TRIBUNAL DE CONTAS
Estado de Mato Grosso do Sul

PREGÃO ELETRÔNICO N. 14/2024

PROCESSO TC-CP/1186/2024

TERMO DE CONTRATO N. 005/2026

CONTRATO DE PESSOA JURÍDICA PARA SERVIÇOS DE OUTSOURCING DA SOLUÇÃO DE SEGURANÇA DA INFORMAÇÃO: INCLUINDO O FORNECIMENTO DE SOLUÇÃO COMO SERVIÇO, ENVOLVENDO HARDWARE, SOFTWARE, ASSINATURAS DE ATUALIZAÇÃO, INSTALAÇÃO, TREINAMENTO, CUSTOMIZAÇÃO, SUPORTE TÉCNICO E MANUTENÇÃO, QUE FIRMAM O TRIBUNAL DE CONTAS DO ESTADO DE MATO GROSSO DO SUL E IMAGETECH TECNOLOGIA EM INFORMÁTICA LTDA

TERMO DE CONTRATO

O Tribunal de Contas do Estado e Mato Grosso do Sul, com sede na Rua Des. José Nunes da Cunha Bloco 29 - Parque dos Poderes – CEP 79.031-902, Campo Grande/MS, inscrito (a) no CNPJ sob o 15.424.948/0001-41, neste ato representado(a) pelo(a) seu Presidente, Conselheiro Flávio Esgaib Kayatt, doravante denominado CONTRATANTE, e o(a) IMAGETECH TECNOLOGIA EM INFORMÁTICA LTDA , inscrito(a) no CNPJ/MF sob o nº 05.583.680/0001-37, sediado(a) na 15 de novembro 2.668, loja anexo ao Edifício Terrace Tower, Jardim dos Estados, CEP: 79020-300 em Campo Grande - MS doravante designado CONTRATADO, neste ato representado (a) por seu responsável legal, Senhor ARTHUR AFFONSO DE BARROS MARINHO, conforme atos constitutivos da empresa ou procuração apresentada nos autos, tendo em vista o que consta no PROCESSO TC-CP/1186/2024, mediante ato autorizativo da contratação constante às fls. 7567 e.7568, e em observância às disposições da Lei nº 14.133, de 1º de abril de 2021, e demais legislação aplicável, resolvem celebrar o presente Termo de Contrato, decorrente da Pregão Eletrônico n.

TRIBUNAL DE CONTAS
Estado de Mato Grosso do Sul

14/2025, mediante as cláusulas e condições a seguir enunciadas.

CLÁUSULA PRIMEIRA - DO OBJETO:

1.1. O Objeto do presente instrumento é a Contratação de empresa especializada em serviços de outsourcing da solução de segurança da informação: incluindo o fornecimento de solução como serviço, envolvendo hardware, software, assinaturas de atualização, instalação, treinamento, customização, suporte técnico e manutenção.

1.2. Objeto da contratação:

Lote	Item	Tipo	Descrição do Componente / Serviço	Unidade de medida	Qtde	Valor Unitário	Valor Total
ÚNICO	1	Equipamentos	Equipamentos: Hardware para proteção de perímetro, balanceamento de carga, proteção de aplicações e endpoints, conforme especificações técnicas e requisitos de desempenho do projeto.	Mensal	12	R$ 134.767,29	R$ 1.617.207,48
	2	Licenciamentos	Licenciamentos: Licenças de software necessárias para ativação e funcionamento das soluções de segurança, balanceamento, monitoramento, gerenciamento de TI e SNOC/SOC.	Mensal	12	R$ 212.095,14	R$ 2.545.141,68
	3	Serviços de instalação e configuração	Serviços de Instalação e Configuração: Atividades de instalação física dos equipamentos, configuração dos sistemas de segurança, rede e monitoramento segundo normas	Único	1	R$ 24.602,04	R$ 24.602,04

TRIBUNAL DE CONTAS
Estado de Mato Grosso do Sul

			e diretrizes do fabricante				
	4.	Serviço de suporte técnico, operação e manutenção, incluindo SNOC	Serviço de suporte técnico, operação e manutenção, incluindo SNOC: Serviços de suporte especializado para todas soluções contratadas, operação contínua, manutenção preventiva e corretiva, administração de incidentes e resposta rápida a problemas, com equipe certificada e dedicada (perfis detalhados no termo técnico).	Mensal	12	R$ 94.476,76	R$ 1.133.721,12
	5	Despesas administrativas e indiretas	Despesas administrativas e indiretas: Custos relacionados à administração, gestão de contratos, controle operacional, infraestrutura de apoio e despesas indiretas necessárias para execução do contrato	Mensal	12	R$ 23.110,64	R$ 277.327,68
Valor Total						R$ 464.449,83	R$ 5.598.000,00

1.3. Vinculam esta contratação, independentemente de transcrição:

1.3.1. O Termo de Referência;

1.3.2. O Edital da Licitação;

1.3.3. A Proposta de Preços do contratado;

1.3.4. Eventuais anexos dos documentos supracitados.

CLÁUSULA SEGUNDA - VIGÊNCIA E PRORROGAÇÃO:

TRIBUNAL DE CONTAS
Estado de Mato Grosso do Sul

2.1. O prazo de vigência da contratação é de 12 (doze) meses, contados da assinatura do contrato, prorrogável por até 10 (dez) anos, na forma dos artigos 106 e 107 da Lei n° 14.133/2021.

2.1.1 A prorrogação de que trata este item é condicionada ao ateste, pela autoridade competente, de que as condições e os preços permanecem vantajosos para a Administração, permitida a negociação com o Contratado, atentando, ainda, para o cumprimento dos seguintes requisitos:

2.1.2 Estar formalmente demonstrado no processo que a forma de prestação dos serviços tem natureza continuada;

2.1.3. Seja juntado relatório que discorra sobre a execução do contrato, com informações de que os serviços tenham sido prestados regularmente;

2.1.4. Seja juntada justificativa e motivo, por escrito, de que a Administração mantém interesse na realização do serviço;

2.1.5. Haja manifestação expressa do CONTRATADO informando o interesse na prorrogação;

2.1.6. Seja comprovado que o CONTRATADO mantém as condições iniciais de habilitação.

2.2. O contratado não tem direito subjetivo à prorrogação contratual.

2.3. A prorrogação de contrato deverá ser promovida mediante celebração de termo aditivo.

2.4. O contrato não poderá ser prorrogado quando o contratado tiver sido penalizado nas sanções de declaração de inidoneidade ou impedimento de licitar e contratar com poder público, observadas as abrangências de aplicação.

CLÁUSULA TERCEIRA - MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAIS:

3.1. O regime de execução contratual, os modelos de gestão e de execução, assim como os prazos e condições de conclusão, entrega, observação e recebimento do objeto constam no item 6 do Termo de Referência.

CLÁUSULA QUARTA - SUBCONTRATAÇÃO:

4.1. Não será admitida a subcontratação do objeto contratual.

CLÁUSULA QUINTA - PREÇO:

5.1. O valor mensal da contratação é de R$ 464.449,83 (quatrocentos e sessenta e quatro mil quatrocentos e quarenta e nove reais e oitenta e três

TRIBUNAL DE CONTAS
Estado de Mato Grosso do Sul

centavos), mais o valor da parcela única referente ao item 3, de R$ 24.602,04 (vinte e quatro mil seiscentos e dois reais e quatro centavos), perfazendo o valor anual de R$ 5.598.000,00 (Cinco milhões quinhentos e noventa e oito mil reais).

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

CLÁUSULA SEXTA – PAGAMENTO

6.1. O prazo para pagamento ao contratado e demais condições a ele referentes encontram-se definidos no item 8 do Termo de Referência.

CLÁUSULA SÉTIMA – REAJUSTE

7.1. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do orçamento estimado, em 22/01/2026.

7.2. Após o interregno de um ano, e independentemente de pedido do contratado, os preços iniciais serão reajustados, mediante a aplicação, pelo contratante, do Índice de Custos de Tecnologia da Informação – ICTI, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

7.3. Caso o índice estabelecido para reajustamento não seja atualizado, venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o Índice de Preços ao Consumidor – IPCA.

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

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

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

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

7.8. Na ausência de previsão legal quanto ao índice substituto, as partes

TRIBUNAL DE CONTAS
Estado de Mato Grosso do Sul

elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

7.9. O reajuste será realizado por apostilamento.

CLÁUSULA OITAVA – OBRIGAÇÕES DO CONTRATANTE

8.1. São obrigações do Contratante, **além das previstas no Termo de Referência:**

8.1.1. Exigir o cumprimento de todas as obrigações assumidas pelo Contratado, de acordo com o contrato e seus anexos;

8.1.2. Receber o objeto no prazo e condições estabelecidas no Termo de Referência;

8.1.3. 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;

8.1.4. Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pelo Contratado;

8.1.5. Comunicar a empresa para emissão de Nota Fiscal no que pertine à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento, quando houver controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, conforme o art. 143 da Lei nº 14.133, de 2021;

8.1.6. Efetuar o pagamento ao Contratado do valor correspondente à execução do objeto, no prazo, forma e condições estabelecidos no presente Contrato e no Termo de Referência;

8.1.7. Aplicar ao Contratado as sanções previstas na lei e neste Contrato;

8.1.8. 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.

8.1.9. A Administração terá o prazo de 15 (quinze) dias úteis, a contar da data do protocolo do requerimento para decidir, admitida a prorrogação motivada, por igual período.

8.1.10. Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pelo contratado no prazo máximo de 15 (quinze) dias úteis.

8.1.11. Notificar os emitentes das garantias quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.

TRIBUNAL DE CONTAS
Estado de Mato Grosso do Sul

8.1.12. Comunicar o Contratado na hipótese de posterior alteração do projeto pelo Contratante, no caso do art. 93, §2º, da Lei nº 14.133, de 2021.

8.1.13. A Administração 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.

CLÁUSULA NONA – OBRIGAÇÕES DO CONTRATADO

9.1. O Contratado deve cumprir todas as obrigações constantes deste Contrato e de seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas, **além das previstas no Termo de Referência:**

9.1.1. Manter preposto aceito pela Administração no local ou do serviço para representá-lo na execução do contrato.

9.1.2. A indicação ou a manutenção do preposto da empresa poderá ser recusada pelo órgão ou entidade, desde que devidamente justificada, devendo a empresa designar outro para o exercício da atividade.

9.1.3. Atender às determinações regulares emitidas pelo fiscal ou gestor do contrato ou autoridade superior (art. 137, II, da Lei n.º 14.133, de 2021) e prestar todo esclarecimento ou informação por eles solicitados;

9.1.4. Alocar os empregados necessários ao perfeito cumprimento das cláusulas deste contrato, com habilitação e conhecimento adequados, fornecendo os materiais, equipamentos, ferramentas e utensílios demandados, cuja quantidade, qualidade e tecnologia deverão atender às recomendações de boa técnica e a legislação de regência;

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

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

9.1.7. Não contratar, durante a vigência do contrato, cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente do contratante ou do fiscal ou gestor do contrato, nos termos do artigo 48,

TRIBUNAL DE CONTAS
Estado de Mato Grosso do Sul

parágrafo único, da Lei nº 14.133, de 2021.

9.1.8. Quando não for possível a verificação da regularidade no Sistema de Cadastro de Fornecedores – SICAF, o contratado deverá entregar ao setor responsável pela fiscalização do contrato, junto com a Nota Fiscal para fins de pagamento, os seguintes documentos: 1) prova de regularidade relativa à Seguridade Social; 2) certidão conjunta relativa aos tributos federais e à Dívida Ativa da União; 3) certidões que comprovem a regularidade perante a Fazenda Estadual ou Distrital do domicílio ou sede do contratado; 4) Certidão de Regularidade do FGTS – CRF; e 5) Certidão Negativa de Débitos Trabalhistas – CNDT;

9.1.9. Responsabilizar-se pelo cumprimento de todas as obrigações previstas em Acordo, Convenção, Dissídio Coletivo de Trabalho ou equivalentes das categorias abrangidas pelo contrato, por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao Contratante;

9.1.10. Comunicar ao Fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local dos serviços.

9.1.11. Prestar todo esclarecimento ou informação solicitada pelo Contratante ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do empreendimento.

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

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

9.1.14. Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local dos serviços e nas melhores condições de segurança, higiene e disciplina;

9.1.15. Submeter previamente, por escrito, ao Contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo ou instrumento congêneres.

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

TRIBUNAL DE CONTAS
Estado de Mato Grosso do Sul

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

9.1.18. Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas na legislação (art. 116, da Lei n.º 14.133, de 2021);

9.1.19. Comprovar a reserva de cargos a que se refere a cláusula acima, no prazo fixado pelo fiscal do contrato, com a indicação dos empregados que preencheram as referidas vagas (art. 116, parágrafo único, da Lei n.º 14.133, de 2021);

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

9.1.21. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da contratação, exceto quando ocorrer algum dos eventos arrolados no art. 124, II, d, da Lei nº 14.133, de 2021.

9.1.22. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança do contratante;

CLÁUSULA DÉCIMA – OBRIGAÇÕES PERTINENTES À LGPD

10.1. As partes se comprometem a proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, relativos ao tratamento de dados pessoais, inclusive nos meios digitais, nos termos da Lei Geral de Proteção de Dados - LGPD (Lei n. 13.709, de 14 de agosto de 2018), independentemente de declaração ou de aceitação expressa.

PARAGRÁFO ÚNICO: O tratamento de dados pessoais dar-se-á de acordo com as bases legais previstas nas hipóteses dos artigos 7º, 11 e/ou 14 da Lei 13.709/2018 às quais se submeterão os serviços e/ou o objeto da contratação, e para propósitos legítimos, específicos, explícitos e informados ao titular.

10.2. A CONTRATADA obriga-se ao dever de proteção, confidencialidade, sigilo de toda informação, dados pessoais e base de dados a que tiver acesso, nos termos da LGPD, suas alterações e regulamentações posteriores, durante o cumprimento do objeto descrito no instrumento contratual.

PARÁGRAFO PRIMEIRO: A CONTRATADA não poderá se utilizar de

TRIBUNAL DE CONTAS
Estado de Mato Grosso do Sul

informação, dados pessoais ou base de dados a que tenham acesso, para fins distintos da execução dos serviços especificados no instrumento contratual, observada a boa-fé e os princípios do art. 6º da LGPD.

PARÁGRAFO SEGUNDO: Em caso de necessidade de coleta de dados pessoais dos titulares mediante consentimento, indispensáveis à própria prestação do serviço, esta será realizada após prévia aprovação do TRIBUNAL DE CONTAS DO ESTADO DE MATO GROSSO DO SUL, responsabilizando-se a CONTRATADA pela obtenção e gestão.

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

10.3. A CONTRATADA obriga-se a implementar medidas técnicas e administrativas aptas a promover a segurança, a proteção, a confidencialidade e o sigilo de toda informação, dados pessoais e/ou base de dados que tenha acesso, a fim de evitar acessos não autorizados, acidentes, vazamentos acidentais ou ilícitos que causem destruição, perda, alteração, comunicação ou qualquer outra forma de tratamento inadequado ou ilícito; tudo isso de forma a reduzir o risco ao qual o objeto do contrato ou o TRIBUNAL DE CONTAS DO ESTADO DE MATO GROSSO DO SUL está exposto.

PARÁGRAFO ÚNICO: A critério do TRIBUNAL DE CONTAS DO ESTADO DE MATO
GROSSO DO SUL, a CONTRATADA poderá ser provocada a colaborar na elaboração do relatório de impacto, conforme a sensibilidade e o risco inerente dos serviços objeto deste contrato, no tocante a dados pessoais.

10.4. A CONTRATADA deverá manter os registros de tratamento de dados pessoais que realizar, assim como aqueles compartilhados, com condições de rastreabilidade e de prova eletrônica a qualquer tempo.

PARÁGRAFO PRIMEIRO: Bancos de dados formados a partir de contratos administrativos, notadamente aqueles que se proponham a armazenar dados pessoais, devem ser mantidos em ambiente virtual controlado, com registro individual rastreável de tratamentos realizados (LGPD, art. 37), com cada acesso, data, horário e registro da finalidade, para efeito de responsabilização, em caso de eventuais omissões, desvios ou abusos.

PARÁGRAFO SEGUNDO: Os referidos bancos de dados devem ser desenvolvidos em formato interoperável, a fim de garantir a reutilização desses

TRIBUNAL DE CONTAS
Estado de Mato Grosso do Sul

dados pela Administração nas hipóteses previstas na LGPD.

PARÁGRAFO TERCEIRO: A CONTRATADA deverá permitir a realização de auditorias e disponibilizar toda a informação necessária para demonstrar o cumprimento das obrigações

relacionadas à sistemática de proteção de dados.

PARÁGRAFO QUARTO: A CONTRATADA deverá apresentar ao TRIBUNAL DE CONTAS
DO ESTADO DE MATO GROSSO DO SUL, sempre que solicitado, toda e qualquer informação e documentação que comprovem a implementação dos requisitos de segurança especificados na contratação, de forma a assegurar a auditabilidade do objeto contratado, bem como os demais dispositivos legais aplicáveis.

10.5. A CONTRATADA se responsabilizará por assegurar que todos os seus colaboradores, consultores, e/ou prestadores de serviços que, no exercício das suas atividades, tenham acesso e/ou conhecimento da informação e/ou dos dados pessoais, respeitem o dever de proteção, confidencialidade e sigilo, devendo estes assumir compromisso formal de preservar a confidencialidade e segurança de tais dados, documento que estiver disponível em caráter permanente para exibição ao TRIBUNAL DE CONTAS DO ESTADO DE MATO GROSSO DO SUL, mediante solicitação.

PARÁGRAFO ÚNICO: A CONTRATADA deverá promover a revogação de todos os privilégios de acesso aos sistemas, informações e recursos do TRIBUNAL DE CONTAS DO ESTADO DE MATO GROSSO DO SUL, em caso de desligamento de funcionário das atividades inerentes à execução do presente Contrato.

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

PARAGRÁFO ÚNICO: Caso autorizada transmissão de dados pela CONTRATADA a terceiros, as informações fornecidas/compartilhadas devem se limitar ao estritamente necessário para o fiel desempenho da execução do instrumento contratual.

10.7. A CONTRATADA deverá adotar planos de resposta a incidentes de segurança eventualmente ocorridos durante o tratamento dos dados coletados para a execução das finalidades deste contrato, bem como dispor de mecanismos que possibilitem a sua correção, de modo a evitar ou minimizar eventuais danos aos titulares dos dados.

10.8. A CONTRATADA deverá comunicar formalmente e de imediato ao

TRIBUNAL DE CONTAS
Estado de Mato Grosso do Sul

TRIBUNAL DE CONTAS DO ESTADO DE MATO GROSSO DO SUL a ocorrência de qualquer risco, ameaça ou incidente de segurança que possa acarretar comprometimento ou dano potencial ou efetivo a Titular de dados pessoais.

PARAGRÁFO ÚNICO: A comunicação acima mencionada não eximirá a CONTRATADA das obrigações, e/ou sanções que possam incidir em razão da perda de informação, dados pessoais e/ou base de dados.

10.9. Encerrada a vigência do contrato ou após a satisfação da finalidade pretendida, a CONTRATADA interromperá o tratamento dos dados pessoais disponibilizados pelo

TRIBUNAL DE CONTAS DO ESTADO DE MATO GROSSO DO SUL e, em no máximo trinta
dias, sob instruções e na medida do determinado por este, eliminará completamente os Dados Pessoais e todas as cópias porventura existentes (seja em formato digital ou físico), salvo quando a CONTRATADA tenha que manter os dados para cumprimento de obrigação legal.

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

10.10. A CONTRATADA ficará obrigada a assumir total responsabilidade e ressarcimento por todo e qualquer dano e/ou prejuízo sofrido incluindo sanções aplicadas pela autoridade nacional decorrentes de tratamento inadequado dos dados pessoais compartilhados pelo TRIBUNAL DE CONTAS DO ESTADO DE MATO GROSSO DO SUL para as finalidades pretendidas neste contrato.

10.11. A CONTRATADA ficará obrigada a assumir total responsabilidade pelos danos patrimoniais, morais, individuais ou coletivos que venham a ser causados em razão do descumprimento de suas obrigações legais no processo de tratamento dos dados compartilhados pelo TRIBUNAL DE CONTAS DO ESTADO DE MATO GROSSO DO SUL.

PARAGRÁFO ÚNICO: Eventuais responsabilidades serão apuradas de acordo com o que dispõe a Seção III, Capítulo VI da LGPD.

10.12. A Administração deverá ser informada no prazo de 5 (cinco) dias úteis sobre todos os contratos de suboperação firmados ou que venham a ser celebrados pelo Contratado.

10.13. O Contratado deverá exigir de suboperadores e subcontratados o cumprimento dos deveres da presente cláusula, permanecendo integralmente responsável por garantir sua observância.

TRIBUNAL DE CONTAS
Estado de Mato Grosso do Sul

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

10.15. O Contratado deverá prestar, no prazo fixado pelo Contratante, prorrogável justificadamente, quaisquer informações acerca dos dados pessoais para cumprimento da LGPD, inclusive quanto a eventual descarte realizado.

10.16. O contrato está sujeito a ser alterado nos procedimentos pertinentes ao tratamento de dados pessoais, quando indicado pela autoridade competente, em especial a ANPD por meio de opiniões técnicas ou recomendações, editadas na forma da LGPD.

10.17. Os contratos e convênios de que trata o § 1º do art. 26 da LGPD deverão ser
comunicados à autoridade nacional.

CLÁUSULA DÉCIMA PRIMEIRA – GARANTIA DE EXECUÇÃO

11.1. As regras relativas à garantia de execução são as previstas no item 4.9 do Termo de Referência, anexo a este Contrato.

CLÁUSULA DÉCIMA SEGUNDA – INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

12.1. As regras acerca de infrações e sanções administrativas referentes à execução do contrato são aquelas definidas no item 8.10 do Termo de Referência, anexo a este Contrato.

CLÁUSULA DÉCIMA TERCEIRA – PLANO DE TRANSIÇÃO CONTRATUAL

13.1. Em caso de rescisão ou não renovação contratual, a CONTRATADA obriga- se a prestar para o TCE-MS ou a terceiro por ele designado, toda a assistência a fim de que os serviços continuem sendo prestados sem interrupção ou efeito adverso, e que haja uma transferência ordenada de conhecimento dos serviços, processos e tecnologias para o Tribunal ou a seu designado.

13.2. A CONTRATADA deverá apresentar um plano de transição contratual com no prazo máximo de 3 (três) meses a contar da data prevista para encerramento das atividades. O Tribunal analisará, no prazo de 5 (cinco) dias úteis, o plano apresentado, aprovando-o ou recusando-o de forma fundamentada. No caso de não aprovação, a CONTRATADA deverá apresentar novo plano, no prazo

TRIBUNAL DE CONTAS
Estado de Mato Grosso do Sul

máximo de 3 (três) dias úteis, após o recebimento da recusa do plano anterior.

13.3. O plano de transição contratual e sua execução deverão ser viabilizados sem ônus adicionais a contratante e deverá conter no mínimo, os seguintes itens:

a) Identificação dos profissionais designados pela CONTRATADA que irão compor a equipe de transferência de conhecimentos, bem como os seus papéis e as suas responsabilidades;
b) Cronograma geral do repasse;
c) Identificação das etapas e as atividades com suas respectivas datas de início e término, os produtos gerados, os recursos envolvidos e os marcos intermediários, quando aplicável;
d) Plano de gerenciamento de riscos e plano de contingência;
e) Descrição da forma de entrega para o Tribunal de todos os dados em poder da CONTRATADA, incluindo-se a totalidade dos dados contidos no Sistema de Gestão de Demandas da CONTRATADA, se existir;

f) Relação das Ordens de Serviço canceladas automaticamente em razão do encerramento do contrato, com relatório detalhado da parte dos serviços executados e possíveis pendências de execução.

13.4. É de responsabilidade da CONTRATADA a execução do plano de transição contratual, a prestação de serviços de operação assistida, bem como a garantia do repasse bem sucedido de todas as informações necessárias à continuidade dos serviços pela contratante ou empresa por ele designada.

13.5. A elaboração e a execução do plano de transição contratual ocorrerão em paralelo ao atendimento das ordens de serviços demandadas pelo TCE-MS.

13.6. O Tribunal reserva-se o direito de reduzir ou dispensar o plano de transição contratual, desde que o novo provedor contratado venha a comprovar que detém pleno domínio sobre as atividades previstas em contrato.

CLÁUSULA DÉCIMA QUARTA – DA EXTINÇÃO CONTRATUAL (art. 92, XIX)

14.1. O contrato será extinto quando vencido o prazo nele estipulado, observado o regime de transição contratual disposto na Cláusula 13 deste Contrato.

14.2. O contrato poderá ser extinto antes do prazo nele fixado, sem ônus para o contratante, quando esta não dispuser de créditos orçamentários para sua continuidade ou quando entender que o contrato não mais lhe oferece vantagem.

14.3. A extinção nesta hipótese ocorrerá na próxima data de aniversário do

TRIBUNAL DE CONTAS
Estado de Mato Grosso do Sul

contrato, desde que haja a notificação do contratado pelo contratante nesse sentido com pelo menos 2 (dois) meses de antecedência desse dia.

14.4. Caso a notificação da não-continuidade do contrato de que trata este subitem ocorra com menos de 2 (dois) meses da data de aniversário, a extinção contratual ocorrerá após 2 (dois) meses da data da comunicação.

14.5. O contrato poderá ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no artigo 137 da Lei nº 14.133/21, bem como amigavelmente, assegurados o contraditório e a ampla defesa.

14.5.1. Nesta hipótese, aplicam-se também os artigos 138 e 139 da mesma Lei.

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

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

14.6. O termo de extinção, sempre que possível, será precedido:

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

14.6.2. Relação dos pagamentos já efetuados e ainda devidos;

14.6.3. Indenizações e multas.

14.7. A extinção do contrato não configura óbice para o reconhecimento do desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório (art. 131, caput, da Lei n.º 14.133, de 2021).

14.8. O contrato poderá ser extinto caso se constate que o contratado mantém vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que tenha desempenhado função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau (art. 14, inciso IV, da Lei n.º 14.133, de 2021).

CLÁUSULA DÉCIMA QUINTA – DOTAÇÃO ORÇAMENTÁRIA

15.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento do tribunal de Contas do Estado de mato Grosso do Sul deste exercício, na dotação abaixo discriminada:

TRIBUNAL DE CONTAS
Estado de Mato Grosso do Sul

Unidade Orçamentária	3101
Funcional Programática	10.03101.01.032.0002.2011.0001
Fonte de recursos	1500
Natureza da Despesa	3.3.90.40.79
Descrição da Despesa	Serviço de Suporte a Usuário e de Infraestrutura de TIC
Natureza da Despesa	3.3.90.40.11
Descrição da Despesa	Despesas com Licenças de Uso de Software de Processamento de Dados

Despesas com Licenças de Uso de Software de Processamento de Dados

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

CLÁUSULA DÉCIMA SEXTA –DOS CASOS OMISSOS

16.1. A legislação aplicável ao presente contrato encontra-se disciplinada na Lei nº 14.133/2021 e demais normas federais aplicáveis, incluindo as instruções normativas do Governo Federal, e os casos omissos serão decididos pelo contratante subsidiariamente com base nas disposições contidas na Lei 8.078/1990 e normas e princípios gerais dos contratos.

CLÁUSULA DÉCIMA SÉTIMA – ALTERAÇÕES

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

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

17.3. As alterações contratuais deverão ser promovidas mediante celebração de termo aditivo, submetido à prévia aprovação da consultoria jurídica do contratante, salvo nos casos de justificada necessidade de antecipação de seus efeitos, hipótese em que a formalização do aditivo deverá ocorrer no prazo máximo de 1 (um) mês (art. 132 da Lei nº 14.133, de 2021).

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

CLÁUSULA DÉCIMA OITAVA – PUBLICAÇÃO

TRIBUNAL DE CONTAS
Estado de Mato Grosso do Sul

18.1. Incumbirá ao contratante divulgar o presente instrumento no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no art. 94 da Lei 14.133, de 2021, bem como no respectivo sítio oficial na Internet, em atenção ao art. 91, *caput,* da Lei n.º 14.133, de 2021, e ao art. 8º, §2º, da Lei n. 12.527, de 2011, c/c art. 7º, §3º, inciso V, do Decreto n. 7.724, de 2012.

CLÁUSULA DÉCIMA NONA – FORO

19.1. Fica eleito o Foro da Campo Grande - MS para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não puderem ser compostos pela conciliação, conforme art. 92, §1º, da Lei nº 14.133/21.

Campo Grande – MS, data da assinatura digital.

TRIBUNAL DE CONTAS DO ESTADO E MATO GROSSO DO SUL
Conselheiro Flávio Esgaib Kayatt
Presidente

Grupo Imagetech
ARTHUR AFFONSO DE BARROS MARINHO:70206376120
GRUPO IMAGETECH
2026.01.30 13:42:40-04'00'

IMAGETECH TECNOLOGIA EM INFORMÁTICA LTDA
Arthur Affonso de Barros Marinho

Testemunha 1. ROBERTA BARBETA DOS RIOS DE MATOS:84181478149 Assinado de forma digital por ROBERTA BARBETA DOS RIOS DE MATOS:84181478149 Dados: 2026.01.30 12:57:34 -04'00'

Testemunha 2. _____

gov.br Documento assinado digitalmente
LUIZA ABREU MEDEIROS
Data: 30/01/2026 14:04:50-0300
Verifique em https://validar.iti.gov.br

Protocolo de Assinatura(s)

O documento acima foi proposto para assinatura digital. Para verificar as assinaturas acesse o endereço http://df.tce.ms.gov.br/docflow/digitalSignChecker.jsf e utilize o código abaixo para verificar se este documento é válido.

Código de verificação: JSAJ-FSC1-VO0X-LMUH

O(s) nome(s) indicado(s) para assinatura, bem como seu(s) status em 30/01/2026 é(são) :

- FLÁVIO KAYATT - 30/01/2026 12:00:07 (Certificado Digital)

TRIBUNAL DE CONTAS
Estado de Mato Grosso do Sul

CONTRATO_005_2026_ASSINADO

Código do documento: AS4J-S5MU-K2TE-DU8Y

Autenticação Eletrônica

Valide em https://siga.tce.ms.gov.br/flowbee-pub/#/validar/AS4J-S5MU-K2TE-DU8Y
Ou digite o código: AS4J-S5MU-K2TE-DU8Y
Assinado em conformidade à Medida Provisória nº 2.200-2/2001 e Lei 14.063/2020.

TRIBUNAL DE CONTAS
Estado de Mato Grosso do Sul

PROCESSO TC-CP/1186/2024

TERMO DE REFERÊNCIA

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Contratação de serviços de segurança da informação com o objetivo de garantir a proteção eficaz da rede de computadores, assim como a segurança das estações de trabalho, servidores de arquivos e dispositivos móveis, por meio de soluções antimalware de última geração, além de serviços de suporte técnico qualificado do ambiente tecnológico do Tribunal de Contas do Estado de Mato Grosso do Sul (TCE/MS), conforme condições, quantidades, especificações e exigências estabelecidas neste instrumento.

TRIBUNAL DE CONTAS
Estado de Mato Grosso do Sul

Item	Descrição	Catser	Quant.	Unid.	Valor mensal	Valor Anual
1	Contratação de empresa especializada para fornecimento de solução de segurança da informação envolvendo hardware, software, assinaturas de atualização, instalação, treinamento, customização e suporte técnico qualificado em proteção e inspeção de tráfego em redes corporativas, conforme especificações técnicas, incluindo os appliances necessários e suficientes para a prestação destes serviços, com o objetivo de garantir a proteção eficaz da rede de computadores, assim como a segurança das estações de trabalho, servidores de arquivos e dispositivos móveis, por meio de soluções antimalware endpoint com detecção e resposta de última geração.	27014	12	Mês	R$ 1.078.377,50	R$ 12.940.530,00

1.2. O(s) serviço(s) objeto desta contratação são caracterizados como comuns, uma vez que os padrões de desempenho e qualidade podem ser objetivamente definidos.

1.3. A presente contratação será por 12 meses e por se tratar de serviços contínuos, o contrato pode ser celebrado respeitada a vigência máxima decenal, contados do(a) assinatura do contrato na forma do artigo 107 da Lei n° 14.133, de 2021.

1.4. O valor cobrado pelos serviços objetos deste termo de referência será reajustado após um ano, com data-base vinculada à data do orçamento estimado, por meio do competente termo aditivo, aplicando-se o índice de custos de tecnologia da informação (ICTI). Na ausência de atualização do ICTI, será utilizado o Índice de Preços ao Consumidor (IPCA).

2. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

2.1. Este termo de referência visa a locação de uma solução abrangente para segurança da informação na rede de computadores do Tribunal de Contas do Estado de Mato Grosso do Sul (TCE/MS), focando principalmente na implementação de um sistema de firewall robusto. A solução proposta deve garantir a proteção eficaz das estações de trabalho, servidores de arquivos e dispositivos móveis contra ameaças cibernéticas, incluindo, mas não se limitando a, malwares e ataques de ransomware.

2.2. A solução de segurança deverá incluir um firewall avançado que possibilite o controle de acesso e monitoramento contínuo do tráfego de rede, permitindo a identificação e neutralização de potenciais ameaças antes que possam causar danos. Além disso, a implementação de um software de antimalware (antivírus) será fundamental para a proteção em tempo real das máquinas e servidores, com atualizações frequentes para assegurar a detecção de novas ameaças.

2.3. A locação da solução deve contemplar também serviços de implantação, onde a equipe técnica do contratado será responsável pela instalação e configuração e manutenção dos sistemas de segurança cibernéticos, garantindo que todas as normas e políticas de segurança do TCE/MS sejam rigorosamente seguidas.

2.4. O suporte técnico deve estar disponível para resolver quaisquer incidentes ou problemas que possam surgir, garantindo a continuidade e eficácia da proteção. Ademais, a consultoria especializada será necessária para a atualização contínua das práticas de segurança e infraestrutura de rede de computadores, alinhando-as com as melhores práticas de mercado e adaptando-as às novas realidades das ameaças digitais conforme necessário.

2.5. Com esta solução, o TCE/MS busca não apenas atender às demandas de segurança da informação, mas também promover um ambiente digital seguro e confiável, assegurando a integridade e confidencialidade das informações tratadas em suas redes.

3. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

3.1. Este Termo de Referência foi elaborado em cumprimento ao disposto na Lei n. 14.133, de 1º de abril de 2021 e a Instrução Normativa SGD/ME n. 94, de 23 de dezembro de 2022.

3.2. A motivação para a presente contratação de soluções de Tecnologia da Informação e Comunicação (TIC) está enraizada na crescente complexidade e sofisticação das ameaças cibernéticas que permeiam o ambiente digital atual. No cenário em constante evolução das tecnologias, a segurança da informação se estabelece como um pilar fundamental para a manutenção da integridade, disponibilidade e confidencialidade das informações institucionais.

3.3. O Tribunal de Contas do Estado de Mato Grosso do Sul (TCE-MS) reconhece a necessidade de fortalecer suas defesas cibernéticas para preservar a confiança depositada em seus sistemas e assegurar o cumprimento de suas responsabilidades legais e institucionais. A crescente interconexão de dispositivos, a expansão das redes e a ampla utilização de tecnologias móveis tornam imperativo o investimento em soluções que possam antecipar, detectar e mitigar ameaças em tempo real.

3.4. A justificativa para a contratação de uma solução de segurança da informação reside na necessidade de uma abordagem integrada e especializada para proteger a infraestrutura de TIC do TCE-MS. A prevenção e resposta efetiva a incidentes cibernéticos são cruciais para evitar interrupções nas operações, vazamento de informações sensíveis e potenciais danos à imagem e reputação da instituição.

3.5. O contrato 002/2020 em execução segue os termos do art. 57, inc. IV, da Lei n.” 8.666/93, visto que todas as renovações previstas já foram realizadas, diante disso, se faz necessário um novo processo licitatório para a continuidade dos serviços, suportar demandas futuras de crescimento.

3.6. O objeto da contratação está previsto no Plano de Contratações Anual 2024, conforme consta das informações básicas do DFD nº 49/2024 anexo aos autos do processo.

3.7. Além disso, o escopo das ameaças cibernéticas evolui constantemente, exigindo uma abordagem proativa e atualizada para lidar com novas variantes de malware, ataques de engenharia social, vulnerabilidades de sistemas e outras ameaças emergentes. A contratação de uma empresa especializada em segurança da informação permitirá ao TCE-MS contar com um parceiro estratégico capaz de acompanhar a evolução das ameaças e fornecer medidas de proteção ágeis e eficazes.

3.8. A presente motivação encontra respaldo nas disposições da Instrução Normativa SLTI/MPOG nº 94/2022 e do Decreto nº 7.174/2010, que reforçam a importância de adotar soluções de TIC que sejam compatíveis com os padrões e práticas de segurança estabelecidos, garantindo a integridade das informações institucionais e o cumprimento das obrigações legais.

3.9. Dito isso, a motivação para a contratação da solução de segurança da informação reside na necessidade de enfrentar desafios cibernéticos em constante mutação, fortalecer a resiliência digital do TCE-MS e cumprir as exigências de segurança da informação, assegurando assim a continuidade de suas operações, a preservação dos dados e a confiança pública na instituição.

4. REQUISITOS DA CONTRATAÇÃO

4.1. Requisitos e necessidades técnicas

4.1.1. Todos os requisitos que envolvem Necessidade de Negócio, Necessidades Tecnológicas e demais Requisitos Necessários e Suficientes para a Escolha da Solução de TIC encontram-se devidamente detalhados no Estudo Técnico Preliminar (anexo). A fim de evitar redundância e duplicidade de informações, estes requisitos devem ser verificados especificamente nos capítulos 4, 5 e 6 do referido estudo, onde estão dispostos de maneira clara e detalhada.

4.1.2. Dessa forma, o presente documento se abstém de repetir tais informações, recomendando-se que qualquer consulta ou análise relacionada às necessidades de negócio, às especificações tecnológicas ou a outros requisitos relevantes seja feita diretamente nos capítulos indicados, onde constam todas as orientações necessárias para a adequada escolha e implementação da solução de TIC proposta.

4.2. Requisitos de Obrigação da Marca

4.2.1. A marca e identidade da CONTRATANTE não poderá ser utilizada, divulgada ou mesmo citada, sem autorização prévia da CONTRATANTE. Em caso de não cumprimento dos padrões e regras citadas acima, a CONTRATANTE poderá enviar notificações para correções, passível de multas contratuais.

4.3. Requisitos de Segurança da Informação e Privacidade

4.3.1. A CONTRATADA deverá observar integralmente os requisitos de Segurança da Informação e Privacidade da CONTRATANTE.

4.3.2. A CONTRATADA não poderá se utilizar da presente contratação para obter qualquer acesso não autorizado às informações do Tribunal de Contas do Estado de Mato Grosso do Sul.

4.3.3. A CONTRATADA não poderá veicular publicidade acerca do fornecimento a ser contratado, sem prévia autorização, por escrito, do TCE/MS.

4.3.4. A CONTRATADA é responsável civil, penal e administrava quanto à divulgação indevida ou não autorizada de informações, realizada por ela ou por seus empregados.

4.3.5. É de responsabilidade da CONTRATADA garantir que as informações por ela obtidas em decorrência da execução desta contratação sejam mantidas em sigilo, não podendo ser divulgadas, exceto se previamente acordado, por escrito, entre as partes CONTRATANTES.

4.3.6. É de responsabilidade da CONTRATADA garantir o tratamento de

4.3.7. dados pessoais de acordo com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14 de agosto de 2018) com objetivo específico de assegurar a proteção, privacidade e transparência de dados de pessoas físicas.

4.3.8. O Termo de Confidencialidade deverá ser assinado pelo representante legal da CONTRATADA e o Termo de Ciência pelos funcionários.

4.4. Requisitos de Sustentabilidade

4.4.1. A CONTRATADA deverá adotar práticas de sustentabilidade ambiental na execução do objeto, no que couber, conforme disposto na Instrução Normativa SLTI/MP nº 1/2010 e Decreto no 7.746/2012, da Casa Civil, da Presidência da República.

4.4.2. Os serviços prestados deverão pautar-se sempre no uso racional de recursos e equipamentos, de forma a evitar e prevenir o desperdício de insumos e material consumidos, bem como a geração excessiva de resíduos.

4.4.3. A CONTRATADA deverá instruir os seus colaboradores quanto à necessidade de racionalização de recursos no desempenho de suas atribuições, bem como das diretrizes de responsabilidade ambiental adotadas pelo Tribunal.

4.4.4. A licitante deverá apresentar Declaração de Sustentabilidade Ambiental, conforme modelo previsto no Edital de licitação, a ser apresentado na fase de aceitação da proposta.

4.5. Requisitos da Exigência de Carta de Solidariedade

4.5.1. Não se aplica

4.6. Requisitos de Subcontratação

4.6.1. Não é admitida a subcontratação do objeto contratual.

4.7. Requisitos de Confidencialidade das Informações

4.7.1. A CONTRATADA deverá manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse da CONTRATANTE ou de terceiros de que tomar conhecimento em razão da execução do contrato, respeitando todos os critérios estabelecidos aplicáveis aos dados, informações, regras de negócios, documentos, entre outros.

4.7.2. A CONTRATADA deverá manter sigilo absoluto sobre quaisquer dados, informações, códigos-fonte ou artefatos contidos em quaisquer documentos e em quaisquer mídias, incluindo meios de armazenamento e o que lhe for transferido por meio de canal de conectividade, de que venha a ter conhecimento durante a execução dos trabalhos de levantamento de requisitos, construção, implantação e execução dos serviços, não podendo, sob qualquer pretexto divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pela CONTRATANTE a tais documentos.

4.7.3. Toda informação confidencial gerada e/ou manipulada em razão desta contratação, seja ela armazenada em meio físico, magnético ou eletrônico, deverá ser devolvida nas seguintes hipóteses, mediante formalização entre as partes:

4.7.3.1. Término ou rompimento do Contrato; ou

4.7.3.2. Solicitação do Tribunal.

4.8. Requisitos de Vistoria Técnica

4.8.1. Os interessados em participar desta licitação poderão realizar uma vistoria no ambiente objeto deste Termo.

4.8.2. O Representante legal da licitante ou seu responsável técnico designado para este fim, deverá apresentar:

4.8.2.1. No caso de diretor, sócio ou proprietário da empresa licitante que comparecer ao local, deverá comprovar a representatividade por meio da apresentação de ato constitutivo, estatuto ou contrato social, do documento de eleição de seus administradores, devidamente registrados na Junta Comercial ou no cartório de pessoas jurídicas.

4.8.2.2. Tratando-se de procurador deverá apresentar instrumento público ou particular de procuração, com firma reconhecida em cartório, com poderes expressos, acompanhado do correspondente documento, dentre os indicados no subitem acima, que comprove os poderes do mandante para a outorga.

4.8.3. O Representante legal da licitante ou seu responsável técnico, deverá realizar visita técnica, onde será emitido atestado declarando que a empresa tomou conhecimento das particularidades inerentes a prestação dos serviços e recebeu todas as informações necessárias para o cumprimento integral das obrigações objeto da licitação, não cabendo qualquer discordância futura, seja de ordem física ou técnica.

4.8.4. A empresa que não realizar a vistoria deverá apresentar, no momento da habilitação, declaração de que possui conhecimento pleno das condições e peculiaridades da contratação, responsabilizando-se por quaisquer ônus.

4.8.5. Agendar previamente as visitas no endereço abaixo, onde receberão o Atestado de Visita:

Órgão: Tribunal de Contas de Mato Grosso do Sul;

Setor: Secretaria de Tecnologia da Informação;

Contato: Gerencia de Segurança e Infraestrutura da Informação;

Fone: (67) 3317-1616;

Localidade: Campo Grande, Estado de Mato Grosso do Sul;

Endereço: Avenida Desembargador José Nunes da Cunha, Jardim Veraneio, Parque dos Poderes, Bloco 29.

OBS.: O local indicado para a visita deverá ser vistoriado até o 1º (primeiro) dia útil que antecede o certame, para atendimento de Segunda a Sexta-feira, das 07:00 às 13:00 horas.

4.9. Requisito da Garantia da Execução

4.9.1. Estamos adotando um percentual de 10% como garantia, conforme estabelecido no artigo 98 da Lei 14.133/2021. Esta medida visa mitigar os riscos associados à execução da licitação, assegurando que o proponente tenha capacidade financeira e técnica para lidar com desafios técnicos complexos que possam surgir durante a implementação do contrato. Essa garantia não apenas protege os interesses da administração pública, garantindo a conclusão bem-sucedida da prestação dos serviços dentro dos parâmetros estabelecidos, mas também promove um ambiente competitivo, incentivando propostas que reflitam um planejamento sólido e uma execução eficiente.

4.10. Requisito de Garantia da Proposta

4.10.1. Em concordância com o art. 58 da Lei n. 14.133/2021, será exigida a garantia da proposta de 1% em razão da complexidade e urgência desta contratação. Este instrumento legal visa proteger os interesses públicos envolvidos, uma vez que mitiga os riscos do retardamento ou fracasso do certame, ocasionado, geralmente, por empresas que se quer possuem capacidade técnica e financeira para participar de licitações deste nível, servindo como eficiente sinalização de condição prévia de aptidão.

TRIBUNAL DE CONTAS
Estado de Mato Grosso do Sul

5. PAPÉIS E RESPONSABILIDADES

5.1. São obrigações da CONTRATANTE:

5.1.1. Nomear Gestor e Fiscais Técnico, Administrativo do contrato para acompanhar e fiscalizar a execução dos contratos;

5.1.2. Encaminhar formalmente a demanda por meio de Ordem de acordo com os critérios estabelecidos no Termo de Referência;

5.1.3. Receber a solução fornecida pelo contratado que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

5.1.4. Aplicar à CONTRATADA as sanções administrativas regulamentares e contratuais cabíveis, quando aplicável;

5.1.5. Liquidar o empenho e efetuar o pagamento à CONTRATADA, dentro dos prazos preestabelecidos em contrato;

5.1.6. Comunicar à CONTRATADA todas e quaisquer ocorrências relacionadas com o fornecimento da solução;

5.1.7. Exigir o afastamento e/ou substituição imediata de empregado que não mereça confiança no trato com os serviços prestados, que adote posturas inadequadas ou incompatíveis com o exercício das atribuições que lhe foram designadas;

5.1.8. Impedir que terceiros, que não seja a empresa CONTRATADA, efetuem os serviços prestados;

5.1.9. Rejeitar os serviços executados em desacordo com as obrigações assumidas pela empresa CONTRATADA, exigindo sua correção, no prazo máximo de 10 (dez) dias sob pena de suspensão do contrato, ressalvados os casos fortuitos ou de força maior desde que devidamente justificados e aceitos pela CONTRATANTE;

5.1.10. Prestar informações e esclarecimentos necessários e proporcionar condições – no que lhe couber – para que a CONTRATADA possa executar os serviços objeto do contrato;

5.1.11. Comunicar à CONTRATADA, com antecedência mínima de 30 (trinta) dias, as eventuais alterações que realizar na solução e nas suas normas, padrões, processos e procedimentos;

5.1.12. Cumprir e fazer cumprir o disposto nas cláusulas do contrato, devendo aplicar as penalidades previstas em lei pelo não-cumprimento das obrigações contratuais ou execução insatisfatória dos serviços;

5.1.13. Solicitar à CONTRATADA todas as providências necessárias ao bom andamento dos serviços;

5.1.14. Zelar para que, durante a vigência do Contrato, sejam mantidas todas as obrigações assumidas pela CONTRATADA, inclusive quanto às condições de habilitação e qualificação exigidas na licitação;

5.1.15. Não praticar atos de ingerência na administração da empresa CONTRATADA, tais como:

5.1.15.1. exercer o poder de mando sobre os empregados desta, devendo reportar-se somente aos prepostos por ela indicados;

5.1.15.2. promover ou aceitar o desvio de funções dos empregados, utilizando-os em atividades distintas daquelas previstas no contrato e na função específica para a qual foram contratados;

5.1.15.3. considerar os trabalhadores da CONTRATADA como colaboradores permanentes e/ou pertencentes a estrutura do Tribunal de Contas do Estado de Mato Grosso do Sul; e

5.1.15.4. exercer qualquer relação com a CONTRATADA que caracterize pessoalidade e subordinação direta.

5.2. São obrigações da Contratada

5.2.1. Indicar formalmente preposto apto a representá-la junto à CONTRATANTE, que deverá responder pela fiel execução do contrato;

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

5.2.3. 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 dos serviços pela CONTRATANTE;

5.2.4. 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;

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

5.2.6. Manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução;

5.2.7. Manter a produtividade ou a capacidade mínima de fornecimento da solução durante a execução do contrato;

5.2.8. Garantir que seus profissionais respeitem e sigam os padrões, processos e procedimentos estabelecidos pela CONTRATANTE para a prestação dos serviços, especialmente a Política de Segurança da Informação a ser informada e disponibilizada por ocasião da contratação, e estejam informados sobre eventuais modificações realizadas pela CONTRATANTE;

5.2.9. Manter sigilo sobre quaisquer informações do CONTRATANTE às quais, durante a vigência do contrato, venha a ter conhecimento ou acesso, devendo entregar a CONTRATANTE o Termo de Confidencialidade, assinado por seu representante legal, e pelos profissionais designados para a prestação de serviços;

5.2.10. Assegurar a transferência à CONTRATANTE, de conhecimentos adquiridos ou produzidos pelos seus profissionais, relativamente a serviços em andamento, nos termos que venham a ser por estes definidos, a fim de garantir a continuidade dos serviços;

5.2.11. Garantir a execução dos serviços sem interrupção, substituindo, caso necessário, sem ônus para a CONTRATANTE, qualquer profissional que estiver em gozo de férias, auxílio doença, auxílio maternidade ou qualquer outro benefício legal / regulamentar, por outro de mesma qualificação ou superior;

5.2.12. Arcar com todos os encargos sociais, trabalhistas, fiscais, comerciais e ambientais previstos na legislação vigente;

5.2.13. Prestar os esclarecimentos necessários ao CONTRATANTE, bem como informações concernentes à natureza e andamento dos serviços executados, ou em execução;

5.2.14. Garantir a integridade e disponibilidade dos documentos e informações que, em função do Contrato, estiverem sob a sua guarda, sob pena de responder por eventuais perdas e/ou danos;

5.2.15. Tratar todas as informações a que tenha acesso, em caráter de estrita confidencialidade, não podendo, sob qualquer pretexto, divulgar, revelar, reproduzir, ou deles dar conhecimento a terceiros estranhos a esta contratação, bem como utilizá-las para fins diferentes dos previstos na presente contratação;

5.2.16. Toda informação confidencial disponível em razão desta contratação, seja ela armazenada em meios físico, magnético ou eletrônico, deverá ser devolvida nas hipóteses de extinção ou rescisão do Contrato ou quando solicitado pela CONTRATANTE;

5.2.17. Manter o CONTRATANTE oficialmente informado sobre quaisquer necessidades de atualização ou mudança na configuração dos serviços prestados;

5.2.18. Substituir de imediato, qualquer profissional cuja conduta seja considerada inconveniente pelo CONTRATANTE e/ou se apresente incompetente para realização dos serviços;

5.2.19. Prestar os serviços dentro dos parâmetros e rotinas estabelecidos neste Termo de Referência;

5.2.20. Responsabilizar-se pelos danos causados diretamente à Administração, equipamentos, ou a terceiros, decorrentes de sua culpa ou dolo na execução dos serviços, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento pelo CONTRATANTE;

5.2.21. Comunicar o TCE/MS sobre qualquer falha no sistema de monitoramento;

5.2.22. Manter o SLA contratado nos serviços de manutenção com acionamento através da central de alarme;

5.2.23. No caso de falha do sistema de monitoramento deverá ser acionado uma equipe volante para verificar o estado do site;

5.2.24. A CONTRATADA, além das obrigações estabelecidas neste documento e em seus demais anexos, deve:

5.2.24.1. Executar os serviços conforme especificações deste Termo de Referência e de sua proposta, com a alocação dos empregados necessários ao perfeito cumprimento das cláusulas contratuais.

5.2.24.2. Manter, durante a vigência do contrato, as condições de habilitação exigidas na licitação, devendo comunicar à CONTRATANTE a superveniência de fato impeditivo da manutenção dessas condições;

5.2.24.3. Responder, nos prazos legais, em relação aos seus empregados, por todas as despesas decorrentes da execução do serviço e por outras correlatas, tais como salários, seguros de acidentes, indenizações, tributos, vale refeição, vale

transporte, uniformes, crachás e outras que porventura venham a ser criadas e exigidas pelo Poder Público;

5.2.24.4. Respeitar as normas e procedimentos de controle interno da CONTRATANTE, inclusive no que se referir ao acesso às dependências onde serão executados os serviços;

5.2.24.5. Responder pelos danos causados diretamente à Administração ou aos bens da CONTRATANTE, ou ainda a terceiros, decorrentes de sua culpa ou dolo, durante a execução deste contrato;

5.2.24.6. Comunicar à Administração da CONTRATANTE qualquer anormalidade constatada e prestar os esclarecimentos solicitados;

5.2.24.7. Fiscalizar regularmente os seus empregados designados para a prestação do serviço, com o intento de verificar as condições em que o serviço está sendo prestado;

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

5.2.24.9. Refazer os serviços que, a juízo do representante da CONTRATANTE, não forem considerados satisfatórios, sem que caiba qualquer acréscimo no preço contratado;

5.2.24.10. Manter seus empregados sob as normas disciplinares da CONTRATANTE, substituindo, no prazo máximo de 24 (vinte e quatro) horas após notificação, qualquer que seja considerado inconveniente pelo representante da CONTRATANTE;

5.2.24.11. Recrutar, selecionar e encaminhar à CONTRATANTE os empregados necessários à realização dos serviços, de acordo com a qualificação mínima exigida;

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

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

5.2.24.14. Treinar e capacitar periodicamente seus empregados no atendimento das Normas Internas e de Segurança e Medicina do Trabalho, bem como prevenção de incêndio, práticas de redução do consumo de água, energia e redução da geração de resíduos para implementação das lições aprendidas durante a prestação dos serviços.

5.2.24.15. Manter os seus empregados devidamente identificados por crachá;

5.2.24.16. Cuidar para que o preposto indicado mantenha permanente contato com a fiscalização do contrato, adotando as providências requeridas relativas à execução dos serviços pelos empregados;

5.2.24.17. Coordenar e controlar a execução dos serviços contratados;

5.2.24.18. Administrar todo e qualquer assunto relativo aos seus empregados;

5.2.24.19. Assumir todas as responsabilidades e tomar as medidas necessárias ao atendimento dos seus empregados acidentados ou acometidos de mal súbito, por meio do preposto;

5.2.24.20. Cuidar da disciplina e da apresentação pessoal dos seus empregados;

5.2.24.21. Solicitar à Administração da CONTRATANTE autorização formal para retirada de quaisquer equipamentos, pertencentes à CONTRATADA, que esta tenha levado para o local de execução do serviço;

5.2.24.22. Responsabilizar-se pelo transporte do seu pessoal até as dependências da CONTRATANTE, por meio próprio ou mediante vale transporte, inclusive em casos de paralisação dos transportes coletivos, bem como nas situações em que se faça necessária a execução dos serviços em regime extraordinário, para assegurar a continuidade normal dos serviços;

5.2.24.23. Manter sede, filial ou escritório na cidade de Campo Grande/MS, onde serão prestados os serviços com capacidade operacional para receber e solucionar qualquer demanda da Administração, bem como realizar todos os procedimentos pertinentes à seleção, treinamento, admissão e demissão dos empregados;

5.2.24.24. A CONTRATADA deverá comprovar, no prazo de 60 (sessenta) dias a contar do início da prestação dos serviços, o cumprimento desta obrigação.

5.2.24.25. A CONTRATADA é responsável pela qualificação técnica de seus profissionais que lhe representam na prestação do serviço, devendo programar treinamentos e reciclagem dos profissionais sempre que perceber tal necessidade, às suas expensas, atualizando o TCE/MS das medidas tomadas.

5.2.24.26. Responsabilizar-se por todos os encargos de possível demanda trabalhista, civil ou penal, relacionada à execução deste contrato, originariamente ou vinculada por prevenção, conexão ou continência;

5.2.24.27. Responsabilizar-se por todos os encargos fiscais e comerciais resultantes desta contratação;

5.2.24.28. A inadimplência da CONTRATADA, com referência aos encargos supracitados, não transfere a responsabilidade por seu pagamento à Administração da CONTRATANTE, nem pode onerar o objeto deste contrato.

5.2.24.29. Notificar a CONTRATADA por escrito da ocorrência de eventuais imperfeições, falhas ou irregularidades constatadas no curso da execução dos serviços, fixando prazo para a sua correção, certificando-se de que as soluções por ela propostas sejam as mais adequadas.

6. MODELO DE EXECUÇÃO DO CONTRATO

6.1. Condições de execução:

6.1.1. A prestação de serviços será contratada por 12 (doze) meses e por se tratar de serviços contínuos, respeitada a vigência máxima decenal, contados do(a) assinatura do contrato na forma do artigo 107 da Lei n° 14.133, de 2021.

6.1.2. O prazo para término da implantação de todos os equipamentos e início da execução dos serviços escopo do objeto deste Termo de Referência deverá ser de até 30 (trinta) dias corridos contados da assinatura do contrato.

6.2. Local e horário da prestação dos serviços:

6.2.1. O local da execução dos serviços será no Tribunal de Contas do Estado de Mato Grosso do Sul, situado na Av. Desembargador José Nunes da Cunha, s/n, Parque dos Poderes - Bloco 29, Campo Grande/MS, CEP 79037-802, Brasil.

6.2.2. O objeto desse termo, deve ser prestado 24x7 365 dias, durante todo prazo em que o contrato esteja vigente.

6.3. Especificação detalhada dos Serviços:

6.3.1. Requisitos do Negócio:

6.3.1.1. Com o provimento da solução, a área requisitante da solução visa a atender a necessidade de atender às demandas crescentes por segurança da informação no Tribunal de Contas do Estado de Mato Grosso do Sul (TCE-MS), no âmbito da Tecnologia da Informação e Comunicação (TIC).

6.3.1.2. A definição de "Solução de Tecnologia da Informação" conforme o inciso VII, art. 2º da Instrução Normativa SLTI/MPOG nº 94/2022, estabelece que se trata de um conjunto integrado de bens e serviços de TI e automação, que se unem para atingir os resultados almejados pela contratação. Neste contexto, a contratação proposta engloba uma solução de softwares e serviços especializados, que inclui não apenas a disponibilização de ferramentas de segurança, mas também a transferência de conhecimento e assistência técnica especializada.

6.3.1.3. A presente contratação é caracterizada como uma solução de TIC, pois agrega elementos diversos, tais como hardware, software e serviços técnicos, de forma a estabelecer uma infraestrutura computacional coesa e abrangente. Isso se alinha com as diretrizes de busca por soluções completas e integradas, garantindo a eficácia das medidas de segurança da informação para a rede de computadores do TCE-MS, bem como a proteção das estações de trabalho, servidores de arquivos e dispositivos móveis.

6.3.1.4. O ambiente de TIC do TCE-MS requer uma modernização significativa das suas medidas de segurança. A solução contratada deve oferecer uma abordagem de segurança proativa e em tempo real, capaz de identificar e mitigar ameaças cibernéticas, ataques maliciosos e vulnerabilidades de sistemas. A modernização abrange desde a detecção precoce até a resposta imediata a incidentes, garantindo assim a proteção contínua dos ativos de informação do Tribunal.

6.3.1.5. Além das demandas de segurança, a empresa contratada deverá também ser responsável por quaisquer modificações realizadas no ambiente de cabeamento estruturado, garantindo que essas alterações não comprometam a integridade e o funcionamento dos sistemas existentes e a conectividade com os equipamentos implantados. Isso inclui, mas não se limita a:

6.3.1.5.1. Qualquer instalação ou substituição de cabos deve ser realizada de acordo com as normas técnicas pertinentes, assegurando que os novos cabos sejam compatíveis com a infraestrutura já existente.

6.3.1.5.2. A contratada será responsável por garantir a correta conectividade dos novos cabos com os equipamentos implantados, assegurando que todas as conexões sejam feitas de maneira adequada e segura, evitando problemas de performance e funcionamento.

6.3.1.5.3. As alterações devem ser realizadas de forma a não comprometer a integridade do cabeamento estruturado, bem como a continuidade das operações dos serviços já instalados.

6.3.1.5.4. A contratada deverá manter documentação atualizada de todas as modificações realizadas, facilitando futuras

manutenções e consultas sobre a infraestrutura de cabeamento.

6.3.1.6. A contratada reconhece sua responsabilidade por qualquer impacto decorrente das alterações mencionadas, isentando a contratante de qualquer responsabilidade por problemas que possam surgir devido a intervenções no ambiente de cabeamento estruturado.

6.3.1.7. A concentração dessas tarefas em um único fornecedor garante uma alta coesão e integração entre as diversas etapas do projeto, evitando problemas de compatibilidade técnica e dificuldades de comunicação entre fornecedores distintos. Isso é essencial para a manutenção da qualidade e continuidade das operações de TIC, uma vez que qualquer falha ou atraso nas instalações de rede pode comprometer a segurança e o desempenho dos sistemas. A empresa, portanto, deve assegurar tanto a proteção em tempo real dos ativos digitais quanto a confiabilidade da infraestrutura de rede (cabeamento estruturado) do Tribunal.

6.3.2. Requisitos Gerais da Solução

6.3.2.1. Os requisitos mínimos exigidos neste subitem são justificados pelas necessidades de: a) contratar uma solução específica de mercado, com tecnologia construída para os fins a que se destinam, através de um processo de engenharia de qualidade, e não um produto adaptado em cima de um hardware ou software genérico, sem garantia de desempenho ou da qualidade de seus componentes; e b) garantir que o produto ofertado tenha as funcionalidades mínimas necessárias para qualquer hardware desta finalidade e que possam ser configurados de acordo com a especificidade da

rede de dados corporativa do Tribunal de Contas do Estado de Mato Grosso do Sul, independentemente de mudanças futuras na topologia da rede;

6.3.2.2. A solução deve ser baseada em equipamentos do tipo appliance;

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

6.3.2.4. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, prevenção de ataques zero-day, filtro de URL, identificação de usuários e controle granular de permissões.

6.3.2.5. Para proteção do ambiente contra ataques, o dispositivo de proteção deve possuir módulos de IPS, Antivírus e Anti-Spyware (para bloqueio de arquivos maliciosos), integrados ao próprio appliance de NGFW.

6.3.2.6. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7.

6.3.2.7. Define-se o termo “appliance” como sendo um equipamento dotado de processamento, memória e outros recursos tecnológicos exclusivos para um determinado serviço. Um appliance é projetado para executar uma tarefa específica de forma eficiente e simplificada, com recursos e software otimizados para essa finalidade.

6.3.2.8. Não serão aceitas soluções baseadas em PC's (personal computers) de uso geral, assim como, soluções de “appliance” que utilizam hardware e software de fabricantes diferentes.

6.3.2.9. Deve ser capaz de atualizar de forma automática o Firmware, patches e atualizações de segurança.

6.3.2.10. A solução deve permitir o uso de armazenamento externo para System Logs, Threat Logs, AppFlow reporting data e

Packet Captures, garantindo persistência de dados após reinicializações do firewall

6.3.2.11. O painel deve exibir detalhes sobre o último contato do Firewall com o gerenciador de licenciamento, mostrando o status de atualização de licenças e atualizações de assinaturas

6.3.2.12. Deve fornece APIs para que os fornecedores externos de NAC possam transmitir o contexto de segurança aos firewalls e que esta funcionalidade seja compatível com a utilização simultânea de fornecedores externos distintos.

6.3.2.13. Deverá ser fornecido 01 (um) clusters de equipamentos, formado por appliances com no mínimo 02 (dois) nodes no cluster, para implementação na proteção de perímetro;

6.3.2.14. Deverá ser fornecido 01 (um) clusters de equipamentos, formado por appliances com no mínimo 02 (dois) nodes no cluster, para implementação de balanceamento de carga e na proteção de aplicações;

6.3.2.15. Deverá ser fornecido solução para proteção de endpoints com funcionalidades EDR e MDR com no mínimo 1.000 (mil) licenças para utilização em microcomputadores com finalidade de uso para estações de trabalho, equipamentos servidores de rede, que ficam instalados no Data Center do órgão e dispositivos móveis utilizados no ambiente de rede do TCE-MS.

6.3.2.16. Todos os produtos de hardware componentes da solução deverão ser homologados e certificados pela ANATEL, conforme preceitua o art. 19, incisos XIII e XIV, e art. 156 da Lei n. 9.472, de 16 de julho de 1997 e ainda pelos art. 55, art. 64, inciso II e art. 67, parágrafo 2° da Resolução ANATEL n. 715, de 23 de outubro de 2019.

6.3.2.17. A Resolução ANATEL nº 715 é um regulamento que estabelece as regras e os procedimentos gerais relativos à

certificação e à homologação de produtos para telecomunicação, incluindo a avaliação da conformidade dos produtos para telecomunicação em relação à regulamentação técnica emitida ou adotada pela Anatel e os requisitos para a homologação de produtos para telecomunicação previstos no regulamento. Desta forma, velando-se pela legalidade, o Tribunal não poderia admitir a contratação de empresa que utilizaria uma solução que envolve características de tráfego em redes corporativas de comunicação de dados, que não atenda às exigências da ANATEL, o que poderia representar um prejuízo à execução do futuro contrato que certamente estaria sujeito à sustação com o advento de qualquer atividade fiscalizadora da agência de regulação.

6.3.3. Requisitos de Capacidade e de Interfaces de cada appliances para implementação na proteção de perímetro

6.3.3.1. Os requisitos mínimos exigidos neste subitem são justificados pela necessidade de garantir que a solução ofertada possua: a) capacidade de operação redundante (energia e refrigeração) provendo resiliência e tolerância à falhas; b) processamento, largura de banda e taxa de transferência suficiente para suportar o alto volume de dados trafegados na rede do Tribunal de Contas pelos diversos sistemas e softwares utilizados; e c) a quantidade de interfaces de rede necessárias para suportar toda a arquitetura do ambiente funcional da rede no núcleo do Tribunal, permitindo o devido gerenciamento, monitoramento e operação da solução sem necessidade de adaptações ou equipamentos sobressalentes;

6.3.3.2. Capacidade de inspeção de firewall superior a 30Gbps ou superior;

6.3.3.3. Desempenho em modo Threat Prevention (Proteção Anti-Malware, IPS e Controle de Aplicação habilitados) mínimo de 18 Gbps ou superior.

6.3.3.4. Desempenho em modo de Inspeção (decriptografia e criptografia) de tráfego criptografado (SSL/TLS) mínimo de 08 Gbps. Os desempenhos solicitados devem ser comprovados por documento de domínio público do fabricante. Não serão aceitas declarações ou cartas de fabricantes para atendimento deste item.

6.3.3.5. Desempenho mínimo de 19 Gbps de IPS.

6.3.3.6. Suporte mínimo de 7.500.000 conexões simultâneas/concorrentes no modo SPI.

6.3.3.7. Suporte mínimo de 225.000 novas conexões por segundo.

6.3.3.8. Deve possuir armazenamento interno de no mínimo 256 GB do tipo M.2 e suportar expansão de armazenamento interno para até 1TB.

6.3.3.9. Deve possuir fonte de alimentação HotSwap com chaveamento automático de 100-240 VAC.

6.3.3.10. Deve (ser capaz de suportar a inserção de/possuir) uma fonte de alimentação "HotSwap" com chaveamento automático de 100-240 VAC redundante

6.3.3.11. Deve possuir 02 interfaces de 40GbE QSFP+, acompanhado de 02 módulos 40GBASE-SR4 QSFP+ 850nm, homologados pelo fabricante do equipamento;

6.3.3.12. Deve possuir pelo menos 08 interfaces de 25GbE SFP28, acompanhado de 08 módulos 25GBASE-SR SFP28 850nm, homologados pelo fabricante do equipamento;

6.3.3.13. Deve possuir pelo menos 04 interfaces de 10GbE padrão SFP+, acompanhado de 04 módulos 10GB-SR SFP+ homologados pelo fabricante do equipamento;

6.3.3.14. Deve possuir pelo menos 04 interfaces de 10GbE padrão RJ-45.

6.3.3.15. Deve possuir pelo menos 16 interfaces de 1GbE padrão RJ-45.

6.3.3.16. Deve possuir pelo menos 01 interface do tipo 1 GbE RJ-45 dedicada para gerenciamento do equipamento.

6.3.3.17. Deve possuir pelo menos 2 interface USB 3.0 com suporte a tecnologias LTE 3G/4G e 5G.

6.3.3.18. A VPN Client-to-Site IPsec deve ser licenciada para, no mínimo, 1500 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 5000 usuários simultâneos.

6.3.3.19. A VPN SSL deve ser licenciada para, no mínimo, 500 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 1200 usuários simultâneos.

6.3.3.20. Deve suportar pelo menos 5.500 túneis de VPN tipo Site-to-Site padrão IPSEC simultâneos.

6.3.3.21. Deve suportar, no mínimo, 18.5 Gbps de desempenho de VPN IPSEC.

6.3.3.22. Os desempenhos apontados devem ser comprovados por documento de domínio público do fabricante. A ausência de tais documentos comprobatórios reservará ao órgão o direito de aferir a performance dos equipamentos em bancada, assim como atendimento de todas as funcionalidades especificadas neste edital. Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, o fornecedor será considerado inabilitados. Todos os custos oriundos do teste de bancada serão custeados pelo fornecedor/vendedor do certame.

6.3.3.23. O fornecimento dos produtos e seus licenciamentos devem ser entregues através de empresa credenciada e autorizada pelo fabricante. Isto deve ser comprovado através de carta de reconhecimento assinada pelo representante legal do fabricante no Brasil.

6.3.3.24. O Equipamento deverá ser homologado pela ANATEL.

6.3.3.25. Não serão aceitas cartas ou declarações de fabricantes para atendimento aos valores de desempenho solicitados.

6.3.3.26. O licenciamento para todos os serviços de Next Generation Firewall deverá permanecer válido durante toda a vigência do contrato.

6.3.3.27. A garantia do hardware deverá ser permanente durante toda a vigência do contrato.

6.3.4. Requisitos de Firewall e SD-WAN para proteção de perímetro

6.3.4.1. Deve implementar controle do tráfego para os protocolos TCP, UDP, ICMP, e serviços como FTP, DNS, P2P entre outros, baseados nos endereços de origem e destino.

6.3.4.2. Implementar recurso de NAT (network address translation) tipo one-to-one, one-to-many, many-to-many, many-to-one, porta TCP de conexão (NAPT) e NAT Traversal em VPN IPSec (NAT-T) e NAT dentro do tunel IPSec.

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

6.3.4.4. Deve possuir proteção anti-spoofing.

6.3.4.5. Suportar protocolos de roteamento RIP, RIPng, OSPF, OSPFv3 e BGP;

6.3.4.6. Suportar Equal Cost Multi-Path (ECMP) no mínimo para roteamento estático e protocolo OSPF.

6.3.4.7. Suporte a Policy-Based Routing (PBR), com a capacidade de roteamento no mínimo, mas não limitado a endereço de origem, endereço de destino, serviço e aplicação.

6.3.4.8. A solução deverá possuir a tecnologia SD-WAN (Software Defined WAN), e que a mesma seja nativa da solução, sem a necessidade de qualquer tipo de licenciamento complementar, para evitar indisponibilidade no ambiente mesmo em caso de expiração do licenciamento vigente.

6.3.4.9. Capacidade de agregar no mínimo 4 (quatro) circuitos WAN distintos em um único canal lógico onde seja possível criar controles de caminho automático baseado em políticas, com habilidade de selecionar o melhor caminho, no mínimo, através dos seguintes parâmetros simultâneos:

6.3.4.9.1. Latência;

6.3.4.9.2. Jitter;

6.3.4.9.3. Perda de pacotes.

6.3.4.10. O administrador da solução deverá ter a capacidade de configurar o canal lógico de SD-WAN para encaminhar tráfego simultaneamente por todos os links pertencentes a esse canal logico.

6.3.4.11. A comutação do SD-WAN deve ocorrer de maneira dinâmica e automática baseada nas políticas previamente aplicadas.

6.3.4.12. A solução de SD-WAN deve permitir encaminhamento de trafego com base em assinaturas de aplicações conhecidas (DPI), como Office 365, Facebook e Youtube, bem como aplicações associadas como Facebook Messenger e Office 365 Outlook.

6.3.4.13. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede.

6.3.4.14. Deve suportar modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas.

6.3.4.15. Implementar proxy transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das máquinas clientes.

6.3.4.16. Possuir servidor de DHCP (Dynamic Host Configuration Protocol) interno com capacidade de alocação de endereçamento IP para as estações conectadas às interfaces do firewall e via VPN.

6.3.4.17. Deve suportar DHCP relay.

6.3.4.18. Possibilitar a aplicação de regras de firewall e IPS por IP e grupo de usuários, permitindo a definição de regras para determinado horário ou período (dia da semana e hora) com matriz de horários que possibilite o bloqueio de serviços em horários específicos, tendo o início e fim das conexões vinculadas a essa matriz de horários.

6.3.4.19. Deve permitir a utilização de regras de Antivírus, Anti-Spyware, IPS e filtro de conteúdo web por segmentos de rede. Todos os serviços devem ser suportados no mesmo segmento de rede, interface (física e virtual) ou zona de segurança.

6.3.4.20. Possuir capacidade de inspecionar e bloquear em tempo real aplicativos e transferências de arquivos de softwares p2p (peer-to-peer) incluindo, no mínimo, Kazaa, Limewire, Morpheus e Napster e de comunicadores instantâneos (Instant Messenger) incluindo, no mínimo, ICQ, WhatsApp, Google Talk, Skype e IRC, para usuários da rede, individualmente ou em grupo.

6.3.4.21. Deve ter suporte à proteção e identificação de hosts possivelmente infectados com “botnets”. A solução ofertada deve permitir ao administrador a possibilidade de apenas

registrar e identificar as máquinas possivelmente contaminadas, além de ter a possibilidade de habilitar e analisar todas as conexões que passam por este dispositivo de segurança, bem como ativar tal funcionalidade especificando análise por regra de firewall, permitindo assim maior granularidade da gestão e do recurso.

6.3.4.22. Possuir assinaturas específicas, ou implementar mecanismo interno no appliance, para mitigação de ataques DoS (denial-of-service) e DDoS devidamente licenciados.

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

6.3.4.24. Detectar e bloquear a origem de portscans.

6.3.4.25. Deve permitir o bloqueio de ataques.

6.3.4.26. Deve permitir o bloqueio de exploits conhecidos.

6.3.4.27. O gateway Anti-Vírus deve suportar a análise de pelo menos os protocolos HTTP, FTP, IMAP e SMTP.

6.3.4.28. Deve ter a capacidade de analisar tráfegos criptografados HTTPS/SSL, que deverá ser descriptografado de forma transparente à aplicação.

6.3.4.29. Implementar DSCP (Differentiated Services Code Points).

6.3.4.30. Possuir mecanismo de forma a possibilitar o funcionamento transparente dos protocolos FTP, SIP, RTP, RTSP e H323, mesmo quando acessados por máquinas através de conversão de endereços. Este suporte deve funcionar tanto para acessos de dentro para fora quanto de fora para dentro da rede.

6.3.4.31. Implementar controle e gerenciamento de banda para a tecnologia VoIP(Voice OverIP) sobre diferentes segmentos de rede com inspeção profunda de segurança sobre este serviço.

6.3.4.32. Implementar mecanismo de sincronismo de horário através do protocolo NTP.

6.3.4.33. Possuir suporte ao protocolo SNMP versões 2 e 3.

6.3.4.34. Possuir suporte a log via Syslog.

6.3.4.35. Possuir suporte aos protocolos de roteamento RIP, OSPF e BGP. As configurações de RIP e OSPF devem ser configuradas através da interface gráfica.

6.3.4.36. O fabricante ou o produto deve possuir certificado ICSA (International Computer Security Association) para FIREWALL, ou CC (Common Criteria). Será aceito certificado equivalente ao ICSA, emitido por órgãos nacionais com competência para tal, desde que nos moldes deste, ou seja, certificado baseado na versão ou release atual do firewall, com manutenção recorrente deste certificado a cada mudança de versão, ou após determinado período de tempo, e baseado em normas nacionais e internacionais de segurança da informação.

6.3.4.37. Visando estabelecer efetividade de segurança dos firewalls de nova geração e assegurar que o fornecedor tenha uma solução já testada e comprovada por um órgão independente de mercado, o fabricante da solução deverá ser avaliado e certificado pelo NetSecOPEN, além de ser avaliado e citado pelo Gartner MQ (Magic Quadrant for Network Firewalls) nos relatórios de 2019 ou mais recentes.

6.3.4.38. Reconhecer aplicações como, no mínimo, peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos e e-mail.

6.3.4.39. Para tráfego criptografado SSL/TLS, deve de-criptografar pacotes possibilitando a leitura de payload dos pacotes para checagem de assinaturas de aplicações conhecidas pelo fabricante.

6.3.4.40. Controle, inspeção e de-criptografia de SSL/TLS por política para tráfego de entrada (Inbound) ou Saída (Outbound) com suporte a no mínimo, SSLv23, SSLv3, TLS 1.0, TLS 1.1, TLS 1.2 e TLS 1.3

6.3.4.41. Deve permitir a funcionalidade de ARP bridging

6.3.4.42. Deve permitir a configuração de limite na taxa de envio ARP para um mesmo IP, para evitar "ARP Storm"

6.3.4.43. A solução deve permitir a visualização gráfica das regras de segurança e acesso.

6.3.5. Requisitos de VPN (Virtual Private Network) para proteção de perímetro

6.3.5.1. Os requisitos mínimos exigidos neste subitem são justificados pela necessidade que a solução proporcione recursos de VPN, para interconexão das diversas localidades atendidas de maneira segura, provendo criptografia e sigilosidade no tráfego de dados entre o Datacenter do Tribunal e outras instituições como bancos, Órgãos do Governo Estadual, Governo Federal e Serpro, através de tecnologia usual de mercado e não proprietária;

6.3.5.2. Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo site-to-site, com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC.

6.3.5.3. Suportar algoritmos de criptografia 3DES, AES 128, AES 256 e AESGCM16-256

6.3.5.4. Suportar algoritmos Hash no mínimo SHA-1, SHA-256 e SHA-384.

6.3.5.5. Diffie-Hellman: Grupo 2 (1024 bits), Grupo 5 (1536 bits) e Grupo 14 (2048 bits.

6.3.5.6. Deverá suportar algoritmo Internet Key Exchange (IKE)v1 e v2.

6.3.5.7. Autenticação via de tuneis IPSec via certificado digital para VPNs Site-to-Site e Client-to-Site.

6.3.5.8. A solução deve suportar VPNs L2TP, incluindo suporte para Apple iOS e Android.

6.3.5.9. Solução deve suportar VPNs baseadas em políticas, e VPNs baseadas em roteamento estático e/ou dinâmico.

6.3.5.10. Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo Site-to-Site com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC.

6.3.5.11. Solução deve incluir a capacidade de estabelecer VPNs com outros firewalls que utilizam IP públicos dinâmicos.

6.3.5.12. Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do circuito primário.

6.3.5.13. Permitir criação de políticas de roteamento estático utilizando IPs de origem, destino, serviços e a própria VPN como parte encaminhadora deste tráfego, sendo este visto pela regra de roteamento como uma interface simples de rede para encaminhamento do tráfego.

6.3.5.14. Suportar a criação de túneis IP sobre IP (IPSEC Tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet.

6.3.5.15. Implementar os esquemas de troca de chaves manual, IKE e IKEv2 por Pré-Shared Key, certificados digitais e XAUTH client authentication.

6.3.5.16. Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do primário.

6.3.5.17. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

6.3.6. Requisitos de Alta Disponibilidade para proteção de perímetro

6.3.6.1. Os requisitos mínimos exigidos neste subitem são justificados pela necessidade de garantia da disponibilidade da solução em caso de queda de um dos equipamentos instalados no Datacenter do Tribunal, ou seja, a solução deve automaticamente se manter operacional na ocorrência de qualquer evento que ocasione a parada de um dos itens da solução;

6.3.6.2. Devem ser fornecidos 02 (dois) appliances de NGFW com gerenciamento unificado, novos e sem uso anterior, funcionando em alta disponibilidade. O modelo ofertado deverá estar em linha de produção, sem previsão de encerramento de fabricação, na data de entrega da proposta. O software deverá ser fornecido em sua versão mais atualizada.

6.3.6.3. A solução deve ser entregue operando em alta disponibilidade no modo Ativo/Passivo, com as implementações de Failover.

6.3.6.4. Não serão permitidas soluções de cluster (HA) que façam com que os equipamentos se reiniciem após qualquer modificação de parâmetro/configuração realizada pelo administrador.

6.3.6.5. A solução deve ter capacidade de fazer monitoramento físico das interfaces dos membros do cluster.

6.3.6.6. A solução deve operar em alta disponibilidade implementando monitoramento lógico de um host na rede, e possibilitar failover.

6.3.6.7. A solução deve permitir o uso de endereço MAC virtual para evitar problemas de expiração de tabela ARP em caso de Failover.

6.3.6.8. A solução deve possibilitar a sincronização de todas as configurações realizadas na caixa principal do cluster incluído, mas não limitado a objetos, regras, rotas, VPNs e políticas de segurança.

6.3.6.9. A solução deve permitir visualizar no equipamento principal, o status da comunicação entre os parceiros do cluster, status de sincronização das configurações, status atual do equipamento redundante.

6.3.6.10. A solução de HA deve permitir que o dispositivo primário trate todo o tráfego, mantendo o dispositivo secundário atualizado em tempo real sobre as informações de conexão de rede, garantindo uma transição transparente para o dispositivo secundário em caso de failover, sem que haja perda das conexões de VPN, FTP, Oracle SQL*NET, RSTP, Real Audio, VPN Client, Dynamic Arp Objects, Informações de DHCP Server, Multicast, IGMP, Usuários ativos, RIP e OSPF.

6.3.7. Requisitos de Controle de Ameaças

6.3.7.1. Os requisitos mínimos exigidos neste subitem são justificados pela necessidade de proteger o ambiente de rede deste Tribunal de ataques dos tipos “vírus” e “botnets”, que podem acarretar na perda de informação crítica, roubo de dados sigilosos, degradação de serviços ou interrupção de funcionamento de sistemas de informações e equipamentos essenciais para continuidade dos serviços públicos prestados, e constituem especificações usuais e padrão de mercado para tecnologias com esta finalidade;

6.3.7.2. Para as ameaças de dia-zero, a solução deve ter a habilidade de prevenir o ataque antes de qualquer assinatura ser criada. Deve possuir módulo de Anti-Vírus e Anti-Bot integrado ao próprio appliance de segurança.

6.3.7.3. A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliances através de assinaturas.

6.3.7.4. Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego.

6.3.7.5. Implementar funcionalidade de detecção e bloqueio de “call-backs”.

6.3.7.6. A solução deverá ser capaz de detectar e bloquear comportamento suspeito ou anormal da rede.

6.3.7.7. A solução Anti-bot deve possuir mecanismo de detecção que inclua reputação de endereço IP.

6.3.7.8. Implementar interface gráfica WEB segura, utilizando o protocolo HTTPS.

6.3.7.9. Implementar interface CLI segura através do protocolo SSH.

6.3.7.10. Possuir Anti-Vírus em tempo real, para ambiente de gateway internet integrado à plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, IMAP, POP3, FTP, CIFS e TCP Stream.

6.3.7.11. A solução deve permitir criar regras de exceção de acordo com a proteção.

6.3.7.12. Deve possuir visualização na própria interface de gerenciamento referente aos top incidentes através de hosts, ou incidentes referentes a vírus e Bots;

6.3.7.13. Permitir o bloqueio de malwares (vírus, worms, spyware e etc).

6.3.7.14. A solução deve ser capaz de proteger contra ataques a DNS.

6.3.7.15. A solução deverá ser gerenciada a partir de uma console centralizada com políticas granulares.

6.3.7.16. A solução deve ser capaz de prevenir acesso a websites maliciosos.

6.3.7.17. A solução deve ser capaz de realizar inspeção de tráfego SSL/TLS e SSH.

6.3.7.18. A solução deverá receber atualizações de um serviço baseado em cloud.

6.3.7.19. A solução deverá ser capaz de bloquear a entrada de arquivos maliciosos.

6.3.7.20. A solução Anti-Vírus deverá suportar análise de arquivos que trafegam dentro do protocolo CIFS.

6.3.7.21. A solução deve suportar funcionalidade de Geo-IP, ou seja, a capacidade de identificar, isolar e controlar tráfego baseado na localização (origem e/ou destino), incluindo a capacidade de configuração de listas customizadas para esta mesma finalidade

6.3.7.22. A solução de segurança deverá ter mecanismos de proteção de ameaças em tempo real pela análise de instruções e do uso da memória, sendo eficientes frente ameaças exploradas por vulnerabilidades do tipo meltdown.

6.3.7.23. A solução de Gateway Anti-Virus deverá ter a tecnologia complementar de Anti Virus-Cloud, para que os mecanismos existentes de verificação sejam ampliados.

6.3.7.24. A solução deve ser capaz de bloquear proativamente o acesso a domínios maliciosos conhecidos por meio de filtragem

DNS, reduzindo assim o risco de infecções por malware e outros ataques cibernéticos.

6.3.8. Requisitos de Proteção Contra Ataques Avançados

6.3.8.1. Os requisitos mínimos exigidos neste subitem são justificados pela necessidade de proteger o ambiente de rede corporativa de ataques dos tipos “APT Malware”, “ameaças de dia zero” e “ameaças não conhecidas”, através da inspeção avançada de tráfego, inclusive criptografado, detectando anomalias e comportamentos suspeitos de aplicações, e que também podem acarretar na perda de informação crítica, roubo de dados sigilosos, degradação de serviços ou interrupção de funcionamento de sistemas de informações e equipamentos essenciais para continuidade dos serviços públicos prestados, e constituem especificações usuais e padrão de mercado para tecnologias com esta finalidade;

6.3.8.2. A solução deverá prover as funcionalidades de inspeção de tráfego de entrada e saída de malwares não conhecidos ou do tipo APT, com filtro de ameaças avançadas e análise de execução em tempo real, e inspeção de tráfego de saída de “call-backs”.

6.3.8.3. Suportar os protocolos HTTP assim como inspeção de tráfego criptografado através de HTTPS.

6.3.8.4. A solução deve ser capaz de inspecionar o tráfego criptografado SSL/TLS e SSH.

6.3.8.5. Identificar e bloquear a existência de malware em comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle.

6.3.8.6. Implementar mecanismo de bloqueio de vazamento não intencional de dados oriundos de máquinas existentes no ambiente LAN em tempo real.

6.3.8.7. Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar arquivo PDF com até 10Mb.

6.3.8.8. Implementar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows e Android.

6.3.8.9. Conter ameaças de dia zero permitindo ao usuário final o recebimento dos arquivos livres de malware.

6.3.8.10. A tecnologia de máquina virtual deverá suportar diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas.

6.3.8.11. A solução deve possuir nuvem de inteligência proprietária do fabricante, onde este seja responsável por atualizar toda a base de segurança dos appliance através de assinaturas.

6.3.8.12. Implementar a visualização dos resultados das análises de malwares de dia zero nos diferentes sistemas operacionais dos ambientes controlados (sandbox) suportados.

6.3.8.13. Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e quaisquer outros mecanismos de redirecionamento de tráfego;

6.3.8.14. Conter ameaças avançadas de dia zero.

6.3.8.15. Toda análise deverá ser realizada de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador.

6.3.8.16. Implementar mecanismo do tipo múltiplas fases para verificação de malware e/ou códigos maliciosos;

6.3.8.17. Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real. Não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos.

6.3.8.18. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx) e Android APKs no ambiente controlado.

6.3.8.19. Implementar a análise de arquivos executáveis, DLLs e ZIP no ambiente controlado.

6.3.8.20. Possuir Anti-Vírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, POP3, FTP, IMAP e CIFS.

6.3.8.21. Mitigar ameaças de dia zero de forma transparente para o usuário final.

6.3.8.22. Mitigar ameaças de dia zero através de tecnologias de emulação e código de registro.

6.3.8.23. Implementar mecanismo de pesquisa por diferentes intervalos de tempo.

6.3.8.24. Mitigar ameaças de dia zero via tráfego de internet.

6.3.8.25. Permitir a contenção de ameaças de dia zero sem a alteração da infraestrutura de segurança.

6.3.8.26. Mitigar ameaças de dia zero que possam burlar o sistema operacional emulado.

6.3.8.27. A solução deve permitir a criação de listas brancas (whitelist) baseadas no MD5 do arquivo.

6.3.8.28. Mitigar ameaças de dia zero antes da execução e evasão de qualquer código malicioso.

6.3.8.29. Conter e mitigar exploits avançados.

6.3.8.30. A análise em nuvem ou local deve prover informações sobre as ações do malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo malware, gerar assinaturas de Anti-Vírus e Anti-Spyware automaticamente, definir URLs não confiáveis utilizadas pelo novo malware e prover Informações sobre o usuário infectado (seu endereço IP e seu login de rede).

6.3.8.31. Suporte a submissão manual de arquivos para análise através do serviço de Sandbox.

6.3.8.32. As estratégias de análise, identificação e mitigação de ameaças devem também oferecer a capacidade de proteção contra ameaças que se alojam em memória, atuando permanentemente e em tempo real.

6.3.8.33. A solução de segurança de Firewalls deverá ter um sistema de inspeção baseado em fluxo que execute análises simultâneas de tráfego de entrada e saída em alta velocidade, sem proxying or buffering.

6.3.8.34. A solução deve unificar diversas funções de segurança em um único conjunto integrado, inspecionando os arquivos de usuários locais, remotos e móveis.

6.3.8.35. A solução deve unificar diversas funções de segurança em um único conjunto integrado inspecionando os arquivos de usuários locais, remotos e móveis.

6.3.8.36. A solução deve descriptografar e inspecionar o tráfego criptografado, como HTTPS, SMTPS, NNTPS, etc., sem afetar o desempenho.

6.3.8.37. A solução de segurança de firewalls deverá fornecer tecnologias avançadas de proteção contra ameaças, com

sandboxing usando multi-mecanismos baseado em nuvem, permitindo:

6.3.8.37.1. Inspeção profunda de memória em tempo real

6.3.8.37.2. Inspeção profunda de pacotes livre de remontagem,

6.3.8.37.3. Descriptografia e inspeção TLS/SSL,

6.3.8.37.4. Inteligência e controle de aplicativos

6.3.8.37.5. Recursos SD-WAN seguros

6.3.9. Requisitos de Filtro de Conteúdo Web

6.3.9.1. Os requisitos mínimos exigidos neste subitem são necessários para prover recurso de controle e gerenciamento de sites Web visitados pelos usuários, proporcionando a criação de políticas de filtragem de conteúdo ilegal, imoral, indevido ou alheio a execução das atividades laborais, garantindo assim conformidade às políticas e normas de segurança e evitando desvios de conduta;

6.3.9.2. Possuir filtro de conteúdo integrado ao NGFW para classificação de páginas web com, no mínimo, 89 (oitenta e nove) categorias distintas, com mecanismo de atualização e consulta automáticas.

6.3.9.3. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs, através da integração com serviços de diretório, Active Directory e base de dados local

6.3.9.4. Devem ser fornecidas licenças de filtro de conteúdo para cada equipamento e quantidade de usuários ilimitada, provendo atualização automática e em tempo real através da categorização contínua de novos sites da Internet, sem custo adicional, por todo o período de vigência da garantia e do contrato de manutenção e suporte técnico.

6.3.9.5. Permitir a customização de página de bloqueio.

6.3.9.6. Controle de conteúdo filtrado por categorias de sites com base de dados continuamente atualizada pelo fabricante.

6.3.9.7. Deve permitir submissão de novos sites para categorização.

6.3.9.8. Permitir a classificação dinâmica de sites web, URLs e domínios.

6.3.9.9. Permitir a associação de grupos de usuários a diferentes regras de filtragem de sites web, definindo quais categorias deverão ser bloqueadas ou permitidas para cada grupo de usuários, podendo ainda adicionar ou retirar acesso a domínios específicos da Internet.

6.3.9.10. Permitir a definição de quais zonas de segurança terão aplicadas as regras de filtragem de web.

6.3.9.11. Permitir aplicar a política de filtro de conteúdo baseada em horário do dia, bem como dia da semana.

6.3.10. Requisitos de autenticação para proteção de perímetro

6.3.10.1. Os requisitos mínimos exigidos neste subitem são necessários para garantir autenticidade (controle de acesso), através da autenticação dos usuários da rede, evitando acesso indevido de usuários ou de equipamentos não autorizados às informações trafegadas entre as localidades da rede corporativa do Tribunal de Contas de Mato Grosso do Sul, e especificam tecnologias padrão de mercado e utilizadas no âmbito do parque computacional;

6.3.10.2. Prover autenticação de usuários para os serviços Telnet, FTP, HTTP e HTTPS, utilizando as bases de dados de usuários e grupos de servidores Windows e Unix, de forma simultânea.

6.3.10.3. Permitir a autenticação dos usuários utilizando servidores LDAP, AD, RADIUS, Tacacs+, Single Sign On e API.

6.3.10.4. Permitir o cadastro manual dos usuários e grupos diretamente no NGFW por meio da interface de gerência remota do equipamento.

6.3.10.5. Permitir a integração com qualquer autoridade certificadora emissora de certificados X.509 que siga o padrão de PKI descrito na RFC 2459, inclusive verificando os certificados expirados/revogados, emitidos periodicamente pelas autoridades certificadoras, os quais devem ser obtidos automaticamente pelo NGFW.

6.3.10.6. Permitir o controle de acesso por usuário, para plataformas Microsoft Windows de forma transparente, para todos os serviços suportados, de forma que ao efetuar o logon na rede, um determinado usuário tenha seu perfil de acesso automaticamente configurado sem a instalação de softwares adicionais nas estações de trabalho e sem configuração adicional no browser.

6.3.10.7. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no NGFW.

6.3.10.8. Permitir aos usuários o uso de seu perfil independentemente do endereço IP da máquina que o usuário esteja utilizando.

6.3.10.9. Permitir a atribuição de perfil por faixa de endereço IP nos casos em que a autenticação não seja requerida.

6.3.10.10. Suportar a criação de túneis seguros sobre IP (IPSEC tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet

6.3.10.11. A solução deve possibilitar SSO via API

6.3.10.12. A solução deve prover o bloqueio de URL baseado em reputação, identificando e bloqueando proativamente entidades suspeitas.

6.3.11. Requisitos de Administração para proteção de perímetro

6.3.11.1. Os requisitos mínimos exigidos neste subitem são justificados pela necessidade da equipe técnica do Tribunal em administrar a solução instalada no Data Center, através de uma interface integrada e com todos os recursos e funcionalidades fornecidos pela solução, com disponibilidade de acesso local e/ou remoto e capacidade de gerenciar a todos os usuários (colaboradores diretos e terceirizados) que utilizam a rede de dados do Tribunal;

6.3.11.2. Permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o NGFW, cada um responsável por determinadas tarefas da administração.

6.3.11.3. Possuir mecanismo para aplicar remotamente, pela interface gráfica, correções e atualizações para o NGFW.

6.3.11.4. Possuir mecanismo para realizar remotamente, através de interface gráfica, cópias de segurança (backup) e restauração de configurações e sistema operacional.

6.3.11.5. Possuir mecanismo para agendamento realização das cópias de segurança(backups) de configuração.

6.3.11.6. Possuir mecanismo para exportar as configurações através de FTP, HTTPs ou SFTP.

6.3.11.7. A solução deve permitir ao administrador aplicar ajustes rápidos das melhores práticas de segurança no dispositivo com apenas um clique, possibilitando implementar as melhores práticas recomendadas pelo fabricante.

6.3.11.8. Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do NGFW e a remoção de qualquer uma destas sessões ou conexões.

6.3.11.9. Permitir a visualização, em forma gráfica, do percentual do uso de CPU e quantidade de tráfego de rede em todas as interfaces do NGFW em tempo real.

6.3.11.10. Permitir a visualização, em tempo real, dos serviços com maior tráfego e os endereços IP mais acessados.

6.3.11.11. Deve suportar minimamente dois tipos de negação de tráfego nas políticas de firewall: Descarte sem notificação do bloqueio ao usuário (discard), descarte com notificação do bloqueio ao usuário (drop), descarte com opção de envio de "ICMP Unreachable" para máquina de origem do tráfego, "TCP-Reset" para o cliente, "TCP-Reset" para o servidor ou para os dois lados da conexão.

6.3.11.12. Ser capaz de visualizar, de forma direta no appliance e em tempo real, as aplicações mais utilizadas, os usuários que mais estão utilizando estes recursos informando sua sessão, total de pacotes enviados, total de bytes enviados e média de utilização em Kbps, URLs acessadas e ameaças identificadas.

6.3.11.13. Ser capaz de visualizar, de forma direta no appliance e em tempo real estado do processamento do produto e volume/desempenho de dados utilizado pela rede de computadores conectada ao equipamento.

6.3.11.14. Possibilitar a geração de relatório de ameaças com avaliação e gerenciamento de riscos e informações detalhadas sobre o ambiente, ajudando a identificar explorações de vulnerabilidades, intrusões e outras ameaças. Deve permitir a emissão deste relatório em formato PDF.

6.3.11.15. Ser capaz de visualizar, de forma direta no appliance e em tempo real, a largura de banda utilizada por política, por protocolo TCP/UDP IPV4 e IPV6.

6.3.11.16. Ser capaz de visualizar, de forma direta no appliance e em tempo real, as conexões estabelecidas, com possibilidade de aplicar filtros na visualização.

6.3.11.17. Possibilitar a geração de pelo menos os seguintes tipos de relatório, mostrados em formato HTML: máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas, ou categorias Web mais acessadas (considerando a existência do filtro de conteúdo Web).

6.3.11.18. Permitir habilitar auditoria de configurações no equipamento, possibilitando o rastreio das configurações aplicadas no produto.

6.3.11.19. Ser capaz de implementar a funcionalidade de “Zero-Touch”, permitindo que o equipamento se provisione autônoma e automaticamente no sistema de gestão centralizada.

6.3.11.20. A solução deve possuir mecanismo de gerenciamento através de aplicativo móvel, com disponibilidade para os sistemas operacionais IOS e Android.

6.3.11.21. O aplicativo móvel deve possibilitar conexão ao dispositivo via protocolo HTTPS e conexão USB.

6.3.11.22. O gerenciamento via aplicativo móvel deve permitir visualização de status de consumo de banda, CPU, conexões ativas dos dispositivos e topologia do NGFW.

6.3.11.23. O aplicativo móvel deve permitir visualização de status das ameaças observadas e bloqueadas pelas funcionalidades de segurança de NGFW.

6.3.11.24. O aplicativo móvel deve permitir visualização dos últimos logs gerados no NGFW.

6.3.11.25. O aplicativo móvel deve permitir diagnósticos simples na solução, como testes ICMP e verificação DNS.

6.3.11.26. O aplicativo móvel deve permitir configurar interfaces, objetos e políticas de acesso, além de exportar configurações.

6.3.11.27. A solução deve possibilitar ao administrador habilitar ou desabilitar as capacidades de auto provisionamento da plataforma através de ponto central de gerenciamento.

6.3.11.28. Deve ser capaz de emitir relatório, mostrando a saúde do ambiente, agendado ou sob demanda, que liste informações de aplicações, risco, atividade WEB, análise de botnets, análise de malware, ameaças, países por tráfego, Arquivos compartilhados por aplicações, sessões e recomendações

6.3.11.29. A solução deve suportar API como alternativa à interface de linha de comando (CLI), para configurar funções diversas.

6.3.11.30. Deve permitir que os administradores criem/recuperem/excluam listas de URLs ou endereços IP a serem bloqueados por meio de chamadas de API RESTful.

6.3.12. Requisitos do Software de Gerenciamento para proteção de perímetro

6.3.12.1. Os requisitos mínimos exigidos neste subitem são justificados pela necessidade da equipe técnica do Tribunal em gerenciar todo o ambiente tecnológico fornecido pela solução nos sites instalados, através de uma interface integrada e com acesso à configuração e ao monitoramento de todos os recursos e funcionalidades fornecidos, com disponibilidade de acesso local e/ou remoto;

6.3.12.2. Os firewalls devem possuir solução de gerenciamento centralizado, possibilitando o gerenciamento de toda a solução.

6.3.12.3. Controle sobre todos os equipamentos da plataforma de segurança em uma única console, com administração de privilégios e funções

6.3.12.4. O gerenciamento centralizado poderá ser entregue como appliance físico ou appliance virtual, sendo todos do mesmo fabricante dos appliances, não sendo aceita solução de software livre;

6.3.12.5. Caso seja entregue em appliance virtual dever ser compatível com VMware ESXi ou Hyper-V.

6.3.12.6. Caso seja entregue em appliance físico, o equipamento deve possuir fonte de chaveamento automático (100-240 VAC), com formato compatível para instalação em rack.

6.3.12.7. Deve suportar organizar os dispositivos administrados em grupos;

6.3.12.8. Deve implementar sistema de hierarquia entre os firewalls gerenciados, onde seja possível aplicar configurações de forma granular em grupos de firewalls;

6.3.12.9. Deve mostrar os status dos firewalls em alta disponibilidade a partir da plataforma de gerenciamento centralizado;

6.3.12.10. Deve permitir a centralização da administração de regras e políticas dos firewalls configurados de forma individual e em cluster.

6.3.12.11. O gerenciamento deve permitir/possuir:

6.3.12.11.1. Criação e administração de políticas de firewall e controle de aplicação

6.3.12.11.2. A solução deve permitir acesso concorrente de administradores

6.3.12.11.3. Deve permitir o provisionamento de configuração por "Zero-Toutch"

6.3.12.11.4. Deve permitir a integração com LDAP ou Radius

6.3.12.12. A solução de gerenciamento deverá ser acessível através de navegador WEB padrão, com criptografia de tráfego SSL

6.3.12.13. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança, possibilitando geração de relatórios analíticos e de forma centralizada de todos os dispositivos gerenciados.

6.3.12.14. A solução deve possuir tela situacional com os inventários de firewalls gerenciados centralizadamente, informando no mínimo para o administrador, nome do Hostname do firewall, número de série, modelo, versão do firmware e status da conectividade do equipamento com a gerência em online ou off-line.

6.3.12.15. Deverá permitir atualizar o sistema operacional de múltiplos equipamentos gerenciados de uma única vez;

6.3.12.16. A solução deve possuir Dashboard com sumario de alertas e informação de status de licença

6.3.12.17. A solução deverá permitir seu gerenciamento por Web GUI utilizando protocolo HTTPS sem a necessidade de uso de cliente ou console do tipo aplicativo

6.3.12.18. Deve manter um canal de comunicação segura, com encriptação baseada HTTPS, entre todos os componentes que fazem parte da solução de firewall, gerência

6.3.12.19. A solução deverá permitir que a partir da console de gerência centralizada seja feito conexão no console de

gerência local do firewall sem a necessidade de o administrador utilizar endereço IP do dispositivo, URL ou FQDN

6.3.12.20. A solução deve permitir a criação de modelos de configuração ou “Templates” para aplicá-los em grupos de dispositivos. Os modelos de configurações devem permitir visualização e edição para sua aplicação nos firewalls

6.3.12.21. Os modelos de configuração ou “templates” devem suportar configurações de interfaces físicas ou virtuais

6.3.12.22. A solução deve permitir a criação de grupos lógicos, para o agrupamento de dispositivos, com isso permitindo a aplicação de modelos de configuração a diversos equipamentos de uma única vez.

6.3.12.23. Deverá permitir visualizar a diferença nas mudanças antes que a configurações sejam implantadas.

6.3.12.24. De forma centralizada deve permitir gerenciar (mas não se limitando a) políticas de firewall, NAT, rotas, PBR (Policy Based Routing), configurar endereçamento IP das interfaces dos equipamentos, criar e administrar políticas de IPS, configurar políticas de antivírus e antimalware, configurar e criar políticas de controle de URL, criar e configurar políticas de controle de aplicações, criar e configurar política de SANDBOX, criar e configurar políticas de controle de banda e criar e configurar os objetos necessários para configurar e criar as políticas.

6.3.12.25. Deverá possibilitar a criação de políticas SD-WAN, baseando-se em parâmetros de latência, perda de pacote e jitter, para a tomada de decisão de encaminhamento de tráfego no firewall.

6.3.12.26. Para cada alteração de configuração a solução deverá confirmar a aplicação da política, possibilitando a

adição de comentários nas políticas instaladas, para futuras consultas de auditoria.

6.3.12.27. Durante a alterações de políticas de segurança dos firewalls, deverá ser possível o agendamento para determinar o horário que as mudanças entrarão em vigor, proporcionando ao administrador aplicar políticas de segurança em horários com menor impacto para o ambiente.

6.3.12.28. Deverá permitir que configurações realizadas pelos administradores da solução sejam validadas e aprovadas (workflow), por um colaborador responsável por aprovação e aplicação de políticas, esse processo de aprovação deve ser encaminhado de forma automatizada para o responsável da aprovação via e-mail ou console da solução, possibilitando mitigar erros de configuração e impactos negativos ao ambiente

6.3.12.29. A funcionalidade de Workflow deve permitir configurar, em dias, a validade dos pedidos de aprovação, caso o pedido de aprovação não seja aprovado no período configurado, essa mudança deve ser expirada e não efetivada.

6.3.13. Requisitos do Software de Relatórios para proteção de perímetro

6.3.13.1. Os requisitos mínimos exigidos neste subitem são justificados pela necessidade da equipe técnica do Tribunal em gerenciar todo o ambiente tecnológico fornecido pela solução nos sites instalados, através de uma interface integrada e com acesso à configuração e ao monitoramento de todos os recursos e funcionalidades fornecidos, com disponibilidade de acesso local e/ou remoto;

6.3.13.2. A solução poderá ser entregue como appliance físico ou appliance virtual, sendo todos do mesmo fabricante dos firewalls, não sendo aceita solução de software livre;

6.3.13.3. Caso seja entregue em appliance virtual, dever ser compatível com VMware ESXi ou Hyper-V;

6.3.13.4. A solução deverá permitir visualizar sumario com as informações referentes as principais ameaças protegidas pelos firewalls;

6.3.13.5. Deverá suportar logs do tipo Netflow, IPFIX ou Syslog, para a gerar reports;

6.3.13.6. O operador da solução de relatórios poderá ter acesso a informações com buscas por um período pré-definido pela solução (última hora, ontem, última semana e último mês) ou customizados para um período específico definido pelo operador;

6.3.13.7. A solução deverá prover relatórios referente as atividades dos usuários;

6.3.13.8. A solução deverá prover relatórios referente ao uso de aplicações web, com no mínimo as seguintes informações: nome da aplicação, nível de ameaça, quantidade de conexões e quantidade de Megabytes trafegados;

6.3.13.9. A solução deverá possuir as informações de "Uptime" dos equipamentos;

6.3.13.10. A solução deverá prover relatórios referente ao consumo de rede por endereço IP, com no mínimo as seguintes informações: endereço IP, quantidade de conexões, Usuário, quantidade de Megabytes trafegados e Mac Address de origem;

6.3.13.11. A solução deverá prover relatórios referente aos acessos web com no mínimo informações referentes às

categorias acessadas, quantitativo de acessos e megabytes transferidos;

6.3.13.12. A solução deverá permitir o agendamento para envio de relatórios periódicos, em formato PDF;

6.3.13.13. A solução deverá mostrar dados de uso de VPN, informando no mínimo dados como:

6.3.13.13.1. IP de origem, usuário, conexões e quantidade de dado trafegado;

6.3.13.14. A solução deve permitir visualização de eventos correlacionados que possam ser investigados por:

6.3.13.14.1. Lista de eventos correlacionados com opção de navegação "drilldown"; ou

6.3.13.14.2. Modo gráfico; ou

6.3.13.14.3. Lista de logs;

6.3.13.15. A solução deve possibilitar a criação de relatórios de uso de VPN;

6.3.14. Requisitos de Hardware do Gateway de Controle de Acesso

6.3.14.1. Não serão aceitos produtos ou serviços do tipo demo, trial, software gratuitos e na nuvem. A solução deve ser proprietária.

6.3.14.2. A solução de Controle de Acesso poderá ser fornecida em appliance físico ou virtual.

6.3.14.3. Caso a solução seja fornecida em appliance virtual, toda infraestrutura de hardware (servidores) e software (sistema operacional, sistema de virtualização, etc) que fornecida(os) e homologada(os) pelo fabricante da solução. A homologação deverá ser comprovada por suportará(ão) a solução deve(m) ser fornecida(os) e homologada(os) pelo fabricante da solução. A homologação deverá ser comprovada por documento formal emitido pelo fabricante.

6.3.14.4. Caso a solução seja fornecida em appliance virtual, também deverá ser disponível para instalação em ambientes virtualizados do tipo VMware ESXi, Microsoft Hyper-V, KVM, AWS e Azure;

6.3.14.5. A solução deve ser capaz de visualizar, via console, as informações de saúde e desempenho de todo o ambiente da solução, incluindo softwares e equipamentos.

6.3.14.6. Possuir suporte a SNMP v2c e v3.

6.3.14.7. Enviar mensagens por e-mail e traps SNMP.

6.3.14.8. Os componentes da solução poderão ser executados num mesmo equipamento, ou poderão ser distribuídos em múltiplos equipamentos, de acordo com a característica de cada produto, respeitadas as características de funcionamento e performance exigidas neste edital.

6.3.14.9. A solução deverá ter o pleno funcionamento independentemente de conexão (física ou lógica) com o fabricante, exceto para atualizações de versões e de segurança.

6.3.14.10. Suportar IPV6.

6.3.14.11. A solução deverá dispor de mecanismos para que novos componentes operem simultaneamente, sendo aceitos clusters de equipamentos ou equipamentos balanceados por DNS.

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

6.3.14.13. Apresentar uma relação descritiva dos componentes fornecidos, incluindo seus códigos Comerciais

6.3.14.14. O(s) appliance(s) físico(s) ou servidores deve(m) possuir as seguintes características:

6.3.14.14.1. O Equipamento será instalado em rack padrão 19" e deve ser apropriado para estas instalações

6.3.14.14.2. Deve conter fonte AC redundante com tensão de entrada 100-127VAC e 200-240VAC.

6.3.14.14.3. Deve permitir a instalação/substituição de transceptores e/ou módulos de interfaces e fonte de alimentação sem ter que remover o aparelho do rack.

6.3.14.14.4. Deve suportar operações com temperaturas externas ao equipamento entre 0º e 40º Celsius

6.3.14.15. Por cada equipamento que compõe a solução, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento

6.3.14.16. Os appliances (hardware) da solução deve ter pelo menos as seguintes características:

6.3.14.16.1. Throughput L4/L7 de no mínimo 1 Gigabit por segundo, mesmo que um nó ou appliance que compõe o cluster esteja indisponível.

6.3.14.16.2. O sistema deve permitir a integração e envio de alertas para terceiros ou ferramentas de correlação (SIEM). Será permitido que a integração seja realizada através da utilizando SYSLOG ou através de RestAPI, Exportação de eventos.

6.3.14.17. O equipamento deve suportar o protocolo de gerenciamento de rede SNMP a ser monitorado por ferramentas de terceiros.

6.3.14.18. Todos os componentes da solução a exemplo de Gbics SFPs, etc. devem ser do mesmo fabricante dos appliances, ou serem homologados pelo mesmo.

6.3.14.19. Os produtos ofertados deverão vir acompanhados de todos os cabos e acessórios necessários à completa instalação, configuração e operação dos mesmos.

6.3.14.20. A capacidade de processamento da solução deverá seguir as melhores práticas de cada fabricante, considerando todos os requisitos de capacidade definidos nesta especificação.

6.3.14.21. Deve possui CPU e memoria suficientes para atender os throughputs definidos no edital sem degradação de performance da solução.

6.3.15. Requisitos de Interfaces do Gateway de Controle de Acesso

6.3.15.1. Cada appliance físico ou servidor deve possuir no mínimo as seguintes quantidades de interfaces físicas.

6.3.15.2. Quantitativo de interfaces:

6.3.15.2.1. Possuir o mínimo de 04 (quatro) interfaces de rede 1 Gbps Base-T

6.3.15.2.2. Possuir no mínimo 01 (uma) interface para configuração através de CLI (Command Line Interface).

6.3.15.2.3. Possuir no mínimo 01 (uma) porta USB.

6.3.15.2.4. Deve possuir dispositivos luminosos que indiquem estado e atividade das interfaces de rede.

6.3.15.3. Não serão aceitas combinações de equipamentos para atingir o número mínimo de portas solicitadas.

6.3.16. Requisitos do Gateway de Controle de Acesso

6.3.16.1. Suporte a, no mínimo, 250 (duzentos e cinquenta) conexões simultâneas de VPN.

6.3.16.2. A solução deverá suportar a função Ativo / Ativo ou Ativo / Passivo.

6.3.16.3. Suportar e garantir a instalação em ambiente de alta disponibilidade.

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

6.3.16.5. A solução deverá dispor de mecanismos de escalabilidade, sendo aceitos clusters de equipamentos ou equipamentos balanceados por DNS.

6.3.16.6. A solução deverá fornecer acesso seguro sem a necessidade de instalação de clients para acesso à recursos via RDP e deve suportar o acesso a recursos via SSH.

6.3.16.7. Implementar o SNTP (Simple Network Time Protocol) ou NTP (Network Time Protocol).

6.3.16.8. Permitir acesso in-band via SSH.

6.3.16.9. Possuir auto complementação de comandos na CLI.

6.3.16.10. Possuir ajuda contextual.

6.3.16.11. Possuir Interface Gráfica via Web.

6.3.16.12. A interface Gráfica deverá permitir a atualização do sistema operacional e/ou a instalação de patches ou Hotfixes sem o uso da linha de comando.

6.3.16.13. Suportar a rollback de imagem.

6.3.16.14. Possuir e fornecer geração de mensagens de syslog para eventos relevantes ao sistema.

6.3.16.15. Possuir configuração de múltiplos syslog servers para os quais o equipamento irá enviar as mensagens de syslog.

6.3.16.16. Possuir armazenamento de mensagens em dispositivo interno ao equipamento.

6.3.16.17. A interface Gráfica deverá permitir a reinicialização do equipamento.

6.3.16.18. Desligamento do equipamento por comando na CLI ou Interface Gráfica

6.3.16.19. Deverá implementar as funcionalidades de Single Sign-on e VPN-SSL, com os seguintes recursos:

6.3.16.19.1. Deve possuir modo "Tunel por aplicação" onde o usuário estabelece túnel para rotear aplicações que devem ser acessadas via data center.

6.3.16.19.2. Deve buscar o conteúdo Web dos portais internos e a possuir o modo "Portal" onde o equipamento se comporta como proxy reverso buscando o conteúdo Web dos portais internos e apresentando-os como links seguros no portal do usuário.

6.3.16.19.3. Deve possuir o modo NetWork, onde um usuário se conecta efetivamente à rede interna, obtendo um endereço IP roteavel pela rede interna.

6.3.16.20. Deve possuir Suporte à compressão HTTP.

6.3.16.21. Deve permitir estabelecimento de conexão segura de acesso remoto sem a necessidade de instalação de um software cliente na máquina do usuário.

6.3.16.22. Deve permitir a utilização do protocolo padrão HTTPS com SSL como transporte

6.3.16.23. Deve possibilidade de compressão de dados.

6.3.16.24. Deve possibilitar a customização da interface gráfica da página de Login e mensagens de apresentação ao usuário. Deve oferecer acesso remoto seguro à rede inteira para qualquer aplicação baseada em IP (TCP ou UDP).

6.3.16.25. Deverá possuir ativo o controle de, no mínimo, 250 (duzentos e cinquenta) usuários concorrentes, e deverá vir com todo o licenciamento necessário para ativação do número de usuários solicitado.

6.3.16.26. Deve possui integração nativa com Active Directory e LDAP.

6.3.16.27. Suporte a Single-Sign-On (SSO), com os seguintes recursos:

6.3.16.27.1. Deverá ser capaz de solicitar as credenciais do usuário somente uma vez, e autenticar o usuário nas regras de acesso que delimitam o que o mesmo pode acessar via VPN.

6.3.16.27.2. Deve ser capaz de realizar Single-Sign-On utilizando Kerberos (AD/ LDAP) ou padrão form based ou SAML.

6.3.16.27.3. O equipamento deverá ser capaz de fazer cache das credenciais do usuário e utilizar a credencial correta para cada sistema.

6.3.16.27.4. O equipamento deverá ser capaz de implementar SSO mesmo quando conectado via pelo portal).

6.3.16.28. Deverá implementar suporte à validação da estação do usuário para, no mínimo, os seguintes recursos:

6.3.16.28.1. Versão do Sistema Operacional;

6.3.16.28.2. Firewall ativado;

6.3.16.28.3. Antivírus instalado;

6.3.16.28.4. Antivírus atualizado;

6.3.16.28.5. Processos em execução;

6.3.16.28.6. Certificados digitais instalados na máquina.

6.3.16.28.7. Deverá ser possível configurar uma ação dependendo da validação da estação do usuário;

6.3.16.28.8. A configuração das dessas ações deverá ser através de interface gráfica.

6.3.16.29. Com base na análise do cliente, o sistema deverá conceder dinamicamente o acesso ao usuário: se o cliente estiver adequado com as políticas de segurança poderá acessar os recursos definidos em sua autenticação, caso

contrário deverá ter acesso limitado definidos pelo administrador.

6.3.16.30. Deve suportar autenticação de múltiplos fatores.

6.3.16.31. Deve possuir capacidade para definir diversos métodos para acesso remoto.

6.3.16.32. Deve possuir capacidade para suportar múltiplos navegadores.

6.3.16.33. Deve possuir capacidade para definir autenticação e autorização web dos usuários para acesso ao virtual server (access sessions).

6.3.16.34. Deve possuir capacidade para definir perfil de acesso a rede através de wizard ou regras.

6.3.16.35. Deve possuir capacidade para definir o tempo de inatividade da conexão de vpn antes de encerrar a sessão do usuário.

6.3.16.36. Deve possuir capacidade para definir a quantidade máxima de conexões de vpn simultâneas por usuário.

6.3.16.37. Deve possuir capacidade para definir os recursos de DNS e WIN.

6.3.16.38. Deve possuir capacidade para definir os recursos de AAA.

6.3.16.39. Deve possuir capacidade para finalizar a sessão do usuário com base em número X de tentativas com credenciais inválidas.

6.3.16.40. Deve possuir capacidade para permitir a troca da senha dos usuários que tenham expirado.

6.3.16.41. Deve possuir capacidade para definir lease pool que contenha endereços IP a serem designados aos usuários com acesso à rede.

6.3.16.42. Deve possuir capacidade para definir servidor virtual em HTTPS com perfil cliente SSL padrão.

6.3.16.43. Deve possuir capacidade de redirecionar tráfego HTTP para HTTPs para um determinado servidor virtual ou para vpn SSL.

6.3.16.44. Deve possuir capacidade para definir que todo tráfego seja tunelado.

6.3.16.45. Deve possuir capacidade para definir regras estáticas e dinâmicas.

6.3.16.46. Deve possuir capacidade para definir segmentação do tráfego tunelado baseado em lista de endereços IP/máscara.

6.3.16.47. A solução deve informar que existem "Mudanças pendentes" para serem aplicadas

6.3.16.48. Deve possuir capacidade para realizar proxy reverso com a finalidade de "ofuscar" a URI promovendo assim o acesso seguro as aplicações web internas.

6.3.16.49. Deve possuir capacidade para personalizar as páginas de login/logout.

6.3.16.49.1. Deve possuir capacidade para realizar Single Sign On (SSO): ntlm v1 & v2, basic, http forms based, kerberos ou oam.

6.3.16.50. Deve possuir capacidade para realizar verificações e validações no dispositivo do cliente antes ou grupo de recursos.

6.3.16.50.1. Anti-Virus.

6.3.16.50.2. Firewall.

6.3.16.50.3. File/process.

6.3.16.50.4. Registry entry.

6.3.16.50.5. Machine certificate.

6.3.16.50.6. SO detection.

6.3.16.51. Deve possuir capacidade para conceder acesso a usuários autorizados os recursos específicos ou grupo de recursos.

6.3.16.52. Deve possuir capacidade para definir bookmark para páginas web externas.

6.3.16.53. Deve possuir capacidade para criar tunel VPN, que permitirão acesso as aplicações internas.

6.3.16.54. Deve possuir capacidade para utilizar compressão no trafego VPN.

6.3.16.55. Deve possuir capacidade para atribuir a aplicação com front-end web autenticação de usuários via SSO.

6.3.16.56. Deve possuir capacidade para definir web perfil de acesso a aplicação através de wizard ou bookmarks e regras de firewall.

6.3.16.57. A solução deve empregar criptografia SSL ou outros algoritmos criptográficos para assegurar a transferência segura dos dados

6.3.16.58. Deverá prover acesso remoto através de VPN SSL para Microsoft Windows, Linux, dispositivos baseados em Android e iOS e MAC OSX.

6.3.16.59. Suportar autenticação de usuários em AAA.

6.3.16.60. A solução deverá realizar federação através de SAML, onde a comunicação será direta entre o Identity Provider (IdP) e o Service Provider (SP).

6.3.16.61. A solução deverá atuar como gateway para o acesso RDP, deverá ser possível realizar autenticação via NTLM dos usuários, sem a necessidade de software adicional.

6.3.16.62. A solução deverá suportar Autenticação Multifator e são elas: Certitificado Digital X.509, Certificado Digital, RSA SecurID, One-Time Password (OTP), 2 fatores (2FA) e tokens.

6.3.16.63. A solução deverá suportar serviço de proxy reverso aprimorado com autenticação que permita que os administradores configurem o portal, bookmarks e carregamento de os recursos deve suportar pelo menos os navegadores Edge, Chrome e Firefox. usuários se conectem facilmente à recursos e aplicativos remotos, incluindo RDP e HTTP.

6.3.16.64. Permitir a criação de regras ou ACL´s para acesso/bloqueio de serviços, redes, segmentado por grupo de usuários do serviço de autenticação sem a necessidade de segregação.

6.3.16.65. Permitir configurações de pool de IP e DNS.

6.3.17. Requisitos de Console de Gerência, Monitoração e Operação do Gateway de Controle de Acesso

6.3.17.1. A solução deve ser gerenciada centralmente (configurações, controle e atualizações), através de interface web ou console de administração, sem necessidades de intervenção nos equipamentos onde está instalada.

6.3.17.2. A console deve permitir monitorar, gerenciar e operar todo o cluster de forma centralizada sem perda desempenho.

6.3.17.3. A Solução deve ser fornecida com equipamento de gerenciamento único que permite a gerencia centralizada unificada de múltiplos appliances.

6.3.17.4. Toda a configuração, administração e monitoramento da solução serão feitos através do console de administração.

6.3.17.5. O gerenciador deve permitir a escalabilidade de gerenciamento para múltiplos appliances.

6.3.17.6. A solução de gerenciamento deve ser do mesmo fabricante da solução de Controle de Acesso.

6.3.17.7. A comunicação entre as estações de trabalho e o console de administração deve ser estabelecida através de um protocolo seguro com criptografia e autenticação por usuários locais, incluindo a possibilidade de usar certificados digitais.

6.3.17.8. Adicionar, excluir ou modificar a configuração em um ambiente gráfico

6.3.17.9. Modifique as regras dos diferentes equipamentos

6.3.17.10. Executar a configuração dos componentes da solução

6.3.17.11. Visualizar registros de auditoria, alertas de segurança e eventos do sistema.

6.3.17.12. Gerar relatórios pelo administrador do sistema.

6.3.17.13. Permitir exportar estatísticas manualmente no formato CSV.

6.3.17.14. O gerenciador deve possuir controle de interface gráfica Web (GUI: Graphical user interface) ou interface por linha de comando (CLI Command Line Interface).

6.3.17.15. A interface gráfica de gerenciamento deve ser cross-platform, em Web via protocolo HTTPS, com suporte a acesso nativo via Microsoft Windows, Linux e Mac-OS.

6.3.17.16. Para interface gráfica do tipo Web, deve suportar no mínimo o navegador Mozilla Firefox e Chrome nas versões mais recentes.

6.3.17.17. Caso possua CLI, deve possuir auto complementação de comandos

6.3.17.18. Deve permitir acesso via SSH ou acesso WEB, criptografado.

6.3.17.19. Permitir visualização gráfica de tráfego.

6.3.17.20. Permitir reinicialização do equipamento.

6.3.17.21. Deve suportar o gerenciamento remoto, seguro, baseado em perfis de administração com granularidade de funções.

6.3.17.22. A solução de gerenciamento deve possuir, no mínimo, três níveis de usuários: Administrador; Usuário com permissões reduzidas; e usuário Somente Leitura.

6.3.17.23. A solução deverá permitir que mais de um usuário possa estar conectado simultaneamente a interface de administração com a permissão de leitura/escrita.

6.3.17.24. A interface gráfica de gerenciamento deverá permitir a atualização do sistema operacional e/ou a instalação de patches ou Hotfixes sem o uso da linha de comando.

6.3.17.25. Utilizar SCP ou HTTPS como mecanismo de transferência de arquivos de configuração e Sistema Operacional.

6.3.17.26. A interface Gráfica deverá permitir a reinicialização do equipamento.

6.3.17.27. Deve suportar rollback de imagem.

6.3.17.28. Manter internamente múltiplos arquivos de configurações do sistema.

6.3.17.29. A solução deverá possuir capacidade de armazenamento de logs

6.3.17.30. Possuir e fornecer geração de mensagens de syslog para eventos relevantes ao sistema.

6.3.17.31. Possuir configuração de múltiplos syslog servers para os quais o equipamento irá enviar as mensagens de syslog.

6.3.17.32. Suporte ao protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol).

6.3.17.33. Implementar uma configuração de endereçamento IP estático ou dinâmico (DHCP/BOOTP) para usuários da VPN

6.3.17.34. Gerar alertas automáticos via:

6.3.17.34.1. Email;

6.3.17.34.2. SNMP;

6.3.17.34.3. Syslog;

6.3.17.35. Os usuários de gerência deverão poder ser autenticados em bases remotas. No mínimo RADIUS, LDAP, TACACS+ e AD deverão ser suportados.

6.3.18. Requisitos de Relatórios do Gateway de Controle de Acesso

6.3.18.1. Deve possui no mínimo os relatórios abaixo, não se limitando a esses:

6.3.18.1.1. Informar o quantitativo de usuários que utilizaram a solução, classificando por hora, dia e mês

6.3.18.1.2. Mostrar visualmente com a utilização de gráficos, a quantidade de acessos classificados pela política utilizada

6.3.18.1.3. Informar o quantitativo de conexões classificando os acessos pelo tipo dos dispositivos.

6.3.18.1.4. Tipo de acesso utilizado pelo usuário, se um acesso total ou através do portal.

6.3.19. Requisitos de Capacidade e de Interfaces de cada appliances para implementação de balanceamento de carga e na proteção de aplicações.

6.3.19.1. Os requisitos mínimos exigidos neste subitem são justificados pela necessidade de garantir que a solução ofertada possua: a) capacidade de operação redundante (energia e refrigeração) provendo resiliência e tolerância à falhas; b) processamento, largura de banda e taxa de transferência suficiente para suportar o alto volume de dados trafegados na rede do Tribunal de Contas de Mato Grosso do

Sul pelos diversos sistemas e softwares utilizados; e c) a quantidade de interfaces de rede necessárias para suportar toda a arquitetura do ambiente funcional da rede no núcleo do Tribunal, permitindo o devido gerenciamento, monitoramento e operação da solução sem necessidade de adaptações ou equipamentos sobressalentes;

6.3.19.2. Os equipamentos deverão ser novos, de primeiro uso e vir em caixas lacradas de fábrica.

6.3.19.3. Os equipamentos são do tipo appliance, devem possuir altura de 1U, e vir acompanhado de kit para instalação em rack de 19”.

6.3.19.4. Possuir fontes AC redundantes, hot swappable, para tensões 110V e 220V, automática sendo que o equipamento deverá continuar totalmente operacional em caso de falha de uma das fontes.

6.3.19.5. Possuir interface serial para configuração por meio de CLI (Command Line Interface).

6.3.19.6. Possuir interface Ethernet RJ-45 autosense (10/100/1000 Mbps) para gerenciamento out-of-band.

6.3.19.7. Possuir, no mínimo, 4 (quatro) interfaces 25G/10G, com transceivers inclusos.

6.3.19.8. Possuir, no mínimo, 4 (quatro) interfaces 10G/1G Ethernet RJ-45.

6.3.19.9. Possuir, no mínimo, 1 (uma) interfaces 1GE, inclusos interfaces de gerência com conectores padrão RJ45.

6.3.19.10. Suportar e garantir a instalação em ambiente de alta disponibilidade.

6.3.19.11. Os appliances devem ser capazes de trabalhar no modo Ativo/Standby com equipamento da mesma marca e modelo.

6.3.19.12. Os appliances devem ser capazes de operar no modo ativo/ativo, mantendo o status das conexões.

6.3.19.13. Assegurar que a operação de 2 ou mais equipamentos, quando implementada em ambiente redundante suporte o sincronismo de sessão entre os dois membros. A falha de um equipamento não deverá causar a interrupção das sessões balanceadas.

6.3.19.14. A solução deve vir com todos os recursos possíveis de redundância, sem que seja necessária nenhuma despesa com licenças adicionais.

6.3.19.15. Fornecer recurso de agregação de portas baseado no protocolo LACP.

6.3.19.16. Possui suporte a LACP em modo passivo e ativo.

6.3.19.17. Fornecer recurso para o transporte de múltiplas VLANs por meio de uma única porta (ou por um conjunto de agregado de portas) utilizando o protocolo 802.1q.

6.3.19.18. Possuir suporte a IPv6.

6.3.19.19. A solução deve suportar múltiplas tabelas de rotas independentes.

6.3.19.20. Possuir, no mínimo, 64 GB de memória RAM.

6.3.19.21. Possuir capacidade de compressão, no mínimo 19 Gbps.

6.3.19.22. Possuir armazenamento do tipo SSD Enterprise Class com capacidade de, no mínimo, 480GB.

6.3.19.23. Possuir capacidade para processar, no mínimo, 30 Gbps de tráfego na camada 7.

6.3.19.24. Possuir capacidade para processar, no mínimo, 40 Gbps de tráfego na camada 4.

6.3.19.25. Possuir capacidade de processar, no mínimo, 29 mil transações SSL por segundo (TPS) com chave de 2048 bits.

6.3.19.26. Possuir capacidade de processar, no mínimo, 1,2 milhões de requisições por segundo em camada 7.

6.3.19.27. Possuir capacidade para processar, no mínimo, 2,4 milhões de requisições HTTP por segundo em camada 4.

6.3.19.28. Possuir capacidade para processar, no mínimo, 485 mil conexões por segundo em camada 4.

6.3.19.29. Possuir capacidade para manter, no mínimo, 37,5 milhões de conexões concorrentes em camada 4.

6.3.20. Requisitos Gerais do Balanceador de Carga e Proteção de Aplicações

6.3.20.1. Os requisitos mínimos exigidos neste subitem são necessários para permitir a implementação de estratégias mais eficazes para diminuir a instabilidade e aumentar a confiabilidade dos sistemas utilizados, otimizando a infraestrutura de TI do TCE-MS. Esses requisitos são considerados essenciais para distribuir cargas de trabalho entre servidores de redes ou recursos que executam tarefas idênticas, com o objetivo de evitar prejuízos e diversos problemas relacionados à sobrecarga e disponibilidade, diante de milhares de requisições que são feitas simultaneamente na Internet.

6.3.20.2. Suportar IPv4 e IPv6;

6.3.20.3. Suportar múltiplas tabelas de roteamento independentes em IPv4 e IPv6;

6.3.20.4. Suportar VXLAN para integração com o ambiente de virtualização;

6.3.20.5. Suportar configuração de endereçamento IP estático e dinâmico (DHCP/BOOTP) para o gerenciamento;

6.3.20.6. Suportar implementação em alta disponibilidade,

6.3.20.7. Implementar modo ativo/standby;

6.3.20.8. Suportar modo ativo/ativo para, pelo menos, as funções de balanceamento de servidores. Aceita-se como ativo/ativo a utilização de dois endereços virtuais, onde cada endereço fica ativo em um elemento e standby no outro;

6.3.20.9. Permitir a sincronização das configurações de forma automática e manual, forçando a sincronização quando necessário;

6.3.20.10. Permitir utilizar qualquer endereçamento IP, inclusive os definidos na RFC 1918, para criação de cluster, heartbeat e sincronização entre os equipamentos;

6.3.20.11. Fornecer todos os recursos de redundância da solução sem nenhuma despesa com licenças adicionais;

6.3.20.12. Permitir expansão do cluster adicionando novos equipamentos inclusive de modelos diferentes;

6.3.20.13. Possuir interface gráfica via web e interface via CLI por SSH e console para administração, gerenciamento e monitoramento do equipamento;

6.3.20.14. Implementar o SNTP (Simple Network Time Protocol) ou NTP (Network Time Protocol);

6.3.20.15. Permitir habilitar e desabilitar acesso administrativo via SSH por qualquer interface do equipamento;

6.3.20.16. Manter internamente múltiplos arquivos de configurações do sistema;

6.3.20.17. Utilizar SCP ou HTTPS como mecanismo de transferência de arquivos de configuração e sistema operacional;

6.3.20.18. Possuir recurso de autocompletar nos comandos na CLI, com ajuda contextual;

6.3.20.19. Permitir a configuração de múltiplas contas locais de administradores;

6.3.20.20. 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;

6.3.20.21. Possuir, no mínimo, três níveis de usuários na GUI: administrador, analista e somente-leitura;

6.3.20.22. Suportar autenticação e autorização externa de usuários administradores através de RADIUS, LDAP, Active Directory e TACACS+;

6.3.20.23. A interface gráfica deve permitir a atualização do sistema operacional, atualização de componentes e instalação de patches;

6.3.20.24. Permitir selecionar pela interface gráfica a versão do sistema operacional para inicialização do equipamento;

6.3.20.25. Possuir um comando, via CLI, que mostre o tráfego de utilização das interfaces (bps e pps);

6.3.20.26. Suportar a rollback de configuração e imagem;

6.3.20.27. 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;

6.3.20.28. 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;

6.3.20.29. Permitir reiniciar o equipamento pela interface gráfica e por CLI;

6.3.20.30. Implementar SNMPv1, SNMPv2c e SNMPV3;

6.3.20.31. Implementar traps SNMP;

6.3.20.32. Permitir a criação de MIBs customizadas;

6.3.20.33. Possuir suporte a monitoração utilizando RMON através de pelo menos 4 grupos: statistics, history, alarms e events

6.3.20.34. Possuir agente integrado de coleta e exportação de métricas de desempenho e eventos:

6.3.20.35. Coleta de métricas de desempenho em formato JSON utilizando cliente HTTP;

6.3.20.36. 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, Splunk e StatsD;

6.3.20.37. Exportação de métricas de desempenho em formato JSON para um servidor HTTP;

6.3.20.38. Permitir definir critérios de inclusão e exclusão de coleta e exportação de métricas;

6.3.20.39. Deve incluir métricas de desempenho relacionadas a servidores virtuais, pool e pool members;

6.3.20.40. Deve incluir métricas de throughtput, conexões, bits, pacotes, disponibilidade;

6.3.20.41. Deve incluir métricas de requisições, respostas;

6.3.20.42. Deve incluir métricas de criptografia, incluindo cifras, algoritmos, versão, conexões, bytes criptografados, bytes descriptografados;

6.3.20.43. Deve incluir métricas de certificados digitais, incluindo data de expiração, issuer e subject;

6.3.20.44. Deve incluir métricas relacionadas a CPU, memória, discos e interfaces;

6.3.20.45. 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;

6.3.20.46. Deve incluir informações de inventário (hostname, id, versão, localização, plataforma, chassi, módulos provisionados);

6.3.20.47. Deve incluir métricas do cluster, incluindo data de sincronização;

6.3.20.48. Deve incluir informações de data da última configuração aplicada;

6.3.20.49. Deve possuir documentação pública do fabricante contendo informações de configurações, exemplos de configuração e modelos de mensagens;

6.3.20.50. Implementar debugging utilizando CLI via console e SSH;

6.3.20.51. Possuir ferramenta interna nativa de captura de tráfego de rede com informações contextuais da solução inseridas em cada pacote/frame;

6.3.20.52. 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;

6.3.20.53. 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

6.3.20.54. Suportar exportação de informações de fluxos através sFlow, NetFlow, IPFIX ou outro protocolo similar;

6.3.20.55. Permitir a criação de códigos ou scripts capazes de manipular o tráfego, incluindo descartar, redirecionar, alterar, substituir e comparar valores e atributos, a partir de informações extraídas da conexão, sessão e protocolos;

6.3.20.56. Permitir utilizar listas de dados como fonte de dados por um script para validar se as conexões a serem estabelecidas obedecem a um dos critérios contidos nessa base de dados;

6.3.20.57. Implementar roteamento IPv4 e IPv6 estático e dinâmico;

6.3.20.58. 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;

6.3.20.59. Permitir que cada domínio de roteamento utilize BGP, OSPF e RIP em IPv4 e IPv6;

6.3.20.60. Suportar integração via BGP para divulgação de prefixos;

6.3.20.61. 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;

6.3.20.62. Suportar Equal Cost Multipath (ECMP);

6.3.20.63. Implementar Bidirectional Forward Detection (BFD);

6.3.21. Requisitos de balanceamento de carga estático e dinâmico

6.3.21.1. Deve implementar funções de entrega de aplicações através do balanceamento de servidores com qualquer hardware, sistema operacional e tipo de aplicação;

6.3.21.2. Suportar os protocolos HTTP/1.0, HTTP/1.1, HTTP/2 e HTTP/3, para comunicação com o cliente e comunicação com o servidor;

6.3.21.3. Implementar a reutilização de conexões entre a solução e os servidores, para diferentes clientes e diferentes requisições;

6.3.21.4. 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;

6.3.21.5. Implementar criptografia de cookies;

6.3.21.6. 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;

6.3.21.7. 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;

6.3.21.8. 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;

6.3.21.9. 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;

6.3.21.10. Suportar balanceamento de carga de servidores SIP para VoIP;

6.3.21.11. Permitir limitar o número de conexões estabelecidas com cada servidor real;

6.3.21.12. Permitir limitar o número de conexões estabelecidas com cada servidor virtual;

6.3.21.13. Implementar Network Address Translation (NAT) do IP do servidor;

6.3.21.14. Implementar Network Address Translation (NAT) do IP do cliente;

6.3.21.15. Implementar proteção contra Denial of Service (DoS) em camada 3, 4 e 7;

6.3.21.16. Implementar proteção contra SYN floods;

6.3.21.17. Suportar servidores virtuais com endereço IPv4 e os servidores reais com endereços IPv6;

6.3.21.18. 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;

6.3.21.19. Suportar Stream Control Transmission Protocol (SCTP);

6.3.21.20. Implementar aceleração de TLS com instalação do certificado digital na solução, troca de chaves e criptografia dos dados;

6.3.21.21. Permitir recriptografar a conexão entre a solução e o servidor;

6.3.21.22. Permitir espelhamento de tráfego de conexões TLS;

6.3.21.23. 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;

6.3.21.24. Em relação ao tráfego TLS, deve suportar:

6.3.21.24.1. Autenticação do servidor pelo cliente, apresentando um certificado previamente configurado;

6.3.21.24.2. Autenticação do cliente pela solução, através da solicitação e verificação do certificado fornecido pelo cliente;

6.3.21.24.3. 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;

6.3.21.25. Encaminhar ao servidor real via cabeçalho HTTP todo o certificado utilizado pelo cliente para se autenticar;

6.3.21.26. Encaminhar ao servidor real via cabeçalho HTTP atributos específicos do certificado utilizado pelo cliente;

6.3.21.27. Suportar os algoritmos para sessões TLS:

6.3.21.27.1. SSL session cache Timeout;

6.3.21.27.2. Session Ticket;

6.3.21.27.3. OCSP (Online Certificate Status Protocol) Stapling;

6.3.21.27.4. Dynamic Record Sizing;

6.3.21.27.5. ALPN (Application Layer Protocol Negotiation);

6.3.21.27.6. Perfect Forward Secrecy;

6.3.21.28. Suportar múltiplos certificados digitais no mesmo servidor virtual, com identificação via SNI (Server Name Indication);

6.3.21.29. Suportar importação de certificados digitais e chaves privadas;

6.3.21.30. Possuir alertas visuais na interface web de certificados com vencimento próximo;

6.3.21.31. Implementar limpeza de cabeçalho HTTP;

6.3.21.32. Implementar compressão de conteúdo HTTP, suportar os algoritmos gzip e deflate e permitir definir compressão especificamente para certos tipos de objetos;

6.3.21.33. 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;

6.3.21.34. 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;

6.3.21.35. 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;

6.3.21.36. 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;

6.3.21.37. Permitir exportar eventos de acesso para servidores externos com configuração das informações exportadas;

6.3.21.38. Permitir a configuração de autenticação e autorização de clientes HTTP, através de base LDAP, RADIUS e certificados digitais;

6.3.21.39. 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;

6.3.21.40. Suportar, pelo menos, as plataformas Kubernetes “Vanilla”, Red Hat OpenShift e VMware Tanzu;

6.3.21.41. Permitir a configuração através de ConfigMaps;

6.3.21.42. Permitir a configuração através de Custom Resource Definition (CRD) da solução;

6.3.21.43. Permitir a configuração através de objetos de serviço (Service) do tipo LoadBalancer na plataforma;

6.3.21.44. Permitir a configuração através de objetos Ingress na plataforma;

6.3.21.45. Permitir a configuração através de objetos Route no OpenShift;

6.3.21.46. Permitir incluir serviços de entrega de aplicações da solução, tais como SSL Offload e proteção de aplicações;

6.3.21.47. 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;

6.3.21.48. Suportar o protocolo FTP com, pelo menos, as seguintes características:

6.3.21.49. Determinar os comandos FTP permitidos;

6.3.21.50. Requests FTP anônimos;

6.3.21.51. Validar conformidade com o protocolo FTP;

6.3.21.52. Proteger contra ataques de força bruta nos logins;

6.3.21.53. Suportar o protocolo SMTP com, pelo menos, as seguintes características

6.3.21.54. Limitar o número de mensagens;

6.3.21.55. Validar registro SPF do DNS;

6.3.21.56. Determinar quais métodos SMTP podem ser utilizados.

6.3.22. Requisitos de Firewall de Aplicações Web – Web Application Firewall (WAF)

6.3.22.1. Os requisitos mínimos exigidos neste subitem são necessários para promover a proteção de aplicações web ataques mal-intencionados e tráfego de internet indesejado, incluindo bots, injeção e negação de serviço da camada de aplicações (DoS). Também são necessários para estabelecer e gerenciar regras para evitar ameaças pela internet, incluindo endereços IP, cabeçalhos HTTP, corpo HTTP, strings de URI, XSS (cross-site scripting), injeção de SQL e outras vulnerabilidades.

6.3.22.2. Implementar proteção para aplicações web e API contra ameaças na camada de aplicação;

6.3.22.3. Possuir tecnologia para mitigação de DDoS em camada 7 a partir de análises comportamentais;

6.3.22.4. Implementar ajustes automáticos e adaptativos de limiares de DoS;

6.3.22.5. Permitir a captura automática do tráfego relativo a ataquesDoS em camada 7, web scraping e força bruta;

6.3.22.6. Implementar proteção para aplicações web contra ameaças listadas no OWASP Top 10 2021;

6.3.22.7. Implementar modelo positivo de segurança de aplicações web;

6.3.22.8. Implementar modelo negativa de segurança, ou seja, adotar assinatura de ataques, ameaças e exploração de vulnerabilidade, de aplicações web;

6.3.22.9. Possuir conjuntos de configurações de segurança pré-definidas para configuração rápida de políticas;

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

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

6.3.22.12. Permitir desativar a inspeção para URL específicas;

6.3.22.13. Implementar identificação do usuário da aplicação web, mantendo a identificação até que o usuário tenha deixado o aplicativo;

6.3.22.14. Permitir a integração com firewall de banco de dados;

6.3.22.15. Suportar aplicações que utilizam protocolo WebSocket;

6.3.22.16. 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;

6.3.22.17. Implementar proteção contra:

6.3.22.17.1. Acesso por força bruta;

6.3.22.17.2. DoS e DDoS em camada 7;

6.3.22.17.3. Buffer Overflow;

6.3.22.17.4. Cross Site Request Forgery (CSRF);
6.3.22.17.5. Cross-Site Scripting (XSS);
6.3.22.17.6. Server-Side Request Forgery (SSRF);
6.3.22.17.7. SQL Injection;
6.3.22.17.8. Parameter tampering;
6.3.22.17.9. Cookie poisoning;
6.3.22.17.10. HTTP Request Smuggling;
6.3.22.17.11. Manipulação de campos escondidos (hidden input);
6.3.22.17.12. Manipulação de cookies;
6.3.22.17.13. Roubo de sessão através de manipulação de cookies;
6.3.22.17.14. Sequestro de sessão;
6.3.22.17.15. Validação de consistência de formulários;
6.3.22.17.16. Validação do cabeçalho do “user-agent” para identificar clientes inválidos;
6.3.22.18. Permitir especificar quais URLs devem ser utilizadas para proteção contra CSRF (Cross-Site Request Forgery);
6.3.22.19. Suportar codificação HTML "application/x-www-form-urlencoded";
6.3.22.20. Suportar HTTP Batched Request com proteções e assinaturas considerando individualmente URIs, cabeçalhos e conteúdo;
6.3.22.21. Suportar codificação fragmentada (chunked encoding);
6.3.22.22. Suportar validações de protocolo:
6.3.22.22.1. Restrição de métodos;
6.3.22.22.2. Restrição de protocolos e versões;
6.3.22.22.3. Validação de conformidade com RFCs;
6.3.22.22.4. Validação de caracteres URL-encoded;
6.3.22.22.5. Validação de codificação fora de padrão %uXXYY.

6.3.22.23. Suportar validações de HTML com nome de parâmetros, tamanho e tipo dos valores de parâmetros e combinação de nome, tipo e tamanho de parâmetros;

6.3.22.24. Possuir técnicas de detecção de evasões:

6.3.22.24.1. URL-decoding;

6.3.22.24.2. Terminação Null Byte String;

6.3.22.24.3. Paths autorreferenciados;

6.3.22.24.4. Case de caracteres misturados;

6.3.22.24.5. Uso excessivo de espaços em branco;

6.3.22.24.6. Decodificação de entidades HTML;

6.3.22.24.7. Caracteres de escape;

6.3.22.25. Permitir a inspeção externa de arquivos enviados por usuários (upload) para os servidores de aplicação utilizando Internet Content Adaptation Protocol (ICAP);

6.3.22.26. Capacidade de filtrar cabeçalhos, corpo e status de respostas;

6.3.22.27. Permitir o uso do parâmetro HTTP X-Forwarded-For como parte da política de controle;

6.3.22.28. Implementar validação de URL;

6.3.22.29. Validação de métodos HTTP utilizados (GET, POST, HEAD, OPTIONS, PUT, TRACE, DELETE, CONNECT) por URL;

6.3.22.30. 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;

6.3.22.31. Suportar aplicações Single-Page Application (SPA);

6.3.22.32. Permitir a customização da resposta de bloqueio;

6.3.22.33. Permitir a configuração de lista de exceções temporárias ou permanentes de endereços IP bloqueados;

6.3.22.34. Permitir adicionar, automaticamente e manualmente, em uma lista de bloqueio, os endereços IP de origem que ultrapassarem limites estabelecido, por um período configurável;

6.3.22.35. Implementar as proteções:

6.3.22.35.1. Proteção contra exposição de informações do ambiente e servidores internos como, sistema operacional e servidor web;

6.3.22.35.2. Ocultar qualquer mensagem de erro HTTP dos usuários;

6.3.22.35.3. Remover as mensagens de erro às páginas que serão enviadas aos usuários;

6.3.22.35.4. Suportar políticas por geolocalização para restrição de acesso a determinados países;

6.3.22.36. Implementar aprendizado automático para identificação da estrutura da aplicação, incluindo URLs, parâmetros URLs, campos de formulários, tipo de dado, tamanho de caracteres, cookies;

6.3.22.37. O aprendizado deve ser capaz de diferenciar atributos com o mesmo nome, mas presentes em URLs diferentes;

6.3.22.38. Implementar aprendizado automático de XML;

6.3.22.39. Permitir a importação de arquivo de esquema XML;

6.3.22.40. Implementar aprendizado automático de JSON;

6.3.22.41. Permitir a importação de arquivo de esquema JSON;

6.3.22.42. Permitir a criação automática de políticas, onde a política de segurança é criada e atualizada automaticamente baseando-se no tráfego real;

6.3.22.43. O perfil aprendido de forma automatizada pode ser ajustado, editado ou bloqueado;

6.3.22.44. Implementar detecção e mitigação de ameaças e ataques com base em assinaturas de ataques, com atualização periódica e automática da base de assinaturas;

6.3.22.45. As assinaturas devem ser atualizadas durante o período do contrato, sem custo adicional;

6.3.22.46. Não serão aceitas soluções que definem assinaturas como sendo uma base de reputação de IP;

6.3.22.47. 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;

6.3.22.48. Permitir a configuração automática de assinaturas com base em uma lista interna de tecnologias utilizadas pela aplicação;

6.3.22.49. Permitir desabilitar assinaturas específicas para determinados parâmetros, se comportando como exceção da configuração geral da política;

6.3.22.50. 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;

6.3.22.51. Possuir assinaturas de ataques para conteúdo em JSON e XML;

6.3.22.52. Possuir proteções contra XML Bomb;

6.3.22.53. 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;

6.3.22.54. 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;

6.3.22.55. 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;

6.3.22.56. Permitir apenas registrar o ataque, sem tomar nenhuma ação de bloqueio;

6.3.22.57. Implementar detecção com base no número de requisições por segundo enviados a uma URL específica;

6.3.22.58. Implementar detecção com base no número de requisições por segundo enviados de um IP específico;

6.3.22.59. Implementar detecção com base na validação do cliente através de código executado no navegador para identificação de bots;

6.3.22.60. Implementar detecção com base no aumento de um determinado percentual do número de transações por segundo (TPS);

6.3.22.61. Implementar detecção com base no aumento de carga e latência do servidor de aplicação;

6.3.22.62. Implementar detecção com base no número máximo de transações por segundo de um determinado IP;

6.3.22.63. 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;

6.3.22.64. Implementar mitigação de ataques DDoS através de assinaturas dinâmicas em tempo real para proteção da aplicação;

6.3.22.65. 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;

6.3.22.66. Identificar ataques com diferentes usuários e mesma origem;

6.3.22.67. Identificar ataques com diferentes origens e mesmo usuário;

6.3.22.68. Identificar ataques de forma global, considerando a quantidade de tentativas e implementando contramedidas de forma global para a política;

6.3.22.69. Possuir funcionalidade para integração com listas externas de credenciais expostas para mitigar ataques Credential Stuffing e Password Sprawl;

6.3.22.70. 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;

6.3.22.71. 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;

6.3.22.72. Implementar detecção e mitigação para proteção contra bots através da combinação de desafios enviados ao navegador do usuário e técnicas avançadas de análise;

6.3.22.73. Não serão aceitas soluções que utilizam apenas o user-agent para detecção de bots;

6.3.22.74. Implementar proteção proativa de ataques automatizados por bots e outras ferramentas, como web scrapers.

6.3.22.75. Possuir atualização automática de definição de bots;

6.3.22.76. Permitir a configuração de bloqueio e permissão de bots benignos conhecidos, como Google, Yahoo! e Microsoft Bing;

6.3.22.77. Permitir a criação de definições de bots;

6.3.22.78. Implementar proteção de APIs através da imposição de regras de endpoint e métodos permitidos;

6.3.22.79. Permitir a configuração de quotas e rate limits para chamadas em APIs de forma global na política;

6.3.22.80. Permitir a configuração de quotas e rate limits para chamadas em APIs por endpoint;

6.3.22.81. Permitir configurar exceções as regras de rate limits para chamadas na API;

6.3.22.82. Implementar proteção de conteúdo no formato JSON (JavaScript Object Notation);

6.3.22.83. 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;

6.3.22.84. 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;

6.3.22.85. Implementar funcionalidade de autenticação e autorização de clientes de API utilizando, pelo menos, os métodos HTTP Basic e OAuth 2.0;

6.3.22.86. 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;

6.3.22.87. 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;

6.3.22.88. Implementar funcionalidade para ocultar erros de aplicação ou infraestrutura do usuário;

6.3.22.89. Permitir a configuração de fluxo de navegação da aplicação, de forma que um usuário só pode alcançar determinada URL se passar por outras anteriormente;

6.3.22.90. Permitir a correção de um falso positivo através da aceitação da requisição e atualização da política de forma automática;

6.3.22.91. Possuir um nível severidade de violação de múltiplos níveis para fácil identificação de violações de maior e menor prioridade;

6.3.22.92. Implementar um identificador único para cada requisição tratada pela solução;

6.3.22.93. Permitir o armazenamento local de eventos e exportação para servidores externos;

6.3.22.94. Permitir configurar a retenção dos eventos por tempo e volume;

6.3.22.95. Implementar a detecção, remoção ou codificação de dados sensíveis dos eventos como, por exemplo, números de cartão de crédito, CPF e senhas;

6.3.22.96. Implementar a criptografia de parâmetros específicos da aplicação, tais como credenciais e dados sensíveis, sem a

necessidade de atualizar a aplicação. Esta criptografia de dados deve ser implementada no payload do HTTP, ou seja, nos dados propriamente ditos e não apenas via protocolo de transporte/túnel (TCP/TLS);

6.3.22.97. Implementar a ofuscação do nome de um parâmetro sensível da aplicação utilizando caracteres aleatórios, devendo ser mudado frequentemente pela solução para dificultar ataques direcionados;

6.3.22.98. Possuir API REST para configuração de servidores virtuais, políticas de segurança, parâmetros, perfis e demais configurações;

6.3.22.99. Permitir exportar as políticas de segurança para arquivos texto, JSON ou XML;

6.3.22.100. 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;

6.3.22.101. 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;

6.3.22.102. Implementar funcionalidade de forma nativa na solução ou possuir integração com serviço em nuvem do mesmo;

6.3.22.103. Implementar proteção de aplicações web, de dispositivos móveis e APIs;

6.3.23. Requisitos de relatórios e dashboards do Firewall de Aplicações Web

6.3.23.1. Possuir relatórios do serviço de DNS incluindo tendência de latência de resposta de DNS, nomes de domínios de DNS mais requisitados, tendência de uso do cache de DNS, clientes de DNS, clientes por domínio de DNS, taxa de consultas de DNS por tipo de registro, taxa de consultas de DNS diária por servidor, pico de consultas diárias de DNS por servidor, NXDOMAIN, SERVFAIL enviados e recebidos, nomes de domínios com conteúdo malicioso, principais domínios maliciosos;

6.3.23.2. Possuir relatórios de proteção do serviço de DNS, incluindo eventos por período, eventos por severidade, eventos por regra, eventos por tendência e eventos por categoria;

6.3.23.3. Suportar a exportação de eventos de DNS utilizando IPFIX;

6.3.23.4. Deve possuir relatórios com a detecção e mitigação dos ataques, incluindo a consolidação através de relatórios analíticos de DoS;

6.3.23.5. Possuir relatório de ataques DDoS com indicação de início e fim do ataque;

6.3.23.6. Possuir relatório em tempo real sobre ataques DDoS, atualizado automaticamente;

6.3.23.7. Possuir relatório de ataques DDoS incluindo quantidade de eventos e severidade, ataques por protocolo, incluindo assinaturas utilizadas e serviços mais afetados;

6.3.23.8. Possuir relatórios de ataques DDoS incluindo a origem dos ataques, país, requisições por segundo, gatilho da proteção e mitigação adotada;

6.3.23.9. Suportar a exportação de eventos de DoS utilizando IPFIX;

6.3.23.10. Possuir painel de acompanhamento de adoção de proteções contra ameaças mais comuns, de acordo com OWASP Top 10 2021;

6.3.23.11. Possuir relatório de desempenho da solução, incluindo processamento total e por servidor virtual protegido;

6.3.23.12. Possuir relatórios consolidados de ataques incluindo, pelo menos, resumo geral com as políticas ativas, anomalias e estatísticas de tráfego, ataques DoS,ataques de força bruta, ataques de bots, violações, URL, endereços IP, países e severidade;

6.3.23.13. Possuir relatório de incidentes com violações detectadas e correlacionadas, separando falsos positivos de atividades maliciosas e para facilitar a resposta a incidentes;

6.3.23.14. Implementar monitoração e análise de performance de aplicações web;

6.3.23.15. Possuir relatórios de métricas de aplicações, incluindo transações por segundo, tempo de reposta, latência do cliente e servidor, throughput de requisição e resposta e sessões;

6.3.23.16. Possuir relatórios de análises históricas detalhamento do tempo de resposta total de carregamento de uma URL e página e correlação de métricas de uso de rede com o comportamento das aplicações para auxiliar processos de manutenções preventivas, de troubleshooting, de planejamento de capacidade e de análise da experiência dos usuários finais no acesso das aplicações;

6.3.23.17. Possuir relatórios para análise de dados por aplicações, por URL, por clientes e por servidores, permitindo assim a identificação mais precisa dos eventuais ofensores do tráfego suportado pela solução;

6.3.23.18. Possuir relatórios para análise de estatísticas de acesso, incluindo métodos HTTP, sistema operacional e navegadores;

6.3.23.19. Permitir exportar as requisições que contém os ataques, pelo menos nos formatos PDF e binário

6.3.23.20. Possuir relatório de ataques DoS em camada 7 com indicação de início e fim do ataque;

6.3.23.21. Possuir relatório em tempo real sobre ataques DoS em camada 7, atualizado automaticamente;

6.3.23.22. Possuir relatório que permite avaliar o impacto de ataques DoS em camada 7 na performance do servidor;

6.3.24. Requisitos técnicos da solução para proteção de Endpoints

6.3.24.1. Características Gerais da Solução de proteção e segurança para Endpoints

6.3.24.1.1. A solução ofertada deverá atender integralmente os requisitos especificados neste documento devendo ser fornecida com todas as licenças necessárias para entrega funcional da solução e completo funcionamento dos recursos contratados.

6.3.24.1.2. A solução ofertada não pode ser do tipo comunidade, software livre, ou possuir componentes e módulos sem suporte oficial do fabricante.

6.3.24.1.3. A solução ofertada deverá possuir todos os produtos na versão estável mais atual do produto, não serão aceitos produtos obsoletos ou fora de linha de produção do fabricante.

6.3.24.1.4. O software deve dispor de gerenciamento com administração centralizada, com facilidades para instalação, administração, monitoramento, atualização e

configuração, com todos os módulos de um único fornecedor sendo disponibilizada on-premisse;

6.3.24.1.5. A solução ofertada deverá possuir módulo de detecção e respostas (EDR);

6.3.24.1.6. A solução ofertada deverá possuir módulo de detecção e resposta gerenciada (MDR);

6.3.24.2. Do Módulo de Proteção de Endpoint

6.3.24.2.1. A solução proposta deverá proteger os sistemas operacionais abaixo:

6.3.24.2.1.1. Windows 7

6.3.24.2.1.2. Windows 8

6.3.24.2.1.3. Windows 8.1

6.3.24.2.1.4. Windows 10

6.3.24.2.1.5. Windows 11

6.3.24.2.2. Servidores:

6.3.24.2.2.1. Windows Small Business Server 2011

6.3.24.2.2.2. Windows MultiPoint Server 2011

6.3.24.2.2.3. Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022

6.3.24.2.3. Servidores de terminal Microsoft:

6.3.24.2.3.1. Serviços de Área de Trabalho Remota da Microsoft baseados no Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022

6.3.24.2.4. Sistemas operacionais Linux de 32 bits:

6.3.24.2.4.1. CentOS 6.7 e posterior

6.3.24.2.4.2. Debian GNU/Linux 11.0 e posterior

6.3.24.2.4.3. Debian GNU/Linux 12.0 e posterior

6.3.24.2.4.4. Red Hat Enterprise Linux 6.7 e posterior

6.3.24.2.5. Sistemas operacionais Linux de 64 bits:

6.3.24.2.5.1. Amazon Linux 2.
6.3.24.2.5.2. CentOS 6.7 e mais tarde
6.3.24.2.5.3. CentOS 7.2 e posterior.
6.3.24.2.5.4. CentOS Stream 8.
6.3.24.2.5.5. CentOS Stream 9.
6.3.24.2.5.6. Debian GNU/Linux 11.0 e posterior.
6.3.24.2.5.7. Debian GNU/Linux 12.0 e posterior.
6.3.24.2.5.8. Linux Mint 20.3 e superior.
6.3.24.2.5.9. Linux Mint 21.1 e posterior.
6.3.24.2.5.10. openSUSE Leap 15.0 e posterior.
6.3.24.2.5.11. Oracle Linux 7.3 e posterior.
6.3.24.2.5.12. Oracle Linux 8.0 e posterior.
6.3.24.2.5.13. Oracle Linux 9.0 e posterior.
6.3.24.2.5.14. Red Hat Enterprise Linux 6.7 e posterior
6.3.24.2.5.15. Red Hat Enterprise Linux 7.2 e posterior.
6.3.24.2.5.16. Red Hat Enterprise Linux 8.0 e posterior.
6.3.24.2.5.17. Red Hat Enterprise Linux 9.0 e posterior.
6.3.24.2.5.18. Rocky Linux 8.5 e posterior.
6.3.24.2.5.19. Rocky Linux 9.1.
6.3.24.2.5.20. SUSE Linux Enterprise Server 12.5 ou posterior.
6.3.24.2.5.21. SUSE Linux Enterprise Server 15 ou posterior.
6.3.24.2.5.22. Ubuntu 20.04 LTS.
6.3.24.2.5.23. Ubuntu 22.04 LTS.
6.3.24.2.5.24. Sistemas operacionais Arm de 64 bits:
6.3.24.2.5.25. CentOS Stream 9.
6.3.24.2.5.26. SUSE Linux Enterprise Server 15.
6.3.24.2.5.27. Ubuntu 22.04 LTS.

6.3.24.2.6. Sistemas operacionais MAC OS:

6.3.24.2.6.1. MacOS 12 – 14

6.3.24.2.7. Ferramentas de virtualização MAC OS:

6.3.24.2.7.1. Parallels Desktop 16 para Mac Business Edition

6.3.24.2.7.2. VMware Fusion 11.5 Professional

6.3.24.2.7.3. VMware Fusion 12 Professional

6.3.24.2.8. A solução proposta deverá suportar as seguintes plataformas virtuais:

6.3.24.2.8.1. VMware Workstation 17.0.2 Pro

6.3.24.2.8.2. VMware ESXi 8.0 Update 2

6.3.24.2.8.3. Microsoft Hyper-V Server 2019

6.3.24.2.8.4. Citrix Virtual Apps e Desktop 7 2308

6.3.24.2.8.5. Citrix Provisioning 2308

6.3.24.2.8.6. Citrix Hypervisor 8.2 Update 1

6.3.24.3. Do Módulo de Gerenciamento Avançado:

6.3.24.3.1. A solução proposta deve suportar arquitetura cloud-native e on-premisse;

6.3.24.3.2. A solução proposta deve incluir suporte para implantação baseada em nuvem por meio de:

6.3.24.3.2.1. Amazon Web Services

6.3.24.3.2.2. Microsoft Azure

6.3.24.3.3. A solução proposta deve incluir as seguintes opções de integração SIEM:

6.3.24.3.3.1. HP (Microfoco) ArcSight;

6.3.24.3.3.2. IBM QRadar;

6.3.24.3.3.3. Splunk;

6.3.24.3.3.4. Kaspersky KUMA.

6.3.24.3.4. A solução proposta deve fornecer a capacidade de integração com as soluções Managed Endpoint Detection and Response (MDR) e Anti-APT do próprio fornecedor,

para caça ativa a ameaças e resposta automatizada a incidentes.

6.3.24.3.5. A solução proposta deve ter a capacidade de permitir aplicações baseadas em seus certificados de assinatura digital, MD5, SHA256, metadados, caminho do arquivo e categorias de segurança pré-definidas;

6.3.24.3.6. A solução proposta deve suportar Single Sign On (SSO) usando NTLM e Kerberos.

6.3.24.3.7. O administrador deve ser capaz de adicionar manualmente novos dispositivos à lista de equipamentos ou editar informações sobre equipamentos já existentes na rede.

6.3.24.3.8. A solução proposta deve suportar API OPEN e incluir diretrizes para integração com sistemas externos de terceiros.

6.3.24.3.9. A solução proposta deve incluir uma ferramenta integrada para realizar diagnósticos remotos e coletar logs de solução de problemas sem exigir acesso físico ao computador.

6.3.24.3.10. A solução proposta deve incorporar no sensor de endpoint distribuição/retransmissão para transferir ou fazer proxy de solicitações de reputação de ameaças dos terminais para o servidor de gerenciamento.

6.3.24.3.11. A solução proposta deve suportar o download de arquivos diferenciais em vez de pacotes completos de atualização.

6.3.24.3.12. A solução proposta deve incluir Role Based Access Control (RBAC) com funções predefinidas personalizáveis.

6.3.24.3.13. O servidor de gerenciamento primário da solução proposta deve ser capaz de retransmitir atualizações e serviços de reputação em nuvem.

6.3.24.3.14. O servidor de gerenciamento da solução proposta deve ter funcionalidade para criar múltiplos perfis dentro de uma política de proteção com diferentes configurações de proteção que possam estar simultaneamente ativas em uns único/múltiplos dispositivos com base nas seguintes regras de ativação:

6.3.24.3.14.1. Status do dispositivo

6.3.24.3.14.2. Tag

6.3.24.3.14.3. Diretório ativo

6.3.24.3.14.4. Proprietários de dispositivos

6.3.24.3.14.5. Hardware

6.3.24.3.15. A solução proposta deve suportar os seguintes canais de entrega de notificação:

6.3.24.3.15.1. E-mail

6.3.24.3.15.2. Registro de sistema

6.3.24.3.15.3. SMS

6.3.24.3.16. A solução proposta deve ter a capacidade de etiquetar/marcar computadores com base em:

6.3.24.3.16.1. Atributos de rede

6.3.24.3.16.2. Nome

6.3.24.3.16.3. Domínio e/ou Sufixo de Domínio

6.3.24.3.16.4. Endereço de IP

6.3.24.3.16.5. Endereço IP para servidor de gerenciamento

6.3.24.3.16.6. Localização no Active Directory

6.3.24.3.16.7. Unidade organizacional

6.3.24.3.16.8. Grupo

6.3.24.3.16.9. Sistema operacional

6.3.24.3.16.10. Número do pacote de serviço

6.3.24.3.16.11. Arquitetura Virtual

6.3.24.3.16.12. Registro de aplicativos

6.3.24.3.16.13. Nome da Aplicação

6.3.24.3.16.14. Versão do aplicativo

6.3.24.3.16.15. Fabricante

6.3.24.3.16.16. Tipo e versão

6.3.24.3.16.17. Arquitetura

6.3.24.3.17. A solução proposta deve ter a capacidade de criar/definir configurações com base na localização de um computador na rede, e não no grupo ao qual pertence no servidor de gestão.

6.3.24.3.18. A solução proposta deve ter a funcionalidade de adicionar um mediador de conexão unidirecional entre o servidor de gerenciamento e o endpoint conectado pela internet/rede pública.

6.3.24.3.19. As informações sobre o equipamento deverão ser atualizadas após cada nova pesquisa na rede. A lista de equipamentos detectados deve abranger o seguinte:

6.3.24.3.19.1. Dispositivos Desktop/Servidores

6.3.24.3.19.2. Dispositivos móveis

6.3.24.3.19.3. Dispositivos de rede

6.3.24.3.19.4. Dispositivos virtuais

6.3.24.3.19.5. Componentes OEM

6.3.24.3.19.6. Periféricos de computador

6.3.24.3.19.7. Dispositivos IoT conectados

6.3.24.3.19.8. Telefones VoIP

6.3.24.3.19.9. Repositórios de rede

6.3.24.3.20. A solução proposta deve permitir ao administrador criar categorias/grupos de aplicação com base em:

6.3.24.3.20.1. Nome da Aplicação

6.3.24.3.20.2. Caminho do aplicativo

6.3.24.3.20.3. Metadados do aplicativo

6.3.24.3.20.4. Aplicativo Certificado digital

6.3.24.3.20.5. Categorias de aplicativos predefinidas pelo fornecedor

6.3.24.3.20.6. SHA256 e MD5

6.3.24.3.21. A solução proposta deverá permitir especificamente o bloqueio dos seguintes dispositivos:

6.3.24.3.21.1. Bluetooth

6.3.24.3.21.2. Dispositivos móveis

6.3.24.3.21.3. Modems externos

6.3.24.3.21.4. CD/DVD

6.3.24.3.21.5. Câmeras e scanners

6.3.24.3.21.6. MTPs

6.3.24.3.21.7. E a transferência de dados para dispositivos móveis

6.3.24.3.22. A solução proposta deve ter capacidade de ler informações do Active Directory para obter dados sobre contas de computadores na organização.

6.3.24.3.23. A solução proposta deve ter funcionalidade integrada para conectar-se remotamente ao endpoint usando a tecnologia Windows Desktop Sharing. Além disso, a solução deve ser capaz de manter a auditoria das ações do administrador durante a sessão.

6.3.24.3.24. A solução proposta deverá possuir a funcionalidade de criar uma estrutura de grupos de administração utilizando a hierarquia de Grupos, com base nos seguintes dados:

6.3.24.3.24.1. Estruturas de domínios e grupos de trabalho do Windows

6.3.24.3.24.2. Estruturas de grupos do Active Directory

6.3.24.3.24.3. Conteúdo de um arquivo de texto criado manualmente pelo administrador

6.3.24.3.25. A solução proposta deve ser capaz de recuperar informações sobre os equipamentos detectados durante uma pesquisa na rede. O inventário resultante deverá abranger todos os equipamentos conectados à rede da organização.

6.3.24.3.26. A solução proposta deve permitir realizar as seguintes ações para endpoints:

6.3.24.3.26.1. Verificação manual;

6.3.24.3.26.2. Verificação no acesso;

6.3.24.3.26.3. Verificação por demanda;

6.3.24.3.26.4. Verificação de arquivos compactados

6.3.24.3.26.5. Verificação de arquivos individuais, pastas e unidades;

6.3.24.3.26.6. Bloqueio e verificação de scripts

6.3.24.3.26.7. Proteção contra alteração de registros;

6.3.24.3.26.8. Proteção contra estouro de buffer;

6.3.24.3.26.9. Verificação em segundo plano/inativa

6.3.24.3.27. Verificação de unidade removível na conexão com o sistema;

6.3.24.3.28. A solução proposta deve suportar a instalação do sensor de endpoint juntamente com soluções de terceiros, seja utilizando somente o módulo de EDR ou anti-malware.

6.3.24.3.29. O servidor de gerenciamento da solução proposta deve manter um histórico de revisões das políticas,

tarefas, pacotes, grupos de gerenciamento criados, para que modificações em uma determinada política/tarefa possam ser revisadas.

6.3.24.3.30. A solução proposta deve ter a capacidade de definir um intervalo de endereços IP, de forma a limitar o tráfego do cliente para o servidor de gestão com base no tempo e na velocidade.

6.3.24.3.31. A solução proposta deve ter a capacidade de realizar inventário em scripts e arquivos, tais como: dll, exe, bat e etc.

6.3.24.3.32. A solução proposta deve prever a criação de uma cópia de segurança do sistema de administração com o auxílio de ferramentas integradas do sistema de administração.

6.3.24.3.33. A solução proposta deve suportar Windows Failover Cluster.

6.3.24.3.34. A solução proposta deve ter um recurso de clustering integrado.

6.3.24.3.35. A solução proposta deve incluir alguma forma de sistema para controlar epidemias de vírus.

6.3.24.3.36. A solução proposta deve incluir Role Based Access Control (RBAC), e isso deve permitir que as restrições sejam replicadas em todos os servidores de gerenciamento na hierarquia.

6.3.24.3.37. O servidor de gestão da solução proposta deverá incluir funções de segurança pré-definidas para o Auditor, Supervisor e Oficial de Segurança.

6.3.24.3.38. A solução proposta deve permitir ao administrador criar um túnel de conexão entre um dispositivo cliente remoto e o servidor de gerenciamento caso a porta usada

para conexão ao servidor de gerenciamento não esteja disponível no dispositivo.

6.3.24.3.39. A solução proposta deve ter a capacidade de priorizar rotinas de varredura personalizadas e sob demanda para estações de trabalho Linux.

6.3.24.3.40. A solução proposta deve ser capaz de registrar operações de arquivos (Escrita e Exclusão) em dispositivos de armazenamento USB.

6.3.24.3.41. A solução proposta deve ter capacidade de bloquear a execução de qualquer executável do dispositivo de armazenamento USB.

6.3.24.3.42. A solução proposta deve contar com filtragem de firewall por endereço local, interface física e Time-To-Live (TTL) de pacotes.

6.3.24.3.43. A solução proposta deverá possuir controles para download de DLL e drivers.

6.3.24.3.44. A solução proposta deve ter a capacidade de restringir as atividades do aplicativo dentro do sistema de acordo com o nível de confiança atribuído ao aplicativo e de limitar os direitos dos aplicativos de acessar determinados recursos, incluindo arquivos do sistema e do usuário utilizando de módulo especifico de prevenção de intrusão.

6.3.24.3.45. A solução proposta deve ter a capacidade de excluir automaticamente as regras de controle de aplicativos se um aplicativo não for iniciado durante um intervalo especificado. O intervalo deve ser configurável.

6.3.24.3.46. A solução proposta deve incluir múltiplas formas de notificar o administrador sobre eventos importantes que ocorreram (notificação por e-mail, anúncio sonoro, janela pop-up, entrada de log).

6.3.24.3.47. A solução proposta deve incluir Controle de inicialização de aplicativos para o sistema operacional Windows Server.

6.3.24.3.48. A solução proposta deve distribuir automaticamente as contas de computador por grupo de gerenciamento caso novos computadores apareçam na rede. Deve fornecer a capacidade de definir as regras de transferência de acordo com o endereço IP, tipo de sistema operacional e localização nas Unidades Organizacionais do Active Directory.

6.3.24.3.49. A solução proposta deve permitir o teste de atualizações baixadas por meio do software de administração centralizado antes de distribuí-las às máquinas dos clientes e a entrega das atualizações aos locais de trabalho dos usuários imediatamente após recebê-las.

6.3.24.3.50. A solução proposta deve permitir a criação de uma hierarquia de servidores de administração a um nível arbitrário e a capacidade de gerir centralmente toda a hierarquia a partir do nível superior.

6.3.24.3.51. A solução proposta deve suportar o Modo de Serviços Gerenciados para servidores de administração, para que instâncias de servidores de administração isoladas logicamente possam ser configuradas para diferentes usuários e grupos de usuários.

6.3.24.3.52. A solução proposta deve dar acesso aos serviços em nuvem do fornecedor de segurança anti-malware através do servidor de administração.

6.3.24.3.53. A solução proposta deve ser capaz de realizar inventários de software e hardware instalados nos computadores dos usuários.

6.3.24.3.54. A solução proposta deve ter um mecanismo de notificação para informar os usuários sobre eventos no software e nas configurações anti-malware instalados, e para distribuir notificações sobre eventos por e-mail.

6.3.24.3.55. A solução proposta deve permitir a instalação centralizada de aplicativos de terceiros em todos ou em computadores selecionados.

6.3.24.3.56. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de retransmissão de atualizações e pacotes de instalação, a fim de reduzir a carga da rede no sistema principal do servidor de administração.

6.3.24.3.57. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de encaminhamento de eventos do sensor de endpoint do grupo selecionado de computadores clientes para o servidor de administração centralizado, a fim de reduzir a carga da rede no sistema do servidor de administração principal.

6.3.24.3.58. A solução proposta deve ser capaz de gerar relatórios gráficos para eventos de software anti-malware e dados sobre inventário de hardware e software, licenciamento, etc.

6.3.24.3.59. A solução proposta deve permitir que o administrador defina configurações restritas nas configurações de política/perfil, para que uma tarefa de verificação de vírus possa ser acionada automaticamente quando um

determinado número de vírus for detectado durante um período de tempo definido. Os valores para o número de vírus e escala de tempo devem ser configuráveis.

6.3.24.3.60. A solução proposta deve permitir ao administrador personalizar relatórios.

6.3.24.3.61. A solução proposta deve ter a funcionalidade de detectar máquinas virtuais não persistentes e excluí-las automaticamente e seus dados relacionados do servidor de gerenciamento quando desligado.

6.3.24.3.62. A solução proposta deve permitir ao administrador definir um período de tempo após o qual um computador não conectado ao servidor de gerenciamento e seus dados relacionados serão automaticamente excluídos do servidor.

6.3.24.3.63. A solução proposta deve permitir ao administrador definir diferentes condições de mudança de status para grupos de endpoint no servidor de gerenciamento.

6.3.24.3.64. A solução proposta deve permitir que o administrador adicione ferramentas de gerenciamento de endpoint personalizadas/de terceiros ao servidor de gerenciamento.

6.3.24.3.65. A solução proposta deve ter um recurso/módulo integrado para coletar remotamente os dados necessários para solução de problemas dos endpoint, sem exigir acesso físico.

6.3.24.3.66. A funcionalidade 'Dispositivo desativado' deve estar disponível, para que tais dispositivos não sejam exibidos na lista de equipamentos.

6.3.24.3.67. O relatório da solução proposta deve incluir detalhes sobre quais componentes de proteção de endpoint estão

ou não instalados em dispositivos clientes, independentemente do perfil de proteção aplicado/existente para esses dispositivos;

6.3.24.3.68. O servidor de gerenciamento primário da solução proposta deve ser capaz de recuperar relatórios de informações detalhadas sobre o status de integridade, etc., dos terminais gerenciados dos servidores de gerenciamento secundários.

6.3.24.3.69. A solução proposta deve suportar integração com solução APT.

6.3.24.3.70. A solução proposta deve suportar a integração com o serviço Managed Detection and Response.

6.3.24.3.71. A solução *proposta deve permitir instalar o modulo de gerenciamento on-premisse nos seguintes sistemas* operacionais:

6.3.24.3.71.1. Windows

6.3.24.3.71.2. Linux

6.3.24.3.72. A solução proposta deverá suportar os seguintes servidores de banco de dados:

6.3.24.3.72.1. Windows:

6.3.24.3.72.1.1. Microsoft SQL Server

6.3.24.3.72.1.2. Microsoft Banco de dados SQL do Azure

6.3.24.3.72.1.3. MySQL Standard e Enterprise

6.3.24.3.72.1.4. MariaDB

6.3.24.3.72.1.5. PostgreSQL

6.3.24.3.72.2. Linux:

6.3.24.3.72.2.1. MySQL

6.3.24.3.72.2.2. MariaDB

6.3.24.3.72.2.3. PostgreSQL

6.3.24.3.73. A solução proposta deverá suportar as seguintes plataformas virtuais:

6.3.24.3.73.1. Windows:

6.3.24.3.73.1.1. VMware vSphere 6.7 e 7.0

6.3.24.3.73.1.2. Estação de trabalho VMware 16 Pro

6.3.24.3.73.1.3. Servidor Microsoft Hyper-V 2012 de 64 bits

6.3.24.3.73.1.4. Servidor Microsoft Hyper-V 2012 R2 de 64 bits

6.3.24.3.73.1.5. Microsoft Servidor Hyper -V 2016 de 64 bits

6.3.24.3.73.1.6. Servidor Microsoft Hyper-V 2019 de 64 bits

6.3.24.3.73.1.7. Servidor Microsoft Hyper-V 2022 de 64 bits

6.3.24.3.73.1.8. Citrix XenServer 7.1 LTSR

6.3.24.3.73.1.9. Citrix XenServer 8.x

6.3.24.3.73.1.10. Oracle VM VirtualBox 6.x

6.3.24.3.73.2. Linux:

6.3.24.3.73.2.1. VMware vSphere 6.7, 7.0 e 8.0

6.3.24.3.73.2.2. VMware Desktop 16 Pro e 17 Pro

6.3.24.3.73.2.3. Servidor Microsoft Hyper-V 2012 de 64 bits

6.3.24.3.73.2.4. Servidor Microsoft Hyper-V 2012 R2 de 64 bits

6.3.24.3.73.2.5. Microsoft Servidor Hyper -V 2016 de 64 bits

6.3.24.3.73.2.6. Servidor Microsoft Hyper-V 2019 de 64 bits

6.3.24.3.73.2.7. Servidor Microsoft Hyper-V 2022 de 64 bits

6.3.24.3.73.2.8. Citrix XenServer 7.1 e 8.x

6.3.24.3.73.2.9. Oracle VM VirtualBox 6.x e7.x

6.3.24.3.74. A solução proposta deve suportar criptografia em vários níveis:

6.3.24.3.74.1. Criptografia completa do disco – incluindo disco do sistema

6.3.24.3.74.2. Criptografia de arquivos e pastas

6.3.24.3.74.3. Criptografia de mídia removível

6.3.24.3.74.4. Gerenciamento de criptografia BitLocker e MacOS Filevault2

6.3.24.3.75. A solução proposta *deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita*:

6.3.24.3.75.1. A criptografia de arquivos em unidades de computador locais.

6.3.24.3.75.2. A criação de listas de criptografia de arquivos por extensão ou grupo de extensões.

6.3.24.3.75.3. A criação de listas criptografadas de pastas em unidades de computador locais.

6.3.24.3.76. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita a criptografia de arquivos em unidades removíveis. Isto deve incluir a capacidade de:

6.3.24.3.76.1. Especifique uma regra de criptografia padrão pela qual o aplicativo aplique a mesma ação a todas as unidades removíveis.

6.3.24.3.76.2. Configure regras de criptografia para arquivos armazenados em unidades removíveis individuais.

6.3.24.3.77. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que suporte vários modos de criptografia de arquivos para unidades removíveis:

6.3.24.3.77.1. A criptografia de todos os arquivos armazenados em unidades removíveis.

6.3.24.3.77.2. A criptografia de novos arquivos somente quando eles são salvos ou criados em unidades removíveis.

6.3.24.3.78. A solução proposta deve oferecer a funcionalidade Integrated File Level Encryption (FLE) que permite que os arquivos em unidades removíveis sejam criptografados em modo portátil. Deve permitir o acesso a arquivos criptografados em unidades removíveis conectadas a computadores sem funcionalidade de criptografia

6.3.24.3.79. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita a criptografia de todos os arquivos que aplicativos específicos possam criar ou modificar, tanto em discos rígidos quanto em unidades removíveis.

6.3.24.3.80. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita o gerenciamento de regras de acesso de aplicativos a arquivos criptografados, incluindo a definição de uma regra de acesso a arquivos criptografados para qualquer aplicativo. Deve permitir o bloqueio do acesso a arquivos criptografados ou permitir o acesso a arquivos criptografados apenas como texto cifrado.

6.3.24.3.81. A solução proposta deve oferecer a capacidade de restaurar dispositivos criptografados se um disco rígido ou unidade removível criptografado estiver corrompido.

6.3.24.3.82. A solução proposta deve oferecer a funcionalidade Integrated Full Disk Encryption (FDE) para discos rígidos e unidades removíveis. Tal como acontece com o FLE, deve haver a capacidade de especificar uma regra de criptografia padrão pela qual o aplicativo aplica a mesma ação a todas as unidades removíveis ou de configurar regras de criptografia para unidades removíveis individuais.

6.3.24.3.83. A solução proposta deve oferecer um módulo de criptografia gerenciado centralmente em todos os computadores, com capacidade de impor políticas de criptografia e modificar/interromper configurações de criptografia.

6.3.24.3.84. A solução proposta deve oferecer a capacidade de monitorar centralmente o status da criptografia e gerar relatórios sobre computadores/dispositivos criptografados.

6.3.24.3.85. A solução proposta deve oferecer criptografia totalmente transparente para os usuários finais e que não tenha impacto adverso no desempenho e na utilização do sistema.

6.3.24.3.86. A solução proposta deve oferecer criptografia completa de disco que suporte o gerenciamento centralizado de usuários autorizados, incluindo adição, remoção e redefinição de senha. Somente usuários autorizados devem ter permissão para inicializar o disco criptografado.

6.3.24.3.87. A solução proposta deve ter a capacidade de bloquear o acesso de aplicativos a dados criptografados, se necessário.

6.3.24.3.88. A solução proposta deverá suportar a encriptação automática de dispositivos de armazenamento amovíveis e deverá ser capaz de impedir a cópia de dados para suportes não encriptados.

6.3.24.3.89. A solução proposta deve proporcionar a possibilidade de criação de contentores protegidos por palavra-passe que possam ser utilizados para o intercâmbio de dados com utilizadores externos.

6.3.24.3.90. A solução proposta deve fornecer um local central para armazenamento de chaves de criptografia e múltiplas opções de recuperação.

6.3.24.3.91. O servidor administrador/gerenciador da solução proposta deve ter a capacidade de descriptografar todos os dados criptografados. independentemente da localização e/ou usuário.

6.3.24.3.92. A solução proposta deve suportar layouts de teclado QWERTY e AZERTY para autorização de pré-inicialização.

6.3.24.3.93. A solução proposta deve fornecer a funcionalidade para gerenciar/aplicar a criptografia do Microsoft Bit Locker.

6.3.24.3.94. A solução proposta deve fornecer a funcionalidade para personalizar as configurações de criptografia do Microsoft BitLocker, incluindo:

6.3.24.3.94.1. Uso do Trusted Platform Module e configurações de senha.

6.3.24.3.94.2. Uso de criptografia de hardware para estações de trabalho e criptografia de software se a criptografia de hardware não estiver disponível.

6.3.24.3.95. Uso de autenticação que exige entrada de dados em um ambiente de pré-inicialização, mesmo que a plataforma não tenha capacidade para entrada de pré-inicialização (por exemplo, com teclados touchscreen em tablets).

6.3.24.3.96. A solução proposta deve suportar criptografia em Microsoft Surface Tablets.

6.3.24.3.97. A solução proposta deverá incluir recursos para gerenciar computadores remotamente, incluindo:

6.3.24.3.97.1. Instalação remota de software de terceiros

6.3.24.3.97.2. Relatórios sobre software e hardware existentes

6.3.24.3.97.3. Monitoramento para instalação de software não autorizado

6.3.24.3.97.4. Remoção de software não autorizado

6.3.24.3.98. A solução proposta deverá incluir recursos de gerenciamento de patches para sistemas operacionais Windows e para aplicativos de terceiros instalados.

6.3.24.3.99. A funcionalidade de gerenciamento de patches da solução proposta deve ser totalmente automatizada, com capacidade de detectar, baixar e enviar patches ausentes para endpoints.

6.3.24.3.100. A solução proposta deve fornecer a possibilidade de selecionar quais patches serão baixados/enviados para os endpoints, com base em sua criticidade.

6.3.24.3.101. A solução proposta deve ser capaz de detectar vulnerabilidades existentes em sistemas operacionais e

outros aplicativos instalados e, em seguida, responder baixando/enviando automaticamente os patches necessários para os terminais.

6.3.24.3.102. A solução proposta deve fornecer relatórios abrangentes sobre vulnerabilidades descobertas e patches ausentes, bem como sobre endpoints e status de implantação de patches.

6.3.24.3.103. A solução proposta deve ter a capacidade de aplicar patches específicos com base na criticidade ou gravidade.

6.3.24.3.104. O servidor de gerenciamento da solução proposta deve ser configurável como uma fonte de atualizações para Microsoft Updates e aplicativos de terceiros.

6.3.24.3.105. A solução proposta deve incluir o aconselhamento sobre vulnerabilidade do fornecedor de aplicativos, bem como do fornecedor de segurança

6.3.24.3.106. A solução proposta deve permitir ao administrador aprovar atualizações.

6.3.24.3.107. A solução proposta deve ser capaz de identificar automaticamente patches ausentes em endpoints individuais e enviar apenas os que são necessários/ausentes.

6.3.24.3.108. A solução proposta deve suportar a agregação de patches para minimizar o número de atualizações necessárias.

6.3.24.3.109. A solução proposta deve notificar o administrador sobre quaisquer patches ausentes nos terminais assim que as informações relevantes estiverem disponíveis.

6.3.24.3.110. A solução proposta deverá proporcionar a possibilidade de gerir separadamente a aplicação de

patches para sistemas operativos e para aplicações de terceiros.

6.3.24.3.111. A solução proposta deverá proporcionar a possibilidade de corrigir vulnerabilidades existentes em qualquer ponto final ou apenas em pontos específicos.

6.3.24.3.112. A solução proposta deve fornecer a facilidade de detectar/instalar automaticamente todos os patches perdidos anteriormente que são necessários para aplicar o patch selecionado (dependências).

6.3.24.3.113. A solução proposta deve suportar a distribuição automatizada de patches e atualizações para mais de 150 aplicações.

6.3.24.3.114. A solução proposta deve ter funcionalidade de suporte ao modo de teste de patch.

6.3.24.3.115. A solução proposta deve incluir campos dedicados que contenham informações sobre 'Exploração encontrada para a vulnerabilidade'.

6.3.24.3.116. A solução proposta deve incluir campos dedicados que contenham informações sobre "Ameaça encontrada para a vulnerabilidade".

6.3.24.3.117. A solução proposta deve permitir que o administrador restrinja a capacidade dos usuários do dispositivo de aplicar eles próprios as atualizações da Microsoft.

6.3.24.3.118. A solução proposta deve permitir ao administrador especificar quais atualizações podem ser instaladas pelos usuários.

6.3.24.3.119. A solução proposta deve permitir ao administrador visualizar uma lista de atualizações e patches não relacionados aos dispositivos clientes.

6.3.24.3.120. A solução proposta deve apoiar a implantação do sistema operacional.

6.3.24.3.121. A solução proposta deve suportar Wake-on LAN e UEFI.

6.3.24.3.122. A solução proposta deve ter funcionalidade integrada de compartilhamento remoto de área de trabalho. Todas as operações de arquivo executadas no endpoint remoto durante a sessão devem ser registradas no Management Server.

6.3.24.3.123. A solução proposta deve ser capaz de fornecer correções de vulnerabilidades aos computadores clientes sem instalar as atualizações.

6.3.24.3.124. A solução proposta deve permitir que o administrador escolha as atualizações do Windows a serem instaladas, após o que o usuário do dispositivo cliente poderá instalar apenas as atualizações permitidas/selecionadas pelo administrador.

6.3.24.3.125. A solução proposta deve informar o administrador sobre atualizações e patches não relacionados no dispositivo cliente.

6.3.24.3.126. A solução proposta deve ser configurável/atribuível como fonte de atualização para atualizações da Microsoft e de terceiros.

6.3.24.3.127. A solução proposta deve permitir ao administrador selecionar o produto Microsoft e os idiomas para os quais as atualizações serão baixadas.

6.3.24.3.128. A solução proposta deve ser capaz de enviar/implantar remotamente arquivos EXE, MSI, bat, cmd, MSP e permitir que o administrador defina o parâmetro de linha de comando para a instalação remota.

6.3.24.3.129. A solução proposta deve ser capaz de desinstalar aplicativos remotamente, não se limitando a programas antivírus incompatíveis.

6.3.24.3.130. A solução proposta deve permitir ao administrador utilizar uma única tarefa/trabalho e definir diferentes regras ou critérios de correção de vulnerabilidades para atualizações de aplicações da Microsoft e de terceiros.

6.3.24.3.131. A solução proposta deve permitir que o administrador configure regras para instalação de patches/atualizações da Microsoft e de terceiros:

6.3.24.3.131.1. Inicie a instalação ao reiniciar ou desligar o computador.

6.3.24.3.131.2. Instale o gerador necessário todos os pré-requisitos do sistema.

6.3.24.3.131.3. Permitir a instalação de novas versões de aplicativos durante as atualizações.

6.3.24.3.131.4. Baixe atualizações para o dispositivo sem instalá-las.

6.3.24.3.132. A solução proposta deve ter a capacidade de testar a instalação de atualizações em uma porcentagem de computadores antes de aplicá-la a todos os computadores de destino. O administrador deve ser capaz de configurar o número de computadores de teste como uma porcentagem e o tempo alocado antes da implementação completa em termos de horas.

6.3.24.3.133. A solução proposta deve permitir a remoção/desinstalação de atualizações específicas de aplicativos e sistemas operacionais.

6.3.24.3.134. O servidor de gerenciamento da solução proposta deve ser capaz de enviar logs para servidores SIEMs e SYSLOG nos seguintes formatos:

6.3.24.3.134.1. CEF;

6.3.24.3.134.2. LEEF;

6.3.24.3.135. A solução proposta deve ser capaz de rastrear licenças de aplicações de terceiros e gerar notificações de quaisquer violações potenciais.

6.3.24.3.136. O relatório da solução proposta deve conter informações CVE.

6.3.24.3.137. A solução proposta deve suportar instalação de aplicações e software de terceiros;

6.3.24.4. Do Módulo de Gerenciamento Simplificado

6.3.24.4.1. A solução proposta deve suportar arquitetura cloud;

6.3.24.4.2. A solução proposta deve incluir um console web integrado para o gerenciamento dos endpoint, que não deve exigir nenhuma instalação adicional.

6.3.24.4.3. O console de gerenciamento web da solução proposta deve ser simples de usar e deve suportar dispositivos com tela sensível ao toque.

6.3.24.4.4. A solução proposta deve permitir ao administrador gerar relatórios pré-definidos.

6.3.24.4.5. A solução proposta deve suportar a descoberta de uso por parte do usuário de aplicações e exibir informações detalhadas de uso de aplicações utilizadas por meios de navegadores e aplicações instaladas no endpoint.

6.3.24.4.6. A solução proposta deve atender as condições apontadas no item e subintes 6.

6.3.24.4.7. A solução proposta deve suportar sistemas operacionais Windows, Mac, Android e iOS.

6.3.24.4.8. A solução proposta deve incluir informações do endpoint:

6.3.24.4.8.1. IP público de internet;

6.3.24.4.8.2. IP interno do dispositivo;

6.3.24.4.8.3. Versão do agente de proteção;

6.3.24.4.8.4. Última comunicação com a console, contendo data e hora;

6.3.24.4.8.5. Informações do sistema operacional;

6.3.24.4.9. A solução proposta deve permitir proteger as caixas de correio do Exchange Online, os utilizadores do OneDrive e os sites do SharePoint Online geridos através do Office 365.

6.3.24.4.10. A solução proposta deve permitir detectar informações críticas em arquivos localizados nos armazenamentos em nuvem do Office 365.

6.3.24.4.11. A solução proposta deve incluir treinamento em segurança cibernética.

6.3.24.5. Dos Requisitos Gerais da Proteção de Endpoint

6.3.24.5.1. A solução proposta deve ser capaz de detectar os seguintes tipos de ameaças:

6.3.24.5.1.1. Malwares, Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, sites e links de phishing, vulnerabilidades do tipo ZeroDay e outros softwares maliciosos e indesejados.

6.3.24.5.2. A solução proposta deve ser de um único fornecedor e suportar todos módulos descritos neste termo de referência.

6.3.24.5.3. A solução proposta deve suportar integração com Anti-malware Scan Interface (AMSI).

6.3.24.5.4. A solução proposta deve ter capacidade de integração com a central de segurança do Windows Defender.

6.3.24.5.5. A solução proposta deve suportar o subsistema Linux no Windows.

6.3.24.5.6. A solução proposta deve fornecer tecnologias de proteção da próxima geração. Sendo no mínimo:

6.3.24.5.6.1. Proteção contra ameaças sem arquivos (Fileless);

6.3.24.5.7. Fornecimento de proteção baseada em machine leaning em várias camadas e análise comportamental durante diferentes estágios da cadeia de ataque;

6.3.24.5.8. A solução proposta deve fornecer varredura de memória para estações de trabalho Windows;

6.3.24.5.9. A solução proposta deve fornecer varredura de memória do kernel para estações de trabalho Linux.

6.3.24.5.10. A solução proposta deve fornecer a capacidade de alternar para o modo nuvem para proteção contra ameaças, diminuindo o uso de RAM e disco rígido em máquinas com recursos limitados.

6.3.24.5.11. A solução proposta deve ter componentes dedicados para monitorar, detectar e bloquear atividades em endpoint: Windows, Linux e Mac. Servidores: Windows e Linux, para proteção contra ataques remotos de criptografia.

6.3.24.5.12. A solução proposta deve incluir componentes sem assinatura para detectar ameaças mesmo sem atualizações frequentes. A proteção deve ser alimentada por machine learning estático para pré-execução e machine learning dinâmico para estágios pós-execução da cadeia de eliminação em endpoints e na nuvem para servidores e estações de trabalho Windows.

6.3.24.5.13. A solução proposta deve fornecer análise comportamental baseada em machine learning.

6.3.24.5.14. A solução proposta deve incluir a capacidade de configurar e gerenciar configurações de firewall integradas aos sistemas operacionais Windows Server e Linux, através de seu console de gerenciamento.

6.3.24.5.15. A solução proposta deve incluir os seguintes componentes no sensor instalado no endpoint:

6.3.24.5.15.1. Controles de aplicativos,

6.3.24.5.15.2. Controle web e dispositivos

6.3.24.5.15.3. HIPS e Firewall

6.3.24.5.15.4. Descoberta de patches e vulnerabilidades de sistemas operacionais Windows;

6.3.24.5.15.5. Gerenciamento de criptografia de arquivos e discos;

6.3.24.5.15.6. Controle adaptativo para detecção de anomalias;

6.3.24.5.16. A capacidade de detectar e bloquear hosts não confiáveis na detecção de atividades semelhantes à criptografia em recursos compartilhados do servidor.

6.3.24.5.17. A solução proposta deve ser protegida por senha para evitar que o processo do anti-malware seja interrompido

sendo a autoproteção, independentemente do nível de autorização do usuário no sistema.

6.3.24.5.18. A solução proposta deve ter bancos de dados de reputação locais e globais.

6.3.24.5.19. A solução proposta deve ser capaz de verificar o tráfego HTTPS, HTTP, SMTP e FTP contra malwares.

6.3.24.5.20. A solução proposta deve incluir um módulo capaz, no mínimo, de:

6.3.24.5.20.1. Bloqueio de aplicativos com base em sua categorização.

6.3.24.5.20.2. Bloqueio/permissão de pacotes, protocolos, endereços IP, portas e direção de tráfego específicos.

6.3.24.5.20.3. A adição de sub-redes e a modificação de permissões de atividade.

6.3.24.5.21. A solução proposta deve impedir a conexão de dispositivos USB reprogramados emulando teclados e permitir o controle do uso de teclados na tela mediante autorização.

6.3.24.5.22. A solução proposta deve ser capaz de bloquear ataques à rede e reportar a origem da infecção.

6.3.24.5.23. A solução proposta deve ter armazenamento local nos endpoint para manter cópias dos arquivos que foram excluídos ou modificados durante a desinfecção. Esses arquivos devem ser armazenados em um formato específico que garanta que não representem qualquer ameaça.

6.3.24.5.24. A solução proposta deve incluir limpeza remota dos dispositivos com as seguintes funcionalidades:

6.3.24.5.24.1. Modo silencioso;

6.3.24.5.24.2. Discos rígidos e dispositivos removíveis;

6.3.24.5.24.3. De todos as contas de usuários do dispositivo.

6.3.24.5.25. A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes modos:

6.3.24.5.25.1. Exclusão imediata de dados;

6.3.24.5.25.2. Exclusão de dados adiada.

6.3.24.5.26. A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes métodos de exclusão de dados:

6.3.24.5.26.1. Excluir usando os recursos do sistema operacional - os arquivos são excluídos;

6.3.24.5.26.2. Excluir completamente, sem recuperação - tornando praticamente impossível restaurar os dados após a exclusão.

6.3.24.5.27. A solução proposta deve ter uma abordagem proativa para impedir que malware explore vulnerabilidades existentes em servidores e estações de trabalho.

6.3.24.5.28. A solução proposta deve suportar a tecnologia AM-PPL (Anti-Malware Protected Process Light) para proteção contra ações maliciosas.

6.3.24.5.29. A solução proposta deve incluir proteção contra ataques que explorem vulnerabilidades no protocolo ARP para falsificar o endereço MAC do dispositivo.

6.3.24.5.30. A solução proposta deve incluir um componente de controle capaz de aprender a reconhecer o comportamento típico do usuário em um indivíduo ou grupo específico de computadores protegidos e, em seguida, identificar e bloquear ações anômalas e potencialmente prejudiciais realizadas por esse terminal ou usuário.

6.3.24.5.31. A solução proposta deve fornecer funcionalidade Anti-Bridging para estações de trabalho Windows para evitar pontes não autorizadas para a rede interna que contornem as ferramentas de proteção de perímetro. Os administradores devem ser capazes de proibir o estabelecimento simultâneo de conexões com fio, Wi-Fi e modem.

6.3.24.5.32. A solução proposta deve incluir um componente dedicado para verificação de conexões criptografadas.

6.3.24.5.33. A solução proposta deve ser capaz de descriptografar e verificar o tráfego de rede transmitido por conexões criptografadas.

6.3.24.5.34. A solução proposta deve ter a capacidade de excluir automaticamente recursos da web quando ocorre um erro de verificação durante a execução de uma verificação de conexão criptografada. Esta exclusão deve ser exclusiva do host e não deve ser compartilhada com outros endpoint;

6.3.24.5.35. A solução proposta deve incluir funcionalidade para apagar dados remotamente das estações de trabalho;

6.3.24.5.36. A solução proposta deve incluir funcionalidade para excluir automaticamente os dados caso não haja conexão com o servidor de gerenciamento de endpoint.

6.3.24.5.37. A solução proposta deve suportar detecção baseadas em multicamadas sendo no mínimo: Assinatura, heurística, machine learning ou assistida por nuvem.

6.3.24.5.38. A solução proposta deve ter a capacidade de gerar um alerta, limpar e excluir uma ameaça detectada.

6.3.24.5.39. A solução proposta deve ser capaz de monitorar e bloquear ações que não são típicas dos computadores da rede de uma empresa.

6.3.24.5.40. A solução proposta deve ter a capacidade de acelerar as verificações ignorando os objetos que não foram alterados desde a verificação anterior.

6.3.24.5.41. A solução proposta deve permitir que o administrador exclua arquivos/pastas/aplicativos/certificados digitais específicos da verificação, seja no acesso (proteção em tempo real) ou durante verificações sob demanda.

6.3.24.5.42. A solução proposta deve verificar automaticamente as unidades removíveis em busca de malware quando elas estiverem conectadas a qualquer endpoint.

6.3.24.5.43. A solução proposta deve ser capaz de bloquear o uso de dispositivos de armazenamento USB ou permitir o acesso apenas aos dispositivos permitidos.

6.3.24.5.44. A solução proposta deve ser capaz de diferenciar dispositivos de armazenamento USB, impressoras, celulares e outros periféricos.

6.3.24.5.45. A solução proposta deve ter a capacidade de bloquear/permitir o acesso do usuário aos recursos da web com base nos sites e tipo de conteúdo.

6.3.24.5.46. A solução proposta deve ter categoria de detecção para bloquear banners de sites.

6.3.24.5.47. A solução proposta deve fornecer a capacidade de configurar redes Wi-Fi com base no nome da rede, tipo de autenticação e tipo de criptografia em dispositivos móveis;

6.3.24.5.48. A solução proposta deve suportar políticas baseadas no usuário para controle de dispositivos, web e aplicativos.

6.3.24.5.49. A solução proposta deve apresentar integração na nuvem, para fornecer atualizações mais rápidas possíveis sobre malware e ameaças potenciais.

6.3.24.5.50. A solução proposta deve ter capacidade de gerenciar direitos de acesso de usuários para operações de leitura e gravação em CDs/DVDs, dispositivos de armazenamento removíveis e dispositivos MTP.

6.3.24.5.51. A solução proposta deve permitir que o administrador monitore o uso de portas personalizadas/aleatórias pelo aplicativo;

6.3.24.5.52. A solução proposta deve suportar o bloqueio de aplicativos proibidos (lista de negações) de serem lançados no endpoint e o bloqueio de todos os aplicativos que não sejam aqueles incluídos nas listas de permissões.

6.3.24.5.53. A solução proposta deve ter um componente de controle de aplicativos integrado à nuvem para acesso imediato às atualizações mais recentes sobre classificações e categorias de aplicativos.

6.3.24.5.54. A solução proposta deve incluir filtragem de malware de tráfego, verificação de links da web e controle de recursos da web com base em categorias de nuvem.

6.3.24.5.55. O componente de controle web da solução proposta deve incluir uma categoria criptomoedas e mineração.

6.3.24.5.56. O componente de controle de aplicações da solução proposta deve incluir os modos operacionais lista de negações e lista de permissões.

6.3.24.5.57. A solução proposta deve suportar o controle de scripts executados em PowerShell.

6.3.24.5.58. A solução proposta deve suportar modo teste com geração de relatórios sobre execução de aplicativos bloqueados.

6.3.24.5.59. A solução proposta deve ter a capacidade de controlar o acesso do sistema/aplicativo do usuário a dispositivos de gravação de áudio e vídeo.

6.3.24.5.60. A solução proposta deve fornecer um recurso para verificar os aplicativos listados em cada categoria baseada em nuvem.

6.3.24.5.61. A solução proposta deve ter capacidade de integração com um sistema avançado de proteção contra ameaças específico do fornecedor.

6.3.24.5.62. A solução proposta deve ter a capacidade de regular automaticamente a atividade dos programas em execução, incluindo o acesso ao sistema de arquivos e ao registro, bem como a interação com outros programas.

6.3.24.5.63. A solução proposta deve ter a capacidade de categorizar automaticamente os aplicativos iniciados antes da instalação da proteção de endpoint.

6.3.24.5.64. A solução proposta deve ter proteção contra ameaças de e-mail de endpoint com:

6.3.24.5.64.1. Filtro de anexos.

6.3.24.5.64.2. Verificação de mensagens de e-mail ao receber, ler e enviar.

6.3.24.5.65. A solução proposta deve ter a capacidade de verificar vários redirecionamentos, URLs encurtados, URLs sequestrados e atrasos baseados em tempo.

6.3.24.5.66. A solução proposta deve permitir que o usuário do computador verifique a reputação de um arquivo;

6.3.24.5.67. A solução proposta deve incluir a verificação de todos os scripts, incluindo quaisquer scripts WSH (JavaScript, Visual Basic Script Scripts WSH (JavaScript, Visual Basic Script etc.);

6.3.24.5.68. A solução proposta deve fornecer proteção contra malware ainda desconhecido com base na análise do seu comportamento e verificação de alterações no registo do sistema, juntamente com mecanismo de remediação para restaurar automaticamente quaisquer alterações no sistema feitas pelo malware.

6.3.24.5.69. A solução proposta deve fornecer proteção contra ataques de hackers por meio de um firewall com sistema de prevenção de intrusões e regras de atividade de rede para aplicações mais populares ao trabalhar em redes de computadores de qualquer tipo, incluindo redes sem fio.

6.3.24.5.70. A solução proposta deve incluir suporte ao protocolo IPv6.

6.3.24.5.71. A solução proposta deve oferecer a verificação de seções críticas do computador como uma tarefa independente.

6.3.24.5.72. A solução proposta deve incorporar a tecnologia de autoproteção de aplicação:

6.3.24.5.72.1. Protegendo contra o gerenciamento remoto não autorizado de um serviço de aplicativo.

6.3.24.5.72.2. Protegendo o acesso aos parâmetros do aplicativo definindo uma senha. Evitando a desativação da proteção por malware, criminosos ou usuários.

6.3.24.5.73. A solução proposta deve oferecer a capacidade de escolher quais componentes de proteção contra ameaças instalar.

6.3.24.5.74. A solução proposta deve incluir a verificação anti-malware e desinfecção de arquivos em arquivos nos formatos RAR, ARJ, ZIP, CAB, LHA, JAR, ICE, incluindo arquivos protegidos por senha.

6.3.24.5.75. A solução proposta deve proteger contra malware ainda desconhecido pertencente a famílias cadastradas, com base em análise heurística.

6.3.24.5.76. A solução proposta deve notificar o administrador sobre eventos importantes que ocorreram através de notificação por e-mail.

6.3.24.5.77. A solução proposta deve permitir ao administrador criar um único pacote de instalação do sensor de proteção com a configuração necessária.

6.3.24.5.78. A solução proposta deve fornecer controles de aplicativos e dispositivos para estações de trabalho Windows.

6.3.24.5.79. A proteção da solução proposta para servidores e estações de trabalho deve incluir um componente dedicado para proteção contra atividades de ransomware/malwares que criptografa os recursos compartilhados.

6.3.24.5.80. A solução proposta deve, ao detectar atividades semelhantes a ransomware/criptografia, bloquear automaticamente o computador atacante por um intervalo especificado e listar informações sobre o IP e carimbo de data/hora do computador atacante e o tipo de ameaça.

6.3.24.5.81. A solução proposta deve fornecer uma lista predefinida de exclusões de verificação para aplicativos e serviços Microsoft.

6.3.24.5.82. A solução proposta deve suportar a instalação de proteção de endpoint em servidores sem a necessidade de reinicialização.

6.3.24.5.83. A solução proposta deve permitir a instalação de software com funcionalidades de anti-malware e detecção e resposta de incidente a partir de um único pacote de distribuição.

6.3.24.5.84. A solução proposta deve suportar endereços IPv6.

6.3.24.5.85. A solução proposta deve suportar verificação em duas etapas (autenticação).

6.3.24.5.86. A solução proposta deve prever a instalação, atualização e remoção centralizada de software antimalware, juntamente com configuração, administração centralizada e visualização de relatórios e informações estatísticas sobre o seu funcionamento.

6.3.24.5.87. A solução proposta deverá contar com a remoção centralizada (manual e automática) de aplicações incompatíveis do centro de administração.

6.3.24.5.88. A solução proposta deve fornecer métodos flexíveis para instalação do sensor de endpoint via: RPC, GPO e um agente de administração para instalação remota e a opção de criar um pacote de instalação independente para instalação do endpoint de segurança localmente.

6.3.24.5.89. A solução proposta deve permitir a instalação remota do sensor de endpoint com os bancos de dados anti-malware mais recentes.

6.3.24.5.90. A solução proposta deve permitir a atualização automática do sensor de endpoint e de bases de dados de anti-malware.

6.3.24.5.91. A solução proposta deve contar com recursos de busca automática de vulnerabilidades em aplicações e no sistema operacional em máquinas protegidas.

6.3.24.5.92. A solução proposta deve permitir a gestão de um componente que proíba a instalação e/ou execução de programas.

6.3.24.5.93. A solução proposta deve permitir a gestão de um componente que controla o trabalho com dispositivos de E/S externos.

6.3.24.5.94. A solução proposta deve permitir o gerenciamento de componente que controle a atividade do usuário na internet.

6.3.24.5.95. A solução proposta deve ser capaz de implantar automaticamente proteção para infraestruturas virtuais baseadas em VMware ESXi, Microsoft Hyper-V, plataforma de virtualização Citrix XenServer ou hipervisor.

6.3.24.5.96. A solução proposta deve incluir a distribuição automática de licenças nos computadores clientes.

6.3.24.5.97. A solução proposta deverá ser capaz de exportar relatórios para arquivos PDF, CSV ou XLS.

6.3.24.5.98. A solução proposta deve proporcionar a administração centralizada de armazenamentos de backup e quarentena em todos os recursos da rede onde o sensor de endpoint está instalado.

6.3.24.5.99. A solução proposta deve prever a criação de contas internas para autenticar administradores no servidor de administração.

6.3.24.5.100. A solução proposta deverá ter capacidade de gerenciar dispositivos móveis através de comandos remotos.

6.3.24.5.101. A solução proposta deve ter a capacidade de excluir atualizações baixadas.

6.3.24.5.102. A solução proposta deve mostrar claramente informações sobre a distribuição de vulnerabilidades entre computadores gerenciados.

6.3.24.5.103. A interface do servidor de gerenciamento da solução proposta deverá suportar o idioma Inglês e português.

6.3.24.5.104. A solução proposta deve ter um painel customizável gerando e exibindo estatísticas em tempo real dos sensores de endpoints.

6.3.24.5.105. A solução proposta deve incorporar funcionalidade de distribuição/retransmissão para suportar a entrega de proteção, atualizações, patches e pacotes de instalação para locais e remotos.

6.3.24.5.106. Os relatórios da solução proposta devem incluir informações sobre cada ameaça e a tecnologia que a detectou.

6.3.24.5.107. A solução proposta deve incluir a opção para implantar uma console de gerenciamento local ou usar o console de gerenciamento baseado em nuvem fornecido pelo fornecedor.

6.3.24.5.108. A solução proposta deve ser capaz de se integrar ao console de gerenciamento baseado em nuvem do fornecedor para gerenciamento de endpoint sem custo adicional.

6.3.24.5.109. A solução proposta deve permitir a migração rápida do console de gerenciamento local para o console de gerenciamento baseado em nuvem do fornecedor.

6.3.24.5.110. A solução proposta deve fornecer mecanismos de atualização de banco de dados, incluindo:

6.3.24.5.110.1. Múltiplas formas de atualização, incluindo canais de comunicação globais através do protocolo HTTPS, recursos compartilhados em rede local e mídia removível.

6.3.24.5.110.2. Verificação da integridade e autenticidade das atualizações por meio de assinatura digital eletrônica.

6.3.24.5.111. A solução proposta deve permitir monitorar vulnerabilidades existentes em dispositivos gerenciados.

6.3.24.5.112. A solução proposta deve gerar relatórios de vulnerabilidades encontradas nos dispositivos com sensor de endpoint instalado.

6.3.24.6. Do Modulo de Gerenciamento de Dispositivos Móveis

6.3.24.6.1. O modulo deve ser integrado a console de gerenciamento;

6.3.24.6.2. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis, incluindo Android:

6.3.24.6.2.1. Android 5.0 ou posterior (incluindo Android 12L, excluindo Go Edition)

6.3.24.6.3. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis iOS:

6.3.24.6.3.1. iOS 10–17 ou iPadOS 13–17

6.3.24.6.4. A solução proposta deve oferecer suporte a dispositivos Android Device Owner.

6.3.24.6.5. A solução proposta deve suportar dispositivos iOS supervisionados.

6.3.24.6.6. A solução proposta deve permitir a proteção do sistema de arquivos do smartphone e a interceptação e varredura de todos os objetos recebidos transferidos através de conexões sem fio (porta infravermelha, Bluetooth), EMS e MMS, ao mesmo tempo em que sincroniza com o computador pessoal e carrega arquivos através de um navegador.

6.3.24.6.7. A solução proposta deve ter a capacidade de bloquear sites maliciosos projetados para espalhar códigos maliciosos e sites de phishing projetados para roubar dados confidenciais do usuário e acessar suas informações financeiras.

6.3.24.6.8. A solução proposta deve ter a funcionalidade de adicionar um site excluído da verificação a uma lista de permissões.

6.3.24.6.9. A solução proposta deve incluir a filtragem de websites por categorias e permitir ao administrador restringir o acesso dos utilizadores a categorias específicas (por exemplo, websites relacionados com jogos de azar ou categorias de redes sociais).

6.3.24.6.10. A solução proposta deve permitir ao administrador obter informações sobre o funcionamento do sensor de endpoint e da proteção web no dispositivo móvel do usuário.

6.3.24.6.11. A solução proposta deverá ter a funcionalidade de detectar a localização do dispositivo móvel via GPS, e mostrá-la no Google Maps.

6.3.24.6.12. A solução proposta deve permitir ao administrador tirar uma foto da câmera frontal do celular quando ele estiver bloqueado.

6.3.24.6.13. A solução proposta deve ter recursos de conteinerização para dispositivos Android.

6.3.24.6.14. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos Android:

6.3.24.6.14.1. Dados em contêineres

6.3.24.6.14.2. Contas de e-mail corporativo

6.3.24.6.14.3. Configurações para conexão à rede Wi-Fi corporativa e VPN

6.3.24.6.14.4. Nome do ponto de acesso (APN)

6.3.24.6.14.5. Perfil do Android for Work

6.3.24.6.14.6. Recipiente KNOX

6.3.24.6.14.7. Chave do gerenciador de licença KNOX

6.3.24.6.15. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos iOS:

6.3.24.6.15.1. Todos os perfis de configuração instalados

6.3.24.6.15.2. Todos os perfis de provisionamento

6.3.24.6.15.3. O perfil iOS MDM

6.3.24.6.16. Aplicativos para os quais a caixa de seleção remover e o perfil iOS MDM foram marcadas

6.3.24.6.17. A solução proposta deve permitir a criptografia de todos os dados do dispositivo (incluindo dados de contas de usuários, unidades removíveis e aplicativos, bem como mensagens de e-mail, mensagens SMS, contatos, fotos e outros arquivos). O acesso aos dados criptografados só deve ser possível em um dispositivo desbloqueado por meio de uma chave especial ou senha de desbloqueio do dispositivo.

6.3.24.6.18. A solução proposta deve oferecer controles para garantir que todos os dispositivos cumpram os requisitos de segurança corporativa. O controlo de conformidade deverá basear-se num conjunto de regras que deverá incluir as seguintes componentes:

6.3.24.6.18.1. Critérios de verificação do dispositivo;

6.3.24.6.18.2. Prazo alocado para o usuário corrigir a não conformidade configurando ação que será tomada no dispositivo caso o usuário não corrija a não conformidade dentro do prazo definido;

6.3.24.6.19. A solução proposta deve ter a funcionalidade de detectar e notificar o administrador sobre hacks de dispositivos, por exemplo, root, Jailbreak e etc.

6.3.24.6.20. A solução proposta deverá permitir a gestão de pelo menos as seguintes características do dispositivo:

6.3.24.6.20.1. Cartões de memória e outras unidades removíveis

6.3.24.6.20.2. Câmera do dispositivo

6.3.24.6.20.3. Conexões Wi-Fi

6.3.24.6.20.4. Conexões Bluetooth

6.3.24.6.20.5. Porta de conexão infravermelha

6.3.24.6.20.6. Ativação do ponto de acesso Wi-Fi

6.3.24.6.20.7. Conexão de área de trabalho remota

6.3.24.6.20.8. Sincronização de área de trabalho

6.3.24.6.20.9. Definir configurações da caixa de correio do Exchange

6.3.24.6.20.10. Configurar caixa de e-mail em dispositivos iOS MDM

6.3.24.6.20.11. Configure contêineres Samsung KNOX.

6.3.24.6.20.12. Definir as configurações do perfil do Android for Work

6.3.24.6.20.13. Configurar e-mail/calendário/contatos

6.3.24.6.20.14. Defina as configurações de restrição de conteúdo de mídia.

6.3.24.6.20.15. Definir configurações de proxy no dispositivo móvel

6.3.24.6.20.16. Configurar certificados e SCEP

6.3.24.6.21. A solução proposta deverá permitir a configuração de uma conexão com dispositivos AirPlay para permitir o streaming de músicas, fotos e vídeos do dispositivo iOS MDM para dispositivos AirPlay.

6.3.24.6.22. A solução proposta deve suportar todos os métodos de implantação abaixo para o sensor móvel:

6.3.24.6.22.1. Google Play, Huawei App Gallery e Apple App Store

6.3.24.6.22.2. Portal de inscrição móvel KNOX

6.3.24.6.22.3. Pacotes de instalação pré-configurados independentes

6.3.24.6.23. A solução proposta deverá permitir a configuração de Nomes de Pontos de Acesso (APN) para conectar um dispositivo móvel a serviços de transferência de dados em uma rede móvel.

6.3.24.6.24. A solução proposta deve permitir que o PIN de um dispositivo móvel seja redefinido remotamente.

6.3.24.6.25. A solução proposta deve incluir a opção de registrar dispositivos Android usando sistemas EMM de terceiros:

6.3.24.6.25.1. VMware AirWatch 9.3 ou posterior

6.3.24.6.25.2. MobileIron 10.0 ou posterior

6.3.24.6.25.3. IBM MaaS360 10.68 ou posterior

6.3.24.6.25.4. Microsoft Intune 1908 ou posterior

6.3.24.6.25.5. SOTI MobiControl 14.1.4 (1693) ou posterior

6.3.24.6.26. A solução proposta deve ter funcionalidade para forçar a instalação de um aplicativo no dispositivo.

6.3.24.6.27. A solução proposta deve suportar a implantação de sensor de endpoint iniciada pelo usuário através de:

6.3.24.6.27.1. Google Play

6.3.24.6.27.2. Galeria de aplicativos Huawei

6.3.24.6.27.3. Loja de aplicativos da Apple

6.3.24.6.28. A solução proposta deve ser capaz de escanear arquivos abertos no dispositivo.

6.3.24.6.29. A solução proposta deve ser capaz de verificar programas instalados a partir da interface do dispositivo.

6.3.24.6.30. A solução proposta deve ser capaz de verificar objetos do sistema de arquivos no dispositivo ou em placas de extensão de memória conectadas, mediante solicitação do usuário ou de acordo com um agendamento.

6.3.24.6.31. A solução proposta deve proporcionar o isolamento confiável de objetos infectados em um local de armazenamento de quarentena.

6.3.24.6.32. A solução proposta deve contar com a atualização dos bancos de dados de antivírus utilizados para busca de programas maliciosos e exclusão de objetos perigosos.

6.3.24.6.33. A solução proposta deve ser capaz de verificar dispositivos móveis em busca de malware e outros objetos indesejados sob demanda e dentro do cronograma e lidar com eles automaticamente.

6.3.24.6.34. A solução proposta deve ser capaz de gerenciar e monitorar dispositivos móveis a partir do mesmo console usado para gerenciar computadores e servidores.

6.3.24.6.35. A solução proposta deve fornecer funcionalidade Anti-Roubo, para que dispositivos perdidos e/ou deslocados possam ser localizados, bloqueados e apagados remotamente.

6.3.24.6.36. A solução proposta deve fornecer a possibilidade de bloquear o lançamento de aplicativos proibidos no dispositivo móvel.

6.3.24.6.37. A solução proposta deve ser capaz de impor configurações de segurança, como restrições de senha e criptografia, em dispositivos móveis.

6.3.24.6.38. A solução proposta deve ter a capacidade de enviar aplicações recomendadas/exigidas pelo administrador para o dispositivo móvel.

6.3.24.6.39. A solução proposta deverá possuir Controle de Aplicativos com os modos de aplicação Proibido/Permitido.

6.3.24.6.40. A solução proposta deve incluir um modelo de assinatura integrado a nuvem do fabricante para proteção de ataques mais recentes;

6.3.24.6.41. A solução proposta deve proteger contra ameaças online em dispositivos iOS.

6.3.24.7. Do Módulo de EDR

6.3.24.7.1. Deve apresentar um gráfico de propagação de ameaças com os principais processos. conexões de rede, DLLs, seções de registro afetado ou envolvido no alerta.

6.3.24.7.2. Todas as detecções são destacadas no gráfico, fornecendo ao analista o contexto completo para o incidente e facilitando o processo de revelação dos componentes afetados.

6.3.24.7.3. A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um gráfico visualizado da cadeia de desenvolvimento de ameaças;

6.3.24.7.4. Dever ser integrado ao portal de inteligência do fornecedor para enriquecimento dos detalhes da análise;

6.3.24.7.5. Deve apresentar informações detalhadas contendo:

6.3.24.7.5.1. Usuário que executou a ação;

6.3.24.7.5.2. Informações acesso privilegiado;

6.3.24.7.6. A solução proposta deve ter sandbox em nuvem do fabricante integrada para verificar automaticamente arquivos e aplicar respostas caso atividades suspeitas sejam detectadas.

6.3.24.7.7. A solução proposta deve suportar integração com serviço de reputação em nuvem.

6.3.24.7.8. A solução proposta deve oferecer suporte ao gerenciamento central e à análise por meio do console Web local e do console de gerenciamento em nuvem avançado. (Dados relacionados ao incidente, status do sistema e dados de verificação de integridade, configurações, etc.)

6.3.24.7.9. O agente EDR deve ter integração com o aplicativo de proteção de endpoint(agente único).

6.3.24.7.10. Soluções EDR e proteção de endpoint devem ter console unificado para administradores e analistas;

6.3.24.7.11. A solução proposta deve suportar a detecção automatizada de atividades maliciosas usando a solução Endpoint Protection e a tecnologia de sandbox na nuvem.

6.3.24.7.12. A solução proposta deve complementar as informações do veredicto da solução Endpoint Protection com artefatos do sistema sobre a detecção.

6.3.24.7.13. A solução proposta deve suportar a geração automática de indicadores de ameaça (IoC) após a detecção ocorrer com capacidade de aplicar ações de resposta.

6.3.24.7.14. A solução deve ter a capacidade de forçar a execução da varredura IoC em todos os endpoints com agentes EDR instalados.

6.3.24.7.15. A solução proposta deve suportar a execução de varredura IoC de acordo com um agendador.

6.3.24.7.16. A solução proposta deve suportar a importação de IoC de terceiros no formato OpenIoC para uso em digitalização em rede.

6.3.24.7.17. A solução proposta deve oferecer suporte à verificação usando conjuntos de IoCs gerados automaticamente, carregados ou externos (de terceiros) para detectar ameaças anteriores não detectadas.

6.3.24.7.18. A solução proposta deve permitir suportar a exportação do IoC gerado pela solução para monitorar vulnerabilidades existentes nos dispositivos gerenciados, um arquivo no formato OpenIoC.

6.3.24.7.19. A solução proposta deve gerar um cartão de incidente detalhado relacionado à ameaça detectada em um endpoint.

6.3.24.7.20. A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um cartão de incidente visualizado. Um cartão de incidente deve incluir pelo menos as seguintes informações sobre a ameaça detectada:

6.3.24.7.21. Gráfico da cadeia de desenvolvimento de ameaças e detalhamento para análise posterior (cadeia de ataque).

6.3.24.7.22. Informações sobre o dispositivo no qual a ameaça foi detectada, contendo: nome, endereço IP, endereço MAC, lista de usuários, sistema operacional.

6.3.24.7.23. Informações gerais sobre a detecção, incluindo modo de detecção.

6.3.24.7.24. Alterações no registro associadas à detecção.

6.3.24.7.25. Histórico da presença de arquivos no dispositivo.

6.3.24.7.26. Ações de resposta executadas pela aplicação.

6.3.24.7.27. O gráfico da cadeia de desenvolvimento de ameaças (kill chain) deve fornecer informações visuais sobre os objetos envolvidos no incidente, por exemplo, sobre os principais processos no dispositivo, conexões de rede, bibliotecas, registro, etc.

6.3.24.7.28. A visualização de incidente deve apresentar uma visão detalhada dos artefatos do sistema e dos dados relacionados ao incidente para análise da causa raiz:

6.3.24.7.28.1. Processo

6.3.24.7.28.2. Conexões de rede

6.3.24.7.28.3. Alterações no registro

6.3.24.7.28.4. Detalhes do download de objeto

6.3.24.7.29. A solução proposta deve fornecer orientação de resposta (resposta guiada).

6.3.24.7.30. A solução proposta deve suportar “clique único” no console de gerenciamento avançado para resposta a um incidente

6.3.24.7.31. A solução proposta deve suportar pelo menos as seguintes ações de resposta que um administrador pode executar quando ameaças são detectadas:

6.3.24.7.31.1. Impedir a execução de objetos

6.3.24.7.31.2. Isolamento de host

6.3.24.7.31.3. Excluir objeto do host ou grupo de hosts

6.3.24.7.31.4. Encerrar um processo no dispositivo

6.3.24.7.31.5. Colocar um objeto em quarentena

6.3.24.7.31.6. Execute a verificação do sistema

6.3.24.7.31.7. Execução remota de programa/processo/comando

6.3.24.7.31.8. Iniciar a varredura IoC para um grupo de hosts.

6.3.24.8. Do Módulo de MDR

6.3.24.8.1. Deve possuir console web própria do serviço, além de integração nativa com a console do “software de segurança e antivírus para servidores físicos, microcomputadores e smartphones/tablets”.

6.3.24.8.2. Deverá ser suportada por qualquer um dos seguintes navegadores:

6.3.24.8.2.1. Apple Safari versões mais recentes

6.3.24.8.2.2. Google Chrome versões mais recentes

6.3.24.8.2.3. Microsoft Edge

6.3.24.8.2.4. Mozilla Firefox versões mais recentes.

6.3.24.8.3. O agente de endpoint dever ser compatível com os seguintes sistemas operacionais, para no mínimo a coleta e envio dos dados/telemetria ao SOC do fabricante:

6.3.24.8.3.1. Microsoft Windows 7 e superiores;

6.3.24.8.3.2. MacOS 10.14-11;

6.3.24.8.3.3. CentOS 6.7 ou superior;

6.3.24.8.3.4. Debian GNU / Linux 9.4 ou superior;

6.3.24.8.3.5. Linux Mint 19 ou superior;

6.3.24.8.3.6. Oracle Linux 7.3 ou superior;

6.3.24.8.3.7. Red Hat Enterprise Linux 6.7 ou superior;

6.3.24.8.3.8. SUSE Linux Enterprise Server 12 SP5 ou superior;

6.3.24.8.3.9. Ubuntu 18.04 LTS ou superior.

6.3.24.8.4. Deverá suportar os requisitos de carga de rede:

6.3.24.8.4.1. Em condições médias de carga: um canal full-duplex com largura de banda de pelo menos 1,7 Kbps para cada ativo.

6.3.24.8.4.2. Em condições de carga máxima: um canal full-duplex com largura de banda de pelo menos 2,7 Kbps para cada ativo.

6.3.24.8.5. A console deve possuir das dashboards com as informações principais, apresentando no mínimo:

6.3.24.8.5.1. Número de incidentes e status

6.3.24.8.5.2. Quantidade de dispositivos monitorados

6.3.24.8.6. Deve possuir mecanismo de notificações, com no mínimo as seguintes opções:

6.3.24.8.6.1. E-mail

6.3.24.8.6.2. Telegram

6.3.24.8.7. Deve permitir o envio de relatórios.

6.3.24.8.8. O agente deve enviar a telemetria em tempo real para o SOC do fabricante;

6.3.24.8.9. O serviço deve compreender monitoramento dos dados enviados e alertas gerados em um regime 24x7x265.

6.3.24.8.10. O envio e armazenamento da telemetria, devem respeitar as principais legislações de proteção de dados, como GDPR e LGPD.

6.3.24.8.11. O SOC do fabricante deve possuir datacenters em pelo menos duas localidades em diferentes países.

6.3.24.8.12. O SoC do fabricante deve possuir equipes de analistas em pelo menos 3 regiões (países) incluindo Brasil.

6.3.24.8.13. Os dados coletados devem passar por no mínimo:

6.3.24.8.13.1. Modelos de Machine Learning/Inteligência Artificial;

6.3.24.8.13.2. Análise humana;

6.3.24.8.13.3. Correlação com IoA's (indicadores de ataque);

6.3.24.8.13.4. Emulação em sandbox (quando necessário);

6.3.24.8.14. Após análise, informações sobre atividades potencialmente maliciosas, devem ser apresentadas no portal como "Incidentes"

6.3.24.8.15. O Incidente deve possuir no mínimo as seguintes informações:

6.3.24.8.15.1. Emulação em sandbox (quando necessário);

6.3.24.8.15.2. Resumo

6.3.24.8.15.3. Prioridade (Baixa, Média e Alta)

6.3.24.8.15.4. Recomendação

6.3.24.8.15.5. Data de criação e data de atualização

6.3.24.8.15.6. Correlacionamento com táticas/técnicas do Framewok MITRE ATT&CK

6.3.24.8.15.7. Dispositivos afetados

6.3.24.8.15.8. IoC’s de host e de rede

6.3.24.8.15.9. Descrição completa em linha do tempo

6.3.24.8.16. O incidente pode receber ações de resposta recomendada disparadas pela equipe de SoC, compreendendo no mínimo as seguintes ações:

6.3.24.8.16.1. Transferir arquivo para o SoC;

6.3.24.8.16.2. Isolar um dispositivo;

6.3.24.8.16.3. Desabilitar isolamento de dispositivo;

6.3.24.8.16.4. Deletar chave de registro;

6.3.24.8.16.5. Dump de memória

6.3.24.8.17. As ações devem ser aprovadas no portal por profissional da contratante, com a opção de habilitar aprovação automática.

6.3.24.9. Do Monitoramento, Coleta, Identificação e Investigação dos Eventos de Segurança Cibernética

6.3.24.9.1. O serviço de monitoramento deverá utilizar informações extraídas de registros gerados pelos sistemas monitorados.

6.3.24.9.2. Deverá ser instalado agentes específicos nos servidores e desktops, objetivando coletar informações mais detalhadas para o serviço de monitoramento, desde que seja plenamente compatível com o sistema onde será instalado e não afete o desempenho dos serviços

6.3.24.9.3. A análise das informações correlacionadas deve ser realizada com auxílio de bases globais de inteligência cibernética em conjunto com a expertise dos profissionais do fabricante, com vistas a reduzir ao máximo os falsos positivos.

6.3.24.9.4. É obrigatório que a comunicação entre equipamentos e soluções do fabricante instalados nos dispositivos e qualquer infraestrutura onde esses dados sejam processados ocorra de forma segura, utilizando algoritmos criptográficos para preservar o sigilo das informações.

6.3.24.9.5. Deverá ser feita a investigação e a classificação dos eventos monitorados, aplicando os principais frameworks de gestão de incidentes de segurança cibernética bem como boas práticas de mercado na detecção e triagem dos eventos de segurança, objetivando minimizar a presença de falsos positivos na abertura de incidentes de segurança.

6.3.24.9.6. O serviço de monitoramento deverá ser capaz de coletar e realizar a correlação de eventos dos sistemas e ativos monitorados, permitindo uma visão mais abrangente do alcance das ações maliciosas, bem como de possível movimentação lateral do atacante dentro da rede.

6.3.24.9.7. O monitoramento deverá ser capaz de identificar as principais ameaças, bem como táticas, técnicas e procedimentos de ataque descritos na base de conhecimento MITRE ATT&CK, sem prejuízo do uso de outras bases de conhecimento ou serviços de inteligência de ameaças, para complementação da capacidade de identificação de atividades maliciosas.

6.3.24.9.8. Deverá monitorar e avaliar criticamente os serviços, traçando curvas de comportamento, definindo a volumetria média e identificando comportamentos

anômalos, visando antecipar a identificação de incidentes de segurança.

6.3.24.9.9. A solução deverá prover inteligência de proteção contra ataques cibernéticos a nível global, sendo responsável por pesquisar novos tipos de ataques, vírus, malwares, botnets, vulnerabilidades e afins com intuito de melhoria contínua de detecção e mitigação destes males dentro dos serviços e ativos de segurança monitorados.

6.3.24.9.10. O agente deve ter capacidade de coletar e processar dados relacionadas ao veredito e ao contexto da ameaça;

6.3.24.9.11. Deve fornecer graficamente a visualização da cadeia do ataque;

6.3.24.9.12. Deve possuir a capacidade de varredura, para identificar a presença de um artefato detectado em outros dispositivos na rede, através de indicadores de comprometimento (IoC).

6.3.24.9.13. A varredura deve oferecer opções de resposta automatizada (sem intervenção do administrador), para serem executadas caso o IoC seja encontrado em outro dispositivo, com no mínimo as seguintes opções:

6.3.24.9.13.1. Isolar o host;

6.3.24.9.13.2. Iniciar uma varredura nas áreas críticas;

6.3.24.9.13.3. Quarentenar o objeto;

6.3.24.9.14. A solução deve criar um report detalhado sobre o incidente, tendo a capacidade de incluir no mínimo os seguintes dados:

6.3.24.9.14.1. Detecções provenientes da solução de endpoint;

6.3.24.9.14.2. Processos;

6.3.24.9.14.3. Alterações de registro;

6.3.24.9.14.4. Conexões remotas;

6.3.24.9.14.5. Criação de arquivos;

6.3.24.9.15. Varredura por todos os dispositivos executada a partir de indicador de comprometimento (IoC) gerado através da solução e importado pelo administrador.

6.3.24.9.16. Possibilidade de exportar os indicadores de comprometimento (IoC) gerados a partir da solução.

6.3.24.9.17. A solução deve oferecer no mínimo as seguintes opções de resposta:

6.3.24.9.17.1. Prevenir a execução de um arquivo;

6.3.24.9.17.2. Quarentenar um arquivo;

6.3.24.9.17.3. Iniciar uma varredura por IoC;

6.3.24.9.17.4. Parar um processo;

6.3.24.9.17.5. Executar um processo;

6.3.24.9.18. Ferramenta que possibilite o isolamento do host infectado com no mínimo as características abaixo:

6.3.24.9.18.1. A opção de isolamento deve estar disponível junto a visualização do incidente;

6.3.24.9.18.2. Na configuração padrão, o isolamento deve ser feito de forma granular, permitindo o controle do dispositivo pela console administrativa mesmo após ativação da regra;

6.3.24.9.19. O fabricante deverá utilizar solução para registro de incidente de segurança, acessível pela equipe técnica da Contratante, para indicar ações de contenção, comunicar à equipe da Contratante sobre o andamento do tratamento dos incidentes.

6.3.25. Requisitos para Documentação da Solução.

6.3.25.1. A documentação da solução de proteção de endpoint incluindo ferramentas de administração, deve incluir os seguintes documentos:

6.3.25.2. Ajuda on-line para administradores

6.3.25.3. Ajuda on-line para melhores práticas de implementação

6.3.25.4. Ajuda on-line para proteção de servidores de administração

6.3.25.5. A documentação do software anti-malware fornecida deve descrever detalhadamente os processos de instalação, configuração e uso do software anti-malware.

6.3.25.6. Deve estar disponível página com informações de ciclo de vida das soluções e módulos;

6.3.26. Requisitos de segurança:

6.3.26.1. Os requisitos de segurança a serem observados nas aplicações em desenvolvimento ou em manutenção deverão observar as políticas, os padrões, as arquiteturas, os métodos, as técnicas e as regras de negócio previamente estabelecidas pelo TCE-MS e/ou aquelas especificadas em cada demanda.

6.3.26.2. A empresa fornecedora da solução de TI deverá tratar como “confidenciais” quaisquer informações, a que tenha acesso para execução do objeto, não podendo revelá-las ou facilitar sua disponibilização a terceiros. A obrigação permanecerá válida durante o período de vigência contratual e o seu descumprimento implicará em sanções administrativas e judiciais contra a empresa ofertante da solução de TI.

6.3.27. Requisitos de capacitação e transferência de conhecimentos;

6.3.27.1. Os requisitos mínimos exigidos neste subitem são justificados pela necessidade de não somente implantar a

solução, porém mantê-la em funcionamento ininterrupto, provendo disponibilidade e desempenho durante toda a execução do contrato, através de equipe técnica especializada e apoio do fabricante na análise de problemas e atualização de seus produtos quanto à evolução tecnológica, correção de erros e vulnerabilidades e adaptação às mudanças de ambiente;

6.3.27.2. Deverá ser oferecido treinamento da solução ofertada para, no mínimo, 4 (quatro) participantes;

6.3.27.3. O treinamento deverá ser realizado na sede do TCE-MS ou em outro local apropriado, a ser acordado entre as partes, no município de Campo Grande/MS;

6.3.27.4. Deverá ser distribuído material de apoio a cada participante, que poderá ser em português (preferencialmente) ou inglês;

6.3.27.5. O conteúdo do treinamento deverá ser organizado em módulos, sequenciados logicamente, visando o conhecimento cumulativo, contendo, ao final de cada módulo, exercícios práticos com laboratórios para fixação;

6.3.27.6. A Contratada deverá prover os equipamentos que irão compor o laboratório do treinamento, que deverão ser equivalentes aos fornecidos para o TCE-MS ou, quando não for possível, por equipamentos similares com as mesmas funcionalidades;

6.3.27.7. O instrutor deverá ministrar o treinamento em português com carga horária de, no mínimo, 20 (vinte) horas, abordando obrigatoriamente o seguinte conteúdo:

6.3.27.8. Instalação do produto;

6.3.27.9. Utilização da interface gráfica simples;

6.3.27.10. Configuração dos parâmetros básicos e gerenciamento de usuários;

6.3.27.11. Melhores práticas de utilização da solução;

6.3.27.12. Integração com ambientes de virtualização;

6.3.27.13. Criação de regras personalizadas (firewall, antivírus, VPN, IPS, MTA, QoS, Aceleração e outras essenciais para ativação das funcionalidades principais);

6.3.27.14. Criação de perfis de aceleração e otimização de rede e aplicações;

6.3.27.15. Criação de perfis de aceleração web e otimização de protocolo;

6.3.27.16. Configuração de ambiente de alta disponibilidade (cluster);

6.3.27.17. Configuração de parâmetros para balanceamento de carga de serviços;

6.3.27.18. Conceitos de monitoramento;

6.3.27.19. Processamento de tráfego SSL na solução.

6.3.27.20. Abranger todas as funcionalidades especificadas na especificação técnica;

6.3.27.21. O TCE-MS poderá, a seu critério, em qualquer tempo, durante o treinamento, contestar a prestação do serviço, solicitando a troca de instrutor ou equipamentos de laboratório;

6.3.27.22. Caso a deficiência não possa ser sanada sem prejuízo para o andamento do treinamento, esse será suspenso pelo TCE-MS, devendo a Contratada agendar novo treinamento, sem ônus adicional para a Contratante.

6.3.28. Requisitos de experiência profissional da equipe:

6.3.28.1. A licitante deverá prover suporte técnico especializado para a solução ofertada através de equipe técnica especializada e devidamente capacitada;

6.3.28.2. A equipe deverá ser composta por profissionais com as seguintes especialidades:

6.3.28.2.1. No mínimo 02 (dois) profissionais com as seguintes especialidades:

PERFIL 01 – Suporte Técnico e Manutenção para solução de proteção de perímetro	
Responsável por realizar todas as atividades relacionadas à suporte técnico e manutenção da solução de proteção de perímetro ofertada, conforme as normas, padrões e diretrizes da fabricante.	
Experiência/Qualificação	**Modo de Comprovação**
- Qualificação para prestar serviços de suporte técnico ou manutenção nas soluções do fabricante da solução de proteção de perímetro.	- Certificado de conclusão de capacitação fornecido pelo fabricante da solução de proteção de perímetro, com o nível de certificação *Administrator, Professional* ou superior, dentro do período de validade;
Formação	**Modo de Comprovação**
- Formação de nível superior completa nas áreas correlatas de TIC, graduação ou pós-graduação nas áreas correlatas de TIC com carga horária mínima de 360 (trezentos e sessenta) horas.	- Diploma fornecido por instituição reconhecida pelo Ministério da Educação (MEC).

6.3.28.2.2. No mínimo 01 (um) profissional com as seguintes especialidades:

PERFIL 02 – Suporte Técnico e Manutenção para solução de balanceamento de carga e de proteção de aplicações	
Responsável por realizar todas as atividades relacionadas à suporte técnico e manutenção da solução de balanceamento de carga e de proteção de aplicações ofertada, conforme as normas, padrões e diretrizes da fabricante.	
Experiência/Qualificação	**Modo de Comprovação**
- Qualificação para prestar serviços de suporte técnico ou manutenção nas soluções do fabricante	- Certificado de conclusão de capacitação fornecido pelo fabricante da solução de balanceamento de carga e de proteção de aplicações, com o nível de

da solução de balanceamento de carga e de proteção de aplicações.	certificação *Administrator, Professional* ou superior, dentro do período de validade;
Formação	**Modo de Comprovação**
- Formação de nível superior completa nas áreas correlatas de TIC, graduação ou pós-graduação nas áreas correlatas de TIC com carga horária mínima de 360 (trezentos e sessenta) horas.	- Diploma fornecido por instituição reconhecida pelo Ministério da Educação (MEC).

6.3.28.2.3. No mínimo 02 (dois) profissionais com as seguintes especialidades:

PERFIL 03 – Suporte Técnico e Manutenção para solução de proteção e segurança para endpoints	
Responsável por realizar todas as atividades relacionadas à suporte técnico e manutenção da solução de proteção e segurança para endpoints ofertada, conforme as normas, padrões e diretrizes da fabricante.	
Experiência/Qualificação	**Modo de Comprovação**
- Qualificação para prestar serviços de suporte técnico ou manutenção nas soluções do fabricante da solução de proteção e segurança para endpoints.	- Certificado de conclusão de capacitação fornecido pelo fabricante da solução de proteção e segurança para endpoints, com o nível de certificação *Administrator, Professional* ou superior, dentro do período de validade;
Formação	**Modo de Comprovação**
- Formação de nível superior completa nas áreas correlatas de TIC, graduação ou pós-graduação nas áreas correlatas de TIC com carga horária mínima de 360 (trezentos e sessenta) horas.	- Diploma fornecido por instituição reconhecida pelo Ministério da Educação (MEC).

6.3.28.2.4. No mínimo 01 (um) profissional com as seguintes especialidades:

PERFIL 04 – Suporte Técnico e Monitoramento de Rede
Responsável por monitorar os ativos e a gestão dos eventos de TI da solução ofertada, focados na administração e no monitoramento de rede e dos equipamentos que compõem a solução.

Experiência/Qualificação	Modo de Comprovação
- Certificação no software de monitoramento utilizado pelo SNOC.	- Certificado de conclusão de capacitação fornecido por instituto credenciado, dentro do período de validade.
Formação	**Modo de Comprovação**
- Formação de nível superior completa nas áreas correlatas de TIC, graduação ou pós-graduação nas áreas correlatas de TIC com carga horária mínima de 360 (trezentos e sessenta) horas.	- Diploma fornecido por instituição reconhecida pelo Ministério da Educação (MEC).

6.3.28.2.5. No mínimo 01 (um) profissional com as seguintes especialidades:

PERFIL 05 – Analista de gerenciamento de serviços de TI	
Responsável por estabelecer os processos que garantem organização e controle para cumprimento dos objetivos dos serviços contratados, alinhando assim a execução das atividades de TI aos processos de negócios de forma a garantir a execução contratual de forma plena.	
Experiência/Qualificação	**Modo de Comprovação**
- Certificação ITIL (v3 ou superior) e Certificação ISO/IEC 20000.	- Certificado de conclusão ITIL (v3 ou superior), fornecido por instituto credenciado, dentro do período de validade. - Certificado de conclusão ISO/IEC 20000, fornecido por instituto credenciado, dentro do período de validade.
Formação	**Modo de Comprovação**
- Formação de nível superior completa nas áreas correlatas de TIC, graduação ou pós-graduação nas áreas correlatas de TIC com carga horária mínima de 360 (trezentos e sessenta) horas.	- Diploma fornecido por instituição reconhecida pelo Ministério da Educação (MEC).

6.3.28.2.6. No mínimo 05 (cinco) profissionais com as seguintes especialidades:

PERFIL 06 – Analistas SNOC	
Responsável pela configuração, administração e operação de plataformas do SNOC e pelo gerenciamento, detecção e resposta aos incidentes de segurança da informação. Os analistas SNOC deverão executar as atividades de forma presencial, nas dependências da Contratante, em regime 8x5, observando os Níveis de Serviços dispostos no Acordo de Nível de Serviços exigidos.	
Experiência/Qualificação	**Modo de Comprovação**
- Experiência mínima de 4 (quatro) anos em operação de plataformas de NOC e/ou SOC/SIEM e gerenciamento, detecção e resposta aos incidentes de segurança da informação.	- Currículo do profissional.
Formação	**Modo de Comprovação**
- Formação de nível superior completa nas áreas correlatas de TIC, graduação ou pós-graduação nas áreas correlatas de TIC com carga horária mínima de 360 (trezentos e sessenta) horas.	- Diploma fornecido por instituição reconhecida pelo Ministério da Educação (MEC).

6.3.28.3. No ato da assinatura do contrato a licitante vencedora do certame deverá apresentar comprovação de que os profissionais fazem parte do quadro funcional da proponente. A comprovação dar-se-á mediante um dos seguintes documentos:

6.3.28.3.1. Carteira de Trabalho e Previdência Social (CTPS);

6.3.28.3.2. Contrato de Prestação de Serviços, no caso de profissional autônomo;

6.3.28.3.3. Contrato Social, no caso de sócio proprietário.

6.3.29. Requisitos de entrega ou da prestação do serviço

6.3.29.1. A Contratada deverá realizar os procedimentos de transbordo, descarga e armazenamento dos equipamentos (com as embalagens originais) no local indicado para a entrega.

6.3.29.2. A Contratada deverá providenciar equipamentos e/ou mão de obra necessários para a descarga, que será acompanhada e fiscalizada por servidor do Contratante.

6.3.29.3. A verificação quanto ao estado dos produtos após o transporte será de exclusiva responsabilidade da Contratada, sendo que, quaisquer danos ocorridos no transporte dos equipamentos e observados a qualquer tempo, deverão ser reparados pela Contratada, sem qualquer ônus para o Contratante.

6.3.29.4. Todos os softwares, firmwares e drivers de controle necessários ao perfeito funcionamento da solução, na última versão disponível;

6.3.29.5. Todas as licenças de utilização definitivas para os softwares, firmwares e drivers fornecidos;

6.3.29.6. Todos os cabos e acessórios necessários para a perfeita instalação, configuração e uso da solução;

6.3.29.7. Toda a documentação técnica da solução fornecida, completa e atualizada, contendo manuais, guias de instalação e outros pertinentes, referente a equipamentos e procedimentos que a compõem, todos originais e redigidos em português ou inglês, não sendo aceitas cópias. A documentação técnica poderá ser entregue, também, em meio eletrônico;

6.3.29.8. Acesso para o CONTRATANTE à base de conhecimento do fabricante, incluindo documentação e download de atualizações.

6.3.29.9. Os serviços de Suporte Técnico Especializado, Manutenção e Apoio deverão ser prestados pela empresa contratada na forma on-site ou remoto, no regime 24X7, incluindo a atualização de softwares e bases de dados de conhecimento

as suas expensas, e, sempre que for necessário ao bom funcionamento da solução adquirida;

6.3.29.10. Todos os serviços de Suporte Técnico Especializado, Manutenção e Apoio deverão ser executados por técnicos qualificados e com certificação comprovada pelo fabricante da Solução, pertencentes ao quadro de funcionários da CONTRATADA, sem custos adicionais para o CONTRATANTE, durante todo o período de garantia, sendo indispensável a apresentação de documentação original do fabricante que comprove a validade da certificação enquanto durar o vínculo contratual.

6.3.29.11. A comprovação de validade da certificação e comprovação de vínculo empregatício deverão ser apresentados juntamente com o cronograma anual de visitas programadas ou sempre que o técnico credenciado for substituído, podendo ainda, ser solicitada a qualquer momento pela CONTRATANTE;

6.3.29.12. Os serviços de Suporte Técnico Especializado, Manutenção e Apoio, quando presencial deverá ser prestado no endereço local do CONTRATANTE ou outro indicado por ele;

6.3.29.13. Todas as peças e componentes necessários ao perfeito funcionamento de toda a solução, quando necessário devem ser substituídos pela CONTRATADA, sem nenhum custo adicional a CONTRATANTE.

6.3.30. Requisitos de proteção para diferentes ambientes

6.3.30.1. Independentemente do número de ambientes, todos devem possuir protocolos de segurança sempre atualizados,

aplicações de update, monitoramento e todo suporte necessário para que possua alta disponibilidade.

6.3.31. Requisitos de garantia, manutenção e suporte técnico

6.3.31.1. Os requisitos mínimos exigidos neste subitem são justificados pela necessidade de não somente implantar a solução, porém mantê-la em funcionamento ininterrupto, provendo disponibilidade e desempenho durante toda a execução do contrato, através de equipe técnica especializada e apoio do fabricante na análise de problemas e atualização de seus produtos quanto à evolução tecnológica, correção de erros e vulnerabilidades e adaptação às mudanças de ambiente;

6.3.31.2. Quanto ao serviço de prestação dos serviços de Suporte Técnico Especializado, reforçamos que, apesar de fundamentalmente tratar-se de outsourcing de solução de tecnologia da informação, é evidente que o suporte técnico é primordial para a manutenção da plataforma de gerenciamento, proteção e inspeção de tráfego em redes corporativas, conforme justificamos abaixo:

6.3.31.2.1. O ambiente de rede corporativa e o ambiente de rede do Datacenter do Tribunal de Contas do Estado de Mato Grosso do Sul a ser suportado pela solução a ser contratada, é crítico para manutenção dos serviços deste Tribunal. Qualquer evento que ocasione a parada ou mal funcionamento do ambiente computacional assegurado pela tecnologia em questão poderá causar prejuízos diretos e indiretos para o Tribunal, incluindo a interrupção da rede de dados em todos ou em parte dos sistemas de informação, nos serviços prestados em formato digital, ou

consequências mais críticas como a perda ou roubo de dados críticos e/ou sigilosos, ataques de vírus, hackers e outras ameaças virtuais, e ainda a completa paralização da prestação de serviços públicos mantidos pelo ambiente de tecnologia em questão;

6.3.31.2.2. Considerando que as atividades da Secretaria de Tecnologia da Informação são realizadas ininterruptamente, não se justifica que os serviços de suporte técnico sejam prestados somente em horário comercial, bem como não haja meios digitais para que estes sejam solicitados. Ademais, o atendimento local é essencial, considerando que problemas que demandem intervenção física nas plataformas são comumente necessários;

6.3.31.2.3. Destacamos que o modelo de assistência local e ininterrupta não se trata de novação, sendo que é comum no mercado que as empresas que possuem produtos desta natureza, equivalentes ao esperado neste processo, prestem os serviços almejados dentro dos requisitos estabelecidos;

6.3.31.3. Tipos de serviços de suporte técnico e manutenção:

6.3.31.3.1. Manutenção Preventiva: Compreende visitas periódicas, conforme política definida pelo fabricante, no ambiente da Contratante, programadas a fim de verificar a saúde do equipamento e mitigar riscos devido ao uso continuado dos serviços, incluindo:

6.3.31.3.1.1. Procedimentos técnicos destinados a prevenir a ocorrência de erros e defeitos de forma proativa;

6.3.31.3.1.2. Realização de inspeções nos equipamentos, componentes, dispositivos e softwares de configuração gerenciam a solução;

6.3.31.3.1.3. Verificação geral com vistas a manter sua plena funcionalidade e saúde dos equipamentos;

6.3.31.3.1.4. Analisar logs de sistema e sugerir mudanças para uma melhor prática de utilização da ferramenta. A equipe técnica da Contratante decidirá sobre a aplicação ou não das recomendações;

6.3.31.3.1.5. Sugerir, preventivamente, a aplicação de novas correções, patches, fixes, updates, service packs, novas releases, versions, builds e upgrades.

6.3.31.3.2. Manutenção Corretiva: Compreende visitas pontuais, a partir de abertura de chamados advindos do Contratante, a fim de atuar em incidentes ou problemas identificados que impeça o seu funcionamento regular e requeira uma intervenção técnica especializada, na localidade de instalação da solução, incluindo:

6.3.31.3.2.1. Reinstalação de hardwares e softwares, configuração, gerenciamento, com vistas a normalidade da operação dos serviços prestados;

6.3.31.3.2.2. Reparar, corrigir, remover, refazer ou substituir, no todo ou em parte, os serviços, peças ou materiais em que se verificarem imperfeições, vícios, defeitos ou incorreções, dentro dos prazos estabelecidos nos demais subitens deste estudo;

6.3.31.3.2.3. Corrigir defeitos de fabricação ou projeto;

6.3.31.3.2.4. Acondicionar adequadamente os equipamentos cujo reparo não possa ser realizado nas dependências do TCE-MS, de forma a permitir sua completa segurança e identificação durante o transporte, responsabilizando-se pela sua remoção e devolução ao local em que deve ser instalado e pelas despesas operacionais decorrentes;

6.3.31.3.2.5. Substituir os equipamentos que apresentarem defeito de fabricação, dentro dos prazos estabelecidos;

6.3.31.3.2.6. Detectar problemas e limitações de desempenho da solução relacionados a softwares e/ou firmware instalados nos elementos que fazem parte do objeto desta contratação, substituindo-os por nova versão que implemente suas correções;

6.3.31.3.2.7. Substituir software e/ou firmware instalados nos elementos que fazem parte do objeto desta contratação por nova versão eventualmente lançada, quando esta implementar correções a possíveis problemas ou limitações de desempenho da solução.

6.3.31.4. Suporte técnico especializado e manutenção prestados pela Contratada:

6.3.31.4.1. A licitante deverá apresentar declaração de que proverá suporte técnico on-site disponível 24 horas por dia, 07 dias por semana, durante a validade do contrato.

6.3.31.4.2. A licitante deverá apresentar declaração de que possui plataforma de suporte técnico para abertura de chamados disponível através da internet (Web), telefone

ou e-mail, durante a validade do contrato, conforme especificações descritas no subitem - “Requisitos do sistema de gestão de serviços”.

6.3.31.4.3. A Contratada deverá, de acordo com as políticas de assistência técnica do fabricante da solução, prestar os serviços de suporte técnico especializado e manutenção para toda a solução de hardware e software, para orientação de uso e administração, atualização de versões, patchs e correções de bugs, configuração e parametrização, durante toda a vigência do contrato;

6.3.31.4.4. O funcionamento da solução deverá ser garantido pela Contratada durante toda a vigência do contrato, que deverá se valer dos meios necessários para manter a solução operacional;

6.3.31.4.5. Poderão ser prestados pela empresa Contratada em ambiente on-site ou remoto, no regime 24X7, incluindo a atualização de softwares e bases de dados de conhecimento as suas expensas, e, sempre que for necessário ao bom funcionamento da solução adquirida;

6.3.31.4.6. Deverão ser executados por técnicos qualificados, conforme previsto nos requisitos de qualificação da equipe técnica presentes neste documento;

6.3.31.4.7. Quando realizados presencialmente, deverão ser prestados no endereço indicado pelo Contratante;

6.3.31.4.8. Todas as peças e componentes necessários ao perfeito funcionamento de toda a solução, quando necessário, devem ser substituídos pela Contratada, sem nenhum custo adicional a Contratante;

6.3.31.4.9. A Contratada deverá cumprir rigorosamente todos os procedimentos de manutenção definidos pelo TCE-MS,

como horário estabelecido para parada dos equipamentos, autorizações de acesso, entre outros;

6.3.31.4.10. Quando a intervenção implicar interrupção da solução, mesmo que parcial, o TCE-MS poderá determinar que a Contratada a execute fora do horário de expediente do órgão, inclusive em finais de semana, sem qualquer ônus adicional a Contratante;

6.3.31.4.11. Fica vedada a desativação de hardware, software ou quaisquer recursos computacionais da Contratante, sem prévio conhecimento e autorização expressa da Administração;

6.3.31.4.12. Caso seja necessária a desativação de hardware, software ou quaisquer recursos computacionais do TCE-MS, a Contratada deverá disponibilizar equipamento de redundância com capacidade igual ou superior ao que será desativado, até que o problema seja sanado, sob pena de inexecução parcial do contrato;

6.3.31.4.13. Em caso de retirada do equipamento, o TCE-MS poderá, a seu critério, reter as unidades de memória física dos equipamentos, sem custo adicional;

6.3.31.4.14. Havendo necessidade de substituição de hardware (equipamentos), a Contratada deverá efetuar a substituição por mesmo modelo de peça, ou por modelo superior em características técnicas, do mesmo fabricante, sem ônus para o Contratante, quando comprovados defeitos que comprometem seu desempenho, obedecendo os critérios abaixo, sem prejuízo de outras situações que caracterizem necessidade de troca:

6.3.31.4.14.1. Caso ocorram 04 (quatro) ou mais defeitos que comprometam seu uso normal, dentro de qualquer intervalo de 30 (trinta) dias;

6.3.31.4.14.2. O equipamento (hardware) empregado em substituição ao equipamento defeituoso deverá ter os mesmos serviços de suporte técnico e manutenção durante toda a vigência restante do contrato;

6.3.31.4.14.3. No caso de problema recorrente no mesmo hardware, seja na restauração ou substituição das peças, em um período inferior a 2 (dois) meses, a Contratada deverá substituir o equipamento.

6.3.31.4.15. Quando solicitado pelo TCE-MS, a Contratada deverá fornecer, em até 3 (três) dias úteis, manuais, documentação de operação, documentos de troubleshooting e/ou qualquer outro tipo de documento técnico de administração, customização, operação e monitoração dos equipamentos e softwares instalados no TCE-MS;

6.3.31.4.16. As atualizações de versões de todos os componentes da solução (major, minor, patches e fixes) deverão estar disponíveis para uso do TCE-MS durante todo período contratual e sem custo adicional, podendo ser realizado download diretamente do sítio oficial do fabricante, devendo ser entregue, a última versão vigente na data do término do contrato.

6.3.31.5. Suporte técnico especializado e manutenção prestados pelo Fabricante:

6.3.31.5.1. A prestação destes serviços deve ainda contemplar o suporte técnico direto do fabricante da solução, a ser

utilizado sempre que necessário, e pelo período vigente do contrato com, no mínimo, as seguintes características:

6.3.31.5.1.1. O suporte do fabricante deve ter um sistema de abertura de chamados para acompanhamento, 24 horas por dia e 7 dias por semana. Para atendimento telefônico, deve operar em língua portuguesa, pelo menos em regime 8x5 (oito horas por dia, sete dias por semana);

6.3.31.5.1.2. Deve-se assegurar a utilização de novas versões de software da solução sem ônus, sempre que esta estiver disponível;

6.3.31.5.1.3. Deve-se permitir o acesso à base de conhecimento da solução.

6.3.31.6. Sempre que solicitado pela Contratante, deve-se informar o estado do chamado aberto, por telefone da central de atendimento e/ou por sistema de controle de chamados da Contratada disponibilizado pela internet:

6.3.31.6.1. Caso o chamado seja repassado pela Contratada ao fabricante, o TCE-MS deverá ter capacidade visualizar diretamente no sítio do fabricante o andamento desse chamado;

6.3.31.6.2. Deverão ser fornecidas permissões de acesso no sítio do fabricante e da Contratada para acompanhamento de chamados, download e acesso a documentação, patches, fixes, firmwares, arquivos de qualquer tipo e/ou qualquer outro material referente à solução.

6.3.31.7. Núcleo de Operações, Controle e Segurança:

6.3.31.7.1. A licitante deverá manter um SNOC (Centro de Operações de Segurança e Redes), nas dependências da Contratante, para diagnosticar preventivamente e

corretivamente problemas nas soluções fornecidas e tomar as decisões de intervenção para a devida assistência técnica.

6.3.31.7.2. O SNOC deverá ser composto por ambiente de monitoramento das soluções e deverá ser mantido pela Contratada em regime 24 x 7 (vinte e quatro horas por dia, sete dias por semana), durante a vigência do contrato, para prestar o pronto-atendimento as solicitações de suporte de primeiro e segundo nível identificadas no SNOC e/ou usuários finais da solução;

6.3.31.7.3. A contratada deverá implantar, monitorar e administrar os serviços de monitoração da solução implementada, com as atividades de coleta de dados, gerenciamento de configuração de templates e gatilhos nas plataformas de monitoramento Zabbix e Grafana, atualmente utilizadas pelo TCE-MS para monitoramento de sua infraestrutura de TIC como um todo.

6.3.31.7.4. A contratada deverá monitorar e analisar toda a infraestrutura do Tribunal de Contas do Estado do Mato Grosso do Sul, utilizando-se de análise dos logs disponibilizados em tempo real através da Plataforma de SIEM/SOAR que deverá ser fornecida pela Contratada. Para o devido dimensionamento do esforço de trabalho necessário, a Plataforma de SIEM/SOAR deverá coletar eventos que representam aproximadamente 2.000 EPS;

6.3.31.7.5. A estrutura de SNOC é comumente utilizada em ambientes de tecnologia e de comunicação, com o objetivo de exercer gerenciamento proativo, o monitoramento da qualidade, desempenho e nível de serviços e a resposta à incidentes ocorridos ou iminentes.

6.3.31.7.6. Neste aspecto, a existência de um SNOC é essencial para ambientes que possuam soluções complexas ou críticas para continuidade de negócio, o que se configura na contratação em tela, considerando que a solução em questão manterá o gerenciamento de tráfego de aplicações e que envolvem a segurança dos dados e informações críticos, sigilosos e de alto valor para os entes que almejam sua contratação.

6.3.31.7.7. Longe de configurar inovação, os ambientes de SNOC são corriqueiramente utilizados por empresas que prestam tais serviços, visto que os incidentes envolvidos em ambientes não monitorados por vezes gera impacto maior do que o próprio custo da manutenção do núcleo.

6.3.31.7.8. Por fim, esclarecemos que a planilha de composição de custos prevê os valores referentes ao “serviço de suporte 24x7”, sendo que os custos para manutenção do SNOC estão incluídos neste quesito, pois o ambiente em questão é voltado para o suporte técnico das soluções.

6.3.31.8. Acordos de Nível de Serviços

6.3.31.8.1. Para a prestação dos serviços de Suporte Técnico Especializado, Manutenção e Apoio:

6.3.31.8.2. A CONTRATADA deverá cumprir rigorosamente todos os procedimentos de manutenção definidos pelo TCE-MS, como horário estabelecido para parada dos equipamentos, autorizações de acesso, entre outros.

6.3.31.8.3. Quando a intervenção implicar interrupção da solução, mesmo que parcial, o TCE-MS poderá determinar que a CONTRATADA a execute fora do horário de expediente do órgão, inclusive em finais de semana, sem qualquer ônus adicional ao TCE-MS.

6.3.31.8.4. Fica vedada a desativação de hardware, software ou quaisquer recursos computacionais da CONTRATANTE, sem prévio conhecimento e autorização expressa da Administração;

6.3.31.8.5. Caso seja necessária a desativação de hardware, software ou quaisquer recursos computacionais do TCE-MS, a CONTRATADA deverá disponibilizar equipamento de redundância com capacidade igual ou superior ao que será desativado, até que o problema seja sanado, sob pena de inexecução parcial do contrato;

6.3.31.8.6. Em caso de retirada do equipamento, o TCE-MS poderá, a seu critério, reter as unidades de memória física dos equipamentos, sem custo adicional.

6.3.31.8.7. Havendo necessidade de substituição de hardware (equipamentos), a Contratada deverá efetuar a substituição por mesmo modelo de peça, ou por modelo superior em características técnicas, do mesmo fabricante, sem ônus para o Contratante, quando comprovados defeitos que comprometem seu desempenho, obedecendo os critérios abaixo, sem prejuízo de outras situações que caracterizem necessidade de troca:

6.3.31.8.8. Caso ocorram 04 (quatro) ou mais defeitos que comprometam seu uso normal, dentro de qualquer intervalo de 30 (trinta) dias;

6.3.31.8.9. O(s) equipamento(s) (hardware) empregado em substituição ao equipamento defeituoso deverá possuir prazo equivalente a vigência do contrato;

6.3.31.8.10. No caso de problema recorrente no mesmo hardware, seja na restauração ou substituição das peças, em um

período inferior a 2 (dois) meses, a CONTRATADA deverá substituir o equipamento.

6.3.31.8.11. Mensalmente, deverá ser entregue um “Relatório de Atividades Técnicas” indicando todos os eventos de suporte técnico e manutenção atendidos no período. O Relatório deverá conter no mínimo:

6.3.31.8.11.1. Identificação de cada chamado;

6.3.31.8.11.2. Identificação do tipo de atendimento;

6.3.31.8.11.3. Data de atendimento (abertura e conclusão);

6.3.31.8.11.4. Descrição do atendimento;

6.3.31.8.11.5. Procedimentos adotados para a solução do problema;

6.3.31.8.12. Sem prejuízo da entrega do Relatório Gerencial, a CONTRATANTE poderá solicitar, em formato digital, informações analíticas e sintéticas dos chamados técnicos abertos e fechados no período;

6.3.31.8.13. Quando solicitado pelo TCE-MS, a CONTRATADA deverá fornecer, em até 3 (três) dias úteis, manuais, MIB de monitoração, documentação de interfaces API, documentos de troubleshooting e/ou qualquer outro tipo de documento técnico de administração, customização, operação e monitoração dos equipamentos e softwares instalados no TCE-MS.

6.3.31.8.14. As atualizações de versões de todos os componentes da solução (major, minor, patches e fixes) deverão estar disponíveis para uso do TCE-MS durante todo período contratual e sem custo adicional, podendo ser realizado download diretamente do sítio oficial do fabricante, devendo ser entregue, a última versão vigente na data do término do contrato.

6.3.31.8.15. A licitante deverá apresentar declaração de que cumprirá os tempos para resolução de chamados abertos, seguindo as seguintes premissas de S.L.A. (Acordos de Níveis de Serviços):

6.3.31.8.16. O tempo de solução será contabilizado entre a abertura do chamado e restabelecimento do sistema em sua totalidade, bem como se entende por término do reparo do equipamento a sua disponibilidade para uso em perfeitas condições de funcionamento no local onde está instalado.

6.3.31.8.17. O tempo de atendimento inicia-se com a primeira intervenção pelo representante da CONTRATADA, local ou remotamente.

6.3.31.8.18. A contratada deverá se adequar aos seguintes níveis de serviço quando ocorrerem os chamados para Suporte Técnico Especializado, Manutenção e Apoio:

MANUTENÇÃO PREVENTIVA					
Indicador	Tipo do Chamado	Descrição	Inicio do atendimento	Prazo de Solução	Multa por descumprimento % em relação a fatura de suporte
N01	Manutenção Programada	Suporte programado para verificação da saúde dos equipamentos e proposição de melhorias.	Na data Programada mensalmente conforme cronograma	Execução dentro do período programado no chamado	2% por mês em que houver descumprimento por não atendimento.
MANUTENÇÃO CORRETIVA					

Indicador	Tipo do Chamado	Descrição	Inicio do atendimento	Prazo de Solução	Multa por descumprimento % em relação a fatura de suporte
N02	Urgente	Solução parada, no todo ou em parte, no ambiente de produção provocando uma indisponibilidade parcial ou total do ambiente de produção da CONTRATANTE durante programas de governo em período de sazonalidade.	Em até 02 (duas) horas	Em até 06 (seis) horas	2% por hora para as 4 primeiras horas que excederem o prazo; 4% por hora para as demais horas que excederem as primeiras 4 horas de descumprimento prazo.
N03	Alto Impacto	Solução parada, no todo ou em parte, no ambiente de produção provocando ao menos uma indisponibilidade parcial do ambiente de produção da CONTRATANTE.	Em até 04 (quatro) horas	Em até 12 (doze) horas	1% por hora para as 4 primeiras horas que excederem o prazo; 2% por dia que exceder o descumprimento prazo de solução.
N04	Muito Importante	Erros ou problemas reincidentes que impactam	Em até 08 (quatro) horas	Em até 24 (vinte e quatro) horas	1% por dia que exceder o descumprimento do prazo de

		o ambiente de produção.			solução.
N05	Importante	Problemas contornáveis que não causem lentidão ou indisponibilidade dos serviços ou aqueles para os quais houver solução de contorno.	Em até 24 (vinte e quatro) horas	Em até 2 dias	0,5% dia que exceder o descumprimento do prazo de solução.

NÍVEL DE SERVIÇO PARA A DOCUMENTAÇÃO DE TODOS OS SERVIÇOS		
Indicador	Descrição	Multa por descumprimento % em relação a fatura de suporte
N10	Relatório de Atendimento Técnico não entregue	0,25% em relação ao valor do equipamento por dia ocorrência ou documento.
N11	Reincidência na entrega de Relatório de Atendimento Técnico	1 % por ocorrência ou documento reincidente. Caso exceda 3 ocorrências, de forma cumulativa ou não, será considerado inexecução parcial do objeto.

6.3.31.8.19. Somente será admitido pedido de prorrogação dos prazos descritos na tabela de níveis de serviços mediante justificativas por escrito, plenamente fundamentadas e entregues à Administração dentro do período correspondente ao atendimento ou resolução do chamado aberto;

6.3.31.8.20. A não resolução dos chamados dentro do prazo acima estipulado ensejará às multas e sanções previstas. Após o limite estabelecido para aplicação das multas a

CONTRATADA deverá substituir os equipamentos conforme prazos e condições descritas abaixo, sob pena de incorrer em inexecução total do contrato:

6.3.31.8.21. Se o atendimento classificado como URGENTE não for resolvido dentro do prazo estabelecido, mesmo após a execução dos serviços de reparo (atualização de softwares/substituição de peças de hardware), o equipamento deverá ser integralmente substituído no prazo máximo de 02 (dois) dias, segundo as características técnicas e de desempenho iguais ou superiores ao bem anterior de modo que não cause nenhum impacto no serviço sustentado pelos equipamentos, sem ônus para a CONTRATANTE, sob pena de caracterizar inexecução parcial do contrato;

6.3.31.8.22. Se o problema identificado como ALTO IMPACTO persistir pós-atendimento técnico, e não for resolvido de forma definitiva pela empresa contratada dentro do prazo estabelecido, podendo ser prorrogado por igual período (corrido), desde que justificado, o produto deverá ser integralmente substituído no prazo máximo de 04 (quatro) dias, segundo as características técnicas e de desempenho iguais ou superiores ao bem anterior, sem ônus para a CONTRATANTE, sob pena de caracterizar inexecução parcial do contrato;

6.3.31.8.23. Se o problema identificado como MUITO IMPORTANTE persistir pós-atendimento técnico, e não for resolvido de forma definitiva pela empresa contratada dentro do prazo estabelecido, podendo ser prorrogado por igual período (corrido), desde que justificado, o produto deverá ser integralmente substituído no prazo

máximo de 07 (sete) dias, segundo as características técnicas e de desempenho iguais ou superiores ao bem anterior, sem ônus para a CONTRATANTE, sob pena de caracterizar inexecução parcial do contrato;

6.3.31.8.24. Se o problema identificado como IMPORTANTE não for resolvido de forma definitiva pela empresa contratada dentro do prazo estabelecido, podendo ser prorrogado por igual período (corrido), desde que justificado, a partir do sétimo dia, será aplicada glosa de 1% (um por cento) ao dia sobre o valor do faturamento mensal até que o problema seja integralmente sanado, limitado a 30 (trinta) dias, após esse prazo será caracterizado inexecução parcial do contrato;

6.3.31.8.25. Se após 30 (trinta) dias a contar da notificação de aplicação da multa por inexecução parcial do contrato a CONTRATADA não substituir os equipamentos, será caracterizado inexecução total do contrato, sem prejuízo da continuidade do suporte técnico dos demais equipamentos em garantia;

6.3.31.8.26. Sempre que o TCE-MS solicitar, o estado do chamado aberto com a CONTRATADA deverá ser informado por telefone da central de atendimento e/ou por sistema de controle de chamados da CONTRATADA disponibilizado pela internet.

6.3.31.8.27. Caso o chamado seja repassado pela CONTRATADA ao fabricante, o TCE-MS deverá ter capacidade visualizar diretamente no sítio do fabricante o andamento desse chamado.

6.3.31.8.28. Deverão ser fornecidas permissões de acesso no sítio do fabricante e da CONTRATADA para acompanhamento

de chamados, download e acesso a documentação, patches, fixes, firmwares, arquivos de qualquer tipo e/ou qualquer outro material referente à solução.

6.3.31.8.29. Todos os firmwares publicados deverão estar disponíveis para consulta e download pelo TCE-MS diretamente no sítio do fabricante.

6.3.31.8.30. A inobservância das condições aqui estabelecidas sujeitará a CONTRATADA às penalidades previstas neste estudo e sanções administrativas a serem definidas na minuta de contrato.

6.3.31.8.31. Quanto ao serviço de prestação dos serviços de Suporte Técnico Especializado, reforçamos que, apesar de fundamentalmente tratar-se de outsourcing de solução de tecnologia da informação, é evidente que os serviços de suporte técnico a serem prestados pela empresa Contratada são primordiais para a manutenção da plataforma de gerenciamento de tráfego de aplicações e aceleração web, conforme justificamos abaixo:

6.3.31.8.32. O ambiente suportado pelas soluções de gerenciamento de tráfego de aplicações e aceleração web a serem contratadas é crítico para manutenção dos serviços públicos dos entes em questão. Qualquer evento que ocasione a parada ou mal funcionamento do ambiente computacional assegurado pela tecnologia em questão poderá causar prejuízos diretos e indiretos para o Estado, incluindo a interrupção da rede de dados dos órgãos atendidos, a perda ou roubo de dados críticos e/ou sigilosos, ataques de vírus, hackers e outras ameaças virtuais, e ainda a completa paralização da prestação de

serviços públicos mantidos pelo ambiente de tecnologia em questão.

6.3.31.8.33. Considerando que as atividades desta Coordenadoria são realizadas ininterruptamente, não se justifica que os serviços de suporte técnico sejam prestados somente em horário comercial, bem como não haja meios digitais para que estes sejam solicitados. Ademais, o atendimento local é essencial, considerando que problemas que demandem intervenção física nas plataformas são comumente necessários.

6.3.31.8.34. Destacamos que o modelo de assistência local e ininterrupta não se trata de novação, sendo que é comum no mercado que as empresas que possuem produtos de gerenciamento de tráfego de aplicações e aceleração web equivalentes ao esperado neste processo prestem os serviços almejados dentro dos requisitos estabelecidos.

6.3.31.8.35. As empresas participantes com sede em outras localidades deverão apresentar declaração de que caso seja vencedora do certame, se compromete a estabelecer equipe de suporte técnico local para atender de forma satisfatória os acordos de níveis de serviço (SLA) previstos neste Termo de Referência em até 15 dias, a contar da assinatura do contrato.

6.3.31.8.36. Quanto a exigência prevista no item anterior, reforçamos que a exigência está diretamente relacionada a prestação dos serviços de suporte técnico on-site, previstos neste termo de referência.

6.3.31.8.37. Neste cenário, e considerando ainda os acordos de níveis de serviço previstos neste termo de referência, não há viabilidade para que a Contratada realize o suporte on-

site, iniciando o atendimento em até 2 horas e encerrando-o em até 6 horas, caso não possua escritório no município onde a solução esteja instalada.

6.3.31.8.38. Destarte, esclarecemos que a empresa terá até 15 dias para providenciar a instalação de tal ambiente, caso sagre-se vencedora do certame, a contar da assinatura do contrato, o que novamente afasta a criação de ônus antecipado aos licitantes e ainda não restringe a participação de empresas de outras localidades.

6.3.32. Requisitos de implantação

6.3.32.1. O gerenciamento dos equipamentos e serviços dará de forma remota e presencial, manutenção preventiva e corretiva desta. Essa medida visa garantir a adequada gestão, manutenção preventiva, corretiva dos serviços, considerando a ausência de mão de obra especializada no quadro de pessoal do tribunal para acompanhar as tarefas que envolvem tais tecnologias.

6.3.32.2. As especificações detalhadas do gerenciamento presencial e remoto estão descritas no Estudo Técnico Preliminar.

6.3.32.3. A contratada também disponibilizará um preposto para acompanhar a execução do contrato, atuar como interlocutor principal junto à CONTRATANTE, receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual.

6.3.33. Requisito de experiencia profissional

6.3.33.1. Todos os serviços deverão ser prestados por profissionais devidamente capacitados na solução técnica em questão, bem como com todos os recursos ferramentais necessários para a execução dos serviços.

6.3.33.2. As qualificações e requisitos mínimos de experiência exigidas dos profissionais que deverão ser disponibilizadas pela CONTRATADA para executar as atividades objetos desta contratação são detalhados abaixo:

6.3.33.2.1. Os profissionais em atividade no contrato deverão apresentar comprovação documental de certificações e domínio técnico relacionados às atividades periódicas previstas no termo de referência futuro.

6.3.33.2.2. É imprescindível que os profissionais possuam experiência comprovada nos sistemas que compõem o ambiente técnico desta contratação, com ênfase no atendimento às necessidades específicas deste Tribunal.

6.3.34. Requisitos do sistema de gestão de serviços:

6.3.34.1. A CONTRATADA deverá dispor de solução informatizada de Gestão de Serviços, com interface Web, voltada à operação e gestão dos atendimentos realizados, a ser acessada a partir das dependências da CONTRATANTE. Esta solução poderá conter interfaces para controle dos processos de gerenciamento de incidentes, de problemas, de configurações, de mudanças e da base de conhecimento.

6.3.34.2. A solução deverá ser baseada em ITIL;

6.3.34.3. A seguir são detalhados os recursos mínimos obrigatórios e as características operacionais e de tecnologia requeridos para o Sistema de Gestão da Central de Serviços a ser disponibilizado e implantado pela CONTRATADA:

6.3.34.3.1. Ser multiusuário.

6.3.34.3.2. Possuir manuais e help de utilização atualizados.

6.3.34.3.3. Manter registro de log das atividades.

6.3.34.3.4. A Solução Informatizada deve ter implementados os seguintes processos:

6.3.34.3.4.1. Gerenciamento de Incidente.

6.3.34.3.4.2. Gerenciamento de Problema.

6.3.34.3.4.3. Gerenciamento de Filas de atendimento

6.3.34.3.4.4. Gerenciamento de Mudança.

6.3.34.3.4.5. Gerenciamento de Catálogo de Serviços.

6.3.34.3.4.6. Gerenciamento de Conhecimento.

6.3.34.3.4.7. Gerenciamento de Configuração e Ativos.

6.3.34.3.4.8. Gerenciamento de Níveis de Serviço.

6.3.34.3.4.9. Gerenciamento de Pesquisa Satisfação

6.3.34.3.4.10. Gerenciamento de SLA

6.3.34.3.4.11. Gerenciamento de Integrações com outras ferramentas.

6.3.34.3.5. Os processos descritos no item anterior deverão fazer parte de uma Solução Informatizada única.

6.3.34.3.6. A CONTRATADA deverá possuir meios para alterar, configurar e adaptar o sistema às necessidades da CONTRATANTE.

6.3.34.3.7. A base de dados do Sistema de Gestão deverá ser implementada, obrigatoriamente, em SGBD (Sistema de Gerenciamento de Banco de Dados) de domínio da CONTRATADA: ORACLE, MYSQL ou POSTGRES, com versões compatíveis com as existentes e suportadas pelo TCE-MS.

6.3.34.3.8. A solução deverá permitir registrar, em banco de dados, todos os atendimentos realizados, com número do chamado, horário de abertura/alteração/conclusão, status do atendimento, identificador do equipamento (tipo, patrimônio, marca, modelo), demandante (nome, email, telefone, lotação), técnico responsável pelo atendimento, descrição da situação transmitida pelo demandante,

procedimentos adotados (solução), identificação da tarefa.

6.3.34.3.9. A ferramenta deverá registrar o horário e o responsável por quaisquer alterações nos registros.

6.3.34.3.10. Todos os chamados (incidentes, requisições, problemas, mudanças) deverão referenciar a um item de configuração.

6.3.34.3.10.1. Caso, na abertura do chamado, identifique-se que o IC (item de configuração) não esteja cadastrado no CMDB (Banco de Dados de Gerenciamento de Configuração), a Solução Informatizada deverá abrir uma requisição de mudança, de forma automática, solicitando o cadastro do IC. O chamado do usuário deverá ser atendido normalmente.

6.3.34.3.10.2. A requisição de mudança gerada no item anterior deverá ser automaticamente associada ao chamado do usuário.

6.3.34.3.11. A solução deverá permitir:

6.3.34.3.11.1. O encaminhamento/escalonamento automático e manual das solicitações de serviços e chamados para um técnico ou para um grupo de trabalho responsável.

6.3.34.3.11.2. A parametrização e a customização dos Níveis Mínimos de Serviço exigidos em Edital, e de acordo com as necessidades dos usuários, departamentos, unidades da CONTRATANTE e assunto, sempre determinando de forma automática os prazos previstos para cada chamado.

6.3.34.3.11.3. O agendamento de lembretes com notificação por e-mail ou na tela inicial da Solução (mural de informações).

6.3.34.3.11.4. A integração com sistemas de e-mail.

6.3.34.3.11.5. A importação de IC's já existentes em inventário e gestão de ativos.

6.3.34.3.11.6. A abertura de chamados via e-mail, web e ferramentas de monitoramento de rede.

6.3.34.3.11.7. A abertura de chamados, devolvendo automaticamente, via e-mail, ao usuário solicitante, um recibo de comprovação da abertura do chamado, quando este informar e-mail institucional da CONTRATANTE.

6.3.34.3.11.8. O autoatendimento logo que o usuário abrir um incidente. O autoatendimento deve prover soluções de contorno, acesso a base de conhecimento (de acordo com o tipo do incidente), telas de perguntas e respostas (possíveis erros e suas possíveis soluções).

6.3.34.3.11.9. Que Níveis Mínimos de Serviço (NMS) sejam especificados por aplicação ou por combinação aplicação/servidor, e possuir janela na interface gráfica que demonstre a situação de acordo com os parâmetros estabelecidos. Caso sejam ultrapassados a solução fará a notificação através da console e/ou envio de mensagem eletrônica.

6.3.34.3.11.10. A criação de alertas, de acordo com regras pré-estabelecidas.

6.3.34.3.11.11. Notificar os níveis superiores de gestão de maneira automática caso um chamado se aproxime dos valores-limite (thresholds) pré-definidos.

6.3.34.3.12. Cada técnico e analista da CONTRATADA deverá ter um login e uma senha específicos para acesso, possibilitando a realização de análises pessoais e o mapeamento de atendimentos.

6.3.34.3.13. A CONTRATADA deverá disponibilizar acessos licenciados à CONTRATANTE em quantidade necessária para que todas as solicitações vinculadas aos serviços de TI possam ser registradas na ferramenta, de forma a possibilitar a criação e a atualização de requisições de serviços, eventos e incidentes, problemas, mudanças, liberações, geração de pesquisas e relatórios, catálogo de serviços, conhecimento, configurações, níveis de serviços e quaisquer outros que requererem a permissão de acesso.

6.3.34.3.14. A ferramenta deverá permitir:

6.3.34.3.15. Operar em ambiente WEB, possibilitando ao usuário abertura de chamados, consultas de chamado e acesso à base de conhecimentos, acesso a uma base de FAQ (perguntas e respostas frequentes) com o uso de browser padrão de mercado.

6.3.34.3.16. Consultar scripts de atendimento armazenados em base de conhecimento.

6.3.34.3.17. Controlar e gerenciar os chamados registrados.

6.3.34.3.18. Monitorar os ativos e serviços, com a atribuição de limites de alertas por meio do envio de mensagens de correio eletrônico aos técnicos e administradores cadastrados.

6.3.34.3.19. Enviar e-mail ao usuário demandante quando da conclusão do chamado no sistema.

6.3.34.3.20. Dispor de rotinas de backup que permitam recuperação da base de dados em caso de perda.

6.3.34.3.21. Fornecer, pelo menos, os seguintes relatórios/consultas, exportáveis para os formatos (HTML, PDF, XLS, CSV, dentre outros):

6.3.34.3.22. Relatórios para aferição dos níveis de serviço.

6.3.34.3.23. Indicadores de desempenho dos grupos de 1°, 2° e 3° níveis, incluindo quantidade de chamados atendidos, quantidade de chamados abertos e concluídos, tempo médio de atendimento e tempo de trabalho efetivo.

6.3.34.3.24. Estatísticas de atendimento por itens, período, assunto, usuário, grupos, departamentos, status dos chamados e outros.

6.3.34.3.25. Estatísticas de atendimento confrontando níveis de serviço definidos versus os alcançados, por chamado ou, sinteticamente, por tarefa, sub-tarefa, tipo, assunto, usuário, grupos, departamentos e outros.

6.3.34.3.26. Resultados mensais de tempo de atendimento, histórico de falhas e ações de recuperação de serviços e equipamentos.

6.3.34.3.27. Relatórios de gestão e controle de chamados.

6.3.34.3.28. Permitir elaboração de inúmeras pesquisas de satisfação com perguntas chaves, utilizando filtros de fila e tipos de serviço.

6.3.34.3.29. Realizar estatísticas sobre as pesquisas de satisfação.

6.3.34.3.30. Enviar pesquisa de satisfação por e-mail do solicitante.

6.3.34.3.31. Exibir notificação sobre pesquisa de satisfação não respondida na interface do solicitante.

6.3.34.3.32. Os indicadores e relatórios deverão permitir o filtro de periodicidades, localidades, fornecedores, níveis de atendimento, categorização do catálogo de serviços, dentre outros.

6.3.34.3.33. Além dos relatórios e indicadores de desempenho solicitados neste Edital, novos itens podem ser adicionados aos relatórios e indicadores, desde que previamente acordados.

6.3.34.3.34. O sistema deverá possuir ainda, as seguintes funcionalidades:

6.3.34.3.34.1. Permitir o acompanhamento de todo o andamento do processo de atendimento de chamados técnicos e de requerimento de serviços.

6.3.34.3.34.2. Disponibilizar monitoramento de todos os atendimentos abertos e caso eles estejam fora do prazo dos Níveis Mínimos de Serviços acordados, deve-se possibilitar gerar alarmes automáticos.

6.3.34.3.34.3. Possibilitar o encerramento das ocorrências.

6.3.34.3.34.4. Possibilitar o controle de horas válidas.

6.3.34.3.34.5. Separar os tempos de atendimento e solução por nível de atendimento.

6.3.34.3.34.6. Permitir definições dos níveis de prioridade.

6.3.34.3.34.7. Gerenciar o tempo de resposta baseado nas definições de prioridades.

6.3.34.3.34.8. Gerenciar o tempo de solução baseado nas definições de categorias de incidentes.

6.3.34.3.34.9. Acessar a base de conhecimentos de incidentes e problemas resolvidos.

6.3.34.3.34.10. Controlar as dependências para o andamento do chamado.

6.3.34.3.34.11. Permitir a realização de consultas personalizadas.

6.3.34.3.34.12. Possibilitar que haja níveis diferentes para acesso ao sistema.

6.3.34.3.34.13. Gerar relatórios gerenciais.

6.3.34.3.34.14. Controlar os Níveis Mínimos de Serviço.

6.3.34.3.34.15. Interface web, acesso remoto e multiusuário.

6.3.34.3.35. A CONTRATADA manterá base de dados atualizada contendo cadastro de usuários, tabela de unidades funcionais e inventário de equipamentos da CONTRATANTE, com a finalidade de produzir relatórios estatísticos de atendimento por usuário, por unidade funcional e por equipamento.

6.3.34.3.36. A base de dados de equipamentos possuirá, necessariamente, um atributo contendo o número de patrimônio do equipamento, para permitir integração com o sistema de controle de patrimônio da CONTRATANTE.

6.3.34.3.37. A CONTRATANTE terá perfil de acesso permanente ao sistema para extrair informações atualizadas sobre o atendimento (consultas, relatórios, etc.), bem como para realização de auditorias.

6.3.34.3.38. A CONTRATADA disponibilizará à CONTRATANTE os manuais de utilização do sistema e erratas, sempre que forem feitas alterações que reflitam na documentação.

6.3.34.3.39. O sistema de gestão de serviços deverá possuir a capacidade de gerar fluxo conforme a demanda da

CONTRATANTE. Deverá possuir os seguintes os requisitos mínimos:

6.3.34.3.39.1. Capacidade de permite agendamento de criação de chamados automáticos (CRON), permitindo ao usuário descrever todos os requisitos do chamado assim como os horários e datas a serem criados.

6.3.34.3.39.2. A solução deverá oferecer APIs para comunicação com outras ferramentas, permitindo assim a criação, alteração e integração com os chamados.

6.3.34.3.39.3. A solução deverá permitir a implementação de fluxos de processos de acordo com a necessidade do TCE-MS, isto possibilita o encaminhamento do chamado por um caminho orientado pelo usuário, permitindo a customização de cada fase do fluxo onde os papéis de cada área, setor, departamento ou usuário serão definidos, conforme ilustração abaixo.

6.3.34.3.39.4. A solução deverá permitir a criação de formulários baseados em serviços, e também modelos de solicitações de acordo com a necessidade.

6.3.34.3.39.5. A solução deverá permitir a criação automática de chamados baseados em listas de tarefas. Onde um chamado baseando-se em um serviço pode seguir a regra de um modelo e gerar vários chamados

filhos para áreas diferentes, aguardando a conclusão destes para o chamado inicial ser concluído.

6.3.34.3.40. A CONTRATADA deverá prestar o suporte técnico da solução informatizada de Central de Serviços durante a vigência contratual.

6.3.35. Requisitos de execução do serviço e metodologia de trabalho:

6.3.35.1. A Contratada deverá designar profissionais conforme as necessidades que se verificarem com acompanhamento da equipe técnica exigida para esta contratação em observância ao volume e complexidade dos trabalhos, além das características decorrente da metodologia de trabalho.

6.3.35.2. Todas as atividades técnicas serão desempenhadas de acordo com o ambiente tecnológico do Tribunal de Contas do Estado de Mato Grosso do Sul, devendo, portanto, haver compatibilidade do perfil do profissional exigido para o desempenho da atividade.

6.3.35.3. Os serviços serão realizados no ambiente físico da Contratada que possibilitará todos os meios necessários para a Contratante acompanhar os trabalhos por meio do Gestor do Contrato designado ou qualquer outro servidor designado.

6.3.35.4. Quando os serviços forem realizados no ambiente físico da Contratante, os profissionais deverão executá-los conforme jornada de trabalho do TCE-MS, o que será controlado pela Contratada.

6.3.35.5. A licitante vencedora não poderá subcontratar, subempreitar, ceder ou transferir, total ou parcialmente o objeto da presente licitação descrita neste termo de referência.

6.3.35.6. A instalação dos equipamentos e a sua colocação em funcionamento correrão por conta e responsabilidade da Contratada;

6.3.35.7. Todos os itens necessários à instalação da solução correrão por conta da Contratada, como cabos, conectores e demais acessórios;

6.3.35.8. A solução deverá ser instalada em rack de piso, padrão 19", com medidas adequadas para acomodação da solução;

6.3.36. Requisitos de projeto:

6.3.36.1. Proteção Abrangente: A solução deve cobrir toda a rede de computadores do TCE/MS, abrangendo estações de trabalho, servidores de arquivos e dispositivos móveis.

6.3.36.2. Soluções Antimalware: Utilização de ferramentas antimalware de última geração, com capacidade de proteção em tempo real e resposta a incidentes.

6.3.36.3. Suporte Técnico Qualificado: A empresa contratada deve fornecer suporte técnico contínuo, garantindo a operação estável do ambiente tecnológico.

6.3.36.4. Monitoramento Contínuo: A solução deve incluir monitoramento em tempo real e atualizações regulares para mitigar ameaças.

6.3.36.5. Capacitação e Treinamento: Oferecimento de treinamento para a equipe de TI, assegurando o uso correto das soluções.

6.3.36.6. Manutenção Proativa: A solução deve prever manutenção preventiva e corretiva para evitar interrupções no serviço e garantir a segurança contínua.

6.3.36.7. Escalabilidade e Integração: A solução deve ser facilmente integrável ao ambiente atual do TCE/MS e flexível para futuras expansões.

6.3.36.8. Manutenção e As Built: Manutenção preventiva e corretiva, além de documentação "as built" para garantir conformidade e futuras expansões.

6.3.37. Requisitos sociais, ambientais e culturas:

6.3.37.1. Os produtos gerados em função da prestação dos serviços, bem como todas as documentações, deverão ser entregues no idioma Português do Brasil (pt-BR), com exceção de termos técnicos usuais que poderão ser apresentados em língua estrangeira.

6.3.37.2. Deverá a empresa contratada adotar práticas de sustentabilidade ambiental na execução do objeto, quando couber, conforme disposto na Instrução Normativa SLTI nº 01/2010, de 1º de janeiro de 2010, do Ministério do Planejamento, Desenvolvimento e Gestão.

6.3.38. Requisitos Legais:

6.3.38.1. Lei nº 14.133, de 1º de abril de 2021, que estabelece normas gerais de licitação e contratação para as Administrações Públicas diretas, autárquicas e fundacionais da União, dos Estados, do Distrito Federal e dos Municípios.

6.3.38.2. Instrução Normativa SGD/ME Nº 94, de 23 de dezembro de 2022, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

6.3.39. Requisitos da forma de seleção do fornecedor:

6.3.39.1. O serviço objeto desta contratação é caracterizado como serviço comum, pois possui especificação usual de mercado e padrão de qualidade definidas em Edital, para os fins do disposto no inciso XIII do art.6º da Lei Federal nº 14.133/2021.

6.3.39.2. Por esta razão, em cumprimento ao disposto no art. 25, Parágrafo único, da IN/SGD/ME nº 94/2022 c/c o art. 17, §2º, da Lei n. 14.133/2021, a futura licitação deverá ser processada por meio da modalidade “Pregão”.

6.3.39.3. Requisitos de segurança da informação e privacidade

6.3.39.4. A CONTRATADA deverá observar integralmente os requisitos de Segurança da Informação e Privacidade da CONTRATANTE.

6.3.39.5. A contratada não poderá se utilizar da presente contratação para obter qualquer acesso não autorizado às informações do Tribunal de Contas do Estado de Mato Grosso do Sul.

6.3.39.6. A contratada não poderá veicular publicidade acerca do fornecimento a ser contratado, sem prévia autorização, por escrito, do TCE/MS.

6.3.39.7. A contratada é responsável civil, penal e administrativa quanto à divulgação indevida ou não autorizada de informações, realizada por ela ou por seus empregados.

6.3.39.8. É de responsabilidade da contratada garantir que as informações por ela obtidas em decorrência da execução desta contratação sejam mantidas em sigilo, não podendo ser divulgadas, exceto se previamente acordado, por escrito, entre as partes contratantes.

6.3.39.9. É de responsabilidade da contratada garantir o tratamento de dados pessoais de acordo com a Lei Geral de Proteção de

Dados Pessoais com objetivo específico de assegurar a proteção, privacidade e transparência de dados de pessoas físicas.

6.3.39.10. O Termo de Confidencialidade deverá ser assinado pelo representante legal da Contratada e o Termo de Ciência pelos funcionários.

7. MODELO DE GESTÃO DO CONTRATO

7.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

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

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

7.4. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

7.5. Preposto

7.5.1. A CONTRATADA designará formalmente o preposto da empresa, antes do início da prestação dos serviços, indicando no instrumento os poderes e deveres em relação à execução do objeto contratado.

7.5.2. O TCE/MS poderá recusar, desde que justificadamente, a indicação ou a manutenção do preposto da empresa, hipótese em que a CONTRATADA designará outro para o exercício da atividade

7.5.3. O preposto atuará como ponto de contato principal entre a CONTRATADA e o TCE/MS e será responsável por receber, comunicar e tomar as devidas providências em relação a todas as questões contratuais.

7.5.4. Qualquer alteração no preposto designado pela CONTRATADA deve ser comunicado por escrito ao TCE/MS, e a CONTRATADA deve nomear um novo preposto dentro de 2 (dois) dias.

7.5.5. A CONTRATADA deve garantir que seu preposto seja plenamente informado sobre as obrigações contratuais, normas e regulamentos aplicáveis, bem como as políticas e procedimentos da instituição.

7.6. Reunião Inicial

7.6.1. Após a assinatura do Contrato e a nomeação do Gestor e Fiscais do Contrato, será realizada a Reunião Inicial de alinhamento com o objetivo de nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e seus anexos, e esclarecer possíveis dúvidas acerca da execução dos serviços.

7.6.2. A reunião será realizada em conformidade com o previsto no inciso I do Art. 31 da IN SGD/ME nº 94, de 2022, seguindo todos os prazos conforme estipulado em Item citado.

7.6.3. A pauta desta reunião observará, pelo menos:

7.6.4. Presença do representante legal da CONTRATADA, que apresentará o seu preposto;

7.6.5. Entrega, por parte da CONTRATADA, do Termo de Compromisso e dos Termos de Ciência;

7.6.6. esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato;

7.6.7. A Carta de apresentação do Preposto deverá conter no mínimo o nome completo e CPF do funcionário da empresa designado para acompanhar a execução do contrato e atuar como interlocutor

principal junto à CONTRATANTE, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual;

7.6.8. Apresentação das declarações/certificados do fabricante, comprovando que o produto ofertado possui a garantia solicitada neste termo de referência.

7.7. Fiscalização

7.7.1. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput), nos termos do art. 33 da IN SGD nº 94, de 2022, observando-se, em especial, as rotinas a seguir.

7.8. Fiscalização Técnica

7.8.1. O fiscal técnico do contrato, além de exercer as atribuições previstas no art. 33, II, da IN SGD nº 94, de 2022, acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração. (Decreto nº 11.246, de 2022, art. 22, VI);

7.8.2. 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. (Lei nº 14.133, de 2021, art. 117, §1º, e Decreto nº 11.246, de 2022, art. 22, II);

7.8.3. Identificada qualquer inexatidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção. (Decreto nº 11.246, de 2022, art. 22, III);

7.8.4. O fiscal técnico do contrato informará ao gestor do contato, 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. (Decreto nº 11.246, de 2022, art. 22, IV).

7.8.5. 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. (Decreto nº 11.246, de 2022, art. 22, V).

7.8.6. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual (Decreto nº 11.246, de 2022, art. 22, VII).

7.9. Fiscalização Administrativa

7.9.1. O fiscal administrativo do contrato, além de exercer as atribuições previstas no art. 33, IV, da IN SGD nº 94, de 2022, verificará a manutenção das condições de habilitação do contratado, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário (Art. 23, I e II, do Decreto nº 11.246, de 2022).

7.9.2. Caso ocorra descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência; (Decreto nº 11.246, de 2022, art. 23, IV).

7.10. Gestor do Contrato

7.10.1. O gestor do contrato, além de exercer as atribuições previstas no art. 33, I, da IN SGD nº 94, de 2022, coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo

todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração. (Decreto nº 11.246, de 2022, art. 21, IV).

7.10.2. 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. (Decreto nº 11.246, de 2022, art. 21, II).

7.10.3. O gestor do contrato acompanhará a manutenção das condições de habilitação do contratado, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais. (Decreto nº 11.246, de 2022, art. 21, III).

7.10.4. O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações. (Decreto nº 11.246, de 2022, art. 21, VIII).

7.10.5. O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso. (Decreto nº 11.246, de 2022, art. 21, X).

7.10.6. O gestor do contrato deverá elaborará 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 Administração. (Decreto nº 11.246, de 2022, art. 21, VI).

7.10.7. O gestor do contrato deverá enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do contrato.

7.10.8. A CONTRATADA deverá apresentar ao TCE/MS, no prazo de 10 (dez) dias corridos, contados da data da assinatura do contrato, comprovante de garantia, no valor correspondente a 10% (cinco por cento) total do contrato, cabendo-lhe optar por uma das modalidades de garantia previstas no art. 95, § 1º da Lei n.º 14.133/21:

7.10.8.1. Caução em dinheiro ou títulos da dívida pública;

7.10.8.2. Seguro garantia;

7.10.8.3. Fiança bancária

7.10.9. A garantia deverá ter validade de 03 (três) meses após o término da vigência contratual e necessitará ser renovada a cada prorrogação efetivada no contrato.

7.10.10. A garantia somente será liberada ante a comprovação de que a CONTRATADA pagou todas as verbas rescisórias trabalhistas decorrentes da contratação. Caso esse pagamento não ocorra até o fim do segundo mês após o encerramento da vigência contratual, a garantia será utilizada para o pagamento dessas verbas trabalhistas diretamente pela Contratante.

7.10.11. Caso a garantia não seja em dinheiro, ela não poderá ser restritiva quanto às obrigações da CONTRATADA com a Contratante advinda de prejuízos diretos ou indiretos, multas, indenizações ou ressarcimento de quaisquer espécies.

7.10.12. Se a garantia for utilizada para pagamento de multa aplicada, a CONTRATADA se obrigará a fazer a respectiva reposição, no prazo máximo de 8 (oito) dias, a contar da data em que for notificada pela Contratante.

7.10.13. Sempre que ocorrer aditamento ao Contrato a garantia deve ser renovada ou atualizada;

7.10.14. Em caso de fiança bancária deverá constar do instrumento a renúncia, expressa pelo fiador, dos benefícios previstos nos Artigos. 827 e 835, do Código Civil

8. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

8.1. O pagamento dos itens será realizado conforme tabela abaixo:

Item	Descrição	Quant.	Unid.	Valor mensal	Valor Anual
1	Contratação de empresa especializada para fornecimento de solução de segurança da informação envolvendo hardware, software, assinaturas de atualização, instalação, treinamento, customização e suporte técnico qualificado em proteção e inspeção de tráfego em redes corporativas, conforme especificações técnicas, incluindo os appliances necessários e suficientes para a prestação destes serviços, com o objetivo de garantir a proteção eficaz da rede de computadores, assim como a segurança das estações de trabalho, servidores de arquivos e dispositivos móveis, por meio de soluções antimalware endpoint com detecção e resposta de última geração.	12	Mês	R$ 1.078.377,50	R$ 12.940.530,00

8.2. A fatura/nota fiscal deverá ser encaminhada para o e-mail atendimento@tce.ms.gov.br

8.3. Relatório Mensal de Atividades:

8.4. Mensalmente, a CONTRATADA deverá elaborar e entregar, até o 5º (quinto) dia útil do mês subsequente à realização dos serviços, à Fiscalização do Contrato, um relatório de atividades para cada item do objeto desta Especificação Técnica, com a discriminação dos serviços realizados.

8.5. O relatório de atividades deverá ser emitido pelo representante técnico ou preposto da CONTRATADA contendo, no mínimo:

8.5.1. Identificação do Relatório de Atividades.

8.5.2. Data da Emissão.

8.5.3. Número do Contrato.

8.5.4. Vigência do Contrato.

8.5.5. Manutenção preventiva:

8.5.5.1. Número de atendimentos preventivos, realizados no mês de referência.

8.5.5.2. Descrição das atividades relacionadas a cada atendimento de manutenção preventiva, detalhando quais as peças foram trocadas para controle do prazo de garantia.

8.5.6. Manutenção corretiva:

8.5.6.1. Número de chamados abertos no período.

8.5.6.2. Número de chamados concluídos no período.

8.5.6.3. Descrição dos incidentes relacionados a cada chamado e a correspondente

8.5.6.4. descrição detalhada da solução aplicada, incluindo as peças trocadas, para controle do prazo de garantia.

8.5.7. Serviços executados de suporte:

8.5.7.1. Número e tipo de chamados de suporte.

8.5.7.2. Número e tipo de chamados de suporte concluídos no período.

8.5.7.3. Descrição dos serviços executados de suporte no período.

8.6. Prazo e Cronograma:

8.6.1. O prazo com vigência do contrato será de 12 meses, contando a partir da assinatura do contrato por ambas as partes.

8.6.2. O cronograma elaborado pela CONTRATADA deverá contemplar atividades para testes e garantia da certificação do ambiente quanto à norma ABNT NBR 15.247, bem como a realização de visitas dos órgãos certificadores, para auditoria e outros fins, quando for o caso.

8.7. SANÇÕES:

8.7.1. A avaliação da execução do objeto utilizará o Acordo de Nível de Serviço (ANS), Do Nível Mínimo de Serviço (NMS):

Nível	Classificação	Prazos
CRÍTICO	Representa um incidente crítico que possa tornar inoperante o sistema do Data Center por inteiro, ou uma parte majoritária que é essencial aos negócios diários.	A partir da abertura do chamado técnico, a CONTRATADA terá um prazo de: • 02 horas para início do atendimento presencial; • 48 horas para solução de contorno do incidente. Apresentação de relatório do incidente com descrição e previsão de solução definitiva em 72 horas.
URGENTE	Representa um incidente que está causando ou irá causar uma degradação do ambiente operacional da Sala de	A partir da abertura do chamado técnico, a CONTRATADA terá um prazo de: • 08 horas para início do atendimento presencial;

	equipamentos de TI. Apesar da degradação do ambiente, a sala continua em operação.	• 48 horas para solução de contorno do incidente. Apresentação de relatório do incidente com descrição e previsão de solução definitiva em 5 dias.
ROTINA	Representam falhas mínimas que não estão afetando a performance, serviço ou operação da Sala de equipamentos de TI, ou ainda a função afetada só é usada eventualmente ou temporariamente.	A partir da abertura do chamado técnico, a CONTRATADA terá um prazo de: • 12 horas para início do atendimento presencial; • 72 horas para solução de contorno do incidente. Apresentação de relatório do incidente com descrição e previsão de solução definitiva em 5 dias.

8.7.2. Nos termos do art. 19, inciso III da Instrução Normativa SGD/ME nº 94, de 2022, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, nos casos em que p contratado:

8.7.2.1. não atingir os valores mínimos aceitáveis fixados nos critérios de aceitação, não produzir os resultados ou deixar de executar as atividades contratadas; ou

8.7.2.2. deixar de utilizar materiais e recursos humanos exigidos para fornecimento da solução de TIC, ou utilizá-los com qualidade ou quantidade inferior à demandada;

8.8. Do recebimento

8.8.1. Os serviços serão recebidos provisoriamente, no prazo de 5 (cinco) dias corridos, pelos fiscais técnico e administrativo, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo. (Art. 140, I, a , da Lei nº 14.133 e Arts. 22, X e 23, X do Decreto nº 11.246, de 2022).

8.8.1.1. O prazo da disposição acima será contado do recebimento de comunicação de cobrança oriunda do contratado com a comprovação da prestação dos serviços a que se referem a parcela a ser paga.

8.8.2. O fiscal técnico do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter técnico. (Art. 22, X, Decreto nº 11.246, de 2022).

8.8.3. O fiscal administrativo do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter administrativo. (Art. 23, X, Decreto nº 11.246, de 2022)

8.8.4. Para efeito de recebimento provisório, ao final de cada período de faturamento, o fiscal técnico do contrato irá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos, que poderá resultar no redimensionamento de valores a serem pagos à contratada, registrando em relatório a ser encaminhado ao gestor do contrato.

8.8.4.1. Será considerado como ocorrido o recebimento provisório com a entrega do termo detalhado ou, em havendo mais de um a ser feito, com a entrega do último;

8.8.5. O Contratado fica obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

8.8.6. A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório. (Art. 119 c/c art. 140 da Lei nº 14133, de 2021)

8.8.7. O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis.

8.8.8. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, sem prejuízo da aplicação das penalidades.

8.8.9. Quando a fiscalização for exercida por um único servidor, o Termo Detalhado deverá conter o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, em relação à fiscalização técnica e administrativa e demais documentos que julgar necessários, devendo encaminhá-los ao gestor do contrato para recebimento definitivo.

8.8.10. Os serviços serão recebidos definitivamente no prazo de 5 (cinco) dias corridos, contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado, obedecendo os seguintes procedimentos:

8.8.10.1. Emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial, quando houver, no cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações, conforme regulamento (art. 21, VIII, Decreto nº 11.246, de 2022).

8.8.10.2. Realizar a análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando à Contratada, por escrito, as respectivas correções;

8.8.10.3. Emitir Termo Detalhado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas; e

8.8.10.4. Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização.

8.8.10.5. Enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão.

8.8.11. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021, comunicando-se à empresa para emissão de Nota Fiscal no que concerne à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

8.8.12. Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pelo contratado, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.

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

8.9. Liquidação

8.9.1. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de dez dias úteis para fins de liquidação, na forma

desta seção, prorrogáveis por igual período, nos termos do art. 7º, §2º da Instrução Normativa SEGES/ME nº 77/2022.

8.9.2. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, no caso de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021.

8.9.3. Para fins de liquidação, o setor competente deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:

8.9.3.1. o prazo de validade;

8.9.3.2. a data da emissão;

8.9.3.3. os dados do contrato e do órgão contratante;

8.9.3.4. o período respectivo de execução do contrato;

8.9.3.5. o valor a pagar; e

8.9.3.6. eventual destaque do valor de retenções tributárias cabíveis.

8.9.4. Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao contratante;

8.9.5. A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133, de 2021.

8.9.6. A Administração deverá realizar consulta ao SICAF para: a) verificar a manutenção das condições de habilitação exigidas no edital; b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, que implique proibição de contratar com

o Poder Público, bem como ocorrências impeditivas indiretas. (INSTRUÇÃO NORMATIVA Nº 3, DE 26 DE ABRIL DE 2018)

8.9.7. Constatando-se, junto ao SICAF, 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 do contratante.

8.9.8. Não havendo regularização ou sendo a defesa considerada improcedente, o contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do contratado, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

8.9.9. Persistindo a irregularidade, o contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao contratado a ampla defesa.

8.9.10. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso o contratado não regularize sua situação junto ao SICAF.

8.10. Prazo de pagamento

8.10.1. O pagamento será efetuado no prazo de até 10 (dez) dias úteis contados da finalização da liquidação da despesa, conforme seção anterior, nos termos da Instrução Normativa SEGES/ME nº 77, de 2022.

8.10.2. No caso de atraso de pagamento, desde que a CONTRATADA não tenha concorrido de alguma forma para tanto, serão devidos pelo CONTRATANTE encargos moratórios à taxa nominal de 6% a.a. (seis

por cento ao ano), capitalizados diariamente em regime de juros simples.

8.10.3. O valor dos encargos será calculado pela fórmula:

8.10.3.1. EM = I x N x VP, onde:

8.10.3.2. EM = Encargos moratórios devidos;

8.10.3.3. N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

8.10.3.4. I= Índice de compensação financeira = 0,00016438; e

8.10.3.5. VP = Valor da prestação em atraso.

8.11. Forma de pagamento

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

8.11.2. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

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

8.11.4. 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.

8.11.5. 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.

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

9.1. **Forma de seleção e critério de julgamento da proposta**:

9.1.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo menor preço global.

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

9.1.3. A análise técnica das propostas será realizada pelos integrantes da equipe responsável pelo planejamento da contratação (integrante da área demandante e/ou integrante técnico) e visa à verificação da conformidade dos serviços ofertados pelas licitantes com as especificações indicadas neste Termo de Referência.

9.1.4. A empresa participante deverá adicionar à proposta de preço para a participação deste certame, todos os catálogos técnicos, manuais e demais documentos necessários para a comprovação técnica das soluções ofertadas para cada item descrito neste Termo de Referência, sob pena de desclassificação.

9.2. Exigências de habilitação:

9.2.1. Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos referentes as habilitações:

9.2.1.1. Habilitação jurídica

9.2.1.1.1. Pessoa física: cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional;

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

9.2.1.1.3. 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;

9.2.1.1.4. 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;

9.2.1.1.5. 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, de 18 de março de 2020.

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

9.2.1.1.7. 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

9.2.1.1.8. Sociedade cooperativa: ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil

das Pessoas Jurídicas da respectiva sede, além do registro de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro 1971.

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

9.2.1.2. Habilitação fiscal, social e trabalhista

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

9.2.1.2.2. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

9.2.1.2.3. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

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

9.2.1.2.5. Prova de inscrição no cadastro de contribuintes Estadual e Municipal/Distrital relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

9.2.1.2.6. Prova de regularidade com a Fazenda Estadual e Municipal/Distrital do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

9.2.1.2.7. Caso o fornecedor seja considerado isento dos tributos Federais Estaduais e/ou Municipais, 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.

9.2.1.2.8. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

9.2.1.3. Qualificação Econômico-Financeira

9.2.1.3.1. Certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do licitante, caso se trate de pessoa física, desde que admitida a sua participação na licitação (art. 5º, inciso II, alínea “c”, da Instrução Normativa Seges/ME nº 116, de 2021), ou de sociedade simples;

9.2.1.3.2. Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - Lei nº 14.133, de 2021, art. 69, caput, inciso II);

9.2.1.3.3. Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, comprovando:

9.2.1.3.3.1. índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um);

9.2.1.3.3.2. 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; e

9.2.1.3.3.3. Os documentos referidos acima limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos.

9.2.1.3.3.4. 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.

9.2.1.3.4. Caso a empresa licitante apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido para fins de habilitação capital mínimo OU patrimônio líquido mínimo de até 10% do valor total estimado da contratação.

9.2.1.3.5. 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. (Lei nº 14.133, de 2021, art. 65, §1º).

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

9.2.1.4. Qualificação técnica:

9.2.1.4.1. Capacitação técnico-operacional (da empresa licitante):

9.2.1.4.1.1. A Licitante deverá comprovar aptidão para desempenho de atividade pertinente e compatível em características, quantidades e prazos com o objeto da licitação mediante apresentação de certidão(ões) ou atestado(s) fornecido(s) por pessoa jurídica de direito público ou privado.

9.2.1.4.1.2. Será admitida a soma dos atestados ou certidões apresentadas pelas licitantes, desde que os mesmos sejam tecnicamente pertinentes e compatíveis em características, quantidades e prazos com o objeto da licitação.

9.2.1.4.1.3. As licitantes deverão disponibilizar, quando solicitadas, todas as informações necessárias à comprovação da legitimidade dos atestados de capacidade técnica apresentados, por meio de cópia do instrumento que deu suporte à contratação, endereço atual da contratante e local em que foram prestados os serviços, dentre outros documentos.

9.2.1.4.1.4. Atestado (s) de Capacidade Técnica emitido (s) por entidade da Administração Federal, Estadual ou Municipal, direta ou indireta e/ou Empresa privada, que comprove a execução, de forma satisfatória, de desempenho de atividades compatíveis e/ou similares de:

I. Implantação de solução de segurança da informação tipo appliances NGFW (Next Generation

Firewall) em ambiente de alta disponibilidade (*High-availability clusters*) com no mínimo 02 nodes;

II. Operação de solução de segurança da informação tipo appliances NGFW (Next Generation Firewall) em ambiente de alta disponibilidade (High-availability clusters) pelo período mínimo de 12 (doze) meses;

III. Fornecimento de solução de segurança da informação tipo appliances NGFW (Next Generation Firewall) em ambiente de alta disponibilidade (High-availability clusters), contendo 02 (dois) appliances NGFW de capacidade mínima cada um de, 15 (quinze) Gbps de performance de firewall e 05 (cinco) Gbps de desempenho de IPS (Intrusion Prevention System);

IV. Implantação de solução de segurança da informação tipo appliances para balanceamento de carga e proteção de aplicações em ambiente de alta disponibilidade (High-availability clusters) com no mínimo 02 nodes;

V. Operação de solução de segurança da informação tipo appliances para balanceamento de carga e proteção de aplicações em ambiente de alta disponibilidade (High-availability clusters) pelo período mínimo de 12 (doze) meses;

VI. Fornecimento de solução de segurança da informação tipo appliances para balanceamento de carga e proteção de aplicações em ambiente de alta disponibilidade (High-availability clusters), contendo 02 (dois) appliances de capacidade mínima cada um

de, 20 (vinte) Gbps de tráfego com análise na camada 4 (OSI) e 15 (quinze) Gbps de tráfego com análise na camada 7 (OSI);

VII. Implantação de solução de segurança da informação tipo Endpoint com recursos EDR (Endpoint Detection and Response) para proteção de estações de trabalho, servidores e dispositivos móveis, com no mínimo 500 (quinhentos) Endpoints.

VIII. Operação de solução de segurança da informação tipo Endpoint com recursos EDR (Endpoint Detection and Response) para proteção de estações de trabalho, servidores e dispositivos móveis, pelo período mínimo de 12 (doze) meses;

IX. Fornecimento de ambiente NOC ou SOC ou SNOC com capacidade de diagnosticar preventivamente problemas técnicos e capacidade de intervenção técnica para resolução, em ambiente Zabbix e Grafana;

X. Criação e operação de dashboards para monitoramento da solução e suporte técnico e geração de relatórios de monitoramento em ambiente Zabbix e Grafana;

XI. Que possui plataforma de suporte técnico para abertura de chamados, baseada em ITIL, disponível através da internet (Web), telefone ou e-mail;

9.2.1.4.1.5. Para comprovação das quantidades mínimas exigidas, será permitida a somatória atestados, que demonstrem que o serviço tenha sido executado de forma simultânea (mesmo período), comprovando assim

a capacidade de logística e infraestrutura da proponente em atender projetos deste porte e capacidade;

9.2.1.4.1.6. Justifica-se a exigência de Atestado de Capacidade Técnica tendo em vista a necessidade de se garantir que a empresa proponente detenha expertise no fornecimento e instalação de solução compatível com o objeto da licitação e na execução dos serviços de suporte e manutenção, considerando o grau de relevância e criticidade da rede corporativa governamental a ser atendida pela solução para continuidade da prestação dos serviços públicos sustentados;

9.2.1.4.1.7. A exigência dos atestados de capacidade técnica para tecnologias específicas justifica-se pelos fundamentos abaixo apresentados:

9.2.1.4.1.8. As exigências de qualificação técnica têm como objetivo garantir a qualidade, compatibilidade e confiabilidade das licitantes para a prestação dos serviços, evitando desta forma prejuízos para a Administração Pública, não podendo ser considerado critério de restrição ao certame licitatório. Invocando a Corte Superior de Justiça, citamos o julgado que corrobora o alegado:

> *"Quando, em procedimento licitatório, exige-se comprovação, em nome da empresa, não está sendo violado o art. 30, § 1º, II, caput, da Lei nº 8.666/93. É de vital importância, no trato da coisa pública, a permanente perseguição ao binômio qualidade e eficiência, objetivando não só a garantir a segurança jurídica do contrato, mas também a consideração de certos fatores que integram a finalidade das licitações, máxime em se tratando daquelas de grande complexidade e de vulto*

financeiro tamanho que imponha ao administrador a elaboração de dispositivos, sempre em atenção à pedra de toque do ato administrativo – a lei – mas com dispositivos que busquem resguardar a Administração de aventureiros ou de licitantes de competência estrutural, administrativa e organizacional duvidosa". Recurso provido (Resp. nº 44.750-SP, rel. Ministro Francisco Falcão, 1ª T., DJ de 25.9.00)".

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

9.2.1.4.1.10. Somente serão aceitos atestados expedidos após a conclusão do contrato ou se decorrido, pelo menos, um ano do início de sua execução, exceto se firmado para ser executado em prazo inferior.

9.2.1.4.1.11. Certidão de registro da empresa e de seu responsável técnico, pertencente ao quadro técnico da licitante, na data prevista para entrega da proposta, no Conselho Regional de Engenharia e Agronomia (CREA), indicando assim, profissional técnico, adequado e disponível para a realização do objeto da licitação, conforme Art. 67, incisos I, II e V da Lei nº 14.133/2021.

I. A exigência de registro no CREA se justifica considerando que a instalação de sistemas de telecomunicações (como o caso dos equipamentos aqui descritos, que atuam sobre redes de comunicação de dados, por meio de cabos metálicos ou ópticos), são competência dos profissionais de engenharia, conforme prevê o art. 9° da Resolução CONFEA n. 218 de 29 de junho de 1973;

II. O requisito é indispensável para fins de apresentação de proposta no certame licitatório, visto que a apresentação de proposta demanda análise dos requisitos de telecomunicações presentes nas especificações deste termo, atividade esta que necessita de registro na entidade competente, para fins de legalidade no exercício regular da profissão, e está em consonância com o art. 67, inciso V da Lei n. 14.133/2021;

9.2.1.4.1.12. A licitante deverá prover suporte técnico especializado para a solução ofertada através de equipe técnica devidamente treinada e certificada pelo fabricante da solução proposta. A equipe deverá estar em conformidade com o Item “Requisitos de experiência profissional da equipe”, presente neste Termo de Referência, com vínculo empregatício ou contrato de prestação de serviços com a empresa licitante;

9.2.1.4.1.13. As comprovações de qualificação técnica dos profissionais exigida para o subitem anterior e o vínculo se darão no momento da assinatura do contrato.

9.2.1.4.1.14. A comprovação de treinamento e certificação deverá ser através de certificados emitidos pelo fabricante;

9.2.1.4.1.15. A comprovação do vínculo formal dos profissionais com o licitante, deverá ser feita mediante apresentação de um dos seguintes documentos, no ato da assinatura do contrato:

I. No caso de vínculo empregatício: cópia da Carteira de Trabalho e Previdência Social (CTPS), expedida pelo Ministério do Trabalho, contendo as folhas que

demonstrem o nº de registro, qualificação civil, contrato de trabalho e última alteração de salário;

II. No caso de vínculo societário: ato constitutivo da empresa devidamente registrado no órgão de Registro de Comércio competente, do domicilio ou da sede do licitante; e

III. No caso de profissional autônomo, contrato de prestação de serviço com a assinatura do profissional e do sócio da empresa.

9.2.1.4.1.16. A justificativa para a exigência apresentada se baseia na necessidade de que a licitante contratada preste os serviços de suporte técnico especializado por meio de profissionais devidamente treinados, capacitados e certificados pelo fabricante da solução ofertada. Embora a experiência da empresa, sua capacidade gerencial e seus equipamentos sejam fatores relevantes, profissionais qualificados são determinantes para o desempenho da contratada. A experiência da empresa na prestação dos serviços a serem contratados é importante, mas não determinante. Sem profissional qualificado, a contratada não tem o mesmo desempenho, mesmo que tenha capacidade gerencial e equipamentos, conforme apresentado no Acórdão nº 534/2016 – Plenário do TCU.

9.3. Outros Documentos

9.3.1. Declaração do Licitante indicando que a empresa é distribuidora ou revenda autorizada da solução ofertada que está ofertando, informando ainda que o fabricante possui suporte no Brasil.

9.3.2. A empresa deve apresentar comprovação mediante a apresentação de Declaração/atestado de capacidade técnica em papel timbrado

contendo: Nome e endereço do emissor; assinatura e telefone de contato do Responsável da empresa emissora.

9.3.3. O(s) Atestado(s) deverá(ão) detalhar o escopo dos serviços prestados, compatível em características, quantidades e prazos com o objeto da licitação (conforme Art. 67, inciso II, da Lei nº 14.133/2021), telefone e nome de pessoa de contato e declaração do cumprimento de todas as exigências técnicas e contratuais em nível satisfatório, em papel timbrado do emitente.

9.3.4. Apresentar declaração do fabricante informando que todos os componentes do objeto são novos (sem uso, reforma ou recondicionamento) e que não estão fora de linha de fabricação;

9.3.5. A licitante deve apresentar uma declaração de que o licitante possui ou instalará escritório na cidade de Campo Grande/MS, a ser comprovado no prazo máximo de 60 (sessenta) dias contado a partir da vigência do contrato.

9.3.6. A licitante deverá apresentar atestado de Vistoria emitido pelo TCE/MS, ou, caso optar pela não realização da vistoria, Declaração formal que possui conhecimento pleno das condições e peculiaridades da contratação, responsabilizando-se por quaisquer ônus.

9.3.7. No caso de equipamentos, deverá apresentar comprovação para todos os itens e subitens, apontando a página e parágrafo da documentação o atendimento destes itens e subitens através de catálogos, folders e/ou outros comprovantes, desde que sejam do próprio fabricante do equipamento podendo ser certificação, catálogo técnico do fabricante ou declaração do fabricante.

10. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

10.1. O custo estimado total da contratação é de R$ 12.940.530,00 (Doze milhões, novecentos e quarenta mil, quinhentos e trinta reais), conforme custos constantes no Estudo Técnico Preliminar e item 1.1 deste Termo.

11. PLANO DE TRANSIÇÃO CONTRATUAL

11.1. Em caso de rescisão ou não renovação contratual, a CONTRATADA obriga- se a prestar para o TCE-MS ou a terceiro por ele designado, toda a assistência a fim de que os serviços continuem sendo prestados sem interrupção ou efeito adverso, e que haja uma transferência ordenada de conhecimento dos serviços, processos e tecnologias para o Tribunal ou a seu designado.

11.2. A CONTRATADA deverá apresentar um plano de transição contratual com no prazo máximo de 3 (três) meses a contar da data prevista para encerramento das atividades. O Tribunal analisará, no prazo de 5 (cinco) dias úteis, o plano apresentado, aprovando-o ou recusando-o de forma fundamentada. No caso de não aprovação, a CONTRATADA deverá apresentar novo plano, no prazo máximo de 3 (três) dias úteis, após o recebimento da recusa do plano anterior.

11.3. O plano de transição contratual e sua execução deverão ser viabilizados sem ônus adicionais a contratante e deverá conter no mínimo, os seguintes itens:

a) Identificação dos profissionais designados pela CONTRATADA que irão compor a equipe de transferência de conhecimentos, bem como os seus papéis e as suas responsabilidades;
b) Cronograma geral do repasse;
c) Identificação das etapas e as atividades com suas respectivas datas de início e término, os produtos gerados, os recursos envolvidos e os marcos intermediários, quando aplicável;
d) Plano de gerenciamento de riscos e plano de contingência;

e) Descrição da forma de entrega para o Tribunal de todos os dados em poder da CONTRATADA, incluindo-se a totalidade dos dados contidos no Sistema de Gestão de Demandas da CONTRATADA, se existir;

f) Relação das Ordens de Serviço canceladas automaticamente em razão do encerramento do contrato, com relatório detalhado da parte dos serviços executados e possíveis pendências de execução.

11.4. As Ordens de Serviço que estiverem em execução ou suspensas ao final do contrato serão canceladas automaticamente, registrando-se como data de cancelamento a data final do contrato. As demandas ou Ordens de Serviços classificadas como Manutenção Corretivas, abertas até o último dia de vigência de contrato, não serão canceladas e deverão ser executadas e entregues em sua plenitude.

11.5. É de responsabilidade da CONTRATADA a execução do plano de transição contratual, a prestação de serviços de operação assistida, bem como a garantia do repasse bem sucedido de todas as informações necessárias à continuidade dos serviços pela contratante ou empresa por ele designada.

11.6. A elaboração e a execução do plano de transição contratual ocorrerão em paralelo ao atendimento das ordens de serviços demandadas pelo TCE-MS.

11.7. O fato de a CONTRATADA ou quaisquer de seus representantes não cooperarem, ou reterem qualquer informação ou dado solicitado pelo Tribunal que venha a prejudicar, de alguma forma, o andamento da transição das tarefas e serviços para um novo prestador, constituirá quebra de contrato, sujeitando-a às responsabilidades em relação a todos os danos causados à contratante por esta falha, sem prejuízo das demais penalidades contratuais previstas. Caso a CONTRATADA não

promova adequadamente a transferência de conhecimento serão aplicadas as sanções cabíveis.

11.8. O Tribunal reserva-se o direito de reduzir ou dispensar o plano de transição contratual, desde que o novo provedor contratado venha a comprovar que detém pleno domínio sobre as atividades previstas em contrato.

12. ADEQUAÇÃO ORÇAMENTÁRIA

12.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Tribunal de Contas do Estado de Mato Grosso do Sul.

12.2. A contratação será atendida pela seguinte dotação:

Unidade Orçamentária	3101
Funcional Programática	10.03101.01.032.0002.2011.0001
Fonte de recursos	1500
Natureza da Despesa	3.3.90.40.79
Descrição da Despesa	Serviço de Suporte a Usuário e de Infraestrutura de TIC

Integrante Técnico	**Integrante Administrativo**
João Victor Costa Santos Matrícula:3145	Marina Wirtti Sanches Matrícula 3056
Integrante Requisitante Elvis Frank Souza Monteiro Matrícula:770	

12.3. Aprovo este Termo de Referência e atesto sua conformidade às disposições da Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022.

TRIBUNAL DE CONTAS
Estado de Mato Grosso do Sul

Autoridade Máxima da Área de STI
José Augusto Alves Ferreira **Matrícula: 3129**

13. Lista de Anexos

I. Termo de Compromisso de Manutenção de Sigilo
II. Termo de Ciência
III. Estudo Técnico Preliminar com seus anexos

Campo Grande, 06 de novembro de 2024.

TRIBUNAL DE CONTAS
Estado de Mato Grosso do Sul

TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO

INTRODUÇÃO
O Termo de Compromisso de Manutenção de Sigilo registra o comprometimento formal da Contratada em cumprir as condições estabelecidas no documento relativas ao acesso e utilização de informações sigilosas da Contratante em decorrência de relação contratual, vigente ou não. **Referência: Art. 18, Inciso V, alínea "a" da IN SGD/ME Nº 94/2022.**

Pelo presente instrumento o Tribunal de Contas do Estado do Mato Grosso do Sul, sediado na Rua Des. José Nunes da Cunha Bloco 29 - Parque dos Poderes – CEP 79.031-902, Campo Grande/MS, CNPJ n°15.424.948/0001-41, doravante denominado **CONTRATANTE**, e, de outro lado, a _____, sediada em _____, CNPJ N° _____, doravante denominada **CONTRATADA**;

CONSIDERANDO que, em razão do **CONTRATO N.º _____** doravante denominado **CONTRATO PRINCIPAL**, a **CONTRATADA** poderá ter acesso a informações sigilosas do **CONTRATANTE**;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na Política de Segurança da Informação e Privacidade da **CONTRATANTE**;

Resolvem celebrar o presente **TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO,** doravante **TERMO**, vinculado ao **CONTRATO PRINCIPAL**, mediante as seguintes cláusulas e condições abaixo discriminadas.

1 – OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sigilosas disponibilizadas pela CONTRATANTE e a observância às normas de segurança da informação e privacidade por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõem a Lei 12.527, de 18 de novembro de 2011, Lei nº 13.709, de 14 de agosto de 2018, e os Decretos 7.724, de 16 de maio de 2012, e 7.845, de 14 de novembro de 2012, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo.

2 – CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquela abrangida pelas demais hipóteses legais de sigilo.

CONTRATO PRINCIPAL: contrato celebrado entre as partes, ao qual este TERMO se vincula.

3 – DA INFORMAÇÃO SIGILOSA

Serão consideradas como informação sigilosa, toda e qualquer informação classificada ou não nos graus de sigilo ultrassecreto, secreto e reservado. O TERMO abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: *know-how*, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes.

4 – DOS LIMITES DO SIGILO

As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

I – Sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;

II – Tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;

III – Sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

5 – DIREITOS E OBRIGAÇÕES

As partes se comprometem a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas INFORMAÇÕES, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento prévio e expresso da CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência à CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela CONTRATANTE.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as INFORMAÇÕES deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados,

contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto – A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das INFORMAÇÕES, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmos judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das INFORMAÇÕES por seus agentes, representantes ou por terceiros;

III – Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das INFORMAÇÕES, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

6 – VIGÊNCIA

O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

7 – PENALIDADES

A quebra do sigilo e/ou da confidencialidade das INFORMAÇÕES, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme previsto nos arts. 155 a 163 da Lei nº. 14.133, de 2021.

8 – DISPOSIÇÕES GERAIS

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa-fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I – A CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente

pela CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL.

III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV – Todas as condições, termos e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações, conforme definição do item 3 deste documento, disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo ao CONTRATO PRINCIPAL;

VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar INFORMAÇÕES para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

9 – FORO

A CONTRATANTE elege o foro de Campo Grande, onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

10 – ASSINATURAS

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes em 2 vias de igual teor e um só efeito.

CONTRATADA	**CONTRATANTE**
_____ Nome:_____ Função:_____	_____ Nome:_____ **Matrícula:**_____
TESTEMUNHAS	
_____ Nome:_____ Função:_____	_____ Nome:_____ Função:_____

Local:_____,____de_____de 20__.

TRIBUNAL DE CONTAS
Estado de Mato Grosso do Sul

TERMO DE CIÊNCIA

INTRODUÇÃO
No caso de substituição ou inclusão de empregados da contratada, o preposto deverá entregar ao Fiscal Administrativo do Contrato os Termos de Ciência assinados pelos novos empregados envolvidos na execução dos serviços contratados. **Referência: Art. 18, Inciso V, alínea "b" da IN SGD/ME Nº 94/2022.**

1 – IDENTIFICAÇÃO			
CONTRATO Nº			
OBJETO			
CONTRATADA		**CNPJ**	
PREPOSTO			
GESTOR DO CONTRATO		**MATR.**	

2 – CIÊNCIA

Por este instrumento, os funcionários abaixo identificados declaram ter ciência e conhecer o inteiro teor do Termo de Compromisso de Manutenção de Sigilo e as normas de segurança vigentes da Contratante.

Funcionários da Contratada		
Nome	**Matrícula**	**Assinatura**

Local:_____,____de_____de 20__.

Protocolo de Assinatura(s)

O documento acima foi proposto para assinatura digital. Para verificar as assinaturas acesse o endereço http://df.tce.ms.gov.br/docflow/digitalSignChecker.jsf e utilize o código abaixo para verificar se este documento é válido.

Código de verificação: ASK2-PDYG-RQOA-FXY4

O(s) nome(s) indicado(s) para assinatura, bem como seu(s) status em 25/03/2026 é(são) :

- ELVIS FRANK SOUZA MONTEIRO - 26/11/2024 08:05:56 (Certificado Digital)
- JOÃO VICTOR COSTA SANTOS - 26/11/2024 08:02:40 (Certificado Digital)
- JOSE AUGUSTO ALVES FERREIRA - 26/11/2024 08:22:11 (Certificado Digital)
- MARINA WIRTTI SANCHES - 26/11/2024 08:41:04 (Certificado Digital)
- THIAGO CARDOSO PEREIRA - 31/10/2024 10:01:36 (Certificado Digital)