TERMO DE REFERÊNCIA

N. 51/2025

AUTORES

NOME	CARGO	E-MAIL
Patricia Barbosa Gatts	Assessora da Superintendência de Informação e Tecnologia/SITEC	pgatts@sed.ms.gov.br
José Flavio Rodrigues Siqueira	Coordenador de Tecnologia Educacional/COTED/SITEC	jose.130137@edutec.sed.ms.gov.br

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

1. DO OBJETO

1.1. Contratação de serviços de segurança da informação envolvendo solução de 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 para atender a demanda da Secretaria de Estado de Educação de MS, conforme condições, quantidades, especificações e exigências estabelecidas neste instrumento.

LOTE ÚNICO				
Item	**Descrição Complementar**	**Código**	**UNIDADE DE MEDIDA**	**QUANTIDADE**
001	Contratação de empresa especializada para fornecimento de serviços de segurança da informação envolvendo solução de hardware, software, assinaturas de atualização, 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.	0017117	Mês	12
002	Serviços de Implantação - Serviços Técnicos especializados	0020310	Unid.	01

1.2. Os serviços objetos desta contratação são caracterizados como comuns, para os fins do disposto no inciso XIII do art. 6º da Lei Federal nº 14.133/2021.

1.3. O prazo de vigência da contratação é de 12 (doze) meses contados da assinatura do contrato, podendo ser prorrogado, respeitando a vigência máxima de 10 (dez) anos, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

1.3.1 A contratação compreende a prestação de serviços de natureza mista, envolvendo parcela de caráter pontual e parcela de caráter continuado, em razão das características da solução pretendida.

1.3.2.A fase de implantação, correspondente às atividades iniciais de instalação, configuração, parametrização e disponibilização da solução, possui caráter pontual, sendo executada uma única vez, no início da execução contratual.

1.3.3. Por sua vez, a prestação dos serviços associados à disponibilização da solução — incluindo licenciamento, suporte técnico especializado, atualização, monitoramento, análise de vulnerabilidades, resposta a incidentes e ajustes operacionais — possui natureza continuada, uma vez que não se exaure em uma única prestação, demandando execução permanente e ininterrupta para garantir a proteção dos ativos de tecnologia da informação e a continuidade das operações institucionais.

1.3.4 A segurança da informação envolve monitoramento constante, aplicação de atualizações e correções, gerenciamento de incidentes, suporte técnico especializado e ajustes periódicos de configuração. Tais serviços, por sua própria natureza, não possuem caráter eventual, sendo imprescindíveis de forma contínua para assegurar a integridade, a confidencialidade e a disponibilidade dos sistemas e dados da Administração Pública.

1.3.4.1 Ademais, a descontinuidade desses serviços expõe a organização a riscos significativos, como vazamento de informações sensíveis, indisponibilidade de sistemas críticos e vulnerabilidade a ataques cibernéticos, o que reforça o enquadramento da parcela continuada da contratação como serviço indispensável à manutenção da eficiência administrativa e da segurança institucional.

1.3.5 Assim, resta evidenciado que a contratação da solução de segurança da informação atende aos requisitos legais e técnicos para ser classificada como prestação de serviços continuados, permitindo inclusive a prorrogação contratual sucessiva nos termos previstos na legislação vigente, sendo a vigência plurianual mais vantajosa, atendendo, assim, o disposto no inciso I do artigo 106 da Lei nº 14.133, de 2021.

1.4 A presente contratação adotará como regime de execução a empreitada por preço global, nos termos do art. 6º, inciso XXIX, da Lei nº 14.133/2021, considerando a natureza integrada do objeto e a possibilidade de sua definição prévia com nível adequado de precisão.

1.4.1. Justifica-se a adoção do referido regime em razão da possibilidade de definição clara e suficiente do escopo contratual, bem como de seus quantitativos e especificações técnicas, conforme demonstrado no Estudo Técnico Preliminar e no Termo de Referência.

1.4.2. A solução pretendida consiste em um conjunto integrado de bens e serviços de tecnologia da informação e comunicação, abrangendo fornecimento de hardware, software, licenças, implantação, configuração, treinamento e serviços técnicos especializados, cujos componentes são interdependentes e demandam execução coordenada e padronizada.

1.4.3. Nesse contexto, verifica-se que:

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

1.4.3.1.os requisitos técnicos e operacionais encontram-se adequadamente definidos, permitindo a delimitação do objeto contratual;

1.4.3.2. os quantitativos foram estimados com base em levantamento da infraestrutura existente, nas necessidades institucionais e em projeções de uso, possibilitando dimensionamento compatível com a realidade do ambiente;

1.4.3.3.a adoção do regime por preço global favorece a obtenção de proposta mais vantajosa, ao permitir que os licitantes considerem ganhos de escala e sinergia entre os componentes da solução;

1.4.3.4. o modelo contribui para maior eficiência na gestão contratual, ao estabelecer previamente o escopo e o valor global da contratação, sem prejuízo da necessidade de aferição da execução dos serviços continuados;

1.4.3.5.a natureza integrada da solução recomenda sua contratação em lote único, de modo a evitar fragmentação do objeto, riscos de incompatibilidade entre componentes e dificuldades na atribuição de responsabilidades técnicas.Ressalta-se que, embora adotado o regime de empreitada por preço global, a execução contratual observará a distinção entre parcelas de natureza pontual e serviços de natureza continuada, sendo:a implantação da solução, de caráter pontual, remunerada mediante pagamento único, condicionado à sua efetiva conclusão e aceite pela Administração;

1.4.3.6.os serviços continuados de disponibilização da solução, incluindo licenciamento, suporte, atualização e monitoramento, remunerados de forma mensal, condicionados à efetiva prestação dos serviços e ao cumprimento dos níveis de serviço estabelecidos.

1.4.4.Dessa forma, o regime adotado mostra-se adequado ao caso concreto, por assegurar a coerência entre a modelagem da contratação, a forma de execução e o modelo de remuneração, em consonância com os princípios da eficiência, economicidade e planejamento.

1.4.5 O instrumento contratual conterá o detalhamento das regras aplicáveis à vigência e execução da contratação.

1.4.6 No que se refere às especificações dos produtos e serviços, informa-se que foi verificada a aplicabilidade do Catálogo Eletrônico de Padronização, nos termos do art. 19 da Lei nº 14.133/2021, não tendo sido identificados itens compatíveis com o objeto da presente contratação, em razão de sua natureza integrada e da necessidade de especificação técnica individualizada.

1.4.7 Ressalta-se que a não utilização do catálogo não afronta o princípio da padronização, previsto no art. 40, inciso V, da Lei nº 14.133/2021, uma vez que a utilização do catálogo eletrônico possui caráter preferencial, cabendo à Administração avaliar sua aplicabilidade ao caso concreto.

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO

2.1. A fundamentação da contratação e de seus quantitativos encontra-se pormenorizada nos tópicos, respectivamente, “necessidade da contratação” e “estimativa de quantidade para a contratação” do Estudo Técnico Preliminar, apêndice deste Termo de Referência.

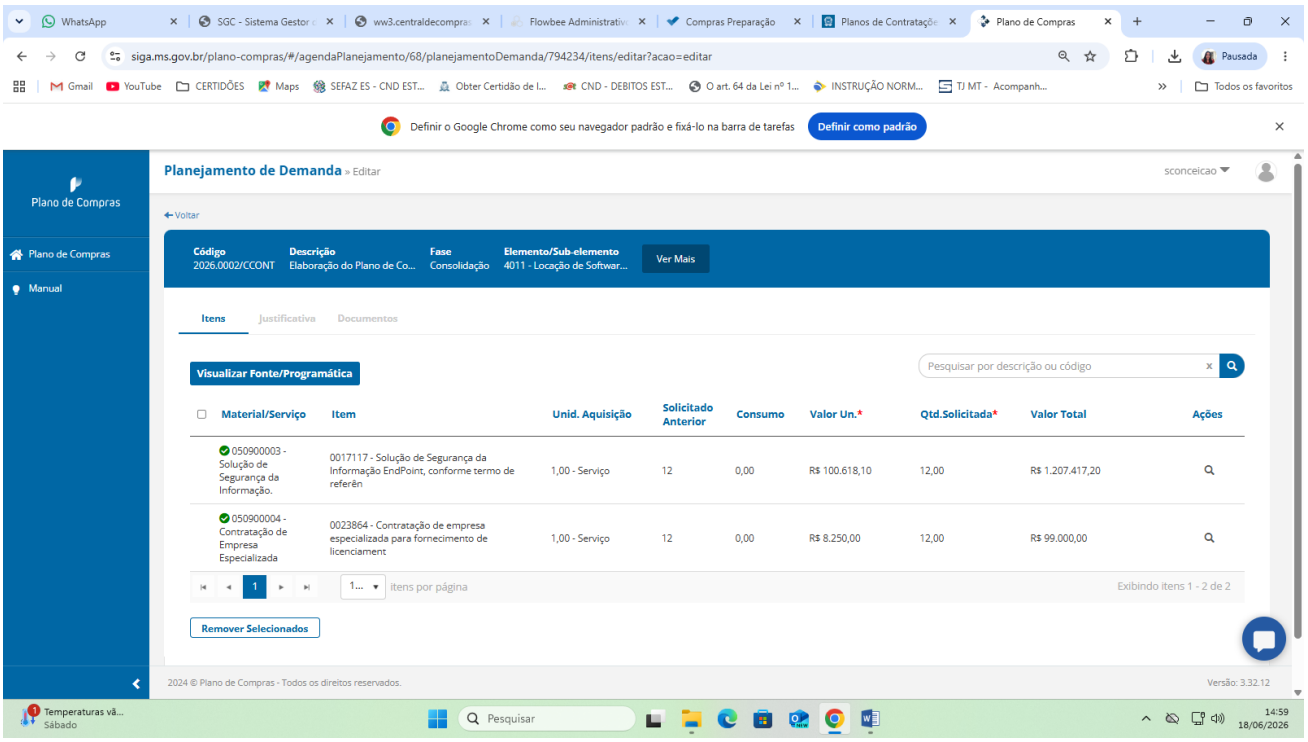
Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

2.2. Demonstração da Previsão no Plano Anual de Contratações

2.2.1. Em conformidade com o Decreto n. 16.121, de 9 de março de 2.023, que dispõe sobre o Plano de Contratação Anual (PCA) do Poder Executivo Estadual, a previsão de empresa especializada para a prestação de serviços de fornecimento de licença de uso de software para gestão integrada de processos de desenvolvimento de política pública educacional, foi estipulada no PCA, para aprimorar a fase preparatória das contratações por meio da previsibilidade das demandas, visando a eficiência e à qualidade do gasto público.

2.2.2. Nesse sentindo, esclarecemos que a contratação em tela se encontra no PCA de 2026 através do link: https://pncp.gov.br/app/pca/02585924000122/2026/2



2.2.3. A presente contratação observa a compatibilidade com os instrumentos de planejamento orçamentário, em especial com o Plano Plurianual – PPA vigente, no âmbito das ações relacionadas à modernização e à segurança da infraestrutura de tecnologia da informação.

2.2.4. Adicionalmente, a contratação encontra-se alinhada à Lei de Diretrizes Orçamentárias – LDO e à Lei Orçamentária Anual – LOA, sendo compatível com o planejamento institucional da Administração.

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO E REQUISITO DA CONTRATAÇÃO

3.1 DA EXIGÊNCIA DE PROVA DE CONCEITO/AMOSTRA

3.1.1.Não se aplica.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.2. INDICAÇÃO DE MARCAS OU MODELOS

3.2.1. Não se aplica.

3.3. DA EXIGÊNCIA DE CARTA DE SOLIDARIEDADE

3.3.1. Não se aplica.

3.4. GARANTIA DA EXECUÇÃO DO CONTRATO

3.4.1. Será exigida a garantia da contratação de que tratam os arts. 96 e seguintes da Lei nº 14.133, de 2021, no percentual de 5% (cinco por cento) do valor inicial do contrato.

3.4.1.1. A exigência de garantia de execução contratual justifica-se em razão da natureza, complexidade e criticidade do objeto contratado, que envolve a disponibilização de solução integrada de segurança da informação, essencial à proteção dos ativos de tecnologia da informação da Administração.

3.4.1.2. A solução contempla componentes tecnológicos interdependentes, incluindo proteção de perímetro, proteção de endpoints e mecanismos de detecção e resposta a incidentes, cuja adequada implementação e operação são indispensáveis à continuidade dos serviços institucionais.

3.4.1.3. A eventual inexecução contratual, total ou parcial, pode acarretar riscos relevantes, tais como indisponibilidade de sistemas críticos, exposição a vulnerabilidades, comprometimento da integridade e confidencialidade de dados institucionais e prejuízos operacionais à Administração.

3.4.1.4. Nesse contexto, a exigência de garantia tem por finalidade mitigar riscos de inadimplemento, assegurar maior segurança na execução contratual e resguardar o interesse público, em consonância com os princípios da eficiência, economicidade e planejamento.

3.4.1.5. Adicionalmente, a garantia contribui para o fortalecimento dos mecanismos de responsabilização da contratada, especialmente em contratações que envolvem serviços continuados e soluções tecnológicas de alta relevância estratégica.

3.4.1.6. Dessa forma, a exigência de garantia contratual mostra-se adequada e necessária, em observância aos princípios da eficiência, da economicidade e da proteção ao interesse público.

3.4.2. A garantia deverá ser apresentada no seguinte prazo:

I - nas modalidades caução e fiança bancária deverá ser prestada em até 15 (quinze) dias após assinatura do contrato;

II - no caso de seguro-garantia sua apresentação deverá ocorrer, no máximo, até 30 (trinta) dias, a contar da publicação da decisão homologatória do certame licitatório, em atenção ao disposto no artigo 96, §3º, da Lei Federal n. 14.133/2021.

3.4.3.A garantia em dinheiro deverá ser efetuada em favor do contratante, em conta específica a ser informada na assinatura do contrato, com correção monetária.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.4.4. No caso de garantia na modalidade de fiança bancária, deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

3.4.5. Caso utilizada a modalidade de seguro-garantia, a apólice deverá ter validade durante a vigência do contrato.

3.4.6.A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento das despesas enumeradas no art. 139, inciso III, alíneas “a” a “c”, da Lei nº 14.133/2021.

3.4.6.1.A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no item 3.4.6, observada a legislação que rege a matéria.

3.4.6.2. Fica assegurado o direito de retenção da garantia, por parte da Administração Pública, para pagamento das despesas enumeradas no item 3.4.6 deste Termo de Referência.

3.4.7. Se o valor da garantia for utilizado total ou parcialmente em pagamento a qualquer obrigação, o Contratado obriga-se a fazer a respectiva reposição no prazo máximo de 20 (vinte) dias úteis, contados da data em que for notificada.

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

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

3.4.10. O garantidor não é parte para figurar em processo administrativo instaurado pelo contratante com o objetivo de apurar prejuízos e/ou aplicar sanções à contratada.

3.4.11. A garantia de execução é independente de eventual garantia do produto prevista especificamente no Termo de Referência.

3.5. DA SUSTENTABILIDADE

3.5.1. Considerando a natureza do objeto contratado, consistente na disponibilização de solução de tecnologia da informação e comunicação, a contratada deverá observar, na execução do contrato, práticas que promovam o uso racional de recursos e a redução de impactos ambientais, nos termos da legislação aplicável às contratações públicas sustentáveis.

3.5.1.1 Aspectos Ambientais

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.5.1.2. Adotar soluções que promovam a eficiência energética, de modo a reduzir o consumo de energia elétrica associado à operação da infraestrutura tecnológica;

3.5.1.3. Utilizar, quando aplicável, ambientes de processamento de dados que adotem boas práticas de gestão energética e otimização de recursos computacionais;

3.5.1.4.Assegurar a adequada gestão de resíduos eletroeletrônicos eventualmente gerados, em conformidade com a legislação vigente, especialmente no que se refere à destinação ambientalmente adequada;

3.5.1.5. Priorizar, sempre que tecnicamente viável, a execução remota dos serviços de monitoramento, suporte e manutenção, de modo a reduzir deslocamentos e impactos associados.

3.5.2. Aspectos Sociais

3.5.2.1. Observar a legislação trabalhista vigente e assegurar condições adequadas de trabalho na execução contratual;

3.5.2.2. Garantir a conformidade com a Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018), no tratamento de dados eventualmente envolvidos na execução dos serviços;

3.5.2.3. Promover a capacitação contínua de sua equipe técnica, especialmente no que se refere à segurança da informação e à proteção de dados.

3.5.3. Aspectos de Governança

3.5.3.1. Adotar boas práticas de segurança da informação e gestão de riscos, compatíveis com a natureza dos serviços prestados;

3.5.3.2. Manter controles internos adequados à execução contratual, assegurando a rastreabilidade das ações e a conformidade com os requisitos estabelecidos;

3.5.3.3. Comprovar, quando solicitado, a adoção de padrões técnicos reconhecidos de segurança da informação, podendo tal comprovação ser realizada por meio de certificações, relatórios técnicos ou outros meios idôneos.

3.5.4. Fundamentação Normativa

3.5.4.1. Os requisitos de sustentabilidade previstos neste item fundamentam-se na legislação aplicável às contratações públicas, em especial:

3.5.4.2. Lei nº 12.305/2010 (Política Nacional de Resíduos Sólidos)

Decreto nº 7.746/2012;

3.5.4.3. Instrução Normativa SLTI/MPOG nº 01/2010;

3.5.4.4. Lei nº 14.133/2021, quanto à promoção do desenvolvimento nacional sustentável.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.6. CONSÓRCIO

3.6.1. NÃO será permitida a participação de empresas em regime de consórcio, pelas seguintes razões:

3.6.1.1. A presente contratação tem por objeto a prestação de serviços de segurança da informação, considerados de natureza estratégica e sensível para a Administração Pública.

3.6.1.2. Nos termos do art. 15, §1º, inciso III, da Lei nº 14.133/2021, é facultado à Administração vedar a participação de consórcios em licitações quando devidamente justificado.

3.6.1.3. No caso em questão, a vedação fundamenta-se nos seguintes aspectos:

I. Confidencialidade e sigilo das informações: a execução contratual envolve o tratamento de dados sensíveis e estratégicos. A participação de consórcios, que pressupõe a atuação conjunta de diversas empresas, aumenta o risco de exposição indevida e dificulta o controle da circulação de informações sigilosas.

II. Responsabilidade técnica e contratual: os serviços de segurança da informação exigem centralização de responsabilidades, de modo a permitir a apuração clara de eventuais falhas. A divisão de atribuições entre consorciados pode gerar conflitos de responsabilidade e dificultar a gestão contratual pela Administração.

III. Gestão de incidentes e continuidade dos serviços: a segurança da informação requer pronta resposta a incidentes e efetiva gestão de riscos. A atuação consorciada pode ocasionar entraves burocráticos na tomada de decisão, prejudicando a agilidade necessária para garantir a continuidade dos serviços.

IV. Boas práticas e conformidade normativa: normas e diretrizes, como a ABNT NBR ISO/IEC 27001 e a Instrução Normativa SGD/ME nº 1/2019, recomendam controles rigorosos sobre terceiros e clareza na responsabilidade pela gestão da segurança, o que se torna mais complexo na execução por consórcios.

V. Eficiência e segurança jurídica: a contratação de empresa individual proporciona maior eficiência, clareza na responsabilização contratual, facilidade na fiscalização e maior mitigação de riscos, atendendo, assim, ao interesse público.

3.6.1.4. Diante do exposto, a vedação à participação de consórcios no certame encontra-se devidamente justificada, nos termos do art. 15, §1º, inciso III, da Lei nº 14.133/2021, constituindo medida necessária para assegurar a confidencialidade, a integridade, a disponibilidade das informações e a efetividade da execução contratual.

3.7. SUBCONTRATAÇÃO

3.7.1. Não será admitida a subcontratação do objeto contratual.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.7.2. A vedação à subcontratação fundamenta-se na natureza técnica, integrada e crítica dos serviços a serem prestados, os quais envolvem solução de tecnologia da informação e comunicação voltada à segurança da informação da Secretaria de Estado de Educação de Mato Grosso do Sul.

3.7.3. A execução do objeto demanda elevado grau de especialização, controle e padronização, abrangendo fornecimento, implantação, configuração, monitoramento e suporte técnico contínuo de soluções que atuam diretamente na proteção da infraestrutura tecnológica institucional, incluindo redes, servidores e estações de trabalho.

3.7.4. A solução a ser contratada é composta por componentes interdependentes, que operam de forma integrada, compartilhando políticas de segurança, inteligência de ameaças e mecanismos de correlação de eventos, cuja efetividade depende da atuação coordenada e da gestão unificada por um único responsável técnico.

3.7.5. Nesse contexto, a eventual subcontratação poderia comprometer a uniformidade da execução, fragmentar a responsabilidade técnica, dificultar a rastreabilidade das ações e aumentar os riscos operacionais, especialmente no que se refere à segurança, integridade e confidencialidade das informações tratadas.

3.7.6. Ademais, a centralização da execução contratual em um único responsável favorece a eficiência na gestão do contrato, a comunicação entre as partes e a responsabilização direta em caso de falhas ou incidentes de segurança, aspectos essenciais em contratações dessa natureza.

3.7.7. Ressalta-se que a vedação à subcontratação não configura restrição indevida à competitividade, tendo em vista que o mercado dispõe de empresas aptas a executar integralmente o objeto contratado, conforme evidenciado em levantamento de mercado realizado na fase de planejamento.

3.7.8. Dessa forma, a não admissão de subcontratação mostra-se medida necessária e proporcional para garantir a qualidade, a segurança e a eficiência na execução do contrato, em consonância com o interesse público.

3.8. REQUISITOS DO OBJETO

3.8.1. A aquisição presente compreende os requisitos inseridos na Tabela Descritiva abaixo, que são considerados necessários e indispensáveis para acatar a demanda solicitada.

Item	Descrição Complementar	Métrica	Quantidade
001	Contratação de empresa especializada para fornecimento de serviços de segurança da informação envolvendo solução de hardware, software, assinaturas de atualização, treinamento,	Mês	12

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

	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.		
002	Serviços de Implantação da Solução	Unid.	01

3.9. DEMAIS REQUISITOS

3.9.1. A empresa contratada deverá fornecer uma Solução de Tecnologia da Informação e Comunicação (TIC), abrangendo serviços de segurança da informação, incluindo hardware, software e serviços especializados, de modo a garantir a proteção dos ativos de informação da Secretaria de Estado de Educação de Mato Grosso do Sul (SED/MS).

3.9.2. A solução deverá implementar mecanismos de proteção contra ameaças internas e externas, incluindo firewall de próxima geração (NGFW), sistema de detecção e prevenção de intrusões (IDS/IPS) e antivírus integrado.

3.9.3. Deverá permitir a análise de tráfego em tempo real, com capacidade de bloqueio automático de atividades suspeitas.

3.9.4. A solução deverá garantir alta disponibilidade (mínimo de 99,5% de uptime mensal), com mecanismos de failover automático e redundância.

3.9.5. Deverá incluir suporte técnico especializado com SLA de atendimento de até 4 horas úteis para incidentes críticos.

3.9.6. A solução deverá contemplar proteção para endpoints (estações, notebooks e servidores), com agente de segurança para monitoramento, detecção e resposta a ameaças.

3.9.7. A plataforma deverá permitir gerenciamento centralizado de todos os dispositivos protegidos

3.9.8. A solução deverá realizar filtragem de conteúdo web (Web Filtering) e controle de aplicações (Application Control), com políticas customizáveis por grupo de usuários.

3.9.9. Deverá permitir a geração de relatórios detalhados sobre navegação e tentativas de acesso a conteúdos não autorizados.

3.9.10. O sistema deverá possuir mecanismos proativos de detecção e bloqueio de malwares, com atualizações automáticas de assinaturas.

3.9.11. Deverá incluir sandboxing para análise comportamental de arquivos suspeitos.

3.9.12. A solução deverá incluir ferramentas de monitoramento contínuo de segurança (SOC), com alertas de tentativas de invasão ou exploração de vulnerabilidades.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.9.13. Deverá permitir integração com as plataformas e sistemas corporativos existentes.

3.9.14. A plataforma deverá realizar varreduras automáticas e agendadas de vulnerabilidades em estações, servidores e redes.

3.9.15. Deverá gerar relatórios de vulnerabilidades com recomendações de correção.

3.9.16. A solução deverá possibilitar a realização de auditorias de conformidade, com geração de relatórios de acordo com as políticas de segurança da SED/MS.

3.9.17. Deverá manter logs de eventos de segurança com integridade e rastreabilidade.

3.9.18. A solução deverá fornecer criptografia de tráfego de rede e controle granular de liberação ou bloqueio de fluxos de dados.

3.9.19. Deverá incluir VPN corporativa segura para acesso remoto.

3.9.20. A solução deverá garantir a integridade dos dados disponibilizados ao público e aos usuários internos, com mecanismos de detecção de alterações não autorizadas.

3.9.21. Deverá oferecer dashboards e relatórios analíticos para monitoramento da integridade dos dados

3.10. REQUISITOS TÉCNICOS

3.10.1. 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.

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 da Secretaria de Estado de Educação de Mato Grosso do Sul, independentemente de mudanças futuras na topologia da rede.

c) 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.

3.11. Deverão ser fornecidos equipamentos do tipo Appliances com no mínimo os seguintes requisitos técnicos:

a) Deverá ser fornecido 01 (um) clusters de equipamentos para solução de proteção de perímetro, formado por appliances com no mínimo 02 (dois) nodes cada cluster, para implementação na rede da SED/MS no bloco 5 no Parque dos Poderes, além da instalação, operação e suporte do mesmo;

b) Deverá ser fornecido 01 (um) clusters de equipamentos para solução de proteção de perímetro, formado por appliances com no mínimo 02 (dois) nodes cada cluster, para implementação

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

na rede da SED/MS na Rua dos Dentistas, Tiradentes, além da instalação, operação e suporte do mesmo

c) Deverão ser fornecidos 10.000 (dez mil) licenças para Solução para Proteção de Endpoints, para implementação de proteção Endpoint, que serão instaladas nas estações de trabalho e servidores de rede da SED/MS, além da instalação, operação e suporte.

d) Deverão ser fornecidas 500 (quinhentas) licenças de Módulo de Detecção e Resposta gerenciada - MDR para instalação nos equipamentos servidores de rede da SED/MS.

e) O licenciamento para todas as Soluções deverá permanecer válido durante toda a vigência do contrato.

3.12. Requisitos Gerais da Solução

3.12.1. 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 da Secretaria de Estado de Educação de Mato Grosso do Sul, independentemente de mudanças futuras na topologia da rede;

3.12.2. A solução deve consistir em plataforma de proteção de rede baseada em Appliance com funcionalidades de Next Generation Firewall. O termo Next Generation Firewall doravante será empregado como NGFW ou simplesmente firewall.

3.12.3. Os appliances físicos devem ser novos e de primeiro uso e não constar em listas de end-of-sale, end- of-support e end-of-life do fabricante;

3.12.4. 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;

3.12.5. 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;

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

3.12.7. 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;

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

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.12.9. Os desempenhos apontados nos Requisitos de Capacidade e de Interfaces deverão ser comprovados por documento de domínio público do fabricante.

3.12.10. A comprovação do atendimento aos requisitos técnicos da solução não será exigida na fase de apresentação da proposta.

3.12.11. A licitante classificada em primeiro lugar deverá comprovar o atendimento aos requisitos técnicos estabelecidos neste Termo de Referência, como condição para assinatura do contrato.

3.12.12. A comprovação poderá ser realizada por meio de documentação técnica idônea, tais como catálogos, manuais, fichas técnicas, declarações do fabricante, certificações ou outros documentos que demonstrem o atendimento aos requisitos exigidos.

3.12.13. Ainda deverá ser apresentado uma planilha de aderência técnica (ponto a ponto), indicando o atendimento aos requisitos especificados, com a devida indicação das fontes de comprovação, 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.

3.12.14. A exigência de comprovação técnica justifica-se em razão da complexidade da solução e da necessidade de assegurar a aderência da proposta às especificações estabelecidas, não se configurando como requisito de habilitação, mas como condição para contratação.

3.12.15. O fornecimento dos produtos e seus licenciamentos deverão 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.

3.12.16. 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.

a) 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.

b) Desta forma, velando-se pela legalidade, a SED/MS não poderia admitir a utilização de 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 e que certamente estaria sujeito à sustação com o advento de qualquer atividade fiscalizadora da agência de regulação.

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

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

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

3.13.1. 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 da Secretaria de Estado de Educação 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 da SED/MS, permitindo o devido gerenciamento, monitoramento e operação da solução sem necessidade de adaptações ou equipamentos sobressalentes;

3.13.2. Capacidade de inspeção de firewall superior a 17 Gbps ou superior.

3.13.3. Desempenho em modo Threat Prevention (Proteção Anti Malware, IPS e Controle de Aplicação habilitados) mínimo de 9 Gbps ou superior.

3.13.4. Desempenho em modo de Inspeção (decriptografia e criptografia) de tráfego criptografado (SSL/TLS) mínimo de 4 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.

3.13.5. Desempenho mínimo de 9 Gbps de IPS.

3.13.6. Suporte mínimo de 3.800.000 conexões simultâneas/concorrentes no modo SPI.

3.13.7. Suporte mínimo de 110.000 novas conexões por segundo.

3.13.8. Deve possuir armazenamento interno de no mínimo 128 GB e suportar expansão de armazenamento interno para até 1TB.

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

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

3.13.11. Deve possuir pelo menos 06 interfaces de 10GbE padrão SFP+, acompanhado de 06 módulos 10GB- SR SFP+ homologados pelo fabricante do equipamento.

3.13.12. Deve possuir pelo menos 24 interfaces de 1GbE padrão RJ 45.

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

3.13.14. Deve possuir pelo menos 02 interfaces USB 3.0 com suporte a tecnologias LTE 3G/4G e 5G.

3.13.15. A VPN Client-to-Site IPsec deve ser licenciada para, no mínimo, 350 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 2.500 usuários simultâneos.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.13.16. A VPN SSL deve ser licenciada para, no mínimo, 1 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 800 usuários simultâneos.

3.13.17. Deve suportar pelo menos 3.500 túneis de VPN tipo Site-to Site padrão IPSEC simultâneos.

3.13.18. Deve suportar, no mínimo, 10 Gbps de desempenho de VPN IPSEC.

3.13.19. O Equipamento deverá ser homologado pela ANATEL.

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

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

3.14.1. 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.

3.14.2. 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.

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

3.14.4. Deve possuir proteção anti-spoofing.

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

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

3.14.7. 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.

3.14.8. 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.

3.14.9. 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:

3.14.9.1. Latência;

3.14.9.2. Jitter;

3.14.9.3. Perda de pacotes.

3.14.9.10. 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.

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

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.14.9.12. 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.

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

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

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

3.14.9.16. 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.

3.14.9.17. Deve suportar DHCP relay.

3.14.9.18. 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.

3.14.9.19. 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.

3.14.9.20. 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.

3.14.9.21. 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.

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

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

3.14.9.24. Detectar e bloquear a origem de portscans.

3.14.9.25. Deve permitir o bloqueio de ataques.

3.14.9.26. Deve permitir o bloqueio de exploits conhecidos.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

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

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

3.14.9.29. Implementar DSCP (Differentiated Services Code Points).

3.14.9.30. 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.

3.14.9.31. 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.

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

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

3.14.9.34. Possuir suporte a log via Syslog.

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

3.14.9.36. O fabricante ou o produto deve possuir certificação ICSA (International Computer Security Association) para firewall ou Common Criteria (CC), ou outra certificação equivalente emitida por organismos independentes reconhecidos.

3.14.9.37. Será aceita certificação equivalente ao ICSA ou CC, desde que comprove, de forma objetiva, o atendimento aos requisitos técnicos de segurança e desempenho exigidos, com base em normas nacionais ou internacionais de segurança da informação, considerando versões atualizadas do produto e manutenção periódica da certificação.

3.14.9.38. Adicionalmente, a comprovação do atendimento aos requisitos poderá ser realizada por outros meios idôneos, tais como relatórios técnicos, documentação do fabricante ou testes de desempenho, a critério da Administração.

3.14.9.39. Visando estabelecer a efetividade da segurança dos firewalls de nova geração e assegurar que a solução ofertada possua desempenho validado por entidade independente, o fabricante deverá demonstrar que o produto foi submetido a avaliações técnicas de mercado, podendo tal comprovação ser realizada por meio de relatórios técnicos, certificações reconhecidas, testes comparativos ou outros meios idôneos.

3.14.9.40. Serão admitidos, como referência, relatórios de avaliação de mercado elaborados por entidades independentes, tais como NetSecOPEN, Gartner ou similares, não sendo exigida vinculação a um único organismo ou metodologia específica.

3.14.9.41. Os relatórios e avaliações de mercado referidos no subitem anterior poderão ser utilizados como elementos complementares para subsidiar a análise comparativa das soluções

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

disponíveis e sua aderência aos requisitos técnicos estabelecidos neste Termo de Referência, não constituindo, por si só, requisito de habilitação ou condição de aceitação da proposta.

3.14.9.42. 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.

3.14.9.43. Para tráfego criptografado SSL/TLS, deve de-criptografar pacotes possibilitando 3a leitura de payload dos pacotes para checagem de assinaturas de aplicações conhecidas pelo fabricante.

3.14.9.44. 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.

3.14.9.45. Deve permitir a funcionalidade de ARP bridging.

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

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

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

3.15.1. 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 da SED/MS e outras instituições como bancos, Órgãos do Governo Estadual, Governo Federal e Serpro, através de tecnologia usual de mercado e não proprietária.

3.15.2. 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.

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

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

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

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

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

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

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

3.15.10. 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.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

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

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

3.15.13. 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.

3.15.14. 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.

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

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

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

3.16. Requisitos de Alta Disponibilidade para proteção de perímetro

3.16.1. 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 da SED/MS, ou seja, a solução deve automaticamente se manter operacional na ocorrência de qualquer evento que ocasione a parada de um dos itens da solução.

3.16.2. 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.

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

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

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

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

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

3.16.8. 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.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.16.9. 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.

3.16.10. 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.

3.17. Requisitos de Controle de Ameaças para proteção de perímetro

3.17.1. Os requisitos mínimos exigidos neste subitem são justificados pela necessidade de proteger o ambiente de rede da SED/MS 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.

3.17.2. 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.

3.17.3. 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.

3.17.4. 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.

3.17.5. Implementar funcionalidade de detecção e bloqueio de “call backs”.

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

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

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

3.17.9. Implementar interface CLI segura através do protocolo SSH.

3.17.10. 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.

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

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

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

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

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

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

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

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

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

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

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

3.17.21. 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.

3.17.22. 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.

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

3.17.24. A solução deve ser capaz de bloquear proativamente o acesso a domínios maliciosos conhecidos por meio de filtragem reduzindo assim o risco de infecções por malware e outros ataques cibernéticos.

3.18. Requisitos de Proteção Contra Ataques Avançados para proteção de perímetro

3.18.1. Os requisitos mínimos exigidos neste subitem são justificados pela necessidade de proteger o ambiente de rede corporativa da SED/MS 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.

3.18.2. 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”.

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

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

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

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

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

3.18.7. 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.

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

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

3.18.10. 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.

3.18.11. 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.

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

3.18.13. 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.

3.18.14. Conter ameaças avançadas de dia zero.

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

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

3.18.17. 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.

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

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

3.18.20. 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.

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

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

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

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

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

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

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

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

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

3.18.29. Conter e mitigar exploits avançados.

3.18.30. 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).

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

3.18.32. 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.

3.18.33. 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.

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

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

3.18.36. A solução de segurança de firewalls deverá fornecer tecnologias avançadas de proteção contra ameaças, com sandboxing usando multi-mecanismos baseado em nuvem, permitindo:

3.18.36.1. Inspeção profunda de memória em tempo real;

3.18.36.2. Inspeção profunda de pacotes livre de remontagem;

3.18.36.3. Descriptografia e inspeção TLS/SSL;

3.18.36.4. Inteligência e controle de aplicativos;

3.18.36.5. Recursos SD-WAN seguros.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.19. Requisitos de Filtro de Conteúdo Web para proteção de perímetro

3.19.1. 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.

3.19.2. 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.

3.19.3. 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.

3.19.4. 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.

3.19.5. Permitir a customização de página de bloqueio.

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

3.19.7. Deve permitir submissão de novos sites para categorização.

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

3.19.9. 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.

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

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

3.20. Requisitos de autenticação para proteção de perímetro

3.20.1. 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 da SED/MS, e especificam tecnologias padrão de mercado e utilizadas no âmbito do parque computacional.

3.20.2. 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.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

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

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

3.20.5. 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.

3.20.6. 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.

3.20.7. 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.

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

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

3.20.10. 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.

3.20.11. A solução deve possibilitar SSO via API.

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

3.20.13. Requisitos de Administração para proteção de perímetro

3.20.13.1. Os requisitos mínimos exigidos neste subitem são justificados pela necessidade da equipe técnica da SED/MS 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 da SED/MS.

3.20.13.2. 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.

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

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

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

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

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

3.20.13.7. 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.

3.20.13.8. 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.

3.20.13.9. 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.

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

3.20.13.11. 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.

3.20.13.12. 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.

3.20.13.13. 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.

3.20.13.14. 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.

3.20.13.15. 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.

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

3.20.13.17. Possibilitar a geração de pelo menos os seguintes tipos de relatório, mostrados em formato HTML: máquinas mais acessadas, serviços mais utilizados, usuários que mais

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

utilizaram serviços, URLs mais visualizadas, ou categorias Web mais acessadas (considerando a existência do filtro de conteúdo Web).

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

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

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

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

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

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

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

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

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

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

3.20.13.28. 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.

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

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

3.21. Requisitos do Software de Gerenciamento para proteção de perímetro

3.21.1. Os requisitos mínimos exigidos neste subitem são justificados pela necessidade da equipe técnica da SED/MS em gerenciar todo o ambiente tecnológico fornecido pela solução nos sites instalados, através de uma interface integrada e com acesso à configuração e ao

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

monitoramento de todos os recursos e funcionalidades fornecidos, com disponibilidade de acesso local e/ou remoto.

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

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

3.21.4. 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.

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

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

3.21.7. Deve suportar organizar os dispositivos administrados em grupos.

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

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

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

3.21.11. O gerenciamento deve permitir/possuir:

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

3.21.11.2. A solução deve permitir acesso concorrente de administradores.

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

3.21.11.4. Deve permitir a integração com LDAP ou Radius.

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

3.21.11.6. 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.

3.21.11.7. 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.

3.21.11.8. Deverá permitir atualizar o sistema operacional de múltiplos equipamentos gerenciados de uma única vez**.**

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

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

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

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

3.21.11.12. 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.

3.21.11.13. 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.

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

3.21.11.15. 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.

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

3.21.11.17. 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.

3.21.11.18. 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.

3.21.11.19. 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.

3.21.11.20. 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.

3.21.11.21. 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

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

automatizada para o responsável da aprovação via e-mail ou console da solução, possibilitando mitigar erros de configuração e impactos negativos ao ambiente.

3.21.11.22. 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.

3.22. Requisitos do Software de Relatórios para proteção de perímetro

3.22.1. Os requisitos mínimos exigidos neste subitem são justificados pela necessidade da equipe técnica da SED/MS 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.

3.22.2. 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.

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

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

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

3.22.6. 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.

3.22.7. A solução deverá prover relatórios referente as atividades dos usuários.

3.22.8. 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.

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

3.22.10. 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.

3.22.11. A solução deverá prover relatórios referente aos acessos web com no mínimo informações referentes às categorias acessadas, quantitativo de acessos e megabytes transferidos.

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

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

3.22.13.1. IP de origem, usuário, conexões e quantidade de dado trafegado.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

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

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

3.22.14.2. Modo gráfico; ou

3.22.14.3. Lista de logs.

3.22.14.4. A solução deve possibilitar a criação de relatórios de uso de VPN.

3.22.15. Requisitos técnicos da solução para proteção de Endpoints.

3.22.15.1. Características Gerais da Solução de proteção e segurança para Endpoints:

3.22.15.1.1.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.

3.22.15.1.2. A solução ofertada não pode ser do tipo comunidade, software livre, ou possuir componentes e módulos sem suporte oficial do fabricante.

3.22.15.1.3. 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.

3.22.15.1.4. 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.

3.22.15.1.5. A solução ofertada deverá possuir módulo de detecção e respostas (EDR).

3.22.15.1.6. A solução ofertada deverá possuir módulo de detecção e resposta gerenciada (MDR).

3.22.16. Do Módulo de Proteção de Endpoint

3.22.16.1. A solução proposta deverá proteger os sistemas operacionais abaixo:

3.22.16.1.1. Windows 7;

3.22.16.1.2. Windows 8;

3.22.16.1.3. Windows 8.1;

3.22.16.1.4. Windows 10;

3.22.16.1.5. Windows 11.

3.22.16.2. Servidores:

3.22.16.2.1. Windows Small Business Server 2011;

3.22.16.2.2. Windows MultiPoint Server 2011;

3.22.16.2.3. Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022;

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.22.16.3. Servidores de terminal Microsoft:

3.22.16.3.1. Serviços de Área de Trabalho Remota da Microsoft baseados no Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022.

3.22.16.4. Sistemas operacionais Linux de 32 bits:

3.22.16.4.1. CentOS 6.7 e posterior;

3.22.16.4.2. Debian GNU/Linux 11.0 e posterior;

3.22.16.4.3. Debian GNU/Linux 12.0 e posterior;

3.22.16.4.4. Red Hat Enterprise Linux 6.7 e posterior;

3.22.16.5. Sistemas operacionais Linux de 64 bits:

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.22.16.5.1. Amazon Linux 2;

3.22.16.5.2. CentOS 6.7 e mais tarde;

3.22.16.5.3. CentOS 7.2 e posterior;

3.22.16.5.4. CentOS Stream 8;

3.22.16.5.5. CentOS Stream 9;

3.22.16.5.6. Debian GNU/Linux 11.0 e posterior;

3.22.16.5.7. Debian GNU/Linux 12.0 e posterior;

3.22.16.5.8. Linux Mint 20.3 e superior;

3.22.16.5.9. Linux Mint 21.1 e posterior;

3.22.16.5.10. openSUSE Leap 15.0 e posterior;

3.22.16.5.11. Oracle Linux 7.3 e posterior;

3.22.16.5.12. Oracle Linux 8.0 e posterior;

3.22.16.5.13. Oracle Linux 9.0 e posterior;

3.22.16.5.14. Red Hat Enterprise Linux 6.7 e posterior;

3.22.16.5.15. Red Hat Enterprise Linux 7.2 e posterior;

3.22.16.5.16. Red Hat Enterprise Linux 8.0 e posterior;

3.22.16.5.17. Red Hat Enterprise Linux 9.0 e posterior;

3.22.16.5.18. Rocky Linux 8.5 e posterior;

3.22.16.5.19. Rocky Linux 9.1;

3.22.16.5.20. SUSE Linux Enterprise Server 12.5 ou posterior;

3.22.16.5.21. SUSE Linux Enterprise Server 15 ou posterior;

3.22.16.5.22. Ubuntu 20.04 LTS;

3.22.16.5.23. Ubuntu 22.04 LTS.

3.22.16.6. Sistemas operacionais Arm de 64 bits:

3.22.16.6.1. CentOS Stream 9;

3.22.16.6.2. SUSE Linux Enterprise Server 15;

3.22.16.6.3. Ubuntu 22.04 LTS.

3.22.16.7. Sistemas operacionais MAC OS:

3.22.16.7.1. MacOS 12 – 14.

3.22.16.8. Ferramentas de virtualização MAC OS:

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.22.16.8.1. Parallels Desktop 16 para Mac Business Edition;

3.22.16.8.2. VMware Fusion 11.5 Professional;

3.22.16.8.3. VMware Fusion 12 Professional.

3.22.16.9. A solução proposta deverá suportar as seguintes plataformas virtuais:

3.22.16.9.1. VMware Workstation 17.0.2 Pro;

3.22.16.9.2. VMware ESXi 8.0 Update 2;

3.22.16.9.3. Microsoft Hyper-V Server 2019;

3.22.16.9.4. Citrix Virtual Apps e Desktop 7 2308;

3.22.16.9.5. Citrix Provisioning 2308;

3.22.16.9.6. Citrix Hypervisor 8.2 Update 1;

3.22.17. Do Módulo de Gerenciamento Avançado:

3.22.17.1. A solução proposta deve suportar arquitetura cloud native e on-premisse;

3.22.17.2. A solução proposta deve incluir suporte para implantação baseada em nuvem por meio de:

3.22.17.2.1. Amazon Web Services;

3.22.17.2.2. Microsoft Azure.

3.22.17.3. A solução proposta deve incluir as seguintes opções de integração SIEM:

3.22.17.3.1. HP (Microfoco) ArcSight;

3.22.17.3.2. IBM QRadar;

3.22.17.3.3. Splunk;

3.22.17.3.4. Kaspersky KUMA.

3.22.17.4. 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.

3.22.17.5. 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.

3.22.17.6. A solução proposta deve suportar Single Sign On (SSO) usando NTLM e Kerberos.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.22.17.7. O administrador deve ser capaz de adicionar manualmente novos dispositivos à lista de equipamentos ou editar informações sobre equipamentos já existentes na rede.

3.22.17.8. A solução proposta deve suportar API OPEN e incluir diretrizes para integração com sistemas externos de terceiros.

3.22.17.9. 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.

3.22.17.10. 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.

3.22.17.11. A solução proposta deve suportar o download de arquivos diferenciais em vez de pacotes completos de atualização.

3.22.17.12. A solução proposta deve incluir Role Based Access Control (RBAC) com funções predefinidas personalizáveis.

3.22.17.13. O servidor de gerenciamento primário da solução proposta deve ser capaz de retransmitir atualizações e serviços de reputação em nuvem.

3.22.17.14. 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:

3.22.17.14.1. Status do dispositivo;

3.22.17.14.2. Tag;

3.22.17.14.3. Diretório ativo;

3.22.17.14.4. Proprietários de dispositivos;

3.22.17.14.5. Hardware.

3.22.17.15. A solução proposta deve suportar os seguintes canais de entrega de notificação:

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.22.17.15.1. E-mail;

3.22.17.15.2. Registro de sistema;

3.22.17.15.3. SMS.

3.22.17.16. A solução proposta deve ter a capacidade de etiquetar/marcar computadores com base em:

3.22.17.16.1. Atributos de rede;

3.22.17.16.2. Nome;

3.22.17.16.3. Domínio e/ou Sufixo de Domínio;

3.22.17.16.4. Endereço de IP;

3.22.17.16.5. Endereço IP para servidor de gerenciamento;

3.22.17.16.6. Localização no Active Directory;

3.22.17.16.7. Unidade organizacional;

3.22.17.16.8. Grupo;

3.22.17.16.9. Sistema operacional;

3.22.17.16.10. Número do pacote de serviço;

3.22.17.16.11. Arquitetura Virtual;

3.22.17.16.12. Registro de aplicativos;

3.22.17.16.13. Nome da Aplicação;

3.22.17.16.14. Versão do aplicativo;

3.22.17.16.15. Fabricante;

3.22.17.16.16. Tipo e versão;

3.22.17.16.17. Arquitetura.

3.22.17.17. 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.

3.22.17.18. 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.

3.22.17.19. As informações sobre o equipamento deverão ser atualizadas após cada nova pesquisa na rede. A lista de equipamentos detectados deve abranger o seguinte:

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.22.17.19.1. Dispositivos Desktop/Servidores;

3.22.17.19.2. Dispositivos móveis;

3.22.17.19.3. Dispositivos de rede;

3.22.17.19.4. Dispositivos virtuais;

3.22.17.19.5. Componentes OEM;

3.22.17.19.6. Periféricos de computador;

3.22.17.19.7. Dispositivos IoT conectados;

3.22.17.19.8. Telefones VoIP;

3.22.17.19.9. Repositórios de rede.

3.22.17.20. A solução proposta deve permitir ao administrador criar categorias/grupos de aplicação com base em:

3.22.17.20.1. Nome da Aplicação;

3.22.17.20.2. Caminho do aplicativo;

3.22.17.20.3. Metadados do aplicativo;

3.22.17.20.4. Aplicativo Certificado digital;

3.22.17.20.5. Categorias de aplicativos predefinidas pelo fornecedor;

3.22.17.20.6. SHA256 e MD5.

3.22.17.21. A solução proposta deverá permitir especificamente o bloqueio dos seguintes dispositivos:

3.22.17.21.1. Bluetooth;

3.22.17.21.2. Dispositivos móveis;

3.22.17.21.3. Modems externos;

3.22.17.21.4. CD/DVD;

3.22.17.21.5. Câmeras e scanners;

3.22.17.21.6. MTPs;

3.22.17.21.7. E a transferência de dados para dispositivos móveis

3.22.17.22. A solução proposta deve ter capacidade de ler informações do Active Directory para obter dados sobre contas de computadores na organização.

3.22.17.23. 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.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.22.17.24. 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:

3.22.17.24.1. Estruturas de domínios e grupos de trabalho do Windows;

3.22.17.24.2. Estruturas de grupos do Active Directory;

3.22.17.24.3. Conteúdo de um arquivo de texto criado manualmente pelo administrador.

3.22.17.25. 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.

3.22.17.26. A solução proposta deve permitir realizar as seguintes ações para endpoints:

3.22.17.26.1. Verificação manual;

3.22.17.26.2. Verificação no acesso;

3.22.17.26.3. Verificação por demanda;

3.22.17.26.4. Verificação de arquivos compactados;

3.22.17.26.5. Verificação de arquivos individuais, pastas e unidades;

3.22.17.26.6. Bloqueio e verificação de scripts

3.22.17.26.7. Proteção contra alteração de registros;

3.22.17.26.8. Proteção contra estouro de buffer;

3.22.17.26.9. Verificação em segundo plano/inativa.

3.22.17.26.10. Verificação de unidade removível na conexão com o sistema.

3.22.17.27. 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.

3.22.17.28. 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.

3.22.17.29. 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.

3.22.17.30. A solução proposta deve ter a capacidade de realizar inventário em scripts e arquivos, tais como: dll, exe, bat e etc.

3.22.17.31. 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.

3.22.17.32. A solução proposta deve suportar Windows Failover Cluster.

3.22.17.33. A solução proposta deve ter um recurso de clustering integrado.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.22.17.34. A solução proposta deve incluir alguma forma de sistema para controlar epidemias de vírus.

3.22.17.35. 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.

3.22.17.36. O servidor de gestão da solução proposta deverá incluir funções de segurança pré-definidas para o Auditor, Supervisor e Oficial de Segurança.

3.22.17.37. 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.

3.22.17.38. A solução proposta deve ter a capacidade de priorizar rotinas de varredura personalizadas e sob demanda para estações de trabalho Linux.

3.22.17.39. A solução proposta deve ser capaz de registrar operações de arquivos (Escrita e Exclusão) em dispositivos de armazenamento USB.

3.22.17.40. A solução proposta deve ter capacidade de bloquear a execução de qualquer executável do dispositivo de armazenamento USB.

3.22.17.41. A solução proposta deve contar com filtragem de firewall por endereço local, interface física e Time- To-Live (TTL) de pacotes.

3.22.17.42. A solução proposta deverá possuir controles para download de DLL e drivers.

3.22.17.43. 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.

3.22.17.44. 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.

3.22.17.45. 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).

3.22.17.46. A solução proposta deve incluir Controle de inicialização de aplicativos para o sistema operacional Windows Server.

3.22.17.47. 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.

3.22.17.48. 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.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.22.17.49. 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.

3.22.17.50. 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.

3.22.17.51. A solução proposta deve dar acesso aos serviços em nuvem do fornecedor de segurança anti- malware através do servidor de administração.

3.22.17.52. A solução proposta deve ser capaz de realizar inventários de software e hardware instalados nos computadores dos usuários.

3.22.17.53. 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.

3.22.17.54. A solução proposta deve permitir a instalação centralizada de aplicativos de terceiros em todos ou em computadores selecionados.

3.22.17.55. 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.

3.22.17.56. 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.

3.22.17.57. 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.

3.22.17.58. 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.

3.22.17.59. A solução proposta deve permitir ao administrador personalizar relatórios.

3.22.17.60. 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.

3.22.17.61. 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.

3.22.17.62. A solução proposta deve permitir ao administrador definir diferentes condições de mudança de status para grupos de endpoint no servidor de gerenciamento.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.22.17.63. A solução proposta deve permitir que o administrador adicione ferramentas de gerenciamento de endpoint personalizadas/de terceiros ao servidor de gerenciamento.

3.22.17.64. 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.

3.22.17.65. A funcionalidade 'Dispositivo desativado' deve estar disponível, para que tais dispositivos não sejam exibidos na lista de equipamentos.

3.22.17.66. 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.

3.22.17.67. 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.

3.22.17.68. A solução proposta deve suportar integração com solução APT.

3.22.17.69. A solução proposta deve suportar a integração com o serviço Managed Detection and Response.

3.22.17.70. A solução proposta deve permitir instalar o modulo de gerenciamento on-premisse nos seguintes sistemas operacionais:

3.22.17.70.1. Windows;

3.22.17.70.2. Linux.

3.22.17.71. A solução proposta deverá suportar os seguintes servidores de banco de dados:

3.22.17.1. Windows:

3.22.17.1.1. Microsoft SQL Server;

3.22.17.1.2. Microsoft Banco de dados SQL do Azure;

3.22.17.1.3. MySQL Standard e Enterprise;

3.22.17.1.4. MariaDB;

3.22.17.1.5. PostgreSQL.

3.22.17.71.1. Linux:

3.22.17.71.1.1. MySQL;

3.22.17.71.1.2. MariaDB;

3.22.17.71.1.3. PostgreSQL.

3.22.17.72. A solução proposta deverá suportar as seguintes plataformas virtuais:

3.22.17.72.1. Windows:

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.22.17.72.1.1. VMware vSphere 6.7 e 7.0;

3.22.17.72.1.2. Estação de trabalho VMware 16 Pro;

3.22.17.72.1.3. Servidor Microsoft Hyper-V 2012 de 64 bits;

3.22.17.72.1.4. Servidor Microsoft Hyper-V 2012 R2 de 64 bits;

3.22.17.72.1.5. Microsoft Servidor Hyper -V 2016 de 64 bits;

3.22.17.72.1.6. Servidor Microsoft Hyper-V 2019 de 64 bits;

3.22.17.72.1.7. Servidor Microsoft Hyper-V 2022 de 64 bits;

3.22.17.72.1.8. Citrix XenServer 7.1 LTSR;

3.22.17.72.1.9. Citrix XenServer 8.x;

3.22.17.72.1.10. Oracle VM VirtualBox 6.x.

3.22.17.72.2. Linux:

3.22.17.72.2.1. VMware vSphere 6.7, 7.0 e 8.0;

3.22.17.72.2.2. VMware Desktop 16 Pro e 17 Pro;

3.22.17.72.2.3. Servidor Microsoft Hyper-V 2012 de 64 bits;

3.22.17.72.2.4. Servidor Microsoft Hyper-V 2012 R2 de 64 bits;

3.22.17.72.2.5. Microsoft Servidor Hyper -V 2016 de 64 bits;

3.22.17.72.2.6. Servidor Microsoft Hyper-V 2019 de 64 bits;

3.22.17.72.2.7. Servidor Microsoft Hyper-V 2022 de 64 bits;

3.22.17.72.2.8. Citrix XenServer 7.1 e 8.x;

3.22.17.72.2.9. Oracle VM VirtualBox 6.x e7. x.

3.22.17.73. A solução proposta deve suportar criptografia em vários níveis:

3.22.17.73.1. Criptografia completa do disco – incluindo disco do sistema;

3.22.17.73.2. Criptografia de arquivos e pastas;

3.22.17.73.3. Criptografia de mídia removível;

3.22.17.73.4. Gerenciamento de criptografia BitLocker e MacOS Filevault2.

3.22.17.74. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita:

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.22.17.74.1. A criptografia de arquivos em unidades de computador locais;

3.22.17.74.2. A criação de listas de criptografia de arquivos por extensão ou grupo de extensões;

3.22.17.74.3. A criação de listas criptografadas de pastas em unidades de computador locais.

3.22.17.75. 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:

3.22.17.75.1. Especifique uma regra de criptografia padrão pela qual o aplicativo aplique a mesma ação a todas as unidades removíveis;

3.22.17.75.2. Configure regras de criptografia para arquivos armazenados em unidades removíveis individuais.

3.22.17.76. 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:

3.22.17.76.1. A criptografia de todos os arquivos armazenados em unidades removíveis;

3.22.17.76.2. A criptografia de novos arquivos somente quando eles são salvos ou criados em unidades removíveis.

3.22.17.77. 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.

3.22.17.78. 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.

3.22.17.79. 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.

3.22.17.80. A solução proposta deve oferecer a capacidade de restaurar dispositivos criptografados se um disco rígido ou unidade removível criptografado estiver corrompido.

3.22.17.81. 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

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

ação a todas as unidades removíveis ou de configurar regras de criptografia para unidades removíveis individuais.

3.22.17.82. 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.

3.22.17.83. A solução proposta deve oferecer a capacidade de monitorar centralmente o status da criptografia e gerar relatórios sobre computadores/dispositivos criptografados.

3.22.17.84. 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.

3.22.17.85. 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.

3.22.17.86. A solução proposta deve ter a capacidade de bloquear o acesso de aplicativos a dados criptografados, se necessário.

3.22.17.87. 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.

3.22.17.88. 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.

3.22.17.89. A solução proposta deve fornecer um local central para armazenamento de chaves de criptografia e múltiplas opções de recuperação.

3.22.17.90. O servidor administrador/gerenciador da solução proposta deve ter a capacidade de descriptografar todos os dados criptografados independentemente da localização e/ou usuário.

3.22.17.91. A solução proposta deve suportar layouts de teclado QWERTY e AZERTY para autorização de pré inicialização.

3.22.17.92. A solução proposta deve fornecer a funcionalidade para gerenciar/aplicar a criptografia do Microsoft Bit Locker.

3.22.17.93. A solução proposta deve fornecer a funcionalidade para personalizar as configurações de criptografia do Microsoft BitLocker, incluindo:

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.22.17.93.1. Uso do Trusted Platform Module e configurações de senha;

3.22.17.93.2. Uso de criptografia de hardware para estações de trabalho e criptografia de software se a criptografia de hardware não estiver disponível;

3.22.17.93.3. 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).

3.22.17.94. A solução proposta deve suportar criptografia em Microsoft Surface Tablets.

3.22.17.95. A solução proposta deverá incluir recursos para gerenciar computadores remotamente, incluindo:

3.22.17.95.1. Instalação remota de software de terceiros;

3.22.17.95.2. Relatórios sobre software e hardware existentes;

3.22.17.95.3. Monitoramento para instalação de software não autorizado;

3.22.17.95.4. Remoção de software não autorizado.

3.22.17.96. A solução proposta deverá incluir recursos de gerenciamento de patches para sistemas operacionais Windows e para aplicativos de terceiros instalados.

3.22.17.97. A funcionalidade de gerenciamento de patches da solução proposta deve ser totalmente automatizada, com capacidade de detectar, baixar e enviar patches ausentes para endpoints.

3.22.17.98. A solução proposta deve fornecer a possibilidade de selecionar quais patches serão baixados/enviados para os endpoints, com base em sua criticidade.

3.22.17.99. 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.

3.22.17.100. A solução proposta deve fornecer relatórios abrangentes sobre vulnerabilidades descobertas e patches ausentes, bem como sobre endpoints e status de implantação de patches.

3.22.17.101. A solução proposta deve ter a capacidade de aplicar patches específicos com base na criticidade ou gravidade.

3.22.17.102. O servidor de gerenciamento da solução proposta deve ser configurável como uma fonte de atualizações para Microsoft Updates e aplicativos de terceiros.

3.22.17.103. A solução proposta deve incluir o aconselhamento sobre vulnerabilidade do fornecedor de aplicativos, bem como do fornecedor de segurança.

3.22.17.104. A solução proposta deve permitir ao administrador aprovar atualizações.

3.22.17.105. A solução proposta deve ser capaz de identificar automaticamente patches ausentes em endpoints individuais e enviar apenas os que são necessários/ausentes.

3.22.17.106. A solução proposta deve suportar a agregação de patches para minimizar o número de atualizações necessárias.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.22.17.107. A solução proposta deve notificar o administrador sobre quaisquer patches ausentes nos terminais assim que as informações relevantes estiverem disponíveis.

3.22.17.108. A solução proposta deverá proporcionar a possibilidade de gerir separadamente a aplicação de patches para sistemas operativos e para aplicações de terceiros.

3.22.17.109. A solução proposta deverá proporcionar a possibilidade de corrigir vulnerabilidades existentes em qualquer ponto final ou apenas em pontos específicos.

3.22.17.110. 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).

3.22.17.111. A solução proposta deve suportar a distribuição automatizada de patches e atualizações para mais de 150 aplicações.

3.22.17.112. A solução proposta deve ter funcionalidade de suporte ao modo de teste de patch.

3.22.17.113. A solução proposta deve incluir campos dedicados que contenham informações sobre 'Exploração encontrada para a vulnerabilidade'.

3.22.17.114. A solução proposta deve incluir campos dedicados que contenham informações sobre "Ameaça encontrada para a vulnerabilidade".

3.22.17.115. A solução proposta deve permitir que o administrador restrinja a capacidade dos usuários do dispositivo de aplicar eles próprios as atualizações da Microsoft.

3.22.17.116. A solução proposta deve permitir ao administrador especificar quais atualizações podem ser instaladas pelos usuários.

3.22.17.117. A solução proposta deve permitir ao administrador visualizar uma lista de atualizações e patches não relacionados aos dispositivos clientes.

3.22.17.118. A solução proposta deve apoiar a implantação do sistema operacional.

3.22.17.119. A solução proposta deve suportar Wake-on LAN e UEFI.

3.22.17.120. 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.

3.22.17.121. A solução proposta deve ser capaz de fornecer correções de vulnerabilidades aos computadores clientes sem instalar as atualizações.

3.22.17.122. 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.

3.22.17.123. A solução proposta deve informar o administrador sobre atualizações e patches não relacionados no dispositivo cliente.

3.22.17.124. A solução proposta deve ser configurável/atribuível como fonte de atualização para atualizações da Microsoft e de terceiros.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.22.17.125. A solução proposta deve permitir ao administrador selecionar o produto Microsoft e os idiomas para os quais as atualizações serão baixadas.

3.22.17.126. 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.

3.22.17.127. A solução proposta deve ser capaz de desinstalar aplicativos remotamente, não se limitando a programas antivírus incompatíveis.

3.22.17.128. 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.

3.22.17.129. A solução proposta deve permitir que o administrador configure regras para instalação de patches/atualizações da Microsoft e de terceiros:

3.22.17.129.1. Inicie a instalação ao reiniciar ou desligar o computador;

3.22.17.129.2. Instale o gerador necessário todos os pré-requisitos do sistema;

3.22.17.129.3. Permitir a instalação de novas versões de aplicativos durante as atualizações;

3.22.17.129.4. Baixe atualizações para o dispositivo sem instalá-las.

3.22.17.130. 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.

3.22.17.131. A solução proposta deve permitir a remoção/desinstalação de atualizações específicas de aplicativos e sistemas operacionais.

3.22.17.132. O servidor de gerenciamento da solução proposta deve ser capaz de enviar logs para servidores SIEMs e SYSLOG nos seguintes formatos:

3.22.17.132.1. CEF;

3.22.17.132.2. LEEF;

3.22.17.132.3. A solução proposta deve ser capaz de rastrear licenças de aplicações de terceiros e gerar notificações de quaisquer violações potenciais;

3.22.17.132.4. O relatório da solução proposta deve conter informações CVE;

3.22.17.132.5. A solução proposta deve suportar instalação de aplicações e software de terceiros.

3.22.18. Do Módulo de Gerenciamento Simplificado

3.22.18.1. A solução proposta deve suportar arquitetura cloud.

3.22.18.2. A solução proposta deve incluir um console web integrado para o gerenciamento dos endpoint, que não deve exigir nenhuma instalação adicional.

3.22.18.3. O console de gerenciamento web da solução proposta deve ser simples de usar e deve suportar dispositivos com tela sensível ao toque.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.22.18.4. A solução proposta deve permitir ao administrador gerar relatórios pré-definidos.

3.22.18.5. 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.

3.22.18.6. A solução proposta deve suportar sistemas operacionais Windows, Mac, Android e iOS.

3.22.18.7. A solução proposta deve incluir informações do endpoint:

3.22.18.7.1. IP público de internet;

3.22.18.7.2. IP interno do dispositivo;

3.22.18.7.3. Versão do agente de proteção;

3.22.18.7.4. Última comunicação com a console, contendo data e hora;

3.22.18.7.5. Informações do sistema operacional.

3.22.18.8. 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.

3.22.18.9. A solução proposta deve permitir detectar informações críticas em arquivos localizados nos armazenamentos em nuvem do Office 365.

3.22.18.10. A solução proposta deve incluir uma plataforma de capacitação online em segurança cibernética ou compor com ferramenta do mesmo fabricante que tenha capacidade similar.

3.22.19. Dos Requisitos Gerais da Proteção de Endpoint

3.22.19.1. A solução proposta deve ser capaz de detectar os seguintes tipos de ameaças:

3.22.19.1.1. 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;

3.22.19.2. A solução proposta deve ser de um único fornecedor e suportar todos módulos descritos neste termo de referência;

3.22.19.3. A solução proposta deve suportar integração com Anti-malware Scan Interface (AMSI);

3.22.19.4. A solução proposta deve ter capacidade de integração com a central de segurança do Windows Defender;

3.22.19.5. A solução proposta deve suportar o subsistema Linux no Windows.

3.22.19.6. A solução proposta deve fornecer tecnologias de proteção da próxima geração. Sendo no mínimo:

3.22.19.6.1. Proteção contra ameaças sem arquivos (Fileless);

3.22.19.6.2. Fornecimento de proteção baseada em machine leaning em várias camadas e análise comportamental durante diferentes estágios da cadeia de ataque.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.22.19.7. A solução proposta deve fornecer varredura de memória para estações de trabalho Windows;

3.22.19.8. A solução proposta deve fornecer varredura de memória do kernel para estações de trabalho Linux;

3.22.19.9. 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;

3.22.19.10. 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;

3.22.19.11. 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;

3.22.19.12. A solução proposta deve fornecer análise comportamental baseada em machine learning;

3.22.19.13. 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.

3.22.19.14. A solução proposta deve incluir os seguintes componentes no sensor instalado no endpoint:

3.22.19.14.1. Controles de aplicativos;

3.22.19.14.2. Controle web e dispositivos;

3.22.19.14.3. HIPS e Firewall;

3.22.19.14.4. Descoberta de patches e vulnerabilidades de sistemas operacionais Windows;

3.22.19.14.5. Gerenciamento de criptografia de arquivos e discos;

3.22.19.14.6. Controle adaptativo para detecção de anomalias;

3.22.19.14.7. A capacidade de detectar e bloquear hosts não confiáveis na detecção de atividades semelhantes à criptografia em recursos compartilhados do servidor.

3.22.19.15. 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;

3.22.19.16. A solução proposta deve ter bancos de dados de reputação locais e globais.

3.22.19.17. A solução proposta deve ser capaz de verificar o tráfego HTTPS, HTTP, SMTP e FTP contra malwares;

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.22.19.18. A solução proposta deve incluir um módulo capaz, no mínimo, de:

3.22.19.18.1. Bloqueio de aplicativos com base em sua categorização;

3.22.19.18.2. Bloqueio/permissão de pacotes, protocolos, endereços IP, portas e direção de tráfego específicos;

3.22.19.18.3. A adição de sub-redes e a modificação de permissões de atividade.

3.22.19.19. 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.

3.22.19.20. A solução proposta deve ser capaz de bloquear ataques à rede e reportar a origem da infecção.

3.22.19.21. 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.

3.22.19.22. A solução proposta deve incluir limpeza remota dos dispositivos com as seguintes funcionalidades:

3.22.19.22.1. Modo silencioso;

3.22.19.22.2. Discos rígidos e dispositivos removíveis;

3.22.19.22.3. De todos as contas de usuários do dispositivo.

3.22.19.23. A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes modos:

3.22.19.23.1. Exclusão imediata de dados;

3.22.19.23.2. Exclusão de dados adiada.

3.22.19.24. A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes métodos de exclusão de dados:

3.22.19.24.1. Excluir usando os recursos do sistema operacional - os arquivos são excluídos;

3.22.19.24.2. Excluir completamente, sem recuperação - tornando praticamente impossível restaurar os dados após a exclusão.

3.22.19.25. A solução proposta deve ter uma abordagem proativa para impedir que malware explore vulnerabilidades existentes em servidores e estações de trabalho.

3.22.19.26. A solução proposta deve suportar a tecnologia AM PPL (Anti-Malware Protected Process Light) para proteção contra ações maliciosas.

3.22.19.27. A solução proposta deve incluir proteção contra ataques que explorem vulnerabilidades no protocolo ARP para falsificar o endereço MAC do dispositivo.

3.22.19.28. 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

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

computadores protegidos e, em seguida, identificar e bloquear ações anômalas e potencialmente prejudiciais realizadas por esse terminal ou usuário.

3.22.19.29. 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.

3.22.19.30. A solução proposta deve incluir um componente dedicado para verificação de conexões criptografadas.

3.22.19.31. A solução proposta deve ser capaz de descriptografar e verificar o tráfego de rede transmitido por conexões criptografadas.

3.22.19.32. 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.

3.22.19.33. A solução proposta deve incluir funcionalidade para apagar dados remotamente das estações de trabalho.

3.22.19.34. A solução proposta deve incluir funcionalidade para excluir automaticamente os dados caso não haja conexão com o servidor de gerenciamento de endpoint.

3.22.19.35. A solução proposta deve suportar detecção baseadas em multicamadas sendo no mínimo: Assinatura, heurística, machine learning ou assistida por nuvem.

3.22.19.36. A solução proposta deve ter a capacidade de gerar um alerta, limpar e excluir uma ameaça detectada.

3.22.19.37. A solução proposta deve ser capaz de monitorar e bloquear ações que não são típicas dos computadores da rede de uma empresa.

3.22.19.38. A solução proposta deve ter a capacidade de acelerar as verificações ignorando os objetos que não foram alterados desde a verificação anterior.

3.22.19.39. 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.

3.22.19.40. A solução proposta deve verificar automaticamente as unidades removíveis em busca de malware quando elas estiverem conectadas a qualquer endpoint.

3.22.19.41. A solução proposta deve ser capaz de bloquear o uso de dispositivos de armazenamento USB ou permitir o acesso apenas aos dispositivos permitidos.

3.22.19.42. A solução proposta deve ser capaz de diferenciar dispositivos de armazenamento USB, impressoras, celulares e outros periféricos.

3.22.19.43. 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.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.22.19.44. A solução proposta deve ter categoria de detecção para bloquear banners de sites.

3.22.19.45. 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.

3.22.19.46. A solução proposta deve suportar políticas baseadas no usuário para controle de dispositivos, web e aplicativos.

3.22.19.47. A solução proposta deve apresentar integração na nuvem, para fornecer atualizações mais rápidas possíveis sobre malware e ameaças potenciais.

3.22.19.48. 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.

3.22.19.49. A solução proposta deve permitir que o administrador monitore o uso de portas personalizadas/aleatórias pelo aplicativo.

3.22.19.50. 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.

3.22.19.51. 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.

3.22.19.52. 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.

3.22.19.53. O componente de controle web da solução proposta deve incluir uma categoria criptomoedas e mineração.

3.22.19.54. O componente de controle de aplicações da solução proposta deve incluir os modos operacionais lista de negações e lista de permissões.

3.22.19.55. A solução proposta deve suportar o controle de scripts executados em PowerShell.

3.22.19.56. A solução proposta deve suportar modo teste com geração de relatórios sobre execução de aplicativos bloqueados.

3.22.19.57. A solução proposta deve ter a capacidade de controlar o acesso do sistema/aplicativo do usuário a dispositivos de gravação de áudio e vídeo.

3.22.19.58. A solução proposta deve fornecer um recurso para verificar os aplicativos listados em cada categoria baseada em nuvem.

3.22.19.59. A solução proposta deve ter capacidade de integração com um sistema avançado de proteção contra ameaças específico do fornecedor.

3.22.19.60. 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.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.22.19.61. A solução proposta deve ter a capacidade de categorizar automaticamente os aplicativos iniciados antes da instalação da proteção de endpoint.

3.22.19.62. A solução proposta deve ter proteção contra ameaças de e-mail de endpoint com:

3.22.19.62.1. Filtro de anexos;

3.22.19.62.2. Verificação de mensagens de e-mail ao receber, ler e enviar;

3.22.19.63. A solução proposta deve ter a capacidade de verificar vários redirecionamentos, URLs encurtados, URLs sequestrados e atrasos baseados em tempo.

3.22.19.64. A solução proposta deve permitir que o usuário do computador verifique a reputação de um arquivo.

3.22.19.65. 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.).

3.22.19.66. 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.

3.22.19.67. 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.

3.22.19.68. A solução proposta deve incluir suporte ao protocolo IPv6.

3.22.19.69. A solução proposta deve oferecer a verificação de seções críticas do computador como uma tarefa independente.

3.22.19.70. A solução proposta deve incorporar a tecnologia de autoproteção de aplicação:

3.22.19.70.1. Protegendo contra o gerenciamento remoto não autorizado de um serviço de aplicativo;

3.22.19.70.2. Protegendo o acesso aos parâmetros do aplicativo definindo uma senha. Evitando a desativação da proteção por malware, criminosos ou usuários.

3.22.19.71. A solução proposta deve oferecer a capacidade de escolher quais componentes de proteção contra ameaças instalar.

3.22.19.72. 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.

3.22.19.73. A solução proposta deve proteger contra malware ainda desconhecido pertencente a famílias cadastradas, com base em análise heurística.

3.22.19.74. A solução proposta deve notificar o administrador sobre eventos importantes que ocorreram através de notificação por e-mail.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.22.19.75. A solução proposta deve permitir ao administrador criar um único pacote de instalação do sensor de proteção com a configuração necessária.

3.22.19.76. A solução proposta deve fornecer controles de aplicativos e dispositivos para estações de trabalho Windows.

3.22.19.77. 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.

3.22.19.78. 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.

3.22.19.79. A solução proposta deve fornecer uma lista predefinida de exclusões de verificação para aplicativos e serviços Microsoft.

3.22.19.80. A solução proposta deve suportar a instalação de proteção de endpoint em servidores sem a necessidade de reinicialização.

3.22.19.81. 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.

3.22.19.82. A solução proposta deve suportar endereços IPv6.

3.22.19.83. A solução proposta deve suportar verificação em duas etapas (autenticação).

3.22.19.84. 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.

3.22.19.85. A solução proposta deverá contar com a remoção centralizada (manual e automática) de aplicações incompatíveis do centro de administração.

3.22.19.86. 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.

3.22.19.87. A solução proposta deve permitir a instalação remota do sensor de endpoint com os bancos de dados anti malware mais recentes.

3.22.19.88. A solução proposta deve permitir a atualização automática do sensor de endpoint e de bases de dados de anti-malware.

3.22.19.89. A solução proposta deve contar com recursos de busca automática de vulnerabilidades em aplicações e no sistema operacional em máquinas protegidas.

3.22.19.90. A solução proposta deve permitir a gestão de um componente que proíba a instalação e/ou execução de programas.

3.22.19.91. A solução proposta deve permitir a gestão de um componente que controla o trabalho com dispositivos de E/S externos.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.22.19.92. A solução proposta deve permitir o gerenciamento de componente que controle a atividade do usuário na internet.

3.22.19.93. 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.

3.22.19.94. A solução proposta deve incluir a distribuição automática de licenças nos computadores clientes.

3.22.19.95. A solução proposta deverá ser capaz de exportar relatórios para arquivos PDF, CSV ou XLS.

3.22.19.96. 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.

3.22.19.97. A solução proposta deve prever a criação de contas internas para autenticar administradores no servidor de administração.

3.22.19.98. A solução proposta deverá ter capacidade de gerenciar dispositivos móveis através de comandos remotos.

3.22.19.99. A solução proposta deve ter a capacidade de excluir atualizações baixadas.

3.22.19.100. A solução proposta deve mostrar claramente informações sobre a distribuição de vulnerabilidades entre computadores gerenciados.

3.22.19.101. A interface do servidor de gerenciamento da solução proposta deverá suportar o idioma Inglês e português.

3.22.19.102. A solução proposta deve ter um painel customizável gerando e exibindo estatísticas em tempo real dos sensores de endpoints.

3.22.19.103. 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.

3.22.19.104. Os relatórios da solução proposta devem incluir informações sobre cada ameaça e a tecnologia que a detectou.

3.22.19.105. 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.

3.22.19.106. 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.

3.22.19.107. A solução proposta deve permitir a migração rápida do console de gerenciamento local para o console de gerenciamento baseado em nuvem do fornecedor.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.22.19.108. A solução proposta deve fornecer mecanismos de atualização de banco de dados, incluindo:

3.22.19.108.1. Múltiplas formas de atualização, incluindo canais de comunicação globais através do protocolo HTTPS, recursos compartilhados em rede local e mídia removível.

3.22.19.108.2. Verificação da integridade e autenticidade das atualizações por meio de assinatura digital eletrônica.

3.22.19.109. A solução proposta deve permitir monitorar vulnerabilidades existentes em dispositivos gerenciados.

3.22.19.110. A solução proposta deve gerar relatórios de vulnerabilidades encontradas nos dispositivos com sensor de endpoint instalado.

3.22.20. Do Modulo de Gerenciamento de Dispositivos Móveis

3.22.20.1. O modulo deve ser integrado a console de gerenciamento.

3.22.20.2. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis, incluindo:

3.22.20.2.1. Android 5.0 ou posterior (incluindo Android 12L, excluindo Go Edition).

3.22.20.2.2. iOS 10–17 ou iPadOS 13–17.

3.22.20.3. A solução proposta deve oferecer suporte a dispositivos Android Device Owner.

3.22.20.4. A solução proposta deve suportar dispositivos iOS supervisionados.

3.22.20.5. 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.

3.22.20.6. 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.

3.22.20.7. A solução proposta deve ter a funcionalidade de adicionar um site excluído da verificação a uma lista de permissões.

3.22.20.8. 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).

3.22.20.9. 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.

3.22.20.10. A solução proposta deverá ter a funcionalidade de detectar a localização do dispositivo móvel via GPS, e mostrá-la no Google Maps.

3.22.20.11. A solução proposta deve permitir ao administrador tirar uma foto da câmera frontal do celular quando ele estiver bloqueado.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.22.20.12. A solução proposta deve ter recursos de conteinerização para dispositivos Android.

3.22.20.13. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos Android:

3.22.20.13.1. Dados em contêineres;

3.22.20.13.2. Contas de e-mail corporativo;

3.22.20.13.3. Configurações para conexão à rede Wi-Fi corporativa e VPN;

3.22.20.13.4. Nome do ponto de acesso (APN);

3.22.20.13.5. Perfil do Android for Work;

3.22.20.13.6. Recipiente KNOX;

3.22.20.13.7. Chave do gerenciador de licença KNOX.

3.22.20.14. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos iOS:

3.22.20.14.1. Todos os perfis de configuração instalados;

3.22.20.14.2. Todos os perfis de provisionamento;

3.22.20.14.3. O perfil iOS MDM;

3.22.20.14.4. Aplicativos para os quais a caixa de seleção remover e o perfil iOS MDM foram marcadas.

3.22.20.15. 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.

3.22.20.16. 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:

3.22.20.16.1. Critérios de verificação do dispositivo;

3.22.20.16.2. 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.

3.22.20.17. A solução proposta deve ter a funcionalidade de detectar e notificar o administrador sobre hacks de dispositivos, por exemplo, root, Jailbreak e etc.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.22.20.18. A solução proposta deverá permitir a gestão de pelo menos as seguintes características do dispositivo:Cartões de memória e outras unidades removíveis;Câmera do dispositivo;

3.22.20.18.1. Conexões Wi-Fi;

3.22.20.18.2. Conexões Bluetooth;

3.22.20.18.3. Porta de conexão infravermelha;

3.22.20.18.4. Ativação do ponto de acesso Wi-Fi;

3.22.20.18.5. Conexão de área de trabalho remota;

3.22.20.18.6. Sincronização de área de trabalho;

3.22.20.18.7. Definir configurações da caixa de correio do Exchange;

3.22.20.18.8. Configurar caixa de e-mail em dispositivos iOS MDM;

3.22.20.18.9. Configure contêineres Samsung KNOX;

3.22.20.18.10. Definir as configurações do perfil do Android for Work;

3.22.20.18.11. Configurar e-mail/calendário/contatos;

3.22.20.18.12. Defina as configurações de restrição de conteúdo de mídia;

3.22.20.18.13. Definir configurações de proxy no dispositivo móvel;

3.22.20.18.14. Configurar certificados e SCEP.

3.22.20.19. 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.

3.22.20.20. A solução proposta deve suportar todos os métodos de implantação abaixo para o sensor móvel:

3.22.20.20.1. Huawei App Gallery e Apple App Store;

3.22.20.20.2. Portal de inscrição móvel KNOX;

3.22.20.20.3. Pacotes de instalação pré-configurados independentes.

3.22.20.21. 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.

3.22.20.22. A solução proposta deve permitir que o PIN de um dispositivo móvel seja redefinido remotamente.

3.22.20.23. A solução proposta deve incluir a opção de registrar dispositivos Android usando sistemas EMM de terceiros:

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.22.20.23.1. VMware AirWatch 9.3 ou posterior;

3.22.20.23.2. MobileIron 10.0 ou posterior;

3.22.20.23.3. IBM MaaS360 10.68 ou posterior;

3.22.20.23.4. Microsoft Intune 1908 ou posterior;

3.22.20.23.5. SOTI MobiControl 14.1.4 (1693) ou posterior.

3.22.20.24. A solução proposta deve ter funcionalidade para forçar a instalação de um aplicativo no dispositivo.

3.22.20.25. A solução proposta deve suportar a implantação de sensor de endpoint iniciada pelo usuário através de:

3.22.20.25.1. Galeria de aplicativos Huawei;

3.22.20.25.2. Loja de aplicativos da Apple.

3.22.20.26. A solução proposta deve ser capaz de escanear arquivos abertos no dispositivo.

3.22.20.27. A solução proposta deve ser capaz de verificar programas instalados a partir da interface do dispositivo.

3.22.20.28. 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.

3.22.20.29. A solução proposta deve proporcionar o isolamento confiável de objetos infectados em um local de armazenamento de quarentena.

3.22.20.30. 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.

3.22.20.31. 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.

3.22.20.32. A solução proposta deve ser capaz de gerenciar e monitorar dispositivos móveis a partir do mesmo console usado para gerenciar computadores e servidores.

3.22.20.33. A solução proposta deve fornecer funcionalidade Anti Roubo, para que dispositivos perdidos e/ou deslocados possam ser localizados, bloqueados e apagados remotamente.

3.22.20.34. A solução proposta deve fornecer a possibilidade de bloquear o lançamento de aplicativos proibidos no dispositivo móvel.

3.22.20.35. A solução proposta deve ser capaz de impor configurações de segurança, como restrições de senha e criptografia, em dispositivos móveis.

3.22.20.36. A solução proposta deve ter a capacidade de enviar aplicações recomendadas/exigidas pelo administrador para o dispositivo móvel.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.22.20.37. A solução proposta deverá possuir Controle de Aplicativos com os modos de aplicação Proibido/Permitido.

3.22.20.38. A solução proposta deve incluir um modelo de assinatura integrado a nuvem do fabricante para proteção de ataques mais recentes.

3.22.20.39. A solução proposta deve proteger contra ameaças online em dispositivos iOS.

3.22.21. Do Módulo de EDR

3.22.21.1. Deve apresentar um gráfico de propagação de ameaças com os principais processos de conexões de rede, DLLs, seções de registro afetado ou envolvido no alerta.

3.22.21.2. 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.

3.22.21.3. 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.

3.22.21.4. Dever ser integrado ao portal de inteligência do fornecedor para enriquecimento dos detalhes da análise.

3.22.21.5. Deve apresentar informações detalhadas contendo:

3.22.21.5.1. Usuário que executou a ação;

3.22.21.5.2. Informações acesso privilegiado.

3.22.21.6. A solução proposta deve ter sandbox em nuvem do fabricante integrada para verificar automaticamente arquivos e aplicar respostas caso atividades suspeitas sejam detectadas.

3.22.21.7. A solução proposta deve suportar integração com serviço de reputação em nuvem.

3.22.21.8. 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.).

3.22.21.9. O agente EDR deve ter integração com o aplicativo de proteção de endpoint (agente único).

3.22.21.10. Soluções EDR e proteção de endpoint devem ter console unificado para administradores e analistas.

3.22.21.11. A solução proposta deve suportar a detecção automatizada de atividades maliciosas usando a solução Endpoint Protection e a tecnologia de sandbox na nuvem.

3.22.21.12. A solução proposta deve complementar as informações do veredicto da solução Endpoint Protection com artefatos do sistema sobre a detecção.

3.22.21.13. A solução proposta deve suportar a geração automática de indicadores de ameaça (IoC) após a detecção ocorrer com capacidade de aplicar ações de resposta.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.22.21.14. A solução deve ter a capacidade de forçar a execução da varredura IoC em todos os endpoints com agentes EDR instalados.

3.22.21.15. A solução proposta deve suportar a execução de varredura IoC de acordo com um agendador.

3.22.21.16. A solução proposta deve suportar a importação de IoC de terceiros no formato OpenIoC para uso em digitalização em rede.

3.22.21.17. 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.

3.22.21.18. 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.

3.22.21.19. A solução proposta deve gerar um cartão de incidente detalhado relacionado à ameaça detectada em um endpoint.

3.22.21.20. 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:

3.22.21.20.1. Gráfico da cadeia de desenvolvimento de ameaças e detalhamento para análise posterior (cadeia de ataque);

3.22.21.20.2. Informações sobre o dispositivo no qual a ameaça foi detectada, contendo: nome, endereço IP, endereço MAC, lista de usuários, sistema operacional;

3.22.21.20.3. Informações gerais sobre a detecção, incluindo modo de detecção;

3.22.21.20.4. Alterações no registro associadas à detecção;

3.22.21.20.5. Histórico da presença de arquivos no dispositivo;

3.22.21.20.6. Ações de resposta executadas pela aplicação.

3.22.21.21. 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.

3.22.21.22. A visualização de incidente deve apresentar uma visão detalhada dos artefatos do sistema e dos dados relacionados ao incidente para análise da causa raiz:

3.22.21.22.1. Processo;

3.22.21.22.2. Conexões de rede;

3.22.21.22.3. Alterações no registro;

3.22.21.22.4. Detalhes do download de objeto.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.22.21.23. A solução proposta deve fornecer orientação de resposta (resposta guiada).

3.22.21.24. A solução proposta deve suportar “clique único” no console de gerenciamento avançado para resposta a um incidente.

3.22.21.25. A solução proposta deve suportar pelo menos as seguintes ações de resposta que um administrador pode executar quando ameaças são detectadas:

3.22.21.25.1. Impedir a execução de objetos;

3.22.21.25.2. Isolamento de host;

3.22.21.25.3. Excluir objeto do host ou grupo de hosts;

3.22.21.25.4. Encerrar um processo no dispositivo;

3.22.21.25.5. Colocar um objeto em quarentena;

3.22.21.25.6. Execute a verificação do sistema;

3.22.21.25.7. Execução remota de programa/processo/comando;

3.22.21.25.8. Iniciar a varredura IoC para um grupo de hosts.

3.22.22. Do Módulo de MDR

3.22.22.1. 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”;

3.22.22.2. Deverá ser suportada por qualquer um dos seguintes navegadores:

3.22.22.2.1. Apple Safari versões mais recentes;

3.22.22.2.2. Google Chrome versões mais recentes;

3.22.22.2.3. Microsoft Edge;

3.22.22.2.4. Mozilla Firefox versões mais recentes.

3.22.22.3. 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:

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.22.22.3.1. Microsoft Windows 7 e superiores;

3.22.22.3.2. MacOS 10.14-11;

3.22.22.3.3. CentOS 6.7 ou superior;

3.22.22.3.4. Debian GNU / Linux 9.4 ou superior;

3.22.22.3.5. Linux Mint 19 ou superior;

3.22.22.3.6. Oracle Linux 7.3 ou superior;

3.22.22.3.7. Red Hat Enterprise Linux 6.7 ou superior;

3.22.22.3.8. SUSE Linux Enterprise Server 12 SP5 ou superior;

3.22.22.3.9. Ubuntu 18.04 LTS ou superior.

3.22.22.4. Deverá suportar os requisitos de carga de rede:

3.22.22.4.1. Em condições médias de carga: um canal full duplex com largura de banda de pelo menos 1,7 Kbps para cada ativo;

3.22.22.4.2. Em condições de carga máxima: um canal full duplex com largura de banda de pelo menos 2,7 Kbps para cada ativo.

3.22.22.5. A console deve possuir das dashboards com as informações principais, apresentando no mínimo:

3.22.22.5.1. Número de incidentes e status;

3.22.22.5.2. Quantidade de dispositivos monitorados.

3.22.22.6. Deve possuir mecanismo de notificações, com no mínimo as seguintes opções:

3.22.22.6.1. E-mail;

3.22.22.6.2. Telegram.

3.22.22.7. Deve permitir o envio de relatórios.

3.22.22.8. O agente deve enviar a telemetria em tempo real para o SOC do fabricante.

3.22.22.9. O serviço deve compreender monitoramento dos dados enviados e alertas gerados em um regime 24x7x265.

3.22.22.10. O envio e armazenamento da telemetria, devem respeitar as principais legislações de proteção de dados, como GDPR e LGPD.

3.22.22.11. O SOC do fabricante deve possuir datacenters em pelo menos duas localidades em diferentes países.

3.22.22.12. O SoC do fabricante deve possuir equipes de analistas em pelo menos 3 regiões (países) incluindo Brasil.

3.22.22.13. Os dados coletados devem passar por no mínimo:

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.22.22.13.1. Modelos de Machine Learning/Inteligência Artificial;

3.22.22.13.2. Análise humana;

3.22.22.13.3. Correlação com IoA's (indicadores de ataque);

3.22.22.13.4. Emulação em sandbox (quando necessário).

3.22.22.14. Após análise, informações sobre atividades potencialmente maliciosas, devem ser apresentadas no portal como "Incidentes".

3.22.22.15. O Incidente deve possuir no mínimo as seguintes informações:

3.22.22.15.1. Resumo;

3.22.22.15.2. Prioridade (Baixa, Média e Alta);

3.22.22.15.3. Recomendação;

3.22.22.15.4. Data de criação e data de atualização;

3.22.22.15.5. Correlacionamento com táticas/técnicas do Framewok MITRE ATT&CK;

3.22.22.15.6. Dispositivos afetados;

3.22.22.15.7. IoC's de host e de rede;

3.22.22.15.8. Descrição completa em linha do tempo.

3.22.22.16. O incidente pode receber ações de resposta recomendada disparadas pela equipe de SoC, compreendendo no mínimo as seguintes ações:

3.22.22.16.1. Transferir arquivo para o SoC;

3.22.22.16.2. Isolar um dispositivo;

3.22.22.16.3. Desabilitar isolamento de dispositivo;

3.22.22.16.4. Deletar chave de registro;

3.22.22.16.5. Dump de memória.

3.22.22.17. As ações devem ser aprovadas no portal por profissional da contratante, com a opção de habilitar aprovação automática.

3.22.23. Do Monitoramento, Coleta, Identificação e Investigação dos Eventos de Segurança Cibernética:

3.22.23.1. O serviço de monitoramento deverá utilizar informações extraídas de registros gerados pelos sistemas monitorados.

3.22.23.2. 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.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.22.23.3. 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.

3.22.23.4. 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.

3.22.23.5. 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.

3.22.23.6. 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.

3.22.23.7. 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.

3.22.23.8. 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.

3.22.23.9. 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.

3.22.23.10. O agente deve ter capacidade de coletar e processar dados relacionadas ao veredito e ao contexto da ameaça.

3.22.23.11. Deve fornecer graficamente a visualização da cadeia do ataque.

3.22.23.12. 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).

3.22.23.13. 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:

3.22.23.13.1. Isolar o host;

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.22.23.13.2. Iniciar uma varredura nas áreas críticas;

3.22.23.13.3. Quarentenar o objeto.

3.22.23.14. A solução deve criar um report detalhado sobre o incidente, tendo a capacidade de incluir no mínimo os seguintes dados:

3.22.23.14.1. Detecções provenientes da solução de endpoint;

3.22.23.14.2. Processos;

3.22.23.14.3. Alterações de registro;

3.22.23.14.4. Conexões remotas;

3.22.23.14.5. Criação de arquivos.

3.22.23.15. Varredura por todos os dispositivos executada a partir de indicador de comprometimento (IoC) gerado através da solução e importado pelo administrador.

3.22.23.16. Possibilidade de exportar os indicadores de comprometimento (IoC) gerados a partir da solução.

3.22.23.17. A solução deve oferecer no mínimo as seguintes opções de resposta:

3.22.23.17.1. Prevenir a execução de um arquivo;

3.22.23.17.2. Quarentenar um arquivo;

3.22.23.17.3. Iniciar uma varredura por IoC;

3.22.23.17.4. Parar um processo;

3.22.23.17.5. Executar um processo.

3.22.23.18. Ferramenta que possibilite o isolamento do host infectado com no mínimo as características abaixo:

3.22.23.18.1. A opção de isolamento deve estar disponível junto a visualização do incidente;

3.22.23.18.2. Na configuração padrão, o isolamento deve ser feito de forma granular, permitindo o controle do dispositivo pela console administrativa mesmo após ativação da regra.

3.22.23.19. 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.

3.22.24. Requisitos para Documentação da Solução.

3.22.24.1. A documentação da solução de proteção de endpoint incluindo ferramentas de administração, deve incluir os seguintes documentos:

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.22.24.1.1. Ajuda on-line para administradores;

3.22.24.1.2. Ajuda on-line para melhores práticas de implementação;

3.22.24.1.3. Ajuda on-line para proteção de servidores de administração.

3.22.24.2. A documentação do software anti-malware fornecida deve descrever detalhadamente os processos de instalação, configuração e uso do software anti-malware.

3.22.24.3. Deve estar disponível página com informações de ciclo de vida das soluções e módulos.

3.23. DA PRESTAÇÃO DO SERVIÇO

3.23.1. A Contratada deverá realizar os procedimentos de transbordo, descarga e armazenamento dos equipamentos (com as embalagens originais) no local indicado para a entrega.

3.23.2. A Contratada deverá providenciar equipamentos e/ou mão de obra necessários para a descarga, que será acompanhada e fiscalizada por servidor devidamente designado.

3.23.3. 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.

3.23.4. Todos os softwares, firmwares e drivers de controle necessários ao perfeito funcionamento da solução, na última versão disponível.

3.23.5. Todas as licenças de utilização definitivas para os softwares, firmwares e drivers fornecidos.

3.23.6. Todos os cabos e acessórios necessários para a perfeita instalação, configuração e uso da solução.

3.23.7. 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.

3.23.8. Acesso para o CONTRATANTE à base de conhecimento do fabricante, incluindo documentação e download de atualizações.

3.23.9. 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.

3.24. DA IMPLEMENTAÇÃO DA SOLUÇÃO

3.24.1. Para todo os conjuntos (hardware ou software), deverá ser fornecido um Serviço Especializado de Instalação e Customização para a realização de serviços especializados.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.24.2. Entende-se por serviço especializado de instalação e customização de equipamentos, a montagem física dos equipamentos e seus respectivos acessórios pela CONTRATADA, bem como a configuração lógica de todos os equipamentos e softwares envolvidos, de acordo com o cenário requerido pela SED/MS.

3.24.3. Este serviço trata do “Projeto Executivo” e tem como objetivo a instalação física dos equipamentos, sua conectividade com a rede de dados e a configuração das características listadas pelo CONTRATANTE. A CONTRATADA deverá ser responsável pela definição, planejamento e execução de todas as informações a serem configuradas, após terem sido previamente aprovadas pelo CONTRATANTE.

3.24.4. Para a execução do serviço especializado de instalação e configuração, a CONTRATADA entregará, para validação do CONTRATANTE, um Plano de Implementação da Solução composto por, pelo menos, o conteúdo definido a seguir:

3.24.4.1. Plano de Entrega e Instalação dos Produtos – neste documento deverá constar, no mínimo, a relação completa dos equipamentos e softwares a serem fornecidos, discriminando detalhadamente a finalidade de cada um. O plano deverá contemplar e detalhar todos os serviços de instalação e configuração, bem como estabelecer procedimentos de testes de conexão e desempenho da rede para cada etapa de instalação e configuração concluída. Deverá ser informado o prazo para a conclusão de cada etapa do serviço de entrega e instalação. O plano de instalação dos produtos deverá contemplar obrigatoriamente os seguintes itens: endereçamento IP, políticas de VLANs, políticas de segurança, políticas de balanceamento de carga, roteamento, QoS, filtros, alarmes, relatórios a serem configurados e documentação da rede, conforme as features determinadas previamente pelo CONTRATANTE;

3.24.4.2. Projeto Executivo – este documento constitui-se no detalhamento da documentação necessária a correta configuração e parametrização dos equipamentos a serem fornecidos pela CONTRATADA. Neste documento deverão constar todas as informações geradas pela CONTRATADA, abordando os aspectos de arquitetura implantada, configuração, testes, migração e integração ao ambiente de rede do CONTRATANTE.

3.25. REQUISITOS DE TREINAMENTO/CAPACITAÇÃO

3.25.1. 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.

3.25.2. Deverá ser oferecido treinamento da solução ofertada para, no mínimo, 04 (quatro) participantes.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.25.3. O treinamento deverá ser realizado na sede da SED/MS ou em outro local apropriado, a ser acordado entre as partes, no município de Campo Grande/MS.

3.25.4. Deverá ser distribuído material de apoio a cada participante, que poderá ser, preferencialmente, em português ou inglês.

3.25.5. 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.

3.25.6. A Contratada deverá prover os equipamentos que irão compor o laboratório do treinamento, que deverão ser equivalentes aos fornecidos para a SED/MS ou, quando não for possível, por equipamentos similares com as mesmas funcionalidades.

3.25.7. O instrutor deverá ministrar o treinamento em português com carga horária de, no mínimo, 20 (vinte) horas, abordando obrigatoriamente o seguinte conteúdo:

3.25.7.1. Instalação do produto;

3.25.7.2. Utilização da interface gráfica simples;

3.25.7.3. Configuração dos parâmetros básicos e gerenciamento de usuários;

3.25.7.4. Melhores práticas de utilização da solução;

3.25.7.5. Integração com ambientes de virtualização;

3.25.7.6. Criação de regras personalizadas (firewall, antivírus, VPN, IPS, MTA, QoS, Aceleração e outras essenciais para ativação das funcionalidades principais);

3.25.7.7. Criação de perfis de aceleração e otimização de rede e aplicações;

3.25.7.8. Configuração de ambiente de alta disponibilidade (cluster);

3.25.7.9. Configuração de parâmetros para balanceamento de carga de serviços;

3.25.7.10. Conceitos de monitoramento;

3.25.7.11. Processamento de tráfego SSL na solução.

3.25.8. A SED/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;

3.25.9. Caso a deficiência não possa ser sanada sem prejuízo para o andamento do treinamento, esse será suspenso pela SED/MS, devendo a Contratada agendar novo treinamento, sem ônus adicional para a Contratante.

3.26. METODOLOGIA DE TRABALHO

3.26.1. 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.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.26.2. Todas as atividades técnicas serão desempenhadas de acordo com o ambiente tecnológico da Secretaria de Estado de Educação de Mato Grosso do Sul, devendo, portanto, haver compatibilidade do perfil do profissional exigido para o desempenho da atividade.

3.26.3. Os serviços serão realizados no ambiente físico da Contratada que possibilitara todos os meios necessários para a Contratante acompanhar os trabalhos por meio do Gestor do Contrato designado ou qualquer outro servidor designado.

3.26.4. Quando os serviços forem realizados no ambiente físico da Contratante, os profissionais deverão executá-los conforme jornada de trabalho da SED/MS, o que será controlado pela Contratada e supervisionado pela SED/MS.

3.26.5. A Contratada não poderá subcontratar, subempreitar, ceder ou transferir, total ou parcialmente o objeto da presente licitação descrita neste Estudo Técnico Preliminar.

3.26.6. A instalação dos equipamentos e a sua colocação em funcionamento correrão por conta e responsabilidade da Contratada.

3.26.7. Todos os itens necessários à instalação da solução correrão por conta da Contratada, como cabos, conectores e demais acessórios.

3.26.8. A solução deverá ser instalada em rack de piso, padrão 19”, com medidas adequadas para acomodação da solução.

3.27. CONDIÇÕES DE GARANTIA, SUPORTE TÉCNICO E QUALIFICAÇÃO DA EQUIPE

3.27.1. Os requisitos de garantia, suporte técnico especializado, manutenção e apoio são justificados pela necessidade de implantar a solução e mantê-la em funcionamento adequado durante toda a execução contratual, assegurando disponibilidade, desempenho, atualização tecnológica, correção de falhas e mitigação de vulnerabilidades.

3.27.2. O ambiente de rede corporativa e o ambiente de rede do Data Center da SED/MS são críticos para a continuidade dos serviços públicos prestados pela Secretaria de Estado de Educação. Qualquer evento que ocasione paralisação, falha ou mau funcionamento da solução poderá gerar prejuízos diretos e indiretos à Administração, incluindo interrupção de sistemas, indisponibilidade de serviços digitais, perda, vazamento ou comprometimento de dados sensíveis e exposição a ataques cibernéticos.

3.27.3. Os serviços de suporte técnico especializado, manutenção e apoio deverão ser prestados pela contratada durante toda a vigência contratual, abrangendo atualização de softwares, bases de conhecimento, assinaturas de segurança, correção de falhas, tratamento de vulnerabilidades e demais atividades necessárias ao adequado funcionamento da solução.

3.27.4. Os serviços serão prestados preferencialmente de forma remota, especialmente quanto às atividades de monitoramento, suporte técnico, análise de eventos, atualização, manutenção lógica e apoio à resposta a incidentes. O atendimento presencial poderá ocorrer de forma excepcional, quando tecnicamente necessário, especialmente nos casos em que a resolução remota não seja

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

suficiente, houver necessidade de intervenção física em equipamentos ou for indispensável para garantir a continuidade, segurança ou estabilidade da operação.

3.27.5. Considerando a criticidade da solução e a necessidade de continuidade da proteção do ambiente institucional, os serviços de suporte técnico deverão estar disponíveis em regime compatível com os níveis de serviço estabelecidos neste Termo de Referência, observadas as prioridades, severidades e prazos definidos para atendimento e solução dos chamados.

3.27.6. O modelo de suporte técnico, inclusive com atendimento remoto e, quando necessário, presencial, mostra-se compatível com as práticas de mercado aplicáveis a soluções de segurança da informação de natureza crítica, especialmente aquelas que envolvem proteção de perímetro, proteção de endpoints, monitoramento, atualização contínua e resposta a incidentes.

3.27.7. A contratada deverá disponibilizar profissionais qualificados para a execução dos serviços, admitindo-se diferentes formas de vínculo jurídico, desde que assegurada sua responsabilidade integral pela execução contratual. A comprovação da qualificação técnica e da vinculação dos profissionais poderá ser realizada por meio de contrato de trabalho, contrato de prestação de serviços, termo de compromisso ou outro instrumento jurídico idôneo, não sendo exigido vínculo empregatício celetista exclusivo com a contratada.

3.27.8. Os profissionais responsáveis pela execução dos serviços deverão possuir qualificação técnica compatível com a complexidade da solução, podendo tal qualificação ser comprovada por meio de certificações técnicas, treinamentos especializados, experiência comprovada ou outros meios idôneos.

3.27.9. Quando mencionadas certificações específicas, estas serão aceitas como referência técnica, admitindo-se certificações equivalentes ou outros meios de comprovação que demonstrem o domínio técnico necessário à execução dos serviços, desde que compatíveis com os requisitos estabelecidos neste Termo de Referência.

3.27.10. A contratada deverá prover suporte técnico especializado para a solução ofertada, por meio de equipe devidamente capacitada e dimensionada sob sua responsabilidade, cabendo-lhe assegurar a disponibilidade dos profissionais necessários ao cumprimento dos níveis de serviço contratados.

3.27.11. A equipe técnica deverá possuir capacidade para executar, no mínimo, atividades relacionadas à implantação, configuração, suporte, manutenção, monitoramento, atualização, administração e operação assistida da solução, abrangendo proteção de perímetro, proteção de endpoints, monitoramento de rede, gerenciamento de serviços de TI e apoio à detecção e resposta a incidentes de segurança da informação.

3.27.12. A definição, organização, dimensionamento e gestão da equipe técnica caberão exclusivamente à contratada, vedada qualquer ingerência da Administração na sua estrutura interna de pessoal, sem prejuízo da fiscalização quanto ao cumprimento dos resultados, prazos, níveis de serviço e demais obrigações contratuais.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.27.13. A execução dos serviços deverá observar as boas práticas técnicas aplicáveis à solução, inclusive aquelas recomendadas pelo fabricante, desde que compatíveis com as disposições deste Termo de Referência, não sendo admitida a vinculação do contrato a normas, políticas, padrões ou diretrizes externas passíveis de alteração unilateral.

3.28. REQUISITOS DE EXPERIÊNCIA PROFISSIONAL DA EQUIPE DE SUPORTE TÉCNICO

3.28.1. A CONTRATADA deverá prover suporte técnico especializado para a solução ofertada por meio de equipe técnica devidamente capacitada, sob sua responsabilidade, assegurando o atendimento aos níveis de serviço estabelecidos neste Termo de Referência.

3.28.2. A composição mínima da equipe deverá contemplar os perfis a seguir, admitindo-se flexibilidade na organização interna da equipe, desde que garantido o atendimento integral das competências e responsabilidades descritas.

3.28.3. PERFIL 01 – Suporte Técnico e Manutenção para solução de proteção de perímetro

3.28.3.1. Quantidade mínima: 02 (dois) profissionais

3.28.3.2. Responsabilidades: Execução de atividades de suporte técnico, administração, manutenção e operação da solução de proteção de perímetro.

3.28.3.3. Qualificação/Experiência: Experiência comprovada na prestação de serviços de suporte técnico ou manutenção em soluções de segurança de perímetro.

3.28.3.4. Forma de comprovação: 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;

3.28.3.5. Observação: Quando apresentadas certificações do fabricante, estas serão aceitas como referência, admitindo-se certificações equivalentes ou comprovação por experiência técnica compatível.

3.28.3.6. Formação: Formação de nível superior completa em áreas correlatas de TIC.

3.28.3.7. Comprovação: Diploma emitido por instituição reconhecida pelo MEC.

3.28.4. PERFIL 02 – Suporte Técnico e Manutenção para solução de proteção de endpoints

3.28.4.1. Quantidade mínima: 02 (dois) profissionais

3.28.4.2. Responsabilidades: Execução de atividades de suporte técnico, administração, manutenção e operação da solução de proteção de endpoints (incluindo EDR ou equivalente).

3.28.4.3. Qualificação/Experiência: Experiência comprovada em suporte técnico ou manutenção de soluções de proteção de endpoints.

3.28.4.4. Forma de comprovação: 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.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.28.4.5. Observação: Certificações do fabricante poderão ser apresentadas como referência, admitindo-se equivalentes.

3.28.4.6. Formação: Formação de nível superior completa em áreas correlatas de TIC.

3.28.4.7. Comprovação: Diploma emitido por instituição reconhecida pelo MEC.

3.28.5. PERFIL 03 – Suporte Técnico e Monitoramento de Rede

3.28.5.1. Quantidade mínima: 01 (um) profissional

3.28.5.2. Responsabilidades: Monitoramento de ativos, gestão de eventos e apoio à administração da infraestrutura de rede e dos componentes da solução.

3.28.5.3. Qualificação/Experiência: Experiência em monitoramento de redes e ferramentas de gestão de eventos e Certificado de conclusão de capacitação fornecido por instituto credenciado, dentro do período de validade.

3.28.5.4. Forma de comprovação: Certificações técnicas, treinamentos, experiência comprovada ou outros meios idôneos.

3.28.5.5. Formação: Formação de nível superior completa em áreas correlatas de TIC.

3.28.5.6. Comprovação: Diploma emitido por instituição reconhecida pelo MEC.

3.28.6. PERFIL 04 – Analista de Gerenciamento de Serviços de TI

3.28.6.1. Quantidade mínima: 01 (um) profissional

3.28.6.2. Responsabilidades: Gestão dos serviços contratados, definição de processos, acompanhamento de desempenho e garantia do cumprimento dos níveis de serviço.

3.28.6.3. Qualificação/Experiência: Experiência em gestão de serviços de TI.

3.28.6.4. Forma de comprovação: Certificado de conclusão ITIL (v3 ou superior), fornecido por instituto credenciado, dentro do período de validade e Certificado de conclusão ISO/IEC 20000, fornecido por instituto credenciado, dentro do período de validade.

3.28.6.5. Formação: Formação de nível superior completa em áreas correlatas de TIC.

3.28.6.6. Comprovação: Diploma emitido por instituição reconhecida pelo MEC.

3.28.7. PERFIL 05 – Analistas SNOC

3.28.7.1. Quantidade mínima: 02 (dois) profissionais

3.28.7.2. Responsabilidades: Configuração, administração e operação das plataformas de monitoramento, bem como atividades de detecção e resposta a incidentes de segurança.

3.28.7.3. Qualificação/Experiência: Experiência mínima de 4 (quatro) anos em operação de NOC, SOC, SIEM ou ambientes equivalentes.

3.28.7.4. Forma de comprovação: Currículo profissional, atestados, declarações ou outros meios idôneos.

3.28.7.5. Formação: Formação de nível superior completa.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.28.7.6. Comprovação: Diploma emitido por instituição reconhecida pelo MEC.

3.28.7.7. Regime de atuação: Atuação presencial nas dependências da CONTRATANTE, em regime 8x5, observados os níveis de serviço estabelecidos.

3.28.8. A definição dos perfis profissionais exigidos fundamenta-se na complexidade técnica do objeto contratado, consistente na implantação, operação e sustentação de solução integrada de segurança da informação.

3.28.9. Cada perfil foi estabelecido com base nas atividades essenciais à execução do contrato, abrangendo, dentre outras:

3.28.9.1. administração e operação de soluções de proteção de perímetro e endpoints, responsáveis pela prevenção de acessos indevidos e proteção dos ativos de rede;

3.28.9.2. monitoramento contínuo e resposta a incidentes de segurança, indispensáveis para a detecção tempestiva de ameaças e mitigação de riscos cibernéticos;

3.28.9.3. suporte técnico especializado e manutenção da solução, necessários para garantir a continuidade operacional e a rápida correção de falhas;

3.28.9.4. gestão dos serviços de tecnologia da informação, incluindo o acompanhamento dos níveis de serviço, coordenação das atividades e interface com a Administração.

3.28.10. A ausência de profissionais com tais competências comprometeria diretamente a execução contratual, podendo resultar em falhas na proteção do ambiente, indisponibilidade de sistemas críticos e exposição a incidentes de segurança da informação.

3.28.11. Dessa forma, os perfis definidos mostram-se necessários, suficientes e pertinentes ao objeto da contratação, não configurando restrição indevida à competitividade, mas medida indispensável à garantia da adequada execução do contrato.

3.28.12. DISPOSIÇÕES GERAIS SOBRE A EQUIPE

3.28.12.1. A CONTRATADA será responsável pela disponibilização, substituição e gestão dos profissionais necessários à execução contratual, não havendo exigência de vínculo empregatício específico, sendo admitidas diferentes formas de vínculo jurídico, desde que assegurada a responsabilidade integral da contratada.

3.28.12.2. A Administração não exercerá ingerência sobre a estrutura interna de pessoal da contratada, limitando-se à verificação do cumprimento dos requisitos técnicos, níveis de serviço e resultados contratados.

3.28.12.3. Para fins de participação no certame, será exigida apenas declaração do licitante de que dispõe, ou disporá, de equipe técnica compatível com os perfis estabelecidos neste Termo de Referência.

3.28.12.4. A comprovação da qualificação técnica dos profissionais e de sua vinculação à contratada será exigida apenas no momento da assinatura do contrato ou previamente ao início da

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

execução contratual, por meio de documentação idônea, nos termos da legislação vigente e dos entendimentos dos órgãos de controle.

3.29. TIPOS DE SERVIÇOS DE SUPORTE TÉCNICO E MANUTENÇÃO

3.29.1. Manutenção Preventiva: Compreende visitas periódicas, conforme condições estabelecidas neste instrumento e na proposta da contratada, no ambiente da Contratante, programadas a fim de verificar a saúde do equipamento e mitigar riscos devido ao uso continuado dos serviços, incluindo:

3.29.1.1. Procedimentos técnicos destinados a prevenir a ocorrência de erros e defeitos de forma proativa;

3.29.1.2. Realização de inspeções nos equipamentos, componentes, dispositivos e softwares de configuração gerenciam a solução;

3.29.1.3. Verificação geral com vistas a manter sua plena funcionalidade e saúde dos equipamentos;

3.29.1.4. 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;

3.29.1.5. Sugerir, preventivamente, a aplicação de novas correções, patches, fixes, updates, service packs, novas releases, versions, builds e upgrades.

3.29.2. 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:

3.29.2.1. Reinstalação de hardwares e softwares, configuração, gerenciamento, com vistas a normalidade da operação dos serviços prestados;

3.29.2.2. 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 termo de referência;

3.29.2.3. Corrigir defeitos de fabricação ou projeto;

3.29.2.4. Acondicionar adequadamente os equipamentos cujo reparo não possa ser realizado nas dependências da SED/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;

3.29.2.5. Substituir os equipamentos que apresentarem defeito de fabricação, dentro dos prazos estabelecidos;

3.29.2.6. 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;

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.29.2.7. 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.

3.30. SUPORTE TÉCNICO ESPECIALIZADO E MANUTENÇÃO

3.30.1. A solução deverá prover de suporte técnico on-site disponível 24 horas por dia, 07 dias por semana.

3.30.2. Deverá possuir plataforma de suporte técnico para abertura de chamados disponível através de internet (WEB), telefone ou e-mail.

3.30.3. Deverá 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.

3.30.4. O funcionamento da solução deverá se valer dos meios necessários para manter a solução operacional.

3.30.5. Poderão ser prestados em ambiente on-site ou remoto, no regime 24X7, incluindo a atualização de softwares e baSED de dados de conhecimento as suas expensas, e, sempre que for necessário ao bom funcionamento da solução adquirida.

3.30.6. Deverão ser executados por técnicos qualificados, conforme previsto nos requisitos de qualificação da equipe técnica presentes neste documento.

3.31. ACORDOS DE NÍVEL DE SERVIÇOS

3.31.1. Para a prestação dos serviços de Suporte Técnico Especializado, Manutenção e Apoio:

3.31.2. A CONTRATADA deverá cumprir rigorosamente todos os procedimentos de manutenção definidos pela CONTRATANTE, como horário estabelecido para parada dos equipamentos, autorizações de acesso, entre outros.

3.31.3. Quando a intervenção implicar interrupção da solução, mesmo que parcial, a Contratante poderá determinar que a CONTRATADA a execute fora do horário de expediente do órgão, inclusive em finais de semana, sem qualquer ônus adicional à CONTRATANTE.

3.31.4. Fica vedada a desativação de hardware, software ou quaisquer recursos computacionais da CONTRATANTE, sem prévio conhecimento e autorização expressa da Administração;

3.31.5. Caso seja necessária a desativação de hardware, software ou quaisquer recursos computacionais da CONTRATANTE, a CONTRATADA deverá disponibilizar equipamento de redundância com capacidade igual ou superior ao que será desativado, até que o problema seja sanado.

3.31.6. Em caso de retirada do equipamento, a CONTRATANTE poderá, a seu critério, reter as unidades de memória física dos equipamentos, sem custo adicional.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

3.31.7. 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:

3.31.7.1. Caso ocorram 04 (quatro) ou mais defeitos que comprometam seu uso normal, dentro de qualquer intervalo de 30 (trinta) dias;

3.31.7.2. O(s) equipamento(s) (hardware) empregado em substituição ao equipamento defeituoso deverá possuir prazo equivalente a vigência do contrato;

3.31.7.3. No caso de problema recorrente no mesmo hardware, seja na restauração ou substituição das peças, em um período inferior a 02 (dois) meses, a CONTRATADA deverá substituir o equipamento.

3.31.8. 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:

3.31.8.1. Identificação de cada chamado;

3.31.8.2. Identificação do tipo de atendimento;

3.31.8.3. Data de atendimento (abertura e conclusão);

3.31.8.4. Descrição do atendimento;

3.31.8.5. Procedimentos adotados para a solução do problema;

3.31.9. 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;

3.31.10. Quando solicitado pela CONTRATANTE, a CONTRATADA deverá fornecer, em até 03 (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 na CONTRATANTE.

3.31.11. As atualizações de versões de todos os componentes da solução (major, minor, patches e fixes) deverão estar disponíveis para uso da CONTRATANTE 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.

3.31.12. A CONTRATADA 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):

3.31.12.1. 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

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

equipamento a sua disponibilidade para uso em perfeitas condições de funcionamento no local onde está instalado.

3.31.12.2. O tempo de atendimento inicia-se com a primeira intervenção pelo representante da CONTRATADA, local ou remotamente.

3.31.13. As declarações exigidas deverão ser apresentadas no prazo de até 10 (dez) dias úteis contados da assinatura do contrato.

3.31.14. 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	Glosa 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	Glosa 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	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. A glosa decorrente do descumprimento dos níveis de serviço não poderá

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

		de sazonalidade.			ultrapassar o limite máximo de **20% do valor mensal do contrato**, de modo a assegurar proporcionalidade e viabilidade econômica da execução contratual.
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 o ambiente de produção.	Em até 08 (quatro) horas	Em até 24 (vinte e quatro) horas	1% por dia que exceder o descumprimento do prazo de 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	Glosa por descumprimento % em relação a fatura de suporte
N06	Relatório de Atendimento	0,25% em relação ao valor valor mensal do

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

	Técnico não entregue	contrato por dia ocorrência ou documento.
N07	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.

3.31.15. 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;

3.31.16. A não resolução dos chamados dentro do prazo acima estipulado ensejará às Glosas previstas. Após o limite estabelecido para aplicação das glosas a CONTRATADA deverá substituir os equipamentos conforme prazos e condições descritas abaixo, sob pena de incorrer em inexecução total do contrato:

3.31.16.1. 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;

3.31.16.2. 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;

3.31.16.3. 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;

3.31.16.4. Se o problema identificado como IMPORTANTE não for resolvido de forma definitiva pela contratada dentro do prazo estabelecido, admitida prorrogação por igual período, desde que devidamente justificada, a partir do sétimo dia será aplicada glosa de 1% (um por cento) ao dia sobre o valor mensal do contrato, até que o problema seja integralmente sanado, limitada ao período máximo de 30 (trinta) dias.

3.31.16.5. A aplicação das glosas observará critérios objetivos, vinculados ao efetivo descumprimento dos níveis de serviço, sendo vedada a aplicação cumulativa que resulte em

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

penalização desproporcional, devendo ser observado o limite máximo de glosa mensal estabelecido neste Termo de Referência.

3.31.16.6. Após o prazo máximo, será caracterizada inexecução parcial do contrato.

3.31.16.7. Se, após 30 (trinta) dias contados da notificação da aplicação de glosa decorrente de inexecução parcial do contrato, a contratada não promover a substituição dos equipamentos ou a solução definitiva do problema, poderá ser caracterizada inexecução total do contrato, sem prejuízo da continuidade do suporte técnico dos demais componentes da solução.

3.31.16.8. Caso o atendimento envolva o fabricante da solução, deverá ser assegurada à Contratante a possibilidade de acompanhamento do chamado, diretamente ou por meio da contratada, garantindo transparência na sua tramitação.

3.31.17. Sempre que a CONTRATANTE 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.

3.31.18. Caso o chamado seja repassado pela CONTRATADA ao fabricante, a CONTRATANTE deverá ter capacidade visualizar diretamente no sítio do fabricante o andamento desse chamado.

3.31.19. 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.

3.31.20. Todos os firmwares publicados deverão estar disponíveis para consulta e download pela CONTRATANTE diretamente no sítio do fabricante.

3.31.21. A inobservância das condições aqui estabelecidas sujeitará a CONTRATADA às penalidades previstas neste termo de referência e sanções administrativas a serem definidas na minuta de contrato.

3.31.22. Quanto ao serviço de Suporte Técnico Especializado, reforçamos que 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:

3.31.22.1. 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.

3.31.22.2. Considerando que as atividades da CONTRATANTE são realizadas ininterruptamente, não se justifica que os serviços de suporte técnico sejam prestados somente em

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

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.

3.31.23. 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.

3.32. REQUISITOS TEMPORAIS

3.32.1. Cada entrega deverá ser efetuada mediante solicitação por escrito, formalizada pela contratante, dela devendo constar: a data, o valor unitário da entrega, a quantidade pretendida, o local para a entrega, o prazo, o carimbo e a assinatura do responsável, sendo efetuada diretamente pelo órgão/entidade requisitante, devidamente autorizado pela autoridade superior, e ainda acompanhada pela nota de empenho ou instrumento equivalente.

3.32.2. O prazo para início da execução dos serviços deverá ser de até 30 dias (trinta) dias contados do recebimento da nota de empenho, assinatura do contrato ou instrumento equivalente.

3.32.3. Caso não seja possível a entrega/execução na data assinalada, a contratada deverá comunicar as suas razões, com a devida comprovação, com pelo menos 05 (cinco) dias de antecedência, para que qualquer pleito de prorrogação de prazo seja analisado, ressalvadas situações de caso fortuito e força maior.

3.32.4. A contratada obriga-se a entregar os serviços em conformidade com as especificações descritas na Proposta de Preços e neste instrumento, sendo de sua inteira responsabilidade a substituição, caso não esteja em conformidade com as referidas especificações.

3.32.5. Todas as despesas relativas aos objetos contratados, bem como todos os impostos, taxas e demais despesas decorrentes do contrato correrão por conta exclusiva da contratada.

4. MODELO DE EXECUÇÃO DO OBJETO

4.1. CONDIÇÕES DE EXECUÇÃO

4.1.1. A prestação dos serviços não gera vínculo empregatício entre os empregados da contratada e a contratante, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta.

4.1.2. A execução do objeto seguirá a seguinte dinâmica:

4.1.2.1. Início da execução do objeto: 30 (trinta) dias contados do recebimento da nota de empenho ou instrumento equivalente.

4.1.2.2. Os serviços objeto da contratação serão prestados, preferencialmente, de forma remota, especialmente no que se refere às atividades de monitoramento, suporte técnico, análise de incidentes, atualização e manutenção da solução.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

4.1.2.3. A prestação de serviços na modalidade presencial (on-site) ocorrerá de forma excepcional, mediante solicitação da Administração, quando caracterizada a impossibilidade técnica de resolução remota ou quando necessária para garantir a continuidade ou a segurança da operação.

4.1.2.4. O serviço a ser ofertado pelas licitantes deve observar as características e especificações constante no presente documento.

4.2. CONDIÇÕES DE RECEBIMENTO DO SERVIÇO

4.2.1. Os serviços serão recebidos provisoriamente, de forma detalhada, no prazo de 05 (cinco) dias úteis, pelo(a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência e na proposta.

4.2.1.1. Para os fins do disposto no subitem 4.2.1, o termo detalhado corresponde a documento minucioso, que descreve total e detalhadamente o objeto recebido, devendo ser acompanhado do atesto no verso do documento fiscal ou equivalente, conforme art. 19 do Decreto nº 15.938, de 26 de maio de 2022

4.2.2. Os serviços poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos no prazo de 10 (dez) dias corridos, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

4.2.2.1. Na hipótese de irregularidade não sanada pelo contratado, incluindo o caso de serviço não prestado, o fiscal do contrato reduzirá a termo os fatos ocorridos e encaminhará ao(s) gestor(es) do contrato para procedimentos inerentes à apuração dos fatos e à aplicação das penalidades cabíveis, sendo o valor respectivo descontado da importância mensal devida à contratada.

4.2.3. Os serviços serão recebidos definitivamente, por servidor ou comissão designada pela autoridade competente, no prazo de 10 (dez) dias úteis, contados do recebimento provisório, mediante preenchimento de termo detalhado que comprove o atendimento das exigências contratuais.

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

4.2.4. 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 quanto à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

4.2.5. 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, bem como não exclui a responsabilidade pela garantia do(s) serviços(s) executado(s) por vícios ou disparidades em relação às especificações estabelecidas, verificadas posteriormente.

4.3. DA GARANTIA DO SERVIÇO

4.3.1. Considerando que o objeto da contratação compreende solução integrada de tecnologia da informação e comunicação, envolvendo fornecimento de bens e prestação de serviços continuados, a garantia deverá ser observada conforme a natureza de cada componente.

4.3.2. Para os componentes eventualmente caracterizados como bens, aplica-se a garantia legal, nos termos da Lei nº 8.078/1990, sem prejuízo de eventual garantia complementar ofertada pelo licitante ou fabricante.

4.3.3. Para os serviços continuados e para a solução como um todo, a garantia será caracterizada pela obrigação da contratada de assegurar o pleno funcionamento da solução durante toda a vigência contratual, devendo realizar, às suas expensas, todas as atividades necessárias à sua manutenção, incluindo:

4.3.3.1. suporte técnico especializado;

4.3.3.2. correção de falhas e vulnerabilidades;

4.3.3.3. atualização de softwares, assinaturas e bases de dados;

4.3.3.4. substituição de componentes defeituosos, quando aplicável;

4.3.3.5. monitoramento e resposta a incidentes.

4.3.4. A qualidade dos serviços será aferida por meio dos níveis de serviço (SLA) estabelecidos neste Termo de Referência.

4.3.5. Dessa forma, a garantia da solução não se limita a prazo fixo, estando vinculada à prestação contínua dos serviços e ao cumprimento das obrigações contratuais durante toda a vigência do contrato.

4.4. TRANSIÇÃO CONTRATUAL

4.4.1. Ao término da vigência contratual, a contratada deverá assegurar a transição adequada dos serviços, de modo a garantir a continuidade da operação e a integridade das informações.

4.4.2. Para tanto, deverá:

4.4.2.1. disponibilizar à Administração, ou à futura contratada, as informações técnicas necessárias à continuidade dos serviços;

4.4.2.2. realizar, quando solicitado, reuniões de transferência de conhecimento;

4.4.2.3. manter a operação assistida pelo período necessário à transição, conforme definido pela Administração;

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

4.4.2.4. assegurar que não haja interrupção dos serviços durante o processo de substituição contratual.

5.1. OBRIGAÇÕES DO CONTRATANTE:

5.1.1. São obrigações do Contratante:

5.1.2. Exigir o cumprimento de todas as obrigações assumidas pelo Contratado, de acordo com o instrumento convocatório e seus anexos;

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

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

5.1.5. Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pelo Contratado, inclusive quanto à continuidade da prestação dos serviços, que não deve ser interrompida, ressalvados os casos de força maior justificados e aceitos pelo Contratante.

5.1.6. Comunicar a empresa para emissão de Nota Fiscal quanto 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;

5.1.7. Efetuar o pagamento ao Contratado do valor correspondente ao fornecimento do objeto, no prazo, forma e condições estabelecidos no Termo de Referência;

5.1.8. Aplicar ao Contratado as sanções previstas na lei e no instrumento convocatório;

5.1.9. Cientificar o órgão de representação judicial para adoção das medidas cabíveis quando do descumprimento de obrigações pelo Contratado;

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

5.1.11. Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pelo contratado no prazo máximo de 10 (dez) dias úteis;

5.1.12. Notificar os emitentes das garantias, se houver, quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais (§4º, do art. 137, da Lei nº 14.133, de 2021).

5.1.13. 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;

5.2. Com relação à obrigação delineada no subitem 5.1.10 deste termo de referência, a Administração terá o prazo de 30 (trinta) dias, a contar da data do protocolo do requerimento,

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

para decidir todas as solicitações e reclamações relacionadas à execução dos contratos regidos pela Lei nº 14.133, de 2021, admitida a prorrogação motivada, por igual período.

5.3. OBRIGAÇÕES DO CONTRATADO

5.3.1. O Contratado deve cumprir todas as obrigações constantes do instrumento convocatório e em 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:

5.3.2. Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com o Código de Defesa do Consumidor (Lei nº 8.078, de 1990);

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

5.3.4. Responsabilizar-se 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;

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

5.3.6. Indicar preposto para representá-lo durante a execução do contrato, e manter comunicação com representante da Administração para a gestão do contrato;

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

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

5.3.9. 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. 14.133, de 2021);

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

5.3.11. Alocar os empregados necessários ao perfeito cumprimento das exigências deste Termo de Referência, com habilitação e conhecimento adequados, fornecendo os materiais,

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

equipamentos, ferramentas e utensílios demandados, cuja quantidade, qualidade e tecnologia deverão atender às recomendações de boa técnica e a legislação de regência;

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

5.3.13. 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.

5.3.14. 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;

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

5.3.16. 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 n. 14.133, de 2021;

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

5.3.18. 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, parágrafo único, da Lei n. 14.133, de 2021.

5.4.Com relação à obrigação delineada no subitem 5.3.9 deste Termo de Referência, a comprovação deverá se dar no prazo fixado pelo fiscal do contrato, hipótese em que deverá indicar os empregados que preencheram as referidas vagas (art. 116, parágrafo único, da Lei n. 14.133, de 2021).

6. MODELO DE GESTÃO DE CONTRATO

6.1. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) gestor e fiscal(is) do contrato, ou pelos respectivos substitutos, observado o disposto no art. 117 da Lei Federal nº 14.133, de 2021 e o respectivo regulamento pelo Decreto Estadual nº 15.938, de 2022.

6.2. Compete ao gestor do contrato o exercício das atribuições descritas no art. 15 do Decreto Estadual nº 15.938, de 2022.

6.3. Compete ao fiscal do contrato o exercício das atribuições descritas no art. 16 do Decreto Estadual nº 15.938, de 2022.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

6.4. Os responsáveis pela gestão e fiscalização do contrato serão designados nos termos do art. 6º, 7º e 8º, todos do Decreto Estadual n. 15.938, de 2022.

6.5. Além do disposto acima, a fiscalização contratual obedecerá às seguintes rotinas:

I – 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.

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

III – O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

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

7. CRITÉRIOS DE MEDIÇÃO, PAGAMENTO E REAJUSTE

7.1. PAGAMENTO:

7.1.1. O pagamento, decorrente do fornecimento do objeto do Contrato, será efetuado mediante crédito em conta corrente, no prazo de **até 30 (trinta) dias**, contados da liquidação.

7.1.1. O documento de cobrança da Contratada será mediante nota fiscal/fatura, cujo crédito será realizado na conta corrente indicada pela Contratada.

7.1.1.1. O pagamento será realizado de forma distinta para cada item do objeto:

7.1.1.2. O item de implantação será pago em parcela única, condicionada à sua conclusão e aceite formal pela Administração;

7.1.1.3. Os serviços continuados serão remunerados mensalmente, de forma proporcional à efetiva prestação dos serviços e condicionados ao cumprimento dos níveis de serviço estabelecidos;

7.1.1.4. É vedado o pagamento antecipado, devendo a remuneração observar a efetiva execução contratual.

7.1.2. Caso se constate erro ou irregularidade na nota fiscal/fatura, a Contratante, a seu critério, poderá devolvê-la para as devidas correções, ou aceitá-la, com a glosa da parte que considerar indevida, nesta hipótese, o prazo para pagamento iniciar-se-á após a regularização

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

da situação ou reapresentação do documento fiscal, não acarretando qualquer ônus para a Contratante.

7.1.2.1. Na hipótese de devolução, a nota fiscal/fatura será considerada como não apresentada, para fins de atendimento das condições contratuais.

7.1.3. A Contratante não pagará, sem que tenha autorização prévia e formal, qualquer compromisso que lhe venha a ser cobrado diretamente por terceiros, sejam ou não instituições financeiras.

7.1.4. Os eventuais encargos financeiros, processuais e outros, decorrentes da inobservância, pela Contratada, de prazo de pagamento, serão de sua exclusiva responsabilidade.

7.1.5. A Contratante efetuará retenção, na fonte, dos tributos e contribuições sobre todos os pagamentos devidos à Contratada, na forma da legislação aplicável.

7.1.6. A Contratada, durante toda a execução do contrato, deverá manter todas as condições de habilitação e qualificação exigidas na licitação.

7.1.6.1. Constatada a situação de irregularidade em quaisquer das certidões, a Contratada será notificada, por escrito, sem prejuízo do pagamento pelo objeto já executado, para, no prazo de 05 (cinco) dias úteis, regularizar tal situação ou, no mesmo prazo, apresentar defesa, em processo administrativo instaurado para esse fim específico.

7.1.6.2. O prazo para regularização ou encaminhamento de defesa de que trata o subitem 7.1.7.1 poderá ser prorrogado uma vez e por igual período, a critério da Contratante.

7.1.6.3. Não havendo regularização ou sendo a defesa considerada improcedente, a Contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal e trabalhista quanto à inadimplência do prestador, bem como quanto à existência de pagamento a ser efetuado pela Administração, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

7.1.6.4. Persistindo a irregularidade, a contratante, em decisão fundamentada, deverá aplicar a penalidade cabível nos autos do processo administrativo correspondente.

7.2. REAJUSTE

7.2.1. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do orçamento estimado.

7.2.2. Após o interregno de um ano, os preços iniciais serão reajustados, mediante aplicação, pelo contratante, do índice do ICTI (Indice de Custo da Tecnologia da Informação)

7.2.2.1. A adoção do ICTI – Índice de Custos de Tecnologia da Informação como índice de reajustamento contratual justifica-se pela natureza do objeto contratado, que compreende

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

a prestação de serviços relacionados à tecnologia da informação, conforme determinou o Tribunal de Contas do Estado de Mato Grosso do Sul (TCE/MS) considerando que este representa de forma mais precisa as variações econômicas do setor(Acórdão AC01 - 121/2024), disponível em: https://jurisprudencia-api.tce.ms.gov.br/api/Alfresco/NodesContent/ced3788a-1b7e-47f6-9691-5cdbcc8c0b4e/AC01%20-%20121-2024.

7.2.2.2. O ICTI foi desenvolvido especificamente para mensurar a variação dos custos inerentes ao setor de tecnologia da informação, refletindo de forma mais adequada as oscilações dos insumos, mão de obra especializada, softwares, equipamentos, licenças e demais componentes que influenciam a formação dos preços desses serviços. Além disso, apresenta maior correlação com os custos efetivamente suportados pelas empresas que atuam no segmento de tecnologia da informação, proporcionando maior equilíbrio econômico-financeiro ao contrato.

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

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

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

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

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

7.2.8. O reajuste será realizado por apostilamento.

7.2.9. Caberá à contratada solicitar expressamente o reajuste a partir da data que lhe for devida até a data de eventual assinatura do termo aditivo de prorrogação contratual, sob pena de preclusão.

8. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

8.1. FORMA DE SELEÇÃO E CRITÉRIO DE JULGAMENTO

8.1.1. O fornecedor será selecionado por meio da realização de procedimento de licitação, na modalidade pregão, sob a forma eletrônica, nos termos da Lei Federal nº 14.133/2021.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

8.1.2. A licitação será realizada em lote único, formados por dois itens, conforme tabela constante no Termo de Referência, devendo o licitante oferecer proposta para todos os itens que o compõem.

8.1.3. O critério de julgamento adotado será o menor preço global do lote, observadas as exigências contidas no Edital e seus Anexos quanto às especificações do objeto.

8.1.4. O modo de disputa adotado será o modo aberto.

8.1.5. Nos termos do art. 56 da Lei Federal nº 14.133/2021, será adotado o modo de disputa aberto, em que os licitantes apresentarão lances públicos e sucessivos, com vistas à obtenção da proposta mais vantajosa para a Administração.

8.1.6. A adoção do modo de disputa aberto, na forma eletrônica, justifica-se por possibilitar maior competitividade entre os licitantes, ampliar a transparência do certame e favorecer a obtenção da proposta mais vantajosa.

8.1.7. Adicionalmente, a escolha do modo de disputa aberto mostra-se adequada à natureza do objeto, tendo em vista que:

8.1.7.1. trata-se de solução com características amplamente disponíveis no mercado, ofertada por diversos fornecedores, o que permite a efetiva competição por preço; os requisitos técnicos encontram-se previamente definidos no Termo de Referência, não havendo necessidade de avaliação subjetiva que justifique a adoção de outros modos de disputa;

a modelagem da contratação, estruturada em lote único com julgamento pelo menor preço global, admite a comparação objetiva entre as propostas;

o modo aberto favorece a redução de preços por meio da dinâmica de lances sucessivos, sem comprometer a qualidade da solução, uma vez que o atendimento aos requisitos técnicos é condição obrigatória para a contratação.

8.1.7.2. Dessa forma, conclui-se que o modo de disputa adotado é o mais adequado para assegurar a competitividade, a isonomia entre os licitantes e a obtenção da proposta mais vantajosa para a Administração.

8.2. HABILITAÇÃO

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

8.2.2. Para fins de **HABILITAÇÃO JURÍDICA**, deverá o licitante comprovar os seguintes requisitos:

I - **Empresário individual**: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

II. **Microempreendedor Individual - MEI:** Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

sítio https://www.gov.br/empresas-e- negocios/pt-br/empreendedor;

III - **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;

IV. **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.

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

VI. **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

VII. **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 de 1971.

VIII. **Agricultor familiar**: Declaração de Aptidão ao Pronaf – DAP ou DAP-P válida, ou, ainda, outros documentos definidos pela Secretaria Especial de Agricultura Familiar e do Desenvolvimento Agrário, nos termos do art. 2º, §3º, do Decreto nº 11.802/2023.

IX. **Produtor Rural**: matrícula no Cadastro Específico do INSS – CEI, que comprove a qualificação como produtor rural pessoa física, nos termos da Instrução Normativa RFB n. 2.110/2022 (arts. 15 a 17 e 146).

8.2.2.1. No caso de ME e EPP que queira usufruir dos benefícios da Lei Complementar federal n. 123/2006 e da Lei Complementar estadual n. 303/2022: certidão simplificada original da Junta Comercial da sede da licitante ou documento equivalente, além de declaração escrita, sob as penas da lei, de que cumpre os requisitos legais de qualificação da condição de microempresa ou de empresa de pequeno porte estando apta a usufruir dos benefícios previstos nos art. 42 a art. 49 da Lei Complementar nº 123/2006;

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

8.2.2.1.1. Havendo dúvidas sobre o enquadramento de licitante na condição de microempresa ou de empresa de pequeno porte, considerando os parâmetros estabelecidos no art. 3º da Lei Complementar n. 123/2006, o pregoeiro poderá solicitar da licitante a apresentação dos documentos contábeis aptos a demonstrar a correção e a veracidade de declaração de seu enquadramento;

8.2.3. Para fins de **HABILITAÇÃO FISCAL, SOCIAL E TRABALHISTA**, deverá o licitante comprovar os seguintes requisitos:

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

II. Prova de inscrição no cadastro de contribuintes estadual ou municipal, se houver, relativo à sede da licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

III. Prova de regularidade fiscal, nos seguintes termos:

a) certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), que comprove a regularidade fiscal do licitante referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados;

b) independentemente da sede ou domicílio do licitante, certidão emitida pela Secretaria da Fazenda do Estado de Mato Grosso do Sul (SEFAZ) ou pela Procuradoria-Geral do Estado de Mato Grosso do Sul (PGE) que comprove a regularidade do licitante referente a todos os créditos tributários estaduais e à Dívida Ativa do Estado por elas administrados;

c) certidão emitida pela Fazenda Estadual da sede ou domicílio do licitante que comprove a regularidade de débitos tributários referentes ao Imposto sobre Operações relativas à Circulação de Mercadorias e sobre Prestações de Serviços de Transporte Interestadual, Intermunicipal e de Comunicação - ICMS;

d) certidão emitida pela Fazenda Municipal da sede ou domicílio do licitante que comprove a regularidade de débitos tributários referentes ao Imposto sobre Serviços de Qualquer Natureza – ISSQN;

IV. Prova de regularidade relativa à Seguridade Social e ao Fundo de Garantia do Tempo de Serviço (FGTS), demosntrando situação regular no cumprimento dos encargos sociais instituidos por lei;

V. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de Certidão Negativa de Débitos Trabalhistas (CNDT).

8.2.3.1. As microempresas (ME), empresas de pequeno porte (EPP) ou equiparada deverão apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal e trabalhista, mesmo que esta apresente alguma restrição.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

8.2.3.1.1. Constatada a existência de alguma restrição no que tange à regularidade fiscal e trabalhista, a ME/EPP/Equiparada será convocada para, no prazo de 5 (cinco) dias úteis, comprovar a regularização. O prazo poderá ser prorrogado por igual período, a critério da Administração Pública, quando requerida pela licitante, mediante apresentação de justificativa.

8.2.3.1.2. A não regularização fiscal e trabalhista no prazo previsto no subitem 8.2.3.1.1 implicará na decadência do direito à contratação, sem prejuízo das sanções previstas no art. 156 da Lei Federal n. º 14.133, de 2021, sendo facultado ao órgão ou entidade responsável pelo processo licitatório convocar os licitantes remanescentes, na ordem de classificação, ou revogar a licitação.

8.2.3.2. 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.

8.2.4. O fornecedor deverá encaminhar para fins de **QUALIFICAÇÃO ECONÔMICO-FINANCEIRA** os seguintes documentos:

8.2.4.1. Para pessoa jurídica, certidão negativa de feitos sobre falência expedida pelo distribuidor da sede do licitante.

8.2.4.1.1. No caso de empresa em recuperação judicial ou extrajudicial, o licitante deverá apresentar a comprovação de que o respectivo plano de recuperação foi acolhido judicialmente, na forma do art. 58, da Lei n. 11.101, de 09 de fevereiro de 2005, sob pena de inabilitação, devendo, ainda, comprovar todos os demais requisitos de habilitação.

8.2.4.2. Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrado há mais de 3 (três) meses da data de apresentação da proposta.

8.2.4.2.1. O balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos. (Lei n. 14.133, de 2021, art. 69, §6º).

8.2.4.2.2. 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. (Lei n. 14.133, de 2021, art. 65, §1º).

8.2.4.3. A comprovação da situação financeira da empresa será constatada mediante obtenção de índices de Solvência Geral (SG), superiores a 1 (um), resultantes da aplicação das fórmulas:

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

$$SG = \frac{\text{Ativo Total}}{\text{Passivo Circulante + Passivo Não Circulante}}$$

8.2.4.3.1. As empresas que apresentarem resultado inferior ou igual a 1(um) em qualquer dos índices de Solvência Geral (SG), deverão comprovar, considerados os riscos para a Administração, o capital mínimo ou o patrimônio líquido mínimo de 10% (dez por cento) do valor estimado da contratação ou do item pertinente, devendo a comprovação ser feita relativamente à data da apresentação da proposta de preços.

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

8.2.4.3.3. Da justificativa do índice adotado

8.2.4.3.4. O presente Termo de Referência exige, para comprovação de qualificação econômico-financeira, a apresentação do Balanço Patrimonial. O índice de Solvência Geral (SG), que devem apresentar resultado maior ou igual a 1,0.

8.2.4.3.5. Este índice mostra a base da situação financeira da empresa. A partir do confronto dos ativos circulantes com as dívidas, objetiva-se medir a solidez dessa base financeira. Uma empresa com bom índice de Solvência Geral tem capacidade de pagar suas dívidas e manter as condições de fornecimento, cumprindo seus contratos.

8.2.4.3.6. O Índice de Solvência Geral (SG) é calculado a partir da divisão dos ativos totais pela soma dos passivos circulante (PC) e passivos não circulantes. Sua função é verificar se a empresa terá condições de adimplir todos os seus compromissos financeiros sem comprometer a boa qualidade da execução contratual.

8.2.4.3.7. Assim, a administração escolheu o valor resultante maior ou igual a 1,0, por entender ser o mínimo a exigir de uma empresa para se manter um contrato, dentro de um nível de segurança e equilíbrio.

8.2.4.3.8. Ademais, com o objetivo de não restringir o universo de concorrentes, resolveu não exigir valor acima da unidade.

8.2.4.3.9. Este quociente demonstra a possibilidade de a empresa solver seus compromissos à curto prazo. O quociente de 1 indica que a empresa possui R$ 1,0 de recursos para fazer face a cada R$ 1,0 de obrigações, representando uma boa situação de solvência.

8.2.4.3.10. Portanto, a adoção do índice não viola o caráter competitivo do certame, uma vez que não se vinculam à rentabilidade ou lucratividade dos licitantes, prestando-se tão somente à aferição da equilibrada situação financeira, constituindo-se em segurança para a Secretaria de Estado de Educação na futura execução do contrato, sendo compatíveis com a complexidade exigida no objeto.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

8.2.5. Os critérios de **QUALIFICAÇÃO TÉCNICA** a serem atendidos pelo licitante serão os seguintes:

8.2.5.1. 1 (um) ou mais atestados de capacidade técnica fornecido(s) por pessoa jurídica de direito público ou privado, que comprove(m) a aptidão do licitante para desempenho de atividade pertinente e compatível em características, quantidades e prazos com o(s) lote(s) arrematado(s).

8.2.5.2.1. Para fins de comprovação, os atestados deverão demonstrar a execução de serviços com características compatíveis com o objeto, especialmente no que se refere à implantação, operação e sustentação de soluções de segurança da informação.

8.2.5.2.1.1. A comprovação de aptidão deverá evidenciar a execução de serviços correspondentes, no mínimo, a 50% (cinquenta por cento) das parcelas de maior relevância e valor significativo da contratação, consideradas aquelas relacionadas a:

a) proteção de perímetro, por meio de soluções de firewall de próxima geração ou equivalente, em ambiente de alta disponibilidade;

b) proteção de endpoints, incluindo mecanismos de detecção e resposta a incidentes, em quantidade mínima de 5.000 endpoints;

c) monitoramento, suporte técnico e resposta a incidentes de segurança;

d) integração entre componentes de solução de segurança da informação.

e) implantação e operação de solução de detecção e resposta gerenciada (MDR)

f) fornecimento de ambiente NOC ou SOC ou SNOC com ambiente Zabbix e Grafana

g) serviços de treinamento para solução de segurança da informação endpoint, com no mínimo os seguintes tópicos: visão geral da solução; console central, agentes e endpoint; criação de regras, políticas e relatórios; utilização das melhores práticas

8.2.5.2.2. Para o atendimento do quantitativo exigido no subitem anterior, será permitido o somatório de atestados de capacidade técnica.

8.2.5.3. Os atestados poderão ser apresentados em nome da matriz ou da filial do licitante.

8.2.5.4. O licitante deverá disponibilizar todas as informações necessárias à comprovação da legitimidade dos atestados, podendo a Administração solicitar, a qualquer tempo, documentos complementares, tais como cópia do contrato, dados da contratante e local de execução do objeto.

8.2.5.5. As exigências de qualificação técnico-operacional estabelecidas neste Termo de Referência foram definidas com base nas parcelas de maior relevância e valor significativo da contratação, nos termos da legislação vigente.

8.2.5.6. Consideram-se como parcelas de maior relevância aquelas relacionadas à implantação, operação e sustentação da solução de segurança da informação, especialmente proteção de perímetro, proteção de endpoints, monitoramento e resposta a incidentes, em razão de sua criticidade para a continuidade dos serviços institucionais.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

8.2.5.7. Tais exigências mostram-se necessárias para assegurar que a contratada possua experiência prévia compatível com a complexidade do objeto, não configurando restrição indevida à competitividade.

9. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

9.1. A contratação utilizará exclusivamente recursos estaduais, diante disso, o procedimento para a pesquisa de preços observará o disposto no Decreto Estadual nº 15.940, de 2022;

9.2. Depois de realizada a pesquisa de preços, fica a unidade administrativa competente AUTORIZADA a constar, como anexo do Edital, o valor previamente estimado da contratação.

9.3. A estimativa do valor da contratação está acompanhada com os preços unitários decompostos em planilha de custos e formação de preços.

10. PARTICIPAÇÃO DE MICROEMPRESA E EMPRESA DE PEQUENO PORTE

10.1. Nos termos da Lei Complementar nº 123/2006, em especial os artigos 47 a 49, a Administração Pública deve conceder tratamento diferenciado e favorecido às microempresas e empresas de pequeno porte – ME/EPP.

10.2. Contudo, a legislação admite exceções, desde que devidamente fundamentadas, quando a natureza do objeto não se mostrar compatível com a execução por empresas de menor porte, seja por razões técnicas, econômicas ou de segurança.

10.3. No presente caso, o objeto da contratação consiste na prestação de serviços especializados de segurança da informação em regime de outsourcing, que demanda:

10.3.1. Infraestrutura tecnológica de grande porte**,** com capacidade de monitoramento 24x7;

10.3.2. Equipe multidisciplinar altamente qualificada**,** com certificações técnicas específicas;

10.3.3. Gestão integrada de soluções críticas (firewall, IPS/IDS, SIEM, resposta a incidentes, endpoint protection);

10.3.4. Garantia de continuidade operacional e de segurança institucional, dada a essencialidade do serviço.

10.4. Diante do exposto, a Administração justifica a não adoção do tratamento diferenciado para ME/EPP, conforme faculta o art. 49 da LC nº 123/2006, considerando que o objeto em questão requer capacidade técnica, operacional e financeira incompatível com as características de micro e pequenas empresas, não sendo possível o fracionamento do certame ou a restrição de participação sem comprometer a adequada execução contratual.

11. ADEQUAÇÃO ORÇAMENTÁRIA

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

11.1 As despesas decorrentes da contratação da presente licitação correrão à conta da **funcional programática** 10.29101.12.122.0032.6017.0001, **natureza da despesa** n. 33904011, **fonte de recurso** n. 0150010011.

11.2 A Contratante reserva-se no direito de, a seu critério, utilizar ou não a totalidade da reserva orçamentária prevista.

11.3 As despesas efetuadas no próximo exercício correrão à conta do respectivo orçamento, dentro da mesma programação financeira.

12 INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

12.1. Depois de celebrado o contrato, a contratada será responsabilizada administrativamente pelas infrações descritas neste Termo de Referência.

12.1.1. A disciplina das infrações cometidas no procedimento licitatório deve observar o disposto no item 11 do Edital.

12.2. Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o contratado que:

12.2.1. Der causa à inexecução parcial do contrato;

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

12.2.3. Der causa à inexecução total do contrato;

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

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

12.2.6. Praticar ato fraudulento na execução do contrato;

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

12.2.8. Praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

12.2.9. Entregar objeto com vícios ou defeitos ocultos que o torne impróprio ao uso a que é destinado, ou diminuam-lhe o valor ou, ainda, fora das especificações contratadas;

12.3. Com fulcro na Lei nº 14.133, de 2021, a Administração poderá, garantida a prévia defesa, aplicar à contratada as sanções previstas nos incisos I, II, III e IV do art. 156.

12.3.1. As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar poderão ser aplicadas, cumulativamente ou não, à penalidade de multa compensatória.

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

Sanção de Multa

12.4. Será aplicada MULTA MORATÓRIA nas hipóteses de atraso injustificado na execução do contrato, na seguinte forma:

12.4.1. de 1% (um por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 30 (trinta) dias;

12.4.2. de 1% (um por cento) por dia de atraso injustificado sobre o valor total do contrato, até o máximo de 10% (dez por cento), pela inobservância do prazo fixado para apresentação, suplementação ou reposição da garantia.

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

12.5. A MULTA COMPENSATÓRIA será aplicada nas hipóteses de descumprimento de obrigações contratuais ou decorrentes de atos praticados no procedimento licitatório, por qualquer das infrações administrativas previstas no art. 155 da Lei Federal nº 14.133, de 2021, sendo estabelecida em razão do grau de importância da obrigação desatendida, objetivando-se a compensação das eventuais perdas nas quais a Administração tenha incorrido, nos percentuais estabelecidos no Decreto nº 16.189, de 17 de maio de 2023:

Infração (Subitens)	**Percentual da multa**
12.2.1.	20% (vinte por cento) sobre o valor da parcela do objeto não executada
12.2.2. 12.2.3. 12.2.4. 12.2.5. 12.2.6. 12.2.7. 12.2.8. 12.2.9.	de 20% (vinte por cento) a 30% (trinta por cento) sobre o valor contratado

12.5.1. Na hipótese do subitem 12.2.1, a sanção de multa compensatória poderá atingir o percentual de até 30% (trinta por cento) sobre o valor da parcela do objeto não executada nas hipóteses de que trata o inciso § 1º do art. 35 do Decreto 16.189, de 17 de maio de 2023.

12.6. As penalidades de multa moratória e multa compensatória não serão cumuladas.

12.7. A multa moratória poderá ser convertida em multa compensatória, observado o disposto no art. 162 da Lei Federal nº 14.133, de 2021.

12.8. Quaisquer multas aplicadas deverão ser recolhidas junto ao órgão competente no prazo de até 05 (cinco) dias úteis, contados de sua publicação no Diário Oficial do Estado de Mato Grosso

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

do Sul, podendo, ainda, ser descontadas de qualquer fatura ou crédito existente, a critério da licitante.

12.9. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor de pagamento eventualmente devido pela Administração ao contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente.

Sanção de impedimento de licitar e contratar

12.10. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos itens 12.2.2, 12.2.3 e 12.2.4, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar e contratar no âmbito da Administração Pública direta e indireta com o Estado de Mato Grosso do Sul, pelo prazo máximo de 3 (três) anos, obedecida a seguinte gradação definida no art. 4º do Decreto nº 16.189, de 17 de maio de 2023:

Infração (Subitens)	**Pena**
12.2.2.	impedimento pelo período de até dois anos.
12.2.3.	impedimento pelo período de até três anos
12.2.4.	impedimento pelo período de até um ano

Sanção de declaração de inidoneidade para licitar ou contratar

12.11. A sanção de declaração de inidoneidade para licitar ou contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos itens 12.2.5, 12.2.6, 12.2.7 e 12.2.8, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, obedecida a seguinte gradação definida no art. 5º do Decreto nº 16.189, de 17 de maio de 2023:

Infração (Subitens)	**Pena**
12.2.5.	declaração de inidoneidade de até cinco anos
12.2.6. 12.2.7. 12.2.8.	declaração de inidoneidade de até seis anos

12.12. Será aplicada a sanção de que trata o subitem 12.11 deste Edital nas infrações administrativas previstas nos itens 12.2.2, 12.2.3 e 12.2.4 que justifiquem a imposição de penalidade mais grave que a sanção de impedimento de licitar e contratar.

Da Aplicação e do Cômputo da Sanção

12.13. Os aspectos relacionados à aplicação da sanção, tais como a dosimetria, a cumulação, o cometimento de mais de uma infração em uma mesma licitação ou relação contratual e a soma de diversas sanções aplicadas a uma mesma empresa e derivadas de licitações e

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

contratos distintos, deverá observar o disposto nos arts. 34 a 38 do Decreto nº 16.189, de 17 de maio de 2023.

12.14. A aplicação das sanções previstas neste edital não exclui, em hipótese alguma, a obrigação de reparação integral dos danos causados.

Processo Administrativo Sancionador

12.15. O procedimento para aplicação das sanções seguirá o disposto no Capítulo III do Decreto nº 16.189, de 17 de maio de 2023.

13. VIABILIDADE E A ADEQUAÇÃO DA CONTRATAÇÃO

13.1. A Equipe de Planejamento da Contratação entende que o modelo de solução proposto se apresenta como a melhor alternativa e declara viável para a organização, por atender os principais quesitos de contratação e com base nos princípios da eficácia, eficiência, economicidade e isonomia.

José Flavio Rodrigues Siqueira
Matrícula:130137021 Coordenador de Tecnologia Educacional – COTED/SITEC

Patrícia Barbosa Gatts
Matrícula:123634030
Assessora da Superintendência de Informação e Tecnologia - SITEC

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.

SED Secretaria de Estado de Educação

GOVERNO DE Mato Grosso do Sul

ANEXO I “A”

PLANILHA DE COMPOSIÇÃO DE CUSTOS E FORMAÇÃO DE PREÇOS

Item de Custo	Valor (R$)	Percentual (%)
Equipamentos		
Licenciamentos		
Serviços de instalação e configuração		
Serviço de suporte técnico, operação e manutenção, incluindo SNOC		
Serviço de Implantação		
Despesas operacionais (diárias, deslocamento e outros)		
Despesas administrativas e indiretas		
Tributos		
Encargos		
Lucro		
Total		100%

Documento assinado digitalmente, valide em https://www.siga.ms.gov.br/flowbee-pub/#/validar/YLSE-9VR4-LWBF-7M88. Assinado por: PATRICIA BARBOSA GATTS em 28/10/2026, JOSE FLAVIO RODRIGUES SIQUEIRA em 28/10/2026.

HASH: 801e5f5ac083041bb604a1dc549090a2e953d5aa0fe817420a091fad1fe5524d. Juntado em 28/10/2026 14:14:03 por SILVIA CONCEIÇÃO.