software;
- c) apoio à operação e administração da solução;
- d) esclarecimento de dúvidas técnicas;
- e) análise de problemas de configuração;
- f) apoio em procedimentos de atualização;
- g) análise de desempenho e otimização da solução;
- h) orientação para aplicação de correções e atualizações; e
- i) suporte aos componentes de hardware e software integrantes da solução.

4.2. O serviço de esclarecimento de dúvidas técnicas deverá estar disponível em horário comercial, das 08:00 às 18:00 horas, em dias úteis, sem limite de quantidade de solicitações.

4.3. Sempre que tecnicamente possível, o suporte será realizado remotamente. Caso o problema não seja solucionado remotamente, a CONTRATADA deverá realizar atendimento presencial, observados os níveis de serviço estabelecidos no Anexo I-M.

4.4. A PRODEMGE deverá ter acesso às bases de conhecimento, documentação técnica, manuais, boletins, notas técnicas e demais recursos disponibilizados pelo fabricante para suporte à solução, observadas as condições de licenciamento aplicáveis.

5. Substituição de peças e componentes

5.1. Durante a vigência contratual, a CONTRATADA deverá substituir, sem ônus adicional para a PRODEMGE, os componentes de hardware que apresentarem defeito ou falha, desde que não decorrentes de uso indevido.

5.2. As peças utilizadas na substituição deverão ser novas, originais ou homologadas pelo fabricante, compatíveis com o equipamento e com as especificações técnicas da solução, sendo vedada a utilização de peças recondicionadas ou remanufaturadas. As peças utilizadas deverão ser compatíveis com o modelo e

configuração do equipamento instalado e não poderão reduzir a capacidade, desempenho ou disponibilidade originalmente contratados.

5.3. Na impossibilidade de fornecimento de componente original, a CONTRATADA deverá apresentar justificativa técnica formal à PRODEMGE e solicitar autorização prévia para utilização de componente alternativo.

5.4. As peças substituídas deverão possuir garantia com término coincidente com o período de garantia/ suporte contratado para o equipamento.

5.5. A CONTRATADA será responsável por todos os custos relacionados à substituição de peças, incluindo mão de obra, transporte, retirada, instalação e testes.

5.6. A substituição deverá ocorrer nos prazos estabelecidos no Anexo I-M, observado, quando aplicável, o prazo máximo de 16 (dezesesseis) horas úteis previsto nesta especificação.

5.7. Caso seja necessária a retirada de equipamento ou componente das dependências da PRODEMGE para realização de reparo, a CONTRATADA será responsável pelo transporte e demais custos envolvidos.

5.8. A retirada de equipamentos somente poderá ocorrer mediante autorização prévia da PRODEMGE e assinatura de Termo de Responsabilidade.

Anexo I-H - Laudo técnico de recebimento dos Equipamentos:

Identificação do contrato: _____

Recebimento < Provisório / Definitivo >

Modelo do Equipamento	Número de Série	Data e horário da entrega dos appliances da solução de WAF	Data e horário do Recebimento Provisório	Data e horário do Recebimento Definitivo

Atesto que a entrega ocorreu de acordo com os critérios estabelecidos no contrato supracitado.

Nome do Fiscal do contrato

Local e data

**Anexo I-I - Laudo técnico de Execução de Serviços de instalação, configuração, migração e
operação assistida.**

Identificação do contrato: _____

Modelo do Equipamento	Número de Série	Descrição do serviço realizado	Data e horário do Início do Serviço	Data e horário do Recebimento Definitivo

Nome do responsável técnico da CONTRATADA

Nome do Fiscal do contrato

Anexo I-J - Ordem de Serviço de Capacitação

Ordem de Serviço de Capacitação

Identificação do contrato:

Identificação da Ordem de Serviço:

Serviço de capacitação técnica para turma de 4 alunos

Início planejado para a Capacitação

Nome do responsável técnico da CONTRATADA

Nome do Fiscal do contrato

Data:

Anexo I-K - Laudo técnico da Capacitação

Identificação do contrato: _____

Turma:

Capacitação:

Data de início da capacitação: _____

Data de término da capacitação: _____

Descrição do serviço realizado:

Nome do responsável técnico da CONTRATADA

Nome do Fiscal do contrato

Anexo I-L - Laudo Técnico dos Serviços Associados

Identificação do contrato: _____

Mês / ANO de referência dos serviços executados:

Número do Chamado	Prioridade	Descrição sumária do chamado	Problema de Hardware ou Software	Número de Série dos appliances da solução de WAF	Descrição do serviço realizado incluindo a substituição de peças se for o caso	Data e horário de início de atendimento	Data e horário da finalização do chamado

Quebra de indicadores de qualidade: Listar os chamados que não cumpriram os indicadores e o indicador.

Nome do responsável técnico da CONTRATADA

Nome do Fiscal do contrato

Anexo I-M - Apuração de Níveis de Serviços

1. Níveis de Serviço:

1.1 Definições e condições gerais

1.1.1 A CONTRATADA realizará a prestação de serviços de atendimento para orientações em casos de dúvidas e/ou problemas, assistindo presencialmente ou remotamente a PRODEMGE, em idioma português do Brasil, durante o período do contrato conforme a natureza do chamado e os níveis de severidade estabelecidos neste Anexo.

1.1.2 Os serviços compreendem o diagnóstico e identificação de problemas, apoio técnico na utilização da solução de WAF, correção de erros, defeitos (bugs) ou mau funcionamento sobre qualquer funcionalidade, recurso, componente ou módulo disponível de forma nativa do equipamento ofertado, ou decorrente de qualquer adaptação (customização) e ajuste (tunning) efetuada pela CONTRATADA.

1.1.3 O suporte deve ser centralizado em uma única central de atendimento, por meio de ligação local em Belo Horizonte/MG ou ligação interurbana gratuita (0800) para todos os produtos.

1.1.4 O tratamento dos chamados abertos junto à CONTRATADA visa à disponibilidade e à qualidade da operação da solução e de seus componentes. Para tanto, a CONTRATADA deverá garantir os atendimentos aos chamados dentro dos prazos e graus de severidade explicitados na tabela 2.

1.1.5 Para a realização de manutenções corretivas ou preventivas programadas, a CONTRATADA deverá planejar e negociar com a equipe de gestão de mudanças da PRODEMGE, para obter a autorização do melhor período para as paralisações necessárias.

1.1.6 Adicionalmente ao suporte da CONTRATADA, é requerido que a PRODEMGE possa abrir chamados técnicos diretamente com o fabricante da solução, em site de suporte ou por telefone. O suporte direto com o fabricante seguirá o nível de serviço publicado pelo fabricante. Além disso, faz-se necessário que o fabricante tenha presença local no Brasil.

1.1.7 O serviço deve garantir à PRODEMGE o pleno acesso aos sites dos fabricantes dos produtos ofertados, incluindo a aberturas de chamados técnicos e consultas a quaisquer bases de dados disponíveis para usuários/clientes, e efetuar downloads de quaisquer atualizações de software ou documentação

1.1.8 Deve ser possível interagir com as equipes de suporte do fabricante da solução.

1.1.9 A CONTRATADA sempre será a responsável contratualmente pelos serviços.

1.1.10 O atendimento a um chamado de suporte técnico deverá ocorrer por qualquer uma das seguintes formas:

1.1.11 Atendimento presencial no local de instalação da solução de WAF;

1.1.12 Atendimento remoto;

1.1.13 Contato telefônico;

1.1.14 Videoconferência;

1.1.15 Envio de mensagem eletrônica (e-mail);

1.1.16 Acesso ao site web com controle de acesso por senha.

1.1.17 A PRODEMGE poderá efetuar um número ilimitado de chamados técnicos, por qualquer uma das formas disponíveis, durante a vigência do contrato.

1.1.18 Na abertura ou registro de um chamado técnico, por qualquer uma das formas disponíveis, a PRODEMGE deverá informar: descrição da solicitação, nível de severidade e identificação completa do solicitante.

1.2 Níveis de Severidade

1.2.1 Para apuração do Índice de Tempo de Atendimento para solução de problemas, os chamados são classificados em 4 (quatro) Níveis de Severidade, de acordo com a tabela 1, a seguir:

Severidade	Descrição
1	Problema Crítico Um problema que tenha um impacto crítico na capacidade da PRODEMGE em manter a solução de WAF ativa. O WAF é incapaz de executar adequadamente as suas tarefas. A solução está inoperante ou severamente degradada.
2	Problema Grave Um problema que tenha um impacto na capacidade da PRODEMGE em manter a solução de WAF ativa, cuja severidade seja significativa, porém não crítica, e que possa ser de natureza repetitiva. O funcionamento da solução é afetado, mas o desempenho não foi severamente degradado. Por exemplo: Indisponibilidade parcial, degradação significativa, bloqueio indevido de aplicações críticas, falha de política de segurança ou perda de funcionalidade relevante sem indisponibilidade total.
3	Problema Leve Problema de baixo impacto que não comprometa significativamente a disponibilidade, segurança ou desempenho da solução, permanecendo a maior parte das funcionalidades disponível, ou alguma intervenção pode ser necessária para a utilização da solução.
4	Solicitação de Informações Não é um problema e sim suporte para ajustes, otimizações, consultas técnicas sobre funcionalidades ou operação da solução.

Tabela 1 – Níveis de Severidade

1.2.2 Um chamado somente será considerado contingenciado ou concluído com o aceite da PRODEMGE.

1.2.3 Solução de Contingência ou de Contorno é uma solução temporária para um problema que não elimina a sua causa raiz. Esta solução restabelece a disponibilidade do ambiente, possibilitando assim

a execução plena de suas funções originais, mantendo o mesmo nível de desempenho anterior ao problema.

1.3 Prazos de Atendimento

- 1.3.1 Para os problemas classificados como de severidade 1 (um), a manutenção será prestada em regime 24x7x365, inicialmente remoto, com atendimento on-site quando necessário com início do atendimento em até 1 (uma) hora corrida após o registro do chamado.
- 1.3.2 Em caso de adoção de uma solução de contingência ou de contorno, esta não poderá ser implementada em prazo superior a 4 (quatro) horas corridas, após o registro do chamado, sempre contando com a disponibilidade da PRODEMGE em atender ao especialista de suporte.
- 1.3.3 Após o contingenciamento do problema, caso haja necessidade de troca do equipamento ou peça, de substituição avançada de peças, do serviço de manutenção, esta deverá ser feita em até 1 (um) dia corrido, a partir da identificação da necessidade da troca.
- 1.3.4 Em sendo utilizada uma solução de contingência, a solução definitiva não poderá ultrapassar 3 (três) dias corridos após o registro do chamado.
- 1.3.5 Para os problemas classificados como severidade 2 (dois), a manutenção será prestada em regime 24x7x365, com atendimento em até 2 (duas) horas corridas após o registro do chamado.
- 1.3.6 Após a abertura de chamado, caso o problema não tenha sido contingenciado remotamente após 6 (seis) horas corridas, contando com a atenção do PRODEMGE, a manutenção deverá ser on-site e a solução de contingência ou de contorno não poderá ser implementada em prazo superior a 8 (oito) horas corridas, após o registro do chamado.
- 1.3.7 Caso haja necessidade de troca do equipamento ou peça, de substituição avançada de peças, do serviço de manutenção, esta deverá ser feita em até 6 (seis) dias corridos, a partir da identificação da necessidade da troca.
- 1.3.8 Em sendo utilizada uma solução de contingência ou contorno, a solução definitiva não poderá ultrapassar 10 (dez) dias corridos após o registro do chamado.
- 1.3.9 Para os chamados classificados como severidade 3 (três), a manutenção será prestada em regime 8 x 5, com atendimento em até 4 (quatro) horas úteis após o registro do chamado.
- 1.3.10 A CONTRATADA terá, no máximo, 72 (setenta e duas) horas úteis, após o registro do chamado, para implantar uma solução definitiva ou de contingência.
- 1.3.11 Sendo utilizada uma solução de contingência ou de contorno, a solução definitiva não poderá ultrapassar 30 (trinta) dias corridos após o registro do chamado.
- 1.3.12 Para os chamados classificados como severidade 4 (quatro), a manutenção será prestada em regime 8 x 5, com atendimento em até 4 (quatro) horas úteis após o registro do chamado.
- 1.3.13 A CONTRATADA terá, no máximo, 15 dias corridos para responder ao chamado e solucionar, após o seu registro.
- 1.3.14 O descumprimento de qualquer dos prazos estabelecidos neste item poderá acarretar desconto no pagamento dos serviços de suporte, conforme os critérios definidos para o indicador ICSP.
- 1.3.15 Não será aceito, pela PRODEMGE, a cobrança de eventuais diferenças vinculadas a questões trabalhistas, tais como férias, horas extras, sobreaviso, etc. Adicionalmente, todos os gastos

provenientes de deslocamento, estadia e alimentação, caso sejam necessários, já deverão estar incluídos no preço final da proposta.

1.3.16 A tabela a seguir relaciona, resumidamente, os níveis de severidade e os tempos de atendimento requeridos:

Severidade	Atendimento após abertura do chamado			
	Regime	Prazo de Atendimento	Solução de Contingência	Solução Definitiva
1	24x7x365	Até 1 (uma) hora corrida*	Até 4 (quatro) horas corridas*	Até 3 (três) dias corridos*
2	24x7x365	Até 2 (duas) horas corridas*	Até 8 (oito) horas corridas*	Até 10 (dez) dias corridos*
3	Horário comercial, no regime 8x5	Até 4 (quatro) horas úteis*	Até 72 (setenta e duas) horas úteis*	Até 30 (trinta) dias corridos*
4	Horário comercial, no regime 8x5	Até 4 (quatro) horas úteis*	Suporte / Resposta ao chamado: Até 15 (quinze) dias corridos*	

Tabela 2 – Níveis de Severidade
 (*) prazo após o registro do chamado

1.4 Indicadores de Qualidade

1.4.1 Os prazos de execução das entregas serão avaliados pelos indicadores de qualidade relacionados no quadro abaixo:

Indicador	Descrição
PEE	Prazo efetivo de entrega
PEICOM	Prazo efetivo para instalação, configuração, operação assistida e migração
ICSP	Índice de chamados solucionados no prazo previsto
DispH	Índice de disponibilidade mensal da solução de WAF

1.5 Detalhamento dos indicadores

Prazo de Entrega do Equipamento

PEE – Prazo Efetivo de Entrega	
Tópico	Descrição
Finalidade	Finalidade Reduzir o risco de atrasos na entrega dos equipamentos. Mede a quantidade de dias de atraso na entrega, no data center da PRODEMGE, dos equipamentos
Meta a cumprir	Prazo de entrega menor ou igual ao prazo definido na tabela 2 da seção 1 deste Termo de Consulta
Instrumento de medição	Termo de recebimento provisório emitido pela PRODEMGE.
Forma de Acompanhamento	Uma medição após o recebimento provisório emitido pela PRODEMGE.
Periodicidade	Uma medição após a emissão do termo de recebimento provisório emitido pela PRODEMGE
Mecanismo de Medição e Gestão	PEE = $DRP - DAC$ Onde, DRP = Data de recebimento provisório do equipamento DAC = Data da assinatura do contrato A data de entrega do equipamento deverá ser aquela reconhecida pelo fiscal técnico, conforme critérios constantes neste Termo de Consulta. Para os casos em que o fiscal técnico rejeita a entrega, o prazo de execução continuará a correr, findando-se apenas quanto a CONTRATADA entregar os equipamentos e haja emissão do termo de recebimento provisório por parte do fiscal técnico.
Observações	Obs. 1 - Atrasos decorrentes de atividades de responsabilidade da PRODEMGE, e devidamente documentados, deverão ser desprezados no cálculo do número de dias corridos de atraso na finalização da atividade de instalação e configuração. Obs. 2 - Serão utilizados dias corridos na medição. Obs. 3 - Os dias com expediente parcial ou facultativo na PRODEMGE serão considerados como dias corridos no cômputo do indicador.
Início da vigência	Na assinatura do contrato.
Faixas de ajuste no pagamento e sanções	Meta não atingida implicará em desconto no valor do pagamento, pela PRODEMGE, do valor do Equipamento. Considera-se para o cálculo do desconto referente a este indicador de qualidade: Sem desconto, se $PEE \leq$ prazo de entrega previsto neste Termo de Consulta Desconto de 1% para cada 30 dias corridos de atraso na entrega.

Prazo de instalação, configuração, operação assistida e Migração

PEICOM - Prazo Efetivo para Instalação, Configuração, Operação Assistida e Migração	
Tópico	Descrição
Finalidade	Reduzir o risco de atrasos instalação, configuração, operação assistida e migração da solução de WAF. Mede a quantidade de dias de atraso no processo de instalação, configuração e operação assistida dos equipamentos.
Meta a cumprir	Prazo de entrega menor ou igual ao prazo definido para este serviço na tabela 3 – Prazos de Entrega.
Instrumento de medição	Termo de recebimento definitivo deste serviço emitido pela PRODEMGE.
Forma de Acompanhamento	Uma medição após o recebimento definitivo emitido pela PRODEMGE.
Periodicidade	Uma medição após a emissão do termo de recebimento definitivo emitido pela PRODEMGE
Mecanismo de Medição e Gestão	PEICOM = DES – DRP (em dias úteis) Onde, DES= Data de entrega do serviço DRP = Dia útil seguinte a data do recebimento provisório dos equipamentos. A data de entrega dos serviços pela CONTRATADA deverá ser aquela reconhecida pelo fiscal técnico, conforme critérios constantes neste Termo de Consulta. Para os casos em que o fiscal técnico rejeita a entrega, o prazo de execução continuará a correr, findando-se apenas quanto a CONTRATADA executar os serviços e haja emissão do termo de recebimento definitivo por parte do fiscal técnico.
Observações	Obs. 1 - Atrasos decorrentes de atividades de responsabilidade da PRODEMGE, e devidamente documentados, deverão ser desprezados no cálculo do número de dias corridos de atraso na finalização da atividade de instalação e configuração. Obs. 2 - Serão utilizados dias úteis na medição. Obs. 3 – Feriados, sábados, domingos e os dias com expediente parcial ou facultativo na PRODEMGE não serão considerados como dias úteis no cômputo do indicador
Início da vigência	No dia seguinte ao aceite da entrega dos equipamentos e registrada no termo de recebimento provisório.
Faixas de ajuste no pagamento e sanções	Meta não atingida implicará em desconto no valor do pagamento, pela PRODEMGE, do valor do Serviço. Considera-se para o cálculo do desconto referente a este indicador de qualidade: Sem desconto, se $PEICOM \leq$ prazo de entrega previsto para este serviço neste Termo de Consulta Desconto de 0,5% para cada 5 dias úteis de atraso.

Prazo de resposta aos Chamados Críticos

ICSPP - Índice de Chamados Solucionados, de severidades 1 e 2, no Prazo Previsto	
Tópico	Descrição
Finalidade	Reduzir os atrasos na resolução de problemas, defeitos e no esclarecimento de dúvidas e questionamentos técnicos pela CONTRATADA. Calcula o percentual dos chamados técnicos solucionados, de nível de gravidade 1 e 2, pela CONTRATADA, no prazo máximo previsto, em relação a todos os chamados técnicos efetuados, de gravidade 1 e 2, durante o período de apuração.
Meta a cumprir	99% dos chamados solucionados de gravidade 1 e 2 deverão ser solucionados dentro do prazo máximo de solução definido neste anexo.
Instrumento de medição	Termo de recebimento definitivo deste serviço emitido pela PRODEMGE.
Forma de Acompanhamento	Uma medição após o recebimento definitivo emitido pela PRODEMGE.
Periodicidade	Uma medição após a emissão do termo de recebimento definitivo emitido pela PRODEMGE
Mecanismo de Medição e Gestão	ICSPP = $(TCP / TC) \times 100$, Onde: TCP = Total de chamados de nível de gravidade 1 e 2, encerrados dentro do prazo máximo definido neste Termo de Consulta, durante o período de apuração. TC = Total de chamados com nível de gravidade 1 e 2, encerrados durante o período de apuração e que tenham condição de aferição do prazo. A data de encerramento dos chamados deverá ser aquela reconhecida pelo fiscal técnico, conforme critérios constantes neste Termo de Consulta. Para os casos em que o fiscal técnico rejeita o encerramento, o prazo de execução continuará a correr, findando-se apenas quanto a CONTRATADA encerrar corretamente os chamados e haja reconhecimento por parte do fiscal técnico, conforme definido neste anexo.
Observações	Atrasos decorrentes de atividades de responsabilidade da PRODEMGE, e devidamente documentados, deverão ser desprezados no cálculo do atraso
Início da vigência	No dia seguinte ao aceite dos serviços de instalação, configuração e operação assistida dos equipamentos e registrada no termo de recebimento definitivo destes serviços.
Faixas de ajuste no pagamento e sanções	Meta não atingida implicará em desconto no valor do pagamento, pela PRODEMGE, do valor mensal do Serviço de suporte técnico, substituição de peças e atualização de versão. Considera-se para o cálculo do desconto referente a este indicador de qualidade: Sem desconto, se $99\% \leq \text{ICSPP} \leq 100\%$ Desconto de 3%, se $80\% \leq \text{ICSPP} < 99\%$ Desconto de 7%, se $70\% \leq \text{ICSPP} < 80\%$ Desconto de 10%, se $\text{ICSPP} < 70\%$

Disponibilidade Mensal

DispH - Índice de disponibilidade mensal da solução de WAF	
Tópico	Descrição
Finalidade	Mensurar o nível de disponibilidade mensal do serviço. Calcula o percentual de disponibilidade mensal por cluster, pela CONTRATADA, durante o período de apuração, por lote. Por cluster entende-se o funcionamento da solução em conjunto.
Meta a cumprir	A solução de WAF deverá manter 99,9% de disponibilidade mensal (horas corridas).
Instrumento de medição	Termo de recebimento definitivo deste serviço emitido pela PRODEMGE.
Forma de Acompanhamento	Terá como base os relatórios de chamados técnicos de gravidade 1 relativos a paralisações da solução de WAF.
Periodicidade	Uma medição ao final do mês das horas indisponíveis da solução de WAF.
Mecanismo de Medição e Gestão	$\text{DispH} = ((\text{Tdisp} - \text{Sdown}) / \text{Tdisp}) * 100$ Onde: DispH = Disponibilidade do serviço, medida em %. Tdisp = Tempo acordado para funcionamento do cluster em horas, referente ao mês de medição considerando o horário de 24 x 7, todos os dias, inclusive feriados e finais de semana. Sdown = Somatório dos tempos de falha (downtime), em horas, considerando o horário de 24 x 7, todos os dias, inclusive feriados e finais de semana. O tempo acordado para funcionamento (Tdisp), em horas, será calculado multiplicando o número de horas pela quantidade de dias no mês de apuração. Cada tempo de falha (downtime) será calculado considerando a data e hora de registro do chamado e de seu contingenciamento ou finalização. Para fins de disponibilidade, o término da indisponibilidade ocorrerá quando o serviço estiver efetivamente restaurado, independentemente do chamado permanecer aberto para solução definitiva. O somatório dos tempos de falha (Sdown) será dado pela soma de todos os tempos de falha ocorridos no mês de medição, sejam eles concluídos ou em estado ainda em aberto. Importante ressaltar que no cálculo da variável "Sdown" serão consideradas as regras definidas no item "Paradas Planejadas" deste Termo de Consulta. Também não serão considerados nos somatórios dos tempos de falhas, os problemas decorrentes de falhas ocasionadas comprovadamente pela PRODEMGE
Observações	Atrasos decorrentes de atividades de responsabilidade da PRODEMGE, e devidamente documentados, deverão ser desprezados no cálculo do atraso
Início da vigência	No dia seguinte ao aceite dos serviços de instalação, configuração e operação assistida dos equipamentos e registrada no termo de recebimento definitivo destes serviços.
Faixas de ajuste no pagamento e sanções	Meta não atingida implicará em desconto no valor do pagamento, pela PRODEMGE, do valor mensal do Serviço de suporte técnico, substituição de peças e atualização de versão. Considera-se para o cálculo do desconto referente a este indicador de qualidade:

	Sem desconto, se $99,9\% \leq \text{DispH} \leq 100\%$ Desconto de 5%, se $95\% \leq \text{DispH} < 99,9\%$ Desconto de 7%, se $90\% \leq \text{DispH} < 95\%$ Desconto de 10%, se $\text{DispH} < 90\%$
--	---

1.5.1 Em caso de meta não atingida por 2 meses seguidos, sem uma justificativa plausível, a PRODEMGE poderá abrir processo punitivo contra a CONTRATADA, conforme definido em seção "Sanções Administrativas".

1.5.2 Em caso de adoção de solução de contingência, sem prejuízo da solução definitiva cabível, a CONTRATADA deve emitir laudos, na periodicidade exigida pela PRODEMGE, informando sobre a evolução dos trabalhos para solucionar o problema de forma definitiva.

1.5.3 O chamado deverá continuar aberto, com status de contingenciado, até sua solução definitiva

1.6 Paradas planejadas

1.6.1 Paradas planejadas para reparo dos equipamentos e/ou atualização de software não serão consideradas incidentes.

1.6.2 Paradas planejadas são previamente agendadas e aprovadas pela PRODEMGE, através de comunicação formal entre a PRODEMGE e a CONTRATADA. Estas paralisações devem ser solicitadas com um mínimo de 10 (dez) dias corridos de antecedência, ou de comum acordo entre as partes.

1.6.3 Somente serão consideradas ocorrências de severidade se excederem os prazos pactuados para o reparo e a responsabilidade por esta falha for comprovadamente da CONTRATADA.

1.7 Gestão dos níveis de serviço

1.7.1 Na ABERTURA (REGISTRO) dos CHAMADOS, a PRODEMGE irá comunicar, via mensagem eletrônica (e-mail), à CONTRATADA as seguintes informações:

1.7.1.1 Data e hora de abertura do CHAMADO.

1.7.1.2 Código de identificação do CHAMADO.

1.7.1.3 Descrição do CHAMADO.

1.7.1.4 Nível de Gravidade do CHAMADO.

1.7.1.5 Identificação (nome completo e matrícula) do solicitante da PRODEMGE.

1.7.1.6 Identificação do atendente da CONTRATADA.

1.7.2 O CONTINGENCIAMENTO do CHAMADO será confirmado através do aceite pela PRODEMGE na ordem de serviço (OS) correspondente, desde que incluso as seguintes informações:

1.7.2.1 Código de identificação do CHAMADO.

1.7.2.2 Data e hora de conclusão do contingenciamento.

1.7.2.3 Descrição detalhada do serviço executado.

1.7.3 A CONCLUSÃO definitiva do CHAMADO será confirmada através do aceite pela PRODEMGE na ordem de serviço (OS) correspondente, desde que incluso as seguintes informações:

1.7.3.1 Código de identificação do CHAMADO.

1.7.3.2 Data e hora de conclusão do serviço executado.

1.7.3.3 Descrição detalhada do serviço executado.

1.7.4 A conclusão definitiva de cada chamado, de gravidade 1 e 2, será confirmada através do aceite pela PRODEMGE do atendimento correspondente, conforme definido no Anexo I-L ("Laudo técnico de execução de serviços de suporte técnico e substituição de peças e atualização de versão de software").

1.7.5 Deve ser emitido pela CONTRATADA um relatório mensal consolidado de atendimento (Relatório de Apuração de Níveis de serviço - Anexo I-N), para todos os indicadores e contemplando todos os chamados registrados no mês, contendo as seguintes informações: número de identificação do chamado, data e hora da abertura do chamado, data e hora de contingenciamento do chamado (se for o caso), data e hora de fechamento do chamado (se for o caso).

1.7.6 A CONTRATADA deverá elaborar e enviar à PRODEMGE até o 5º (quinto) dia útil do mês, o relatório de apuração de níveis de serviço.

1.7.7 Neste relatório serão apresentados os resultados referentes aos indicadores de qualidade com período de apuração encerrando no mês que precede à data de sua emissão e, se for o caso, o valor do desconto no pagamento do serviço.

Anexo I-N - Relatório de Apuração de Níveis de Serviços

Identificação do contrato: _____

Modelo e número de série: _____

Código do indicador de qualidade: _____

Período de apuração: ____ / ____ / ____ a ____ / ____ / ____

Valor apurado: _____

Desconto no pagamento: SIM ou NÃO

() desconto de R\$ _____ (_____) na parcela devida no
mês conforme estipulado no contrato supracitado.

Para o indicador relativo às solicitações e atendimento, informar os chamados no período (código do chamado, descrição sumária, data de hora do chamado, do início de atendimento e de conclusão)

Nome do responsável técnico da CONTRATADA

Nome do Fiscal do contrato

Anexo I-O – Laudo Técnico de Inconformidades

Identificação do contrato: _____

Marca e Modelo

Número de Série

Foram encontradas inconformidades na

☐ - Entrega do equipamento

☐ - Serviços de instalação, configuração e operação assistida

Descrição das inconformidades

Nome do responsável técnico da CONTRATADA

Nome do Fiscal do contrato