GOVERNO DO ESTADO DO PARÁ
Secretaria de Estado de Segurança Pública

EDITAL DE DISPENSA ELETRÔNICA
Nº 08/2026 - SEGUP
PAE 2026/3271696

A SECRETARIA DE SEGURANÇA PÚBLICA E DEFESA SOCIAL DO PARÁ, torna público para conhecimento dos interessados que realizará **Dispensa Eletrônica,** a qual será regida pelo Decreto Estadual n.º 2.787/2022, à Lei n.º 14.133/2021, art. 75, inciso III e demais exigências previstas neste edital.

Objeto: **Contratação Emergencial de Empresa Especializada na Prestação Continuada de Serviços de Comunicação Corporativa de Dados**
Horário da abertura do recebimento das propostas: **09:00h (horário de Brasília) do dia 09/11/2026.**
Local do Site: **https://cotacao.banpara.b.br**
Endereço Eletrônico para consulta do Edital: **www.compraspara.pa.gov.br** e **https://cotacao.banpara.b.br**

1. OBJETO

A presente Dispensa Eletrônica tem como objeto a **Contratação Emergencial de Empresa Especializada na Prestação Continuada de Serviços de Comunicação Corporativa de Dados** para atender às necessidades da **SECRETARIA DE SEGURANÇA PÚBLICA E DEFESA SOCIAL DO PARÁ**, conforme descrição do Anexo I deste edital;

1.1. O julgamento e a adjudicação do objeto desta dispensa serão pelo **MENOR PREÇO** ofertado pelo participante;

1.2. Em havendo divergência entre a especificação do item do edital e do sistema de Dispensa Eletrônica, prevalecerá a especificação constante deste edital.

2. DISPOSIÇÕES PRELIMINARES

2.1. A Dispensa Eletrônica será realizada em sessão pública, por meio da Internet, mediante condições de segurança criptografia e autenticação em todas as suas fases a ser realizada na plataforma do site https://cotacao.banpara.b.br;

2.2. Os trabalhos serão conduzidos por um Coordenador, com a chancela do Homologador, servidores deste órgão, mediante a inserção e monitoramento de dados gerados ou transferidos para os sistemas de compras eletrônicas utilizados pela Administração Direta e Indireta, disponível no Portal Eletrônico para Compras Governamentais, no endereço https://cotacao.banpara.b.br.

3. CONDIÇÕES PARA PARTICIPAÇÃO

3.1. Poderá participar da Dispensa Eletrônica o fornecedor que esteja com registro atualizado no Sistema de Cadastramento de Fornecedores do Estado do Pará – SICAF/PA;
3.2. Deverá estar credenciado junto ao provedor do sistema de Dispensa Eletrônica;
3.3. Acompanhar as operações no sistema durante a sessão pública virtual, ficando responsável pelo ônus decorrente da perda de negócios, diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão;
3.4. Responsabilizar-se pelas transações que forem efetuadas em seu nome no sistema, assumindo como firmes e verdadeiras suas propostas e lances, sob pena de ter seu login e senha cancelados junto ao provedor do Sistema;
3.5. A participação do fornecedor na Dispensa Eletrônica presume sua capacidade técnica e jurídica para realização das transações dela decorrentes;

4. DOTAÇÃO ORÇAMENTÁRIA

4.1. As despesas decorrentes desta Dispensa Eletrônica correrão por conta da seguinte dotação orçamentária:

SERVIÇO:
PROGRAMAÇÃO: **06.126.1510.8993**
NATUREZA DA DESPESA: **339040**
FONTE DE RECURSOS: **01500000001**

5. DAS CONDIÇÕES DE PAGAMENTO

5.1. O pagamento dar-se-á após o recebimento e aceitação definitiva do objeto contratado, por parte do servidor designado para proceder ao recebimento e conferência de Materiais da Secretaria de Estado de Segurança Pública e Defesa Social, mediante a apresentação das certidões de regularidade com os tributos federais, estaduais e municipais pertinentes, do INSS e FGTS em vigência, do Recibo e Nota Fiscal devidamente atestada para liquidação e pagamento da despesa pela SEGUP, mediante ordem bancária creditada em conta corrente no prazo de 30 (trinta) dias contados da apresentação dos mesmos;
5.2. No caso de devolução da nota fiscal, fatura ou recibo para correção, o prazo de pagamento estipulado no item anterior passará a ser contado a partir da data de reapresentação dos referidos documentos;
5.3. O pagamento de credores será efetuado **preferencialmente por crédito em conta corrente aberta no Banco do Estado do Pará**;
5.4. O pagamento será realizado em até 30 (trinta) dias após a entrega dos produtos no

local especificado pelo edital e devidamente recebidas conforme Anexo I;
5.5. A Secretaria de Estado de Segurança Pública e Defesa Social poderá deduzir do montante a pagar, os valores correspondentes a multas ou indenizações devidas pela vencedora, nos termos deste edital e seus Anexos;
5.6. Nenhum pagamento será efetuado à participante vencedora enquanto pendente de liquidação, qualquer obrigação financeira, em virtude de penalidade ou inadimplência contratual, sem que isso gere direito a reajustamento de preços;
5.7. Nenhum pagamento isentará a participante vencedora de suas responsabilidades e obrigações nem implicará em aprovação definitiva dos materiais apresentados;
5.8. Ocorrendo fatos impeditivos da liquidação da despesa, provocados pela vencedora, o pagamento não será efetuado até que este providencie as medidas saneadoras necessárias, não se sujeitando a Secretaria de Estado de Segurança Pública e Defesa Social a quaisquer ônus decorrentes dessa suspensão do pagamento.

6. DA APRESENTAÇÃO DE PROPOSTA DE PREÇOS

6.1. O sistema de Dispensa Eletrônica permitirá o encaminhamento eletrônico de propostas de preços, com possibilidade de apresentação, pelo fornecedor, de lances sucessivos, em valor inferior ao último por ele ofertado e registrado pelo sistema, durante a realização da fase competitiva da sessão pública virtual da cotação;
6.2. Após a divulgação do edital no endereço eletrônico, o fornecedor deverá encaminhar exclusivamente por meio do sistema eletrônico, proposta de preços, formulada de acordo com as especificações do objeto contidas neste edital, até a data e hora marcada para a abertura da sessão;
6.3. Nos preços propostos deverão estar incluídos todos os tributos, encargos sociais, frete até o destino e quaisquer outros ônus que porventura possam recair sobre o fornecimento do objeto da Dispensa Eletrônica, os quais ficarão a cargo único e exclusivamente do fornecedor;
6.4. A apresentação da proposta implica obrigatoriedade do cumprimento das disposições nela contidas, em conformidade com o que dispõe o Termo de Referência, assumindo o proponente o compromisso de executar o serviço nos seus termos, em quantidades e qualidade adequadas à perfeita execução contratual;
6.5. A validade da proposta será de, no mínimo, 30 (trinta) dias, contados a partir da data da sua apresentação.

7. FASE DE LANCES

7.1. Durante a sessão pública virtual de lances, todos os fornecedores participantes serão informados, em tempo real, do valor do menor lance apresentado, vedada a identificação de seu proponente;
7.2. Os lances serão aceitos em ordem cronológica e deverão ser registrados, em reais, para a quantidade total de cada item, com validade de 30 (trinta) dias;

7.3. Não serão aceitos dois ou mais lances iguais, prevalecendo aquele que for recebido e registrado primeiro;
7.4. No caso de desconexão do Coordenador da Disputa, no decorrer da etapa de lances, se o sistema eletrônico permanecer acessível aos fornecedores participantes, os lances continuarão sendo recebidos, sem prejuízo dos atos realizados;
7.5. Quando a desconexão do Coordenador da Disputa persistir por tempo superior a dez minutos do encerramento da fase competitiva, a sessão será suspensa e reiniciada somente após comunicação aos participantes, no endereço eletrônico utilizado para divulgação;
7.6. A etapa de lances terá duração mínima de 03 (três) horas, sem prejuízo de sua prorrogação automática pelo sistema por mais 03 (três) minutos, quando houver lance nos últimos 03 (três) minutos dessa etapa, visando à continuidade da disputa, e assim sucessivamente até que não sejam mais registrados quaisquer lances;
7.7. Após o encerramento da etapa de lances da sessão pública, o Coordenador da Disputa poderá encaminhar, pelo sistema eletrônico, contraproposta ao participante que tenha apresentado lance mais vantajoso, para que seja obtida melhor proposta, observado o critério de julgamento, não se admitindo negociar condições diferentes daquelas previstas no instrumento convocatório.

8. DA HABILITAÇÃO:

8.1. Para fins de habilitação nesta Dispensa Eletrônica o fornecedor deverá encaminhar ao Coordenador os seguintes documentos com prazo de validade em vigor:
8.1.1. Documentação Relativa à Seguridade Fiscal;
8.1.2. Prova de regularidade para com a Fazenda Nacional;
8.1.3. Prova de regularidade relativa a Certidão do FGTS;
8.1.4. Certidão Negativa de Débito – CND, junto ao Instituto Nacional de Seguridade Social – INSS;
8.1.5. Prova de regularidade com as fazendas: Estadual e Municipal, por meio da apresentação de Certidão Negativa, comprovando sua regularidade com as Fazendas Estadual e Municipal se houver, relativo ao domicílio do licitante pertinente ao ramo de atividade e compatível com o objeto;
8.1.6. Comprovante de inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ);
8.2. Os documentos exigidos para habilitação, bem como a proposta vencedora ajustada ao lance dado, serão imediatamente encaminhados ao Coordenador, no prazo máximo de 1 (uma) hora contados a partir da convocação do Coordenador na etapa de aceitação na sessão pública, com possibilidade de prorrogação a critério do Coordenador, através do email: crmsegup@yahoo.com.br;
8.3. A habilitação dos fornecedores vencedores poderá ser verificada “on line” no Sistema de Cadastro Unificado de Fornecedores – SICAF, após análise e julgamento das propostas:

8.3.1. É dever do fornecedor atualizar previamente as comprovações constantes no SICAF para que estejam vigentes na data de abertura da sessão pública, ou encaminhar, quando solicitado, a respectiva documentação atualizada;

8.3.2. O descumprimento do subitem acima implicará a inabilitação do fornecedor, exceto se a consulta aos sítios eletrônicos oficiais emissores de certidão lograr êxito em encontrar a(s) certidão(ões) válida(s).

8.4. Da habilitação das microempresas e empresas de pequeno porte que se beneficiarem, nesta Dispensa Eletrônica, do regime diferenciado e favorecido concedido pela Lei Complementar nº 123/06 e Decreto Estadual nº 878/2008:

8.4.1. As microempresas e empresas de pequeno porte que se beneficiarem neste certame do regime diferenciado e favorecido concedido pela Lei Complementar nº 123/06, após a etapa de lances, deverão apresentar toda a documentação exigida para habilitação, inclusive para efeito de comprovação de regularidade fiscal, mesmo que esta apresente alguma restrição.

8.4.2. Havendo alguma restrição na comprovação somente da regularidade fiscal, será assegurado o prazo de 02 (dois) dias úteis, cujo termo inicial corresponderá ao momento em que a proponente for declarada a vencedora do certame na sessão da Dispensa Eletrônica, prorrogáveis por igual período, a critério da Administração Pública, para a regularização da documentação, não podendo ser exigido pela Administração a assinatura do contrato, ou aceitação ou retirada do instrumento equivalente, em prazo inferior ao estabelecido neste subitem.

9. DOS PROCEDIMENTOS DA DISPENSA ELETRÔNICA

9.1. Os editais e seus respectivos avisos, serão divulgados nos sites da Internet: web.banparanet.com.br/cotação e www.compraspara.pa.gov.br;

9.2. A partir do horário previsto no sistema, terá início à sessão pública da Dispensa Eletrônica, com a divulgação das propostas de preço recebidas, passando o Coordenador a avaliar a aceitabilidade das propostas;

9.3. Aberta às etapas competitivas, os representantes dos fornecedores deverão estar conectados ao sistema para participar das sessões de lances. A cada lance ofertado o participante será imediatamente informado de seu recebimento e respectivo horário de registro e valor;

9.4. Só serão aceitos lances cujos valores forem inferiores ao último lance que tenha sido anteriormente registrado no sistema;

9.5. O sistema informará a proposta de menor preço imediatamente após o encerramento da etapa de lances ou, quando for o caso, após negociação e decisão pelo Coordenador acerca da aceitação do lance de menor valor;

9.6. A Administração reserva-se o direito de, julgando necessário, proceder diligências junto aos órgãos emitentes de certidões, bem como solicitar esclarecimentos ou informações complementares relativas a quaisquer dos documentos apresentado.

10. CRITÉRIOS DE JULGAMENTO

10.1. Para julgamento e classificação das propostas será adotado o critério de **MENOR PREÇO**. A especificação da proposta deverá atender fielmente ao solicitado no edital, e os preços deverão ser expressos em reais, com no máximo de 02 (duas) casas decimais após a vírgula;

10.2. Após o encerramento da Dispensa Eletrônica, o sistema divulgará a classificação indicando os valores das propostas e dos lances;

10.3. O sistema disponibilizará campo próprio para troca de mensagens entre o coordenador da disputa e os fornecedores participantes, após o encerramento da fase de lances;

10.4. Se a proposta de menor valor não for aceitável ou se o participante não atender às exigências habilitatórias, o Coordenador da Disputa examinará a proposta subseqüente, e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao instrumento convocatório;

10.5. Será desclassificada a proposta vencedora que:

10.5.1. Contiver vícios insanáveis;

10.5.2. Não obedecer às especificações técnicas pormenorizadas neste edital ou em seus anexos;

10.5.3. Apresentar preços inexequíveis ou permanecerem acima do preço máximo definido para a contratação;

10.5.4. Não tiverem sua exequibilidade demonstrada, quando solicitado pela Administração;

10.5.5. Apresentar desconformidade com quaisquer outras exigências deste edital ou seus anexos, desde que insanável;

10.6. Erros no preenchimento da planilha não constituem motivo para a desclassificação da proposta. A planilha poderá ser ajustada pelo fornecedor, no prazo indicado pelo sistema, desde que não haja majoração do preço:

10.6.1. O ajuste de que trata este dispositivo se limita a sanar erros ou falhas que não alterem a substância das propostas;

10.6.2. Considera-se erro no preenchimento da planilha passível de correção a indicação de recolhimento de impostos e contribuições na forma do Simples Nacional, quando não cabível esse regime;

10.7. O fornecedor classificado com menor preço e que atenda às exigências do edital será considerado vencedor, ficando a critério deste insigne órgão a aquisição/contratação e a adjudicação do objeto;

10.8. Cabe a Secretaria de Estado de Segurança Pública e Defesa Social a adjudicação do objeto ao fornecedor vencedor verificando se o objeto licitado condiz com o seu objetivo social, e homologar a Dispensa de Licitação.

11. HABILITAÇÃO TÉCNICA

11.1. Será exigida a comprovação de registro ou inscrição da licitante no Conselho Regional de Engenharia e Agronomia - CREA, compatível com as atividades relacionadas ao objeto da contratação, considerando que os serviços envolvem infraestrutura de telecomunicações, conectividade de dados, instalação, configuração, operação e suporte técnico de equipamentos e serviços de rede. A exigência tem por finalidade assegurar que a empresa esteja regularmente habilitada para o exercício das atividades técnicas pertinentes.

12. QUALIFICAÇÕES TÉCNICAS

12.1. Declaração de ciência das informações necessárias para o cumprimento da futura obrigação contratual;

12.2. Apresentação de um ou mais Atestados de Capacidade Técnica, emitidos por pessoas jurídicas de direito público ou privado, que comprovem a execução satisfatória de serviços compatíveis em características e complexidade com o objeto da contratação, abrangendo comunicação de dados, acesso corporativo à Internet, gerenciamento de redes, SD-WAN, segurança perimetral UTM/NGFW, monitoramento, suporte técnico especializado e operação de ambientes corporativos de missão crítica, incluindo, quanto aplicável, serviços de proteção e mitigação de ataques DDoS.

13. SANÇÕES ADMINISTRATIVAS

13.1. Comete infração administrativa o fornecedor que cometer quaisquer das infrações previstas no art. 155 da Lei nº 14.133/2021, quais sejam:

13.1.1. Dar causa à inexecução parcial do contrato;

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

13.1.3. Dar causa à inexecução total do contrato;

13.1.4. Deixar de entregar a documentação exigida para o certame;

13.1.5. Não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

13.1.6. Não celebrar o contrato ou não entregar documentação exigida para a contratação, quando convocado dentro do prazo de validade da sua proposta;

13.1.7. Ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

13.1.8. Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a Dispensa Eletrônica ou a execução do contrato;

13.1.9. Fraudar a Dispensa Eletrônica ou praticar ato fraudulento na execução do contrato;

13.1.10. Comporta-se de modo inidôneo ou cometer fraude de qualquer natureza;

13.1.10.1. Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os fornecedores, em qualquer momento da dispensa, mesmo após o encerramento da fase de lances.

13.1.11. Praticar atos ilícitos com vistas a frustrar os objetivos deste certame;

13.1.12. Praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

13.2. O fornecedor que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

13.2.1. Advertência pela falta do subitem 11.1.1 deste Edital, quando não se justificar a imposição de penalidade mais grave;

13.2.2. Multa de 1% (um por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do fornecedor, por qualquer das infrações dos subitens de 11.1.1 a 11.1.12;

13.2.3. Impedimento de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 03 (três) anos, nos casos dos subitens 11.1.1 a 11.1.7 deste Edital, quando não se justificar a imposição de penalidade mais grave;

13.2.4. Declaração de inidoniedade para licitar ou contratar, o que impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 03 (três) anos e máximo de 06 (seis) anos, no caso dos subitens 11.1.8 a 11.1.12, bem como nos demais casos que justifiquem a imposição de penalidade mais grave.

13.3. Na aplicação das sanções serão considerados:

13.3.1. A natureza e a gravidade da infração cometida;

13.3.2. As peculiaridades do caso concreto;

13.3.3. As circunstâncias agravantes ou atenuantes;

13.3.4. Os danos que dela provierem para a Administração Pública.

13.4. Se a multa aplicada e as indenizações cabíveis forem superiores ao pagamento eventualmente devido pela Administração ao contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente;

13.5. A penalidade de multa pode ser aplicada cumulativamente com as demais sanções;

13.6. Nenhuma sanção será aplicada sem o devido processo administrativo que prevê defesa prévia do interessado e recurso nos prazos definidos em lei, sendo-lhe franqueada vista ao processo na SEGUP, localizada à Avenida Almirante Barroso nº 735, Belém/PA, no horário das 08:30h às 16:00h.

14. DISPOSIÇÕES FINAIS

14.1. O procedimento de Dispensa Eletrônica é condicionado ao princípio constitucional da isonomia, a seleção da proposta mais vantajosa para a administração e a promoção do desenvolvimento nacional, e será processada e julgada em estrita conformidade com

os princípios básicos da legalidade, da impessoalidade, da moralidade, da igualdade, da publicidade, da probidade administrativa, da vinculação ao instrumento convocatório, do julgamento objetivo e dos que lhes são correlatos. (Alterada pela MP nº 495, de 19 de julho de 2010);

14.2. A presente Dispensa Eletrônica não importa necessariamente em contratação, podendo a Secretaria de Estado de Segurança Pública e Defesa Social revogá-la, no todo ou em parte, por razões de interesse público, derivado de fato superveniente comprovado ou anulá-la por ilegalidade, de ofício ou por provocação mediante ato escrito e fundamentado disponibilizado no sistema para conhecimento dos participantes da Dispensa Eletrônica;

14.3. O Coordenador poderá, ainda, prorrogar, a qualquer tempo, os prazos para recebimento das propostas ou para sua abertura;

14.4. O proponente é responsável pela fidelidade e legitimidade das informações prestadas e dos documentos apresentados em qualquer fase da Dispensa Eletrônica. A falsidade de qualquer documento apresentado ou a inverdade das informações nele contidas implicará a imediata desclassificação do proponente que o tiver apresentado, ou, caso tenha sido o vencedor, a rescisão do contrato, sem prejuízo das demais sanções cabíveis;

14.5. As normas que disciplinam esta disputa eletrônica serão sempre interpretadas em favor da ampliação da disputa entre os proponentes, desde que não comprometam o interesse da Administração, a finalidade e a segurança da contratação;

14.6. Para fins de contagem, estabelecidos neste edital, excluir-se-á a data do início e incluir-se-á a do vencimento e considerar-se-ão os dias consecutivos, exceto quando for explicitamente disposto em contrário;

14.7. Os casos não previstos neste edital serão decididos pelo Coordenador da disputa;

14.8. A participação do proponente nesta Dispensa Eletrônica implica em aceitação de todos os termos deste edital;

14.9. A indicação do lance vencedor, a classificação dos lances apresentados e demais informações relativas à sessão pública da Dispensa Eletrônica constarão de ata divulgada no sistema eletrônico, sem prejuízo das demais formas de publicidade.

Belém, 03 de novembro de 2026.

LARISSA COELHO BITTENCOURT
Coordenadora de Recursos Logísticos

TERMO DE REFERÊNCIA PARA CONTRATAÇÃO EMERGENCIAL DE SERVIÇOS DE TIC

PAE nº 2026/3271696

O QUE SERÁ CONTRATADO?

Objeto	Contratação emergencial de empresa especializada na prestação continuada de serviços de comunicação corporativa de dados, acesso dedicado à Internet, solução SD-WAN, gerenciamento proativo de redes, fornecimento de equipamentos de comunicação (CPE), soluções de segurança UTM (Unified Threat Management) e Firewall de Nova Geração (NGFW), serviço de prevenção e mitigação de ataques distribuídos de negação de serviço (DDoS), gerenciamento centralizado, monitoramento contínuo, suporte técnico especializado, operação assistida e manutenção preventiva e corretiva, destinados à manutenção da infraestrutura tecnológica da Secretaria de Estado de Segurança Pública e Defesa Social do Estado do Pará – SEGUP, compreendendo os serviços de comunicação de 50 Mbps, 500 Mbps e 1 Gbps, conforme especificações, quantitativos, condições e níveis de serviço estabelecidos neste Termo de Referência e seus anexos.

Lote	Descrição	Código SIMAS	Qtd. Total Mensal	Nº de Meses	Valor Unitário	Valor Total Mensal	Valor Total Anual
1	Serviço de Comunicação 50 Mbps + UTM SD-WAN Tipo B + Tipo E + Gerência de Redes		19	6	R$ 1.935,10	R$ 36.766,90	R$ 220.601,40
2	Serviço de Comunicação 500 Mbps + UTM SD-WAN Tipo E + CPE + Gerência de Redes + Proteção DDoS		1	6	R$ 8.325,68	R$ 8.325,68	R$ 49.954,08
3	Serviço de Comunicação 1 Gbps + UTM SD-WAN Tipo F + CPE + Gerência de Redes + Proteção DDoS		1	6	R$ 19.025,11	R$ 19.025,11	R$ 114.150,66
			VALOR TOTAL ESTIMADO				**R$ 384.706,66**

JUSTIFICATIVA DA NÃO DIVISÃO DO OBJETO EM LOTES E/OU DO AGRUPAMENTO EM GRUPOS

A presente contratação emergencial será em lote único, considerando a necessidade de assegurar a continuidade imediata e integrada dos serviços de conectividade de dados atualmente necessários às unidades da SEGUP/PA.

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

Embora a solução contemple diferentes capacidades e modalidades de conectividade, os serviços possuem finalidade comum e integram uma mesma necessidade institucional: garantir a comunicação de dados e o acesso aos sistemas e serviços essenciais da Administração. A fragmentação do objeto poderia resultar na atuação de múltiplas contratadas sobre a mesma infraestrutura, aumentando a complexidade da gestão contratual, do suporte técnico e da responsabilização pela disponibilidade dos serviços.

Além disso, considerando o caráter emergencial da contratação e a necessidade de evitar descontinuidade dos serviços, a contratação de forma integrada mostra-se tecnicamente e operacionalmente mais adequada, permitindo maior uniformidade na gestão, acompanhamento e suporte dos serviços, bem como maior agilidade na implantação e na transição contratual.

Dessa forma, a não divisão do objeto encontra justificativa na necessidade de preservação da continuidade operacional, na integração dos serviços de conectividade, na simplificação da gestão e fiscalização contratual e na mitigação dos riscos decorrentes da eventual fragmentação da execução, sem prejuízo à competitividade do certame, uma vez que os serviços objeto da contratação são usualmente disponibilizados por empresas especializadas do setor de telecomunicações e tecnologia.

DESCRIÇÃO DA SOLUÇÃO

QUAL O MOTIVO DA CONTRATAÇÃO?	A contratação emergencial da solução integrada de comunicação de dados, conectividade corporativa e segurança de redes tem como objetivo assegurar a continuidade dos serviços essenciais de Tecnologia da Informação e Comunicação da Secretaria de Estado de Segurança Pública e Defesa Social do Pará – SEGUP/PA. A infraestrutura atualmente utilizada é indispensável ao funcionamento dos sistemas corporativos, aplicações institucionais, serviços de comunicação e demais recursos tecnológicos empregados pelas unidades administrativas e operacionais da Secretaria e pelos órgãos integrantes do Sistema Integrado de Segurança Pública e Defesa Social – SIEDS. A interrupção ou degradação desses serviços poderá comprometer a comunicação entre unidades, o acesso aos sistemas institucionais, a troca segura de informações, o funcionamento de aplicações críticas e a continuidade das atividades administrativas e operacionais vinculadas à segurança pública. A contratação, portanto, busca evitar a descontinuidade dos serviços atualmente prestados, preservando a disponibilidade, a integridade e a segurança da infraestrutura tecnológica da SEGUP durante o período necessário à conclusão da contratação definitiva. A solução contempla serviços de conectividade, gerenciamento inteligente de rede por meio de tecnologia SD-WAN, equipamentos de comunicação, mecanismos de segurança perimetral UTM/NGFW, proteção contra ataques DDoS, monitoramento contínuo, gerenciamento proativo, suporte técnico especializado e manutenção preventiva e corretiva. A adoção integrada desses recursos

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

	permite manter a operação da rede corporativa, reduzir riscos de indisponibilidade, proporcionar resposta mais eficiente a incidentes e assegurar níveis adequados de desempenho, disponibilidade e segurança da informação. Considerando o caráter essencial e continuado desses serviços, a contratação possui natureza estritamente emergencial e destina-se a garantir a continuidade operacional da SEGUP e dos serviços públicos de segurança, até que seja concluído o procedimento destinado à contratação definitiva da solução, nos termos e limites aplicáveis à contratação emergencial.

NATUREZA DO SERVIÇO
☒ Comum. ☐ Especial.

PROVA DE QUALIDADE, DESEMPENHO E CONFORMIDADE DA SOLUÇÃO		
HAVERÁ PROVA DE QUALIDADE?	☐ Sim. ☒ Não.	Justificativa: Não será exigida prova específica de qualidade nos moldes aplicáveis ao fornecimento de bens, considerando que o objeto consiste predominantemente na prestação continuada de serviços de comunicação de dados, conectividade corporativa, gerenciamento de redes e segurança cibernética. A conformidade e a qualidade da solução serão verificadas mediante o atendimento às especificações técnicas, requisitos de desempenho, níveis de serviço, critérios de disponibilidade e demais condições estabelecidas neste Termo de Referência.
SERÁ EXIGIDA AMOSTRA OU PROVA DE CONCEITO?	☐ Sim. ☒ Não.	Justificativa: Não será exigida apresentação de amostra ou realização de prova de conceito como condição prévia à contratação, considerando o caráter emergencial da contratação e a natureza continuada dos serviços, cuja conformidade poderá ser aferida por meio da documentação técnica apresentada, da comprovação da capacidade técnica da contratada e dos procedimentos de instalação, configuração, ativação, testes, homologação e acompanhamento dos níveis de serviço previstos neste Termo de Referência.
HAVERÁ GARANTIA DOS EQUIPAMENTOS	☒ Sim.	Os equipamentos e componentes disponibilizados para a execução dos serviços deverão possuir garantia do fabricante durante toda

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

E COMPONENTES DA SOLUÇÃO?	a vigência contratual, quando aplicável, cabendo à CONTRATADA assegurar sua plena operacionalidade, manutenção, atualização e substituição em caso de falha ou defeito, sem ônus adicional para a CONTRATANTE. ☐ Não.
HAVERÁ ASSISTÊNCIA TÉCNICA?	☒ Sim. Durante o período contratual, é incumbida à CONTRATADA a responsabilidade de fornecer atendimento abrangente para garantir a operacionalidade contínua dos serviços, abordando necessidades de manutenção, correção e eventual substituição em caso de defeitos identificados. ☐ Não será prestada assistência técnica em relação aos itens **X** e **Y**.
CRITÉRIOS DE SELEÇÃO	
FORMA DE CONTRATAÇÃO	☐ **Inexigibilidade** de licitação, com fundamento no art. 74, **Y**, da Lei Federal nº 14.133/21. ☐ **Dispensa** de licitação em razão do **valor***, com fundamento no art. 75, II, da Lei Federal nº 14.133/21. * Nesta hipótese, deve-se utilizar preferencialmente a dispensa eletrônica. ☒ **Dispensa** de licitação, com fundamento no art. 75, inciso VIII, da Lei Federal nº 14.133/21. ☐ Pregão eletrônico.
CRITÉRIO DE JULGAMENTO	☒ Menor preço. Desde que atendidos integralmente os requisitos técnicos, operacionais, de habilitação e demais condições estabelecidas neste Termo de Referência. ☐ Maior desconto.
O ORÇAMENTO ESTIMADO É SIGILOSO?	☐ Sim. ☒ Não.

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

CRITÉRIO PARA A PROPOSTA SER ACEITA	A proposta será aceita desde que apresente preços compatíveis com os valores estimados pela Administração e com os praticados no mercado, observe os quantitativos e especificações estabelecidos neste Termo de Referência e seus anexos e demonstre o atendimento integral aos requisitos técnicos, operacionais e de execução da solução.
HÁ ITENS COM PARTICIPAÇÃO EXCLUSIVA PARA MICROEMPRESAS E EMPRESA DE PEQUENO PORTE?	☐ Sim. ☒ Não.

REQUISITOS DA CONTRATADA

SERÁ EXIGIDA HABILITAÇÃO TÉCNICA?	☒ Sim. **Justificativa**: Será exigida a comprovação de registro ou inscrição da licitante no Conselho Regional de Engenharia e Agronomia – CREA, compatível com as atividades relacionadas ao objeto da contratação, considerando que os serviços envolvem infraestrutura de telecomunicações, conectividade de dados, instalação, configuração, operação e suporte técnico de equipamentos e serviços de rede. A exigência tem por finalidade assegurar que a empresa esteja regularmente habilitada para o exercício das atividades técnicas pertinentes. ☐ Não.
QUALIFICAÇÕES TÉCNICAS EXIGIDAS	☒ Declaração de ciência das informações necessárias para o cumprimento da futura obrigação contratual. ☐ Registro na entidade profissional competente. ☐ Indicação de pessoal técnico, instalações e aparelhamento para o cumprimento da futura obrigação contratual com a comprovação de qualificação técnica de cada membro da equipe técnica responsável pela execução dos trabalhos.

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

	☒ Outro. **Especificar**: Apresentação de um ou mais Atestados de Capacidade Técnica, emitidos por pessoas jurídicas de direito público ou privado, que comprovem a execução satisfatória de serviços compatíveis em características e complexidade com o objeto da contratação, abrangendo comunicação de dados, acesso corporativo à Internet, gerenciamento de redes, SD-WAN, segurança perimetral UTM/NGFW, monitoramento, suporte técnico especializado e operação de ambientes corporativos de missão crítica, incluindo, quando aplicável, serviços de proteção e mitigação de ataques DDoS. ☐ Não será exigida prova de qualificação técnica em razão da baixa complexidade da contratação.	**Justificativa**: A exigência visa comprovar a capacidade técnico-operacional da empresa para a execução de serviços especializados e de elevada criticidade, indispensáveis à continuidade e à segurança da infraestrutura tecnológica da SEGUP, observando-se o art. 67 da Lei Federal nº 14.133/2021.
HÁ CRITÉRIO DE SUSTENTABILIDADE?	☒ Sim. ☐ Não.	**Especificar**: A solução deverá observar critérios de sustentabilidade compatíveis com o objeto, incluindo eficiência energética dos equipamentos, redução do consumo de recursos, destinação ambientalmente adequada de equipamentos e resíduos eletrônicos eventualmente substituídos e utilização preferencial de documentação e registros em meio eletrônico.
HÁ RISCOS A SEREM ASSUMIDOS PELA CONTRATADA?	☒ Sim. ☐ Não.	A CONTRATADA assumirá os riscos vinculados às obrigações que estejam sob sua esfera de controle e gerenciamento, especialmente aqueles relacionados à operação da solução, disponibilidade dos serviços, manutenção da infraestrutura, desempenho dos equipamentos, segurança da informação, cumprimento dos níveis de serviço, atualização tecnológica, substituição de equipamentos, gerenciamento de incidentes e demais responsabilidades definidas neste Termo de Referência, observada a matriz de riscos ou a alocação contratual aplicável.

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

FORMA DE EXECUÇÃO DOS SERVIÇOS		
COMO O SERVIÇO DEVE SER PRESTADO?	☒ O início da execução ocorrerá mediante emissão de Ordem de Serviço ou instrumento equivalente, compreendendo implantação, configuração, integração, ativação, testes, homologação técnica e operação assistida, conforme este Termo de Referência. A execução deverá ocorrer de forma coordenada com a equipe técnica da SEGUP, preservando a continuidade dos serviços essenciais. ☐ O bem deve ser entregue em **X** parcelas, sendo a 1ª em até **Y** dias, a contar do recebimento da nota de empenho, e as demais, conforme necessidade da contratante dentro do prazo de vigência contratual, mediante seu aviso com **Z** dias de antecedência.	
LOCAL E HORA DA EXECUÇÃO DO SERVIÇOS	Os serviços devem ser executados na sede da Secretaria de Estado de Segurança Pública e Defesa Social e nas unidades administrativas, operacionais e estratégicas abrangidas pela contratação, no horário compreendido entre 09h às 16h, de segunda e sexta,exceto feriados.	
PRAZO PARA IMPLANTAÇÃO, HOMOLOGAÇÃO E INÍCIO DA OPERAÇÃO	A implantação e a ativação derão ser concluídas no prazo máximo de até 30 (trinta) dias corridos. Após a implantação, serão realizados recebimento provisório, inspeção, testes, correção de inconformidades, homologação e recebimento definitivo, conforme os critérios estabelecidos neste Termo de Referência.	
HÁ POSSIBILIDADE DE SUBCONTRATAÇÃO?	☒ Sim. Parcialmente ☐ Não.	**Justificativa:** Será permitida a subcontratação parcial de atividades relacionadas à execução do objeto, desde que previamente autorizada pela CONTRATANTE, permanecendo vedada a subcontratação integral. A CONTRATADA permanecerá integralmente responsável pelo cumprimento das obrigações contratuais e pela adequada execução dos serviços eventualmente subcontratados.

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

PRAZO, FORMA DE PAGAMENTO E GARANTIA DO CONTRATO		
PRAZO DO CONTRATO	☐ 30 dias (pronta entrega). ☒ 06 meses.	
HAVERÁ POSSIBILIDADE DE PRORROGAÇÃO?	☒Sim, nas hipóteses do art. 75 inciso VIII da Lei Federal nº 14.133/21. ☐ Não.	
FORMA DE PAGAMENTO	**Meio**	Ordem bancária.
	Onde?	Conta corrente da contratada preferencialmente no Banco do Estado do Pará.
	Qual o prazo?	Até 30 dias corridos, a contar do recebimento da nota fiscal (ou fatura) com o comprovante de regularidade fiscal da contratada.
	Prova da regularidade fiscal	A regularidade fiscal pode ser provada: **1.** Por consulta ao SICAF ou Cadastramento Unificado de Licitante. *ou* **2.** Pela apresentação dos documentos constantes no art. 68 da Lei Federal nº 14.133/21, quando não for possível consultar aos sistemas oficiais.

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

QUAL A GARANTIA DO CONTRATO?	☒ 5% do valor inicial do contrato.	**Justificativa**: Considerando a complexidade técnica e a criticidade dos serviços de conectividade, comunicação de dados e segurança de redes, bem como a necessidade de assegurar a continuidade dos serviços essenciais da SEGUP/PA, será exigida garantia contratual correspondente a **5% (cinco por cento) do valor inicial do contrato**. A exigência visa resguardar a Administração quanto ao adequado cumprimento das obrigações assumidas pela CONTRATADA, especialmente aquelas relacionadas à implantação, disponibilidade dos serviços, cumprimento dos níveis de serviço (SLA), manutenção, suporte técnico, substituição de equipamentos e continuidade operacional durante toda a vigência contratual.
	☐ Não há.	**Justificativa**:

Belém, 16 de outubro de 2026

MARCUS SERGIO NUNES QUEIROZ – CEL QOCBM
Diretor do Núcleo de Telemática – MF: 57197268

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

ANEXO I – JUSTIFICATIVA DA CONTRATAÇÃO E ESPECIFICAÇÕES TÉCNICAS

1. PREMISSAS GERAIS DA SOLUÇÃO:

1.1 A solução a ser fornecida deverá atender aos requisitos técnicos, operacionais, de desempenho, disponibilidade, segurança da informação, interoperabilidade, gerenciamento e suporte estabelecidos neste Termo de Referência e seus anexos.

1.2 A solução deverá ser disponibilizada na modalidade de serviço gerenciado, compreendendo o fornecimento integrado de infraestrutura de telecomunicações, circuitos de comunicação de dados, acesso à Internet, equipamentos de comunicação e segurança, softwares, licenças, serviços especializados, monitoramento, gerenciamento e suporte técnico necessários ao pleno funcionamento da infraestrutura tecnológica da Secretaria de Estado de Segurança Pública e Defesa Social do Pará – SEGUP.

1.3 A CONTRATADA deverá fornecer, instalar, configurar, ativar, operar, monitorar e manter todos os equipamentos, componentes, softwares, licenças e demais recursos necessários ao funcionamento da solução, incluindo, conforme aplicável a cada item, equipamentos CPE, soluções SD-WAN, Firewall UTM/NGFW, equipamentos ópticos, módulos de comunicação, conversores, fontes de alimentação, cabeamento, conectores, módulos ópticos e endereçamento IP.

1.4 Todos os equipamentos, softwares, licenças, assinaturas e componentes necessários à execução dos serviços deverão permanecer devidamente licenciados, atualizados e em condições de operação durante toda a vigência contratual, não sendo admitida interrupção dos serviços decorrente de expiração de licenças, assinaturas de segurança, suporte do fabricante ou recursos indispensáveis à solução.

1.5 A CONTRATADA deverá prestar serviço de suporte técnico especializado durante toda a vigência contratual, em regime de atendimento compatível com os níveis de serviço estabelecidos neste Termo de Referência, incluindo atendimento ininterrupto 24 horas por dia, 7 dias por semana, quando previsto para o respectivo serviço ou componente da solução.

1.6 A CONTRATADA deverá prestar serviços de instalação, ativação, configuração, integração, testes, homologação, operação assistida, manutenção preventiva e corretiva e substituição de equipamentos defeituosos nas unidades contempladas pela contratação, sem custos adicionais para a CONTRATANTE, observados os prazos e os Acordos de Nível de Serviço – SLA estabelecidos neste Termo de Referência.

1.7 A CONTRATADA deverá disponibilizar plataforma de gerenciamento e monitoramento centralizado da rede, capaz de acompanhar de forma contínua os enlaces, equipamentos, serviços, disponibilidade, desempenho, utilização de banda, eventos de segurança, indicadores de SLA e demais parâmetros necessários à gestão da infraestrutura contratada.

1.8 A solução deverá contemplar mecanismos de Gerência Proativa de Redes, incluindo monitoramento contínuo, supervisão dos enlaces e equipamentos, gerenciamento da solução SD-WAN, Firewall e, quando aplicável, proteção Anti-DDoS, gerenciamento de incidentes, mudanças e configurações, inventário automatizado, atualização de firmware e assinaturas de segurança e acompanhamento dos indicadores de desempenho.

1.9 A CONTRATADA deverá disponibilizar Portal Web de Gestão, com acesso seguro pela CONTRATANTE, permitindo, no mínimo, o acompanhamento da infraestrutura em tempo real, consulta da disponibilidade dos enlaces, utilização de banda, indicadores de desempenho, acompanhamento de chamados técnicos, inventário dos ativos, eventos de segurança, exportação de relatórios e consulta ao histórico operacional.

1.10 A solução deverá contemplar sistema de abertura, registro, acompanhamento e gerenciamento de chamados técnicos, permitindo o tratamento de incidentes, registro das ocorrências, acompanhamento do atendimento e aferição dos respectivos níveis de serviço, inclusive com abertura automática de chamados quando identificadas falhas ou indisponibilidades pelos mecanismos de monitoramento.

1.11 A CONTRATADA deverá manter em funcionamento permanente o Centro de Operações de Rede – NOC, a plataforma de monitoramento, o Portal de Gestão e os mecanismos de administração centralizada da solução,

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

responsabilizando-se pela continuidade operacional, integridade das informações, disponibilidade dos sistemas de gerenciamento e geração dos relatórios operacionais e gerenciais necessários à fiscalização do contrato.

1.12 A solução deverá contemplar, conforme a composição de cada item contratado, serviços de comunicação de dados, acesso corporativo à Internet, SD-WAN, CPE gerenciado, Firewall UTM/NGFW, gerenciamento centralizado, monitoramento permanente, Gerência Proativa de Redes, endereçamento IP público válido, suporte técnico especializado, manutenção preventiva e corretiva, atualização de software, firmware e assinaturas de segurança e, quando previsto, serviço gerenciado de proteção e mitigação de ataques DDoS.

1.13 A arquitetura da solução deverá permanecer compatível com a infraestrutura tecnológica atualmente em operação na SEGUP, observando requisitos de interoperabilidade, escalabilidade, disponibilidade, desempenho, confiabilidade e segurança da informação, de modo a minimizar impactos durante a implantação e assegurar a continuidade dos serviços essenciais durante a transição contratual.

1.14 A implantação da solução deverá ser realizada com o menor impacto operacional possível, mediante planejamento e coordenação com a equipe técnica da SEGUP, compreendendo as etapas de instalação, configuração, integração, ativação, testes e homologação técnica, de forma a evitar a descontinuidade dos serviços de comunicação, segurança e acesso aos sistemas institucionais.

1.15 Após a implantação, a solução será submetida a procedimento de homologação técnica pela SEGUP, compreendendo, conforme aplicável, inspeção física dos equipamentos, conferência das configurações, verificação dos enlaces de comunicação, testes de desempenho, redundância, SD-WAN, Firewall NGFW, proteção Anti-DDoS, mecanismos de failover, políticas de segurança e validação da documentação e do inventário técnico.

1.16 A CONTRATADA deverá emitir e disponibilizar periodicamente relatórios operacionais e gerenciais contendo informações suficientes para acompanhamento da disponibilidade dos serviços, utilização dos enlaces, incidentes, chamados técnicos, desempenho da infraestrutura, eventos de segurança, cumprimento dos Acordos de Nível de Serviço – SLA e demais indicadores previstos neste Termo de Referência.

1.17 Todos os serviços de instalação, ativação, configuração, integração, testes, homologação, operação assistida, gerenciamento, monitoramento, manutenção, suporte técnico, atualização de software e firmware, renovação de assinaturas de segurança e substituição de equipamentos necessários ao pleno funcionamento da solução deverão estar incluídos no valor da contratação, não sendo admitida cobrança adicional à CONTRATANTE.

2. QUANTIDADES ESTIMADAS

2.1 A contratação observará os quantitativos atualmente utilizados pela SEGUP, correspondentes aos itens constantes do Contrato Administrativo nº 075/2023:

Item	Descrição	Quantidade
01	Serviço de Comunicação 50 Mbps + UTM SD-WAN Tipo B + Tipo E + Gerência de Redes	19 serviços
02	Serviço de Comunicação 500 Mbps + UTM SD-WAN Tipo E + CPE + Gerência de Redes + Proteção DDoS	1 serviço
03	Serviço de Comunicação 1 Gbps + UTM SD-WAN Tipo F + CPE + Gerência de Redes + Proteção DDoS	1 serviço

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

Os quantitativos acima reproduzem aqueles previstos no Contrato Administrativo nº 075/2023 para o Lote 02.

3. FUNDAMENTAÇÃO LEGAL

A presente contratação fundamenta-se:

3.1 Na Constituição Federal, especialmente em seus artigos 37 e 144;
3.2 Na Lei Federal nº 14.133/2021, em especial o art. 75, inciso VIII, relativo à dispensa de licitação em situações emergenciais;
3.3 Na Lei Geral de Proteção de Dados – Lei Federal nº 13.709/2018;
3.4 Nas normas técnicas expedidas pela Agência Nacional de Telecomunicações – ANATEL;
3.5 Nas normas brasileiras aplicáveis à infraestrutura de redes de telecomunicações;
3.6 Nas políticas estaduais de segurança pública e governança de tecnologia da informação;
3.7 Nas especificações técnicas constantes do Pregão Eletrônico nº 082/2022, que originou a Ata de Registro de Preços utilizada para a celebração do Contrato Administrativo nº 075/2023.

A contratação emergencial observará, ainda, os princípios da legalidade, continuidade do serviço público, eficiência, economicidade, interesse público, motivação, planejamento, segurança jurídica e supremacia do interesse público.

4. JUSTIFICATIVA DA CONTRATAÇÃO EMERGENCIAL

4.1 A infraestrutura de telecomunicações atualmente utilizada pela SEGUP constitui elemento essencial para o funcionamento das atividades administrativas, operacionais e estratégicas do Sistema Integrado de Segurança Pública e Defesa Social do Estado do Pará.

4.2 Toda a comunicação entre unidades administrativas, Centros Integrados de Operações, unidades policiais, sistemas corporativos, aplicações críticas, plataformas de inteligência, serviços de autenticação, bancos de dados, sistemas de monitoramento e serviços digitais depende da disponibilidade permanente da infraestrutura de conectividade objeto deste Termo de Referência.

4.3 A interrupção desses serviços poderá acarretar:
4.3.1 indisponibilidade dos sistemas corporativos da SEGUP;
4.3.2 interrupção da comunicação entre unidades administrativas e operacionais;
4.3.3 comprometimento da troca segura de informações entre os órgãos integrantes do SIEDS;
4.3.4 indisponibilidade dos sistemas utilizados nas atividades de segurança pública;
4.3.5 paralisação de serviços administrativos essenciais;
4.3.6 aumento da exposição da infraestrutura tecnológica a ataques cibernéticos; e
4.3.7 prejuízo ao atendimento da população e à continuidade das políticas públicas de segurança.
4.4 O Contrato Administrativo nº 075/2023 demonstra que os serviços contratados possuem natureza continuada e destinam-se ao atendimento das necessidades dos órgãos integrantes do Sistema Integrado de Segurança Pública e Defesa Social do Estado do Pará, conforme definido em sua cláusula de objeto.
4.5 Dessa forma, verifica-se situação emergencial caracterizada pela necessidade de evitar a descontinuidade de serviço público essencial, justificando-se a contratação direta nos termos do art. 75, inciso VIII, da Lei Federal nº 14.133/2021.

5. NECESSIDADE DA SEGUP

5.1 A Secretaria de Estado de Segurança Pública e Defesa Social do Pará – SEGUP mantém infraestrutura de Tecnologia da Informação e Comunicação essencial ao funcionamento de suas unidades administrativas, operacionais e estratégicas, responsável por suportar sistemas corporativos, serviços de comunicação, acesso a aplicações institucionais e atividades críticas relacionadas à segurança pública.

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

5.2 A interrupção ou degradação desses serviços compromete diretamente a continuidade das operações, a comunicação entre as unidades e a capacidade de resposta da Administração às demandas institucionais.
5.3 Diante da rescisão do contrato atualmente vigente e da necessidade de assegurar a continuidade dos serviços essenciais até a conclusão de novo procedimento licitatório, faz-se necessária a contratação emergencial de solução integrada de comunicação de dados e segurança de redes, de forma a evitar a descontinuidade dos serviços públicos e preservar a operacionalidade da infraestrutura tecnológica da SEGUP.
5.4 A solução deverá garantir conectividade segura e permanente entre as unidades, acesso confiável à Internet, gerenciamento centralizado da rede corporativa, monitoramento contínuo da infraestrutura, suporte técnico especializado, gerenciamento proativo de incidentes, elevada disponibilidade dos serviços e proteção avançada contra ameaças cibernéticas, incluindo mecanismos de mitigação de ataques distribuídos de negação de serviço (DDoS), além de recursos de gerenciamento inteligente da rede e segurança perimetral.
5.5 A presente contratação possui caráter estritamente emergencial e visa assegurar a manutenção da disponibilidade, da integridade e da segurança dos serviços de Tecnologia da Informação e Comunicação indispensáveis ao funcionamento da SEGUP, evitando prejuízos à prestação dos serviços públicos de segurança, à continuidade administrativa e ao atendimento da população, até que seja concluída a contratação definitiva da solução.
5.6 Considerando a extensa infraestrutura de Tecnologia da Informação distribuída entre diversas unidades administrativas e operacionais, a solução corporativa integrada deverá ser capaz de garantir:
5.6.1 conectividade permanente entre as unidades;
5.6.2 acesso seguro à Internet;
5.6.3 gerenciamento centralizado da rede corporativa;
5.6.4 proteção contra ameaças cibernéticas;
5.6.5 monitoramento permanente da infraestrutura;
5.6.6 disponibilidade contínua dos sistemas institucionais;
5.6.7 suporte técnico especializado;
5.6.8 gerenciamento proativo de incidentes;
5.6.9 mitigação de ataques distribuídos de negação de serviço (DDoS); e
5.6.10 continuidade operacional das atividades de segurança pública.

6. ESTUDO DA CONTRATAÇÃO

6.1 Em atendimento ao princípio do planejamento previsto na Lei Federal nº 14.133/2021, foi realizada análise das alternativas disponíveis para garantir a continuidade dos serviços de comunicação de dados, conectividade e segurança da infraestrutura de Tecnologia da Informação e Comunicação da Secretaria de Estado de Segurança Pública e Defesa Social – SEGUP.
6.2 A avaliação considerou aspectos técnicos, operacionais, econômicos e de continuidade dos serviços públicos, tendo em vista que a infraestrutura atualmente utilizada suporta sistemas institucionais críticos, comunicação entre unidades operacionais e administrativas, acesso às aplicações corporativas e serviços essenciais à atividade de segurança pública.
6.3. Alternativa 1 – Descontinuidade da Prestação dos Serviços
6.3.1 A alternativa consiste na não contratação de solução substituta até a conclusão do procedimento licitatório ordinário.
6.3.2 Essa alternativa mostrou-se tecnicamente inviável, uma vez que ocasionaria a interrupção dos serviços de comunicação de dados e de segurança da rede corporativa, comprometendo o funcionamento dos sistemas institucionais, o acesso às aplicações corporativas, a comunicação entre as unidades da SEGUP e a continuidade das atividades operacionais.
6.3.3 Tal cenário acarretaria elevado risco à prestação dos serviços públicos de segurança, podendo provocar indisponibilidade de sistemas críticos, perda de conectividade, aumento da exposição a incidentes de segurança cibernética e prejuízos significativos às atividades finalísticas da Secretaria.
6.4. Alternativa 2 – Contratação Individualizada dos Componentes da Solução
6.4.1 A alternativa consiste na contratação separada dos serviços de comunicação de dados, equipamentos de rede, soluções de segurança, monitoramento, gerenciamento e suporte técnico por diferentes fornecedores.
6.4.2 Embora juridicamente possível, a alternativa foi considerada tecnicamente desvantajosa por aumentar significativamente a complexidade da gestão contratual, exigir múltiplas interfaces de suporte, dificultar a identificação de

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

responsabilidades em caso de falhas, elevar o tempo de resposta para resolução de incidentes e ampliar os riscos de incompatibilidade entre equipamentos, softwares e plataformas de gerenciamento.

6.4.3 Além disso, a fragmentação da solução reduziria a eficiência operacional, aumentaria os custos indiretos de administração contratual e comprometeria a padronização tecnológica atualmente existente na infraestrutura da SEGUP.

6.5. Alternativa 3 – Contratação Emergencial de Solução Integrada

6.5.1 A alternativa consiste na contratação de solução única e integrada, abrangendo serviços de comunicação de dados, equipamentos de acesso, gerenciamento centralizado da infraestrutura, segurança de redes, monitoramento contínuo, suporte técnico especializado e demais serviços necessários à manutenção da operação da rede corporativa.

6.5.2 Essa alternativa mostrou-se a mais adequada sob os aspectos técnico, operacional e econômico, por permitir a continuidade imediata dos serviços essenciais sem necessidade de reestruturação da infraestrutura existente, reduzindo significativamente o tempo de implantação e os riscos associados à transição entre contratos.

6.5.3 A adoção de solução integrada proporciona maior eficiência na gestão da rede corporativa, centralização do monitoramento, padronização tecnológica, atendimento unificado, melhor controle dos níveis de serviço (SLA), redução do tempo de resposta a incidentes e maior disponibilidade da infraestrutura crítica da SEGUP.

6.5.4 Adicionalmente, a solução integrada contempla mecanismos avançados de segurança da informação, gerenciamento inteligente da rede por SD-WAN, proteção perimetral por Firewall de Próxima Geração – NGFW, monitoramento proativo, gerenciamento centralizado e mitigação de ataques distribuídos de negação de serviço – DDoS, proporcionando maior resiliência operacional e proteção dos ativos tecnológicos da Administração.

6.6. Análise Comparativa das Alternativas

Critério avaliado	Não contratar	Contratação fragmentada	Solução integrada emergencial
Continuidade dos serviços	Não atende	Atende parcialmente	Atende plenamente
Tempo de implantação	Não aplicável	Elevado	Reduzido
Complexidade operacional	Muito alta	Alta	Baixa
Gerenciamento centralizado	Não	Limitado	Sim
Compatibilidade tecnológica	Não aplicável	Parcial	Total
Segurança da informação	Prejudicada	Parcial	Elevada
Monitoramento integrado	Não	Parcial	Completo
Tempo de resposta a incidentes	Inexistente	Elevado	Reduzido
Risco operacional	Muito elevado	Elevado	Baixo
Continuidade das operações da SEGUP	Comprometida	Parcial	Garantida

6.7 Após a análise das alternativas, conclui-se que a contratação emergencial de solução integrada de comunicação de dados, conectividade, gerenciamento de redes e segurança cibernética representa a opção mais vantajosa para a Administração, por reunir os melhores resultados sob os aspectos técnico, operacional, econômico e de gestão de riscos.

6.8 A solução permite preservar a infraestrutura tecnológica atualmente em operação, assegurar a continuidade dos serviços essenciais prestados pela SEGUP, reduzir riscos de indisponibilidade, manter elevados padrões de segurança da informação e garantir a prestação ininterrupta das atividades de segurança pública até a conclusão do processo destinado à contratação definitiva.

7. QUANTITATIVOS

7.1 A contratação observará os quantitativos atualmente utilizados pela SEGUP, correspondentes aos itens constantes do Contrato Administrativo nº 075/2023:

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

Item	Descrição	Quantidade
01	Serviço de Comunicação 50 Mbps + UTM SD-WAN Tipo B + Tipo E + Gerência de Redes	19 serviços
02	Serviço de Comunicação 500 Mbps + UTM SD-WAN Tipo E + CPE + Gerência de Redes + Proteção DDoS	1 serviço
03	Serviço de Comunicação 1 Gbps + UTM SD-WAN Tipo F + CPE + Gerência de Redes + Proteção DDoS	1 serviço

7.2 Os quantitativos indicados no subitem 7.1 reproduzem aqueles previstos no Contrato Administrativo nº 075/2023 para o Lote 02.

8. DESCRIÇÃO GERAL DA SOLUÇÃO

A solução objeto desta contratação emergencial consiste na prestação de serviços continuados de comunicação de dados, conectividade corporativa e segurança da infraestrutura de redes da Secretaria de Estado de Segurança Pública e Defesa Social – SEGUP, compreendendo o fornecimento de infraestrutura de telecomunicações, equipamentos, licenças, softwares, serviços gerenciados, monitoramento e suporte técnico especializado, necessários para assegurar a continuidade dos serviços de Tecnologia da Informação e Comunicação durante o período de vigência contratual.

A contratação tem por finalidade manter a disponibilidade da infraestrutura de comunicação utilizada pelas unidades administrativas e operacionais da SEGUP, garantindo o funcionamento ininterrupto dos sistemas institucionais, o acesso seguro aos ambientes corporativos e a continuidade das atividades essenciais de segurança pública, reduzindo riscos de indisponibilidade e assegurando a estabilidade operacional da rede corporativa.

Para o atendimento dessas necessidades, a solução deverá contemplar serviços de comunicação de dados dedicados, acesso corporativo à Internet, fornecimento, instalação, configuração, operação e gerenciamento de equipamentos de acesso (CPE), tecnologia de gerenciamento inteligente de tráfego (SD-WAN), soluções de segurança perimetral baseadas em Firewall de Próxima Geração (NGFW/UTM), serviços de proteção contra ataques distribuídos de negação de serviço (DDoS), monitoramento contínuo da infraestrutura, Gerência Proativa de Redes, Centro de Operações de Rede (Network Operation Center – NOC), suporte técnico especializado em regime de atendimento 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, manutenção preventiva e corretiva, gerenciamento centralizado dos eventos da rede, emissão de relatórios gerenciais e acompanhamento dos indicadores de desempenho e dos Acordos de Nível de Serviço (SLA).

A solução deverá ser plenamente compatível com a infraestrutura tecnológica atualmente em operação na SEGUP, permitindo sua integração sem necessidade de substituição dos ambientes existentes, de forma a minimizar impactos operacionais, reduzir o tempo de implantação e assegurar a continuidade dos serviços durante a transição contratual. Deverá, ainda, observar requisitos de interoperabilidade, escalabilidade, disponibilidade, desempenho, confiabilidade e segurança da informação, garantindo a manutenção dos serviços essenciais e a continuidade das operações institucionais da Secretaria até a conclusão da contratação definitiva.

De forma geral, a solução deverá contemplar:

- serviços dedicados de comunicação de dados;
- acesso corporativo à Internet;
- tecnologia SD-WAN para gerenciamento inteligente de tráfego;
- fornecimento, instalação, configuração e gerenciamento de equipamentos CPE;

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

- solução UTM (Unified Threat Management);
- Firewall NGFW;
- proteção contra ataques DDoS;
- monitoramento contínuo da infraestrutura;
- Gerência Proativa de Redes;
- Network Operation Center – NOC;
- suporte técnico especializado em regime 24x7;
- manutenção preventiva, corretiva e evolutiva;
- gerenciamento centralizado de eventos;
- geração de relatórios gerenciais;
- acompanhamento dos indicadores de desempenho;
- atendimento aos Acordos de Nível de Serviço (SLA);
- integração com a infraestrutura atualmente existente na SEGUP.

A arquitetura deverá permanecer compatível com os padrões técnicos estabelecidos, preservando a interoperabilidade, a escalabilidade, a segurança e a continuidade operacional dos serviços corporativos da Secretaria.

9. ESPECIFICAÇÕES GERAIS DA SOLUÇÃO

A solução objeto desta contratação emergencial deverá ser disponibilizada na modalidade de **serviço gerenciado**, compreendendo o fornecimento integrado de infraestrutura de telecomunicações, equipamentos, softwares, licenças, serviços especializados e suporte operacional, de forma a assegurar a continuidade da operação da rede corporativa da Secretaria de Estado de Segurança Pública e Defesa Social – SEGUP durante todo o período de vigência contratual.

Será de inteira responsabilidade da CONTRATADA disponibilizar todos os recursos necessários ao pleno funcionamento da solução, incluindo infraestrutura de comunicação de dados, backbone IP, equipamentos de acesso (CPE), equipamentos destinados ao gerenciamento inteligente da rede (SD-WAN), soluções de segurança perimetral baseadas em Firewall UTM e Firewall de Próxima Geração (NGFW), equipamentos ópticos, módulos de comunicação, conversores, fontes de alimentação, cabeamento, conectores, módulos ópticos, endereçamento IP, bem como todos os componentes de hardware, software e licenciamento indispensáveis ao funcionamento da solução.

Também deverão estar compreendidos, sem qualquer custo adicional para a CONTRATANTE, os serviços de instalação, ativação, configuração, integração, testes, homologação, operação assistida, gerenciamento centralizado, monitoramento contínuo, manutenção preventiva e corretiva, substituição de equipamentos defeituosos, atualização de firmware, atualização de software, renovação das assinaturas de segurança, suporte técnico especializado, Central de Atendimento e Centro de Operações de Rede (Network Operation Center – NOC), garantindo elevado padrão de disponibilidade, desempenho e segurança.

Durante toda a vigência contratual, a solução deverá permanecer plenamente operacional, cabendo à CONTRATADA adotar todas as medidas necessárias para prevenir falhas, corrigir indisponibilidades e assegurar a continuidade dos serviços essenciais utilizados pela SEGUP, observando os níveis mínimos de desempenho e disponibilidade estabelecidos neste Termo de Referência.

A solução deverá ser fornecida como serviço totalmente gerenciado, compreendendo infraestrutura de telecomunicações, equipamentos, softwares, licenciamento, gerenciamento, monitoramento, suporte técnico, manutenção preventiva e corretiva, operação assistida e atualização tecnológica durante toda a vigência contratual.

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

A CONTRATADA será integralmente responsável pelo fornecimento de todos os recursos necessários ao perfeito funcionamento da solução, incluindo:

- Links de comunicação de dados;
- Backbone IP;
- Equipamentos CPE;
- Equipamentos SD-WAN;
- Firewall UTM;
- Firewall NGFW;
- Equipamentos ópticos;
- Conversores;
- Fontes;
- Cabos;
- Patch cords;
- Módulos ópticos;
- Endereçamento IP;
- Serviços de instalação;
- Configuração;
- Operação;
- Gerenciamento;
- Monitoramento;
- Manutenção;
- Atualizações de firmware;
- Atualizações de software;
- Licenciamento completo;
- Central de Atendimento;
- NOC.

A solução deverá permanecer totalmente operacional durante toda a vigência contratual.

10. REQUISITOS GERAIS DA REDE CORPORATIVA

A infraestrutura de comunicação deverá ser composta por tecnologias de padrão corporativo, compatíveis com ambientes de missão crítica, assegurando elevados níveis de disponibilidade, desempenho, confiabilidade, segurança e capacidade de expansão.

Os circuitos de comunicação deverão ser implementados, preferencialmente, por meio de infraestrutura óptica ou tecnologias equivalentes de alta capacidade, admitindo-se soluções baseadas em Fibra Óptica, IP/MPLS, Metro

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

Ethernet, Ethernet Dedicada ou outras tecnologias autorizadas pela Agência Nacional de Telecomunicações – ANATEL que atendam integralmente aos requisitos técnicos desta contratação.

A utilização de meios metálicos será admitida apenas no trecho final de atendimento ao usuário (last mile), quando tecnicamente indispensável e desde que não comprometa os requisitos mínimos de desempenho, disponibilidade, estabilidade e qualidade do serviço.

A CONTRATADA deverá possuir autorização vigente da Agência Nacional de Telecomunicações – ANATEL para exploração do Serviço de Comunicação Multimídia (SCM), bem como todas as demais autorizações e licenças necessárias à prestação dos serviços objeto desta contratação, responsabilizando-se integralmente pelo cumprimento da regulamentação aplicável ao setor de telecomunicações.

A solução deverá operar de forma integrada com a infraestrutura tecnológica atualmente existente na SEGUP, preservando a arquitetura de rede em produção, minimizando impactos operacionais e garantindo a continuidade dos serviços durante toda a execução contratual, sem necessidade de alterações estruturais que possam comprometer o funcionamento dos sistemas institucionais.

Todos os circuitos deverão utilizar infraestrutura profissional de comunicação de dados.

Serão aceitas tecnologias:

- Fibra óptica;
- IP/MPLS;
- Metro Ethernet;
- Ethernet dedicada;
- Tecnologias equivalentes autorizadas pela ANATEL.

A utilização de enlaces metálicos somente será admitida na última conexão entre a infraestrutura óptica e os equipamentos de borda quando tecnicamente indispensável.

A CONTRATADA deverá possuir autorização da ANATEL para prestação do Serviço de Comunicação Multimídia (SCM).

11. REQUISITOS COMUNS A TODOS OS SERVIÇOS

Independentemente da capacidade ou da modalidade de comunicação contratada, todos os serviços deverão ser disponibilizados como solução totalmente gerenciada, contemplando todos os recursos tecnológicos e operacionais necessários ao funcionamento contínuo da rede corporativa da SEGUP.

A CONTRATADA deverá fornecer circuitos com banda compatível ao perfil de utilização de cada unidade, monitoramento contínuo da infraestrutura, gerenciamento proativo da rede, equipamentos de acesso (CPE), tecnologias de gerenciamento inteligente de tráfego (SD-WAN), soluções de segurança compatíveis com cada perfil de serviço, gerenciamento centralizado, endereçamento IP conforme a necessidade da solução, suporte técnico especializado em regime de atendimento ininterrupto (24 horas por dia, 7 dias por semana), além de manutenção preventiva e corretiva, atualização permanente de firmware, softwares e assinaturas de segurança, substituição de equipamentos defeituosos, operação assistida e emissão de relatórios gerenciais.

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

Todos os equipamentos, softwares, licenças e componentes necessários à execução dos serviços deverão possuir licenciamento válido durante toda a vigência contratual, sendo vedada qualquer interrupção decorrente de expiração de licenças, assinaturas ou contratos de suporte do fabricante.

A solução deverá possibilitar gerenciamento centralizado, monitoramento proativo dos enlaces e equipamentos, registro e tratamento de incidentes, acompanhamento dos indicadores de desempenho e cumprimento dos Acordos de Nível de Serviço (SLA), permitindo à CONTRATANTE acompanhar a disponibilidade da infraestrutura, a qualidade dos serviços prestados e a eficiência operacional da rede corporativa.

Considerando o caráter emergencial da presente contratação, a CONTRATADA deverá assegurar a continuidade da infraestrutura atualmente utilizada pela SEGUP, promovendo a implantação e ativação dos serviços com o menor impacto operacional possível, garantindo a manutenção da conectividade, da segurança cibernética e da disponibilidade dos sistemas institucionais, de forma a evitar qualquer descontinuidade na prestação dos serviços públicos essenciais desenvolvidos pela Secretaria.

Todos os serviços deverão contemplar obrigatoriamente:

- Banda garantida;
- Monitoramento permanente;
- Gerência Proativa;
- SD-WAN;
- Equipamento CPE;
- Firewall UTM;
- Gerenciamento centralizado;
- Endereço IP Público válido;
- Suporte técnico especializado;
- Atendimento 24x7;
- Licenciamento integral dos equipamentos;
- Manutenção preventiva;
- Manutenção corretiva;
- Atualização tecnológica.

12. ITEM 01

Item 01 – Assinatura de Serviço de Comunicação de Dados 50 Mbps com SD-WAN, Firewall UTM Tipo B, CPE Gerenciado e Gerenciamento de Redes

Prestação de serviço continuado de comunicação de dados corporativa, contemplando circuito de acesso dedicado à Internet ou MPLS/IP VPN com velocidade mínima de **50 Mbps**, incluindo fornecimento, instalação, configuração, ativação, operação, monitoramento e manutenção de todos os equipamentos e serviços necessários ao pleno funcionamento da solução.

O serviço deverá compreender, obrigatoriamente:

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

- Circuito de comunicação de dados com banda de **50 Mbps**, simétrica ou conforme especificação do projeto executivo, com disponibilidade mínima de **99,7%**;
- Fornecimento de **CPE (Customer Premises Equipment)** em regime de comodato, devidamente instalado, configurado, monitorado e substituído em caso de falha, sem custos adicionais;
- Solução **SD-WAN** totalmente gerenciada, permitindo gerenciamento centralizado dos enlaces, definição de políticas de roteamento inteligente, seleção dinâmica de caminhos, balanceamento de tráfego, priorização de aplicações, QoS, monitoramento em tempo real e alta disponibilidade dos serviços;
- **Firewall UTM Tipo B (Next Generation Firewall – NGFW)** integrado à solução, contemplando, no mínimo, funcionalidades de Firewall Stateful Inspection, Controle de Aplicações, IPS, IDS, VPN IPsec e SSL, Web Filter, Antivírus de Gateway, AntiSpyware, AntiBot, inspeção SSL/TLS, NAT, QoS, controle por usuários, registros de auditoria e gerenciamento centralizado das políticas de segurança;
- Gerenciamento centralizado da infraestrutura de rede, incluindo monitoramento proativo 24x7, supervisão dos enlaces, equipamentos e serviços, abertura automática de chamados, gerenciamento de incidentes, gerenciamento de mudanças, gestão de configuração, atualização de firmware e assinaturas de segurança, inventário automatizado e geração de relatórios operacionais e gerenciais;
- Disponibilização de Portal Web para acompanhamento da operação, consulta de disponibilidade, desempenho dos enlaces, utilização de banda, chamados técnicos, indicadores de SLA, inventário dos ativos e relatórios históricos;
- Serviços de instalação, ativação, configuração, testes, homologação, operação assistida, suporte técnico especializado, manutenção preventiva e corretiva, incluindo substituição de equipamentos defeituosos, sem ônus adicional para a CONTRATANTE;
- Atendimento aos níveis mínimos de serviço (SLA) definidos no Termo de Referência, contemplando atendimento técnico 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, durante toda a vigência contratual.

A solução deverá ser entregue plenamente operacional, integrada ao ambiente tecnológico da CONTRATANTE e compatível com as políticas institucionais de segurança da informação, assegurando confidencialidade, integridade, disponibilidade e rastreabilidade das comunicações corporativas.

Appliance Tipo B

O equipamento Tipo B deverá possuir capacidade mínima para ambientes de pequeno e médio porte, suportando tráfego de até **750 Mbps** em modo Firewall, destinado às unidades remotas de menor demanda.

Deverá possuir, no mínimo:

- Throughput Firewall de 750 Mbps;
- Capacidade para inspeção de aplicações em camada 7;
- Sistema Operacional dedicado para segurança;
- Firewall de Próxima Geração (NGFW);
- Sistema de Prevenção contra Intrusão (IPS);
- Sistema de Detecção de Intrusão (IDS);
- Controle de Aplicações por identidade;
- Antivírus Gateway;
- Antimalware;
- Web Filter com categorização automática de sites;

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

- Inspeção SSL/TLS (SSL Inspection);
- VPN IPSec;
- SSL VPN;
- Tradução de Endereços (NAT);
- DHCP Server e Relay;
- VLAN IEEE 802.1Q;
- QoS;
- Roteamento estático e dinâmico;
- Interface Web HTTPS;
- Interface CLI;
- SNMP;
- Syslog;
- Exportação de logs;
- Gerenciamento remoto seguro.

Unidade de Fornecimento

Assinatura Mensal (Serviço Gerenciado por Unidade Atendida).

Composição Mínima do Item

- Comunicação de Dados 50 Mbps;
- CPE Gerenciado;
- SD-WAN Gerenciado;
- Firewall UTM Tipo B (NGFW);
- Gerenciamento Centralizado da Rede;
- Monitoramento 24x7;
- Manutenção Preventiva e Corretiva;
- Atualizações de Software, Firmware e Assinaturas;
- Portal de Gestão e Relatórios;
- Suporte Técnico Especializado;
- Operação Assistida;
- Garantia Integral durante toda a vigência contratual.

Esse descritivo está alinhado ao padrão de especificações utilizado em contratações de TIC pela Administração Pública e pode ser utilizado tanto no **ETP**, quanto no **Termo de Referência**, **Planilha de Itens** e **Contrato Administrativo**.

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

13. ITEM 02

Item 02 – Assinatura de Serviço de Comunicação de Dados 500 Mbps com SD-WAN, Firewall UTM Tipo E, CPE Gerenciado, Gerenciamento de Redes e Serviço de Proteção Anti-DDoS

Prestação de serviço continuado de comunicação de dados corporativa, contemplando circuito dedicado de acesso à Internet ou MPLS/IP VPN com velocidade mínima de **500 Mbps**, incluindo fornecimento, instalação, configuração, ativação, operação, monitoramento e manutenção de toda a infraestrutura necessária à prestação dos serviços, compreendendo equipamentos, licenças, softwares, gerenciamento centralizado e suporte técnico especializado.

A solução deverá contemplar, obrigatoriamente:

Comunicação de Dados

- Circuito corporativo de comunicação de dados com capacidade mínima de **500 Mbps**, simétrica ou conforme definido no projeto executivo;
- Disponibilidade mínima anual de **99,70%**;
- Monitoramento contínuo da qualidade do enlace;
- Gerenciamento de desempenho, latência, jitter, perda de pacotes e utilização da banda;
- Suporte a protocolos IPv4 e IPv6;
- QoS (Quality of Service) para priorização de aplicações críticas.

Equipamento CPE Gerenciado

Fornecimento de **Customer Premises Equipment (CPE)** em regime de comodato, contemplando:

- instalação;
- configuração;
- gerenciamento remoto;
- monitoramento 24x7;
- atualização de firmware;
- substituição preventiva e corretiva em caso de falha;
- gerenciamento completo durante toda a vigência contratual.

Solução SD-WAN Tipo E

Fornecimento de solução **SD-WAN** totalmente gerenciada, permitindo:

- gerenciamento centralizado;
- orquestração automática da rede;
- roteamento inteligente baseado em políticas;
- seleção dinâmica do melhor enlace;
- balanceamento de carga;
- failover automático;
- alta disponibilidade;
- priorização de aplicações críticas;

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

- segmentação lógica do tráfego;
- monitoramento em tempo real;
- geração de indicadores operacionais.

Firewall UTM Tipo E (Next Generation Firewall)

Fornecimento de solução de segurança de próxima geração (NGFW), integrada ao serviço, contemplando, no mínimo:

Appliance Tipo E

O equipamento Tipo E deverá atender unidades de médio e grande porte, possuindo capacidade mínima de **18 Gbps** para processamento de Firewall e desempenho compatível com inspeção profunda de tráfego criptografado.

Características mínimas:

- Throughput Firewall de 18 Gbps;
- Throughput IPS superior a 5 Gbps;
- Throughput VPN IPSec compatível com enlaces corporativos de alta velocidade;
- SSL VPN corporativa;
- Processamento multicore dedicado;
- Armazenamento SSD interno;
- Alta Disponibilidade (High Availability – HA);
- Cluster ativo/passivo;
- Balanceamento de carga;
- Controle de Aplicações;
- Web Filtering;
- Antivírus;
- Antimalware;
- Sandbox integrado ou compatível;
- IPS baseado em assinaturas e análise comportamental;
- Inspeção SSL completa;
- Controle de usuários por Active Directory;
- Captive Portal;
- SD-WAN integrada;
- QoS por aplicação;
- Roteamento OSPF;
- Roteamento BGP;
- IPv4 e IPv6;
- Gerenciamento centralizado.

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

Serviço Gerenciado de Proteção Anti-DDoS

A solução deverá contemplar serviço permanente de mitigação de ataques distribuídos de negação de serviço (**Distributed Denial of Service – DDoS**), executado de forma automática e transparente ao ambiente da CONTRATANTE.

O serviço deverá possuir, no mínimo:

- detecção automática de ataques;
- mitigação automática;
- proteção contra ataques volumétricos;
- proteção contra SYN Flood;
- proteção contra UDP Flood;
- proteção contra ICMP Flood;
- proteção contra DNS Amplification;
- proteção contra NTP Amplification;
- proteção contra Reflection Attacks;
- proteção contra HTTP Flood;
- proteção contra HTTPS Flood;
- proteção contra ataques de camada de aplicação (Layer 7);
- monitoramento contínuo dos eventos;
- geração automática de alertas;
- emissão de relatórios de mitigação;
- registro de incidentes de segurança;
- suporte especializado durante eventos de ataque.

O mecanismo de mitigação deverá preservar a disponibilidade dos serviços da CONTRATANTE, minimizando impactos operacionais e mantendo a continuidade da comunicação.

Gerenciamento Centralizado da Rede

A CONTRATADA deverá disponibilizar gerenciamento completo da solução, compreendendo:

- monitoramento proativo 24x7;
- supervisão dos enlaces;
- gerenciamento dos equipamentos;
- gerenciamento do SD-WAN;
- gerenciamento do Firewall;
- gerenciamento da proteção Anti-DDoS;
- gerenciamento de incidentes;
- gerenciamento de mudanças;
- gerenciamento de configuração;

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

- inventário automatizado;
- abertura automática de chamados;
- atualização de firmware;
- atualização das assinaturas de segurança;
- acompanhamento dos indicadores de desempenho.

Portal de Gestão

Disponibilização de portal web seguro permitindo:

- acompanhamento em tempo real da infraestrutura;
- consulta da disponibilidade dos enlaces;
- utilização da banda;
- indicadores de desempenho;
- visualização dos eventos de segurança;
- acompanhamento dos chamados técnicos;
- inventário dos ativos;
- exportação de relatórios;
- consulta do histórico operacional.

Serviços Inclusos

O item deverá compreender, sem custos adicionais:

- projeto executivo;
- instalação;
- ativação;
- configuração;
- integração;
- testes;
- homologação;
- operação assistida;
- manutenção preventiva;
- manutenção corretiva;
- substituição de equipamentos;
- suporte técnico especializado;
- monitoramento 24x7;
- atualização de software;
- atualização de firmware;

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

- atualização das assinaturas de segurança;
- gerenciamento integral da solução.

Níveis de Serviço (SLA)

A solução deverá atender aos níveis mínimos de serviço estabelecidos no Termo de Referência, contemplando:

- disponibilidade mínima de **99,70%** para o circuito de comunicação;
- monitoramento contínuo da infraestrutura;
- atendimento técnico em regime **24x7x360**;
- atendimento e solução de incidentes conforme classificação de criticidade;
- emissão periódica de relatórios operacionais e gerenciais.

Unidade de Fornecimento

Assinatura Mensal (Serviço Gerenciado por Unidade Atendida).

Composição Mínima do Item

- Comunicação de Dados 500 Mbps;
- CPE Gerenciado;
- SD-WAN Tipo E;
- Firewall UTM Tipo E (NGFW);
- Serviço Gerenciado de Proteção Anti-DDoS;
- Gerenciamento Centralizado da Rede;
- Monitoramento 24x7;
- Portal de Gestão;
- Suporte Técnico Especializado;
- Operação Assistida;
- Manutenção Preventiva e Corretiva;
- Atualizações de Software, Firmware e Assinaturas;
- Garantia Integral durante toda a vigência contratual.

Este descritivo é adequado para ambientes de missão crítica, como centros de processamento de dados, Centros Integrados de Comando e Controle (CICC), sedes administrativas e unidades estratégicas de segurança pública, garantindo elevada disponibilidade, segurança cibernética e gestão integrada da infraestrutura de comunicação.

14. ITEM 03

Item 03 – Assinatura de Serviço de Comunicação de Dados 1 Gbps com SD-WAN Tipo F, Firewall UTM Tipo F, CPE Gerenciado, Gerenciamento de Redes e Serviço Gerenciado de Proteção Anti-DDoS

Prestação de serviço continuado de comunicação de dados corporativa, por meio de circuito dedicado de alta capacidade com velocidade mínima de 1 Gbps (1.000 Mbps), incluindo fornecimento, instalação, ativação,

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

configuração, operação, monitoramento, gerenciamento e manutenção de toda a infraestrutura necessária à disponibilização da solução, compreendendo equipamentos, softwares, licenças, suporte técnico especializado e serviços gerenciados.

A solução deverá ser destinada a ambientes de missão crítica, assegurando elevada disponibilidade, desempenho, segurança cibernética e continuidade operacional.

Comunicação de Dados

O serviço deverá contemplar:

- Circuito dedicado de comunicação de dados com largura de banda mínima de 1 Gbps, simétrica ou conforme definido no Projeto Executivo;
- Disponibilidade mínima anual de 99,90%;
- Monitoramento permanente da qualidade do enlace;
- Gerenciamento de desempenho, latência, jitter, perda de pacotes e utilização da banda;
- Suporte aos protocolos IPv4 e IPv6;
- Implementação de QoS (Quality of Service) para priorização de aplicações críticas;
- Possibilidade de expansão da capacidade mediante solicitação da CONTRATANTE.

Equipamento CPE Gerenciado

A CONTRATADA deverá fornecer, em regime de comodato, equipamento Customer Premises Equipment (CPE) compatível com a capacidade do circuito contratado, incluindo:

- instalação e configuração;
- gerenciamento remoto;
- monitoramento contínuo;
- atualização de firmware;
- substituição preventiva e corretiva em caso de falha;
- suporte integral durante toda a vigência contratual.

O equipamento deverá possuir capacidade compatível com enlaces Gigabit Ethernet, suportando operação contínua em ambiente corporativo de alta disponibilidade.

Solução SD-WAN Tipo F

A solução deverá disponibilizar plataforma SD-WAN corporativa, totalmente gerenciada, contemplando, no mínimo:

- gerenciamento centralizado;
- orquestração automática da rede;
- roteamento inteligente baseado em políticas;
- seleção dinâmica do melhor enlace;
- balanceamento de carga;
- failover automático;
- alta disponibilidade;
- segmentação lógica do tráfego;

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

- priorização dinâmica de aplicações críticas;
- engenharia de tráfego;
- monitoramento em tempo real;
- geração de indicadores operacionais;
- provisionamento centralizado;
- gerenciamento de múltiplos enlaces.

Firewall UTM Tipo F (Next Generation Firewall)

O serviço deverá contemplar fornecimento de Firewall UTM Tipo F (NGFW), adequado à capacidade do circuito contratado, incluindo, no mínimo:

O equipamento Tipo F deverá atender ambientes críticos, centros de processamento de dados e enlaces de alta capacidade, possuindo desempenho mínimo de **38 Gbps** em Firewall.

Características mínimas:

- Throughput Firewall de 38 Gbps;
- Alto desempenho para inspeção de aplicações;
- VPN IPSec de alta capacidade;
- Cluster de Alta Disponibilidade;
- SSD corporativo;
- Processamento dedicado para IPS;
- Balanceamento de carga;
- Múltiplas interfaces Gigabit e SFP/SFP+;
- Operação redundante;
- Failover automático;
- Controle de aplicações em tempo real;
- IPS avançado;
- IDS;
- Antivirus Gateway;
- Antimalware;
- Web Filter;
- SSL Inspection;
- SD-WAN;
- QoS;
- Segmentação por zonas;
- Controle por identidade;
- Gerenciamento centralizado.

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

Todas as assinaturas de segurança deverão permanecer atualizadas durante toda a vigência contratual.

Serviço Gerenciado de Proteção Anti-DDoS

A solução deverá incluir serviço especializado de mitigação de ataques distribuídos de negação de serviço (Distributed Denial of Service – DDoS), operando de forma contínua e transparente.

O serviço deverá contemplar, no mínimo:

- detecção automática de ataques;
- mitigação automática em tempo real;
- monitoramento contínuo do tráfego;
- proteção contra ataques volumétricos;
- proteção contra SYN Flood;
- proteção contra UDP Flood;
- proteção contra ICMP Flood;
- proteção contra DNS Amplification;
- proteção contra NTP Amplification;
- proteção contra Reflection Attacks;
- proteção contra HTTP Flood;
- proteção contra HTTPS Flood;
- proteção contra ataques de camada de aplicação (Layer 7);
- geração automática de alertas;
- emissão de relatórios técnicos de mitigação;
- registro completo dos eventos;
- suporte especializado durante incidentes.

O mecanismo deverá preservar a disponibilidade dos serviços corporativos, reduzindo impactos decorrentes de ataques cibernéticos.

Gerenciamento Centralizado da Rede

A CONTRATADA deverá disponibilizar gerenciamento completo da solução, compreendendo:

- monitoramento proativo em regime 24x7x360;
- supervisão dos enlaces;
- gerenciamento dos equipamentos;
- gerenciamento do SD-WAN;
- gerenciamento do Firewall;
- gerenciamento da proteção Anti-DDoS;

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

- gerenciamento de incidentes;
- gerenciamento de problemas;
- gerenciamento de mudanças;
- gerenciamento de configuração;
- inventário automatizado;
- abertura automática de chamados;
- atualização de firmware;
- atualização das assinaturas de segurança;
- acompanhamento dos indicadores de desempenho;
- geração de relatórios gerenciais.

Portal de Gestão

A solução deverá disponibilizar portal web seguro para acompanhamento da operação, permitindo:

- visualização em tempo real da infraestrutura;
- consulta da disponibilidade dos enlaces;
- monitoramento da utilização da banda;
- acompanhamento dos indicadores de SLA;
- visualização dos eventos de segurança;
- acompanhamento dos chamados técnicos;
- inventário dos ativos;
- exportação de relatórios;
- consulta do histórico operacional;
- acompanhamento dos eventos de mitigação de ataques DDoS.

Serviços Inclusos

Deverão estar incluídos no preço da assinatura mensal:

- elaboração do projeto executivo;
- instalação;
- ativação;
- configuração;
- integração;
- testes;
- homologação;
- operação assistida;
- manutenção preventiva;

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

- manutenção corretiva;
- substituição de equipamentos defeituosos;
- suporte técnico especializado;
- monitoramento contínuo;
- atualização de software;
- atualização de firmware;
- atualização das assinaturas de segurança;
- gerenciamento integral da solução.

Níveis de Serviço (SLA)

A solução deverá atender, no mínimo, aos seguintes indicadores:

- disponibilidade mínima do circuito de 99,90%;
- monitoramento permanente da infraestrutura;
- atendimento técnico especializado em regime 24x7x360;
- tratamento e solução de incidentes conforme níveis de criticidade definidos no Termo de Referência;
- emissão periódica de relatórios operacionais e gerenciais;
- monitoramento contínuo dos serviços de segurança e mitigação de ataques.

Unidade de Fornecimento

Assinatura Mensal (Serviço Gerenciado por Unidade Atendida).

Composição Mínima do Item

- Comunicação de Dados Dedicada de 1 Gbps;
- CPE Corporativo Gerenciado;
- Solução SD-WAN Tipo F;
- Firewall UTM Tipo F (NGFW);
- Serviço Gerenciado de Proteção Anti-DDoS;
- Gerenciamento Centralizado da Rede;
- Monitoramento Proativo 24x7x360;
- Portal de Gestão e Monitoramento;
- Suporte Técnico Especializado;
- Operação Assistida;
- Manutenção Preventiva e Corretiva;
- Atualizações de Software, Firmware e Assinaturas;
- Relatórios Operacionais e Gerenciais;
- Garantia Integral durante toda a vigência contratual.

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

Este item é destinado a unidades de alta criticidade operacional, como Data Centers, Centros Integrados de Comando e Controle (CICC/CIOPS), Centros de Operações de Segurança (SOC), Centros de Processamento de Dados (CPD), sedes administrativas e ambientes estratégicos, assegurando conectividade de alta capacidade, elevada disponibilidade, proteção avançada contra ameaças cibernéticas e gestão integrada da infraestrutura de TIC.

ACORDO DE NÍVEL DE SERVIÇO (SLA)

15. OBJETIVO DO ACORDO DE NÍVEL DE SERVIÇO

O presente Acordo de Nível de Serviço – SLA (Service Level Agreement) estabelece os indicadores mínimos de desempenho, disponibilidade, continuidade operacional, qualidade da prestação dos serviços e níveis de atendimento que deverão ser observados pela CONTRATADA durante toda a execução contratual.

O SLA constitui instrumento de gestão contratual destinado a assegurar a disponibilidade permanente dos serviços de comunicação de dados, segurança de redes e acesso corporativo à Internet utilizados pela Secretaria de Estado de Segurança Pública e Defesa Social – SEGUP, servindo como referência para fiscalização, medição dos serviços executados e eventual aplicação de glosas ou sanções contratuais.

Todos os indicadores definidos neste Termo de Referência serão monitorados continuamente pelo fiscal do contrato e confrontados com os relatórios emitidos pela plataforma de gerenciamento da CONTRATADA.

16. DISPONIBILIDADE DOS SERVIÇOS

Os serviços deverão permanecer disponíveis durante 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, inclusive sábados, domingos e feriados.

A disponibilidade será calculada mensalmente por circuito.

Não serão considerados períodos programados previamente autorizados pela fiscalização.

A disponibilidade mínima mensal deverá ser:

Serviço	Disponibilidade mínima
Comunicação de Dados	99,70%
SD-WAN	99,90%
Firewall UTM	99,90%
Anti-DDoS	99,95%
Plataforma de Gerenciamento	99,90%
Portal de Monitoramento	99,90%

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

17. CÁLCULO DA DISPONIBILIDADE

A disponibilidade será apurada conforme a seguinte metodologia:

Disponibilidade (%) =

(Total de minutos do mês − Tempo de indisponibilidade) ÷ Total de minutos do mês × 100

Serão desconsiderados:

- manutenções previamente autorizadas;
- indisponibilidades provocadas pela CONTRATANTE;
- interrupções decorrentes de caso fortuito ou força maior devidamente comprovados.

18. JANELAS DE MANUTENÇÃO

As manutenções programadas somente poderão ocorrer:

- entre 00h00 e 05h00;
- mediante autorização formal da SEGUP;
- com antecedência mínima de 05 dias úteis.

A manutenção deverá possuir:

- plano de execução;
- plano de reversão;
- responsáveis técnicos;
- estimativa de impacto;
- comunicação prévia aos usuários afetados.

19. CLASSIFICAÇÃO DOS INCIDENTES

Os chamados técnicos serão classificados conforme seu impacto operacional.

Criticidade 1 – Crítica

Caracteriza-se por:

- indisponibilidade total do serviço;
- perda completa de conectividade;
- indisponibilidade do Firewall;
- falha do SD-WAN;
- indisponibilidade do Anti-DDoS;
- interrupção de serviços essenciais.

Criticidade 2 – Alta

Caracteriza-se por:

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

- degradação significativa do desempenho;
- perda parcial da comunicação;
- degradação superior a 30%;
- falha de redundância;
- indisponibilidade de aplicações críticas.

Criticidade 3 – Média

Caracteriza-se por:

- falhas sem impacto imediato;
- problemas de configuração;
- erros de gerenciamento;
- falhas administrativas.

Criticidade 4 – Baixa

Caracteriza-se por:

- solicitações de configuração;
- dúvidas técnicas;
- informações;
- ajustes operacionais.

20. TEMPOS MÁXIMOS DE ATENDIMENTO

Chamado Crítico

Atendimento: **15 minutos**

Diagnóstico: **30 minutos**

Início da correção: **30 minutos**

Restabelecimento: **Até 4 horas**

Chamado Alto

Atendimento: **30 minutos**

Diagnóstico: **1 hora**

Correção: **Até 6 horas**

Chamado Médio

Atendimento: **2 horas**

Correção: **Até 24 horas**

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

Chamado Baixo

Atendimento: **4 horas**

Conclusão: **Até 72 horas**

21. TEMPO MÁXIMO PARA REPARO

Para qualquer indisponibilidade dos circuitos de comunicação, o tempo máximo para restabelecimento será de até **12 horas**, em conformidade com o Acordo de Nível de Serviço previsto para os serviços de comunicação de dados.

Quando houver indisponibilidade superior ao prazo estabelecido, a CONTRATADA deverá apresentar relatório técnico contendo:

- causa raiz;
- impacto;
- ações corretivas;
- ações preventivas;
- plano de mitigação.

22. MONITORAMENTO DA INFRAESTRUTURA DE COMUNICAÇÃO

Durante toda a vigência da contratação, a CONTRATADA deverá manter serviço de monitoramento contínuo e proativo da infraestrutura de comunicação de dados, operando ininterruptamente em regime 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e 360 (trezentos e sessenta dias), sem necessidade de intervenção da equipe técnica da CONTRATANTE.

O monitoramento deverá ser realizado por meio de plataforma especializada integrada ao Centro de Operações de Rede (Network Operation Center – NOC), permitindo o acompanhamento permanente da disponibilidade e do desempenho dos circuitos de comunicação, equipamentos e serviços contratados.

A solução deverá possibilitar a identificação automática de falhas, degradações de desempenho e indisponibilidades, bem como acompanhar indicadores operacionais, incluindo disponibilidade dos enlaces, utilização de banda, latência, jitter, perda de pacotes, utilização de recursos computacionais dos equipamentos, estado das interfaces, alarmes operacionais e demais parâmetros necessários à gestão da infraestrutura.

Sempre que identificada qualquer anormalidade capaz de comprometer a qualidade dos serviços, a CONTRATADA deverá iniciar imediatamente os procedimentos de diagnóstico e correção, independentemente da abertura de chamado pela SEGUP, adotando as medidas necessárias para restabelecimento da normalidade dentro dos prazos definidos nos Acordos de Nível de Serviço (SLA).

23. MONITORAMENTO DOS EQUIPAMENTOS DE SEGURANÇA

Os equipamentos responsáveis pela segurança perimetral da rede deverão permanecer permanentemente monitorados durante toda a execução contratual, permitindo acompanhamento contínuo de seu estado operacional, desempenho e capacidade de processamento.

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

O monitoramento deverá abranger o funcionamento das funcionalidades de Firewall de Próxima Geração (NGFW), gerenciamento unificado de ameaças (UTM), VPNs, sistemas de prevenção e detecção de intrusão (IPS/IDS), inspeção SSL/TLS, controle de aplicações, filtragem de conteúdo, mecanismos antivírus, políticas de segurança e demais serviços licenciados.

Também deverão ser acompanhados indicadores relacionados ao consumo de processamento, utilização de memória, sessões simultâneas, utilização das interfaces de rede, registros de eventos de segurança e demais informações necessárias para garantir a integridade, disponibilidade e desempenho da solução.

Toda ocorrência relevante deverá gerar registro em sistema de gerenciamento e tratamento conforme os procedimentos operacionais estabelecidos para a contratação.

24. MONITORAMENTO DA SOLUÇÃO SD-WAN

A solução de SD-WAN deverá operar sob gerenciamento permanente, permitindo acompanhamento em tempo real do comportamento da rede corporativa e da qualidade dos serviços prestados.

O gerenciamento deverá possibilitar a visualização da utilização dos enlaces, qualidade das conexões, latência, jitter, perda de pacotes, disponibilidade dos circuitos, distribuição do tráfego por aplicação, utilização por unidade administrativa e demais indicadores que permitam otimizar o desempenho da infraestrutura.

A plataforma deverá identificar automaticamente degradações na qualidade dos enlaces e executar os mecanismos de roteamento inteligente previstos na solução, assegurando a continuidade das comunicações corporativas e minimizando impactos decorrentes de falhas ou degradação da rede.

25. MONITORAMENTO E MITIGAÇÃO DE ATAQUES DDoS

Os serviços que contemplarem proteção contra ataques distribuídos de negação de serviço (Distributed Denial of Service – DDoS) deverão operar de forma contínua, automática e transparente, assegurando a preservação da disponibilidade dos serviços corporativos da SEGUP.

A plataforma deverá realizar monitoramento permanente do tráfego de rede, identificando comportamentos anômalos e eventos compatíveis com ataques volumétricos, ataques baseados em protocolos de comunicação e ataques direcionados à camada de aplicação.

Uma vez identificado evento compatível com ataque cibernético, a solução deverá iniciar automaticamente os mecanismos de mitigação, preservando, sempre que possível, o tráfego legítimo da CONTRATANTE e reduzindo os impactos sobre os serviços institucionais.

Todos os eventos de segurança deverão ser registrados, classificados e documentados, permitindo a emissão de relatórios técnicos contendo informações sobre o tipo de ataque, período de ocorrência, volume de tráfego mitigado, ações executadas e efetividade das medidas adotadas.

Nos casos classificados como incidentes críticos, a CONTRATADA deverá comunicar imediatamente a fiscalização da SEGUP, informando as providências adotadas e acompanhando o evento até sua completa normalização.

26. PORTAL DE GESTÃO E RELATÓRIOS OPERACIONAIS

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

A CONTRATADA deverá disponibilizar portal eletrônico de gerenciamento acessível à equipe técnica da SEGUP, permitindo o acompanhamento da infraestrutura contratada durante toda a vigência do contrato.

O portal deverá disponibilizar informações atualizadas sobre disponibilidade dos serviços, utilização dos enlaces, desempenho da rede, indicadores de capacidade, chamados técnicos, incidentes registrados, inventário dos ativos, eventos de segurança, alarmes operacionais, histórico de ocorrências, gráficos de desempenho e acompanhamento dos indicadores de nível de serviço (SLA).

As informações deverão permanecer disponíveis para consulta durante todo o período contratual, permitindo exportação de relatórios em formato eletrônico e rastreabilidade das ocorrências registradas.

27. RELATÓRIOS MENSAIS DE EXECUÇÃO DOS SERVIÇOS

Como instrumento de acompanhamento contratual, a CONTRATADA deverá apresentar, até o quinto dia útil do mês subsequente ao da prestação dos serviços, relatório técnico consolidado contendo as informações referentes ao desempenho da solução.

O relatório deverá demonstrar, no mínimo, a disponibilidade mensal dos circuitos e equipamentos, os indicadores de desempenho previstos nos Acordos de Nível de Serviço (SLA), os chamados registrados, os incidentes atendidos, as manutenções preventivas e corretivas executadas, as atualizações de software, firmware e assinaturas de segurança realizadas, os eventos de segurança identificados, os ataques cibernéticos mitigados, a utilização dos recursos da infraestrutura, a evolução da capacidade operacional da rede e recomendações técnicas para melhoria contínua dos serviços.

Esses relatórios subsidiarão a fiscalização contratual, a medição dos serviços executados e a autorização para pagamento da remuneração mensal.

28. ACEITAÇÃO DOS SERVIÇOS

Os serviços objeto desta contratação emergencial serão considerados regularmente executados somente quando mantiverem os níveis mínimos de disponibilidade, desempenho, segurança e continuidade estabelecidos neste Termo de Referência.

A aceitação dos serviços dependerá da verificação da efetiva operacionalidade da solução, da conformidade com os Acordos de Nível de Serviço (SLA), da inexistência de falhas críticas pendentes de correção, da apresentação dos relatórios obrigatórios e da emissão do correspondente atesto pela fiscalização da SEGUP.

A simples disponibilização da infraestrutura não caracterizará a execução integral do objeto, permanecendo a CONTRATADA responsável pela operação contínua e pelo atendimento integral das condições contratuais durante todo o período de medição.

29. GLOSAS PELO DESCUMPRIMENTO DOS NÍVEIS DE SERVIÇO

O não atendimento dos indicadores mínimos de desempenho estabelecidos neste Termo de Referência poderá ensejar a aplicação de glosas sobre a remuneração mensal da CONTRATADA, sem prejuízo das demais sanções administrativas previstas na Lei Federal nº 14.133/2021 e no contrato.

A fiscalização poderá aplicar glosas sempre que forem constatadas indisponibilidades superiores aos limites contratualmente estabelecidos, extrapolação dos prazos máximos de atendimento ou de restabelecimento dos serviços, falhas recorrentes sem solução definitiva, ausência de monitoramento da infraestrutura, indisponibilidade das ferramentas de gerenciamento, não apresentação dos relatórios obrigatórios ou qualquer outra situação que comprometa a continuidade, a qualidade ou a segurança dos serviços prestados.

A aplicação das glosas observará os princípios da proporcionalidade, razoabilidade, contraditório e ampla defesa, sendo calculada de forma proporcional ao impacto operacional causado pelo descumprimento dos níveis de ser-

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

viço, sem afastar a possibilidade de aplicação das penalidades contratuais e legais cabíveis quando caracterizada inexecução parcial ou total do objeto contratado.

PRESTAÇÃO DOS SERVIÇOS, OPERAÇÃO ASSISTIDA, MANUTENÇÃO, GESTÃO DE MUDANÇAS, CONTINUIDADE OPERACIONAL E PLANO DE CONTINGÊNCIA

30. PRESTAÇÃO DOS SERVIÇOS

30.1 Escopo da Prestação

A presente contratação emergencial compreende a prestação de serviços especializados de Tecnologia da Informação e Comunicação destinados à manutenção da infraestrutura de conectividade corporativa da Secretaria de Estado de Segurança Pública e Defesa Social – SEGUP, abrangendo serviços de comunicação de dados, acesso corporativo à Internet, gerenciamento inteligente de tráfego por tecnologia SD-WAN, fornecimento e administração de equipamentos de borda (CPE), soluções de segurança perimetral baseadas em Firewall UTM e Next Generation Firewall (NGFW), proteção contra ataques distribuídos de negação de serviço (DDoS), monitoramento permanente da infraestrutura, operação assistida, suporte técnico especializado, manutenção preventiva e corretiva, gerenciamento centralizado e administração de toda a solução.

Considerando o caráter emergencial da contratação, todos os recursos tecnológicos necessários ao funcionamento da solução deverão ser disponibilizados em regime de serviço gerenciado, permanecendo sob responsabilidade exclusiva da CONTRATADA a operação, administração, monitoramento, atualização tecnológica, manutenção e substituição dos componentes que venham a apresentar falhas ou perda de desempenho, garantindo a continuidade dos serviços essenciais da SEGUP sem interrupções decorrentes de limitações técnicas, obsolescência ou indisponibilidade de equipamentos.

A execução contratual compreenderá todas as atividades necessárias para assegurar a plena operacionalidade da infraestrutura durante toda a vigência do contrato, independentemente da necessidade de reconfigurações, atualizações de software e firmware, substituição de equipamentos, adequações técnicas ou demais intervenções indispensáveis à manutenção dos níveis mínimos de desempenho e disponibilidade estabelecidos neste Termo de Referência.

30.2 Regime de Operação

Em razão da natureza crítica dos serviços prestados pela SEGUP, a infraestrutura contratada deverá permanecer em operação contínua e ininterrupta, assegurando disponibilidade permanente dos serviços de comunicação e segurança da informação.

A CONTRATADA deverá manter estrutura operacional apta a atender qualquer ocorrência técnica em regime de **24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e 360 (trezentos e sessenta) dias**, não sendo admitida qualquer distinção entre dias úteis, finais de semana, feriados ou horários comerciais para fins de atendimento, monitoramento ou restabelecimento dos serviços.

Toda ocorrência que possa comprometer a disponibilidade da infraestrutura deverá ser imediatamente identificada, registrada e tratada pela equipe técnica da CONTRATADA, independentemente de solicitação da fiscalização da SEGUP.

Os serviços deverão permanecer disponíveis:

- 24 (vinte e quatro) horas por dia;

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

- 07 (sete) dias por semana;
- 360 (trezentos e sessenta) dias.

Todas as ocorrências deverão ser tratadas independentemente do horário.

Não haverá distinção entre horário comercial, noturno, finais de semana ou feriados.

30.3 Serviços Compreendidos

Os serviços objeto desta contratação deverão compreender todas as atividades necessárias à operação integral da infraestrutura de comunicação de dados e segurança de redes da SEGUP, incluindo monitoramento permanente, gerenciamento proativo da infraestrutura, administração dos enlaces, gerenciamento dos equipamentos CPE, plataformas SD-WAN, soluções Firewall UTM/NGFW, mecanismos de proteção Anti-DDoS, suporte remoto e presencial, manutenção preventiva e corretiva, substituição de equipamentos defeituosos, atualização de software, firmware e assinaturas de segurança, gerenciamento de incidentes, problemas e mudanças, controle de capacidade, geração de relatórios técnicos e apoio permanente à fiscalização contratual.

Todas essas atividades serão consideradas integrantes da remuneração mensal da solução, não sendo admitida cobrança adicional por serviços necessários ao perfeito funcionamento da infraestrutura.

A contratação compreenderá, no mínimo:

- operação integral da infraestrutura;
- gerenciamento proativo;
- monitoramento contínuo;
- suporte remoto;
- suporte presencial;
- manutenção preventiva;
- manutenção corretiva;
- substituição de equipamentos defeituosos;
- atualização de firmware;
- atualização de software;
- atualização das assinaturas de segurança;
- gerenciamento da solução SD-WAN;
- gerenciamento dos equipamentos UTM;
- gerenciamento Anti-DDoS;
- gerenciamento dos equipamentos CPE;
- administração dos enlaces;
- controle de capacidade;
- gerenciamento de incidentes;
- gerenciamento de problemas;
- gerenciamento de mudanças;
- emissão de relatórios técnicos;

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

- apoio à fiscalização contratual.

31. OPERAÇÃO ASSISTIDA

Após a ativação ou migração dos serviços, a CONTRATADA deverá manter período de Operação Assistida destinado à estabilização da infraestrutura e à validação integral da solução implantada.

Durante esse período, será realizado acompanhamento técnico intensivo de todos os componentes da solução, com monitoramento permanente do comportamento dos enlaces, equipamentos, políticas de segurança, mecanismos de roteamento inteligente, disponibilidade dos serviços e desempenho da infraestrutura.

Sempre que identificada qualquer inconsistência operacional, a CONTRATADA deverá promover sua correção imediata, realizando os ajustes necessários para assegurar a estabilidade da solução e o pleno atendimento aos níveis mínimos de serviço estabelecidos neste Termo de Referência.

As atividades de Operação Assistida compreenderão ainda a execução de testes funcionais, validação das rotinas de redundância, testes de failover, verificação das políticas de segurança, análise de desempenho e acompanhamento conjunto com a equipe técnica designada pela SEGUP.

Após a implantação dos serviços, a CONTRATADA deverá executar período de

Operação Assistida.

A Operação Assistida compreenderá:

- acompanhamento permanente da solução;
- correção imediata de falhas;
- ajustes de configuração;
- validação dos enlaces;
- validação dos equipamentos;
- validação das políticas de segurança;
- validação do SD-WAN;
- testes de redundância;
- testes de failover;
- testes de desempenho;
- acompanhamento conjunto com a fiscalização.

Durante esse período, todas as ocorrências deverão possuir tratamento prioritário.

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

31.1 Objetivos da Operação Assistida

A Operação Assistida tem como finalidade assegurar a completa estabilização da infraestrutura contratada, eliminar inconsistências decorrentes da implantação, validar a arquitetura operacional da solução, otimizar seu desempenho, confirmar o atendimento aos indicadores de disponibilidade e desempenho previstos nos Acordos de Nível de Serviço (SLA) e promover a transferência de conhecimento necessária para o adequado acompanhamento da solução pela equipe técnica da CONTRATANTE.

A Operação Assistida terá como finalidade:

- estabilizar a solução;
- eliminar inconsistências;
- validar a arquitetura implantada;
- otimizar o desempenho;
- assegurar o atendimento aos indicadores de SLA;
- capacitar a equipe técnica da SEGUP quanto aos procedimentos operacionais.

32. MANUTENÇÃO PREVENTIVA

A CONTRATADA deverá executar programa permanente de manutenção preventiva em todos os componentes da solução, observando as recomendações dos fabricantes e as melhores práticas de gerenciamento de serviços de Tecnologia da Informação.

As atividades preventivas deverão compreender inspeções periódicas dos equipamentos, análise do desempenho da infraestrutura, atualização de firmware, atualização de software, renovação das assinaturas de segurança, atualização das bases antivírus, verificação da integridade dos enlaces, inspeção dos equipamentos ópticos, análise dos registros operacionais, testes de redundância, avaliação da capacidade instalada e demais procedimentos necessários para reduzir riscos de falhas e preservar a disponibilidade da solução.

As intervenções preventivas deverão ocorrer, sempre que possível, em janelas de manutenção previamente autorizadas pela fiscalização da SEGUP, de forma a minimizar impactos sobre os serviços institucionais.

A CONTRATADA deverá executar manutenção preventiva periódica em todos os componentes da solução.

A manutenção preventiva compreenderá:

- inspeção dos equipamentos;
- atualização de firmware;
- atualização de software;
- atualização de assinaturas de segurança;
- atualização das bases antivírus;
- limpeza lógica;
- otimização de desempenho;
- verificação da capacidade instalada;
- verificação dos discos;
- verificação das fontes;

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

- verificação das interfaces;
- verificação dos enlaces;
- verificação dos logs;
- testes de redundância.

As atividades deverão ocorrer preferencialmente nas janelas de manutenção autorizadas pela CONTRATANTE.

32.1 Atualizações Tecnológicas

Durante toda a vigência contratual, a CONTRATADA deverá manter todos os equipamentos e softwares permanentemente atualizados, disponibilizando, sem qualquer ônus adicional para a CONTRATANTE, novas versões de software, correções de segurança, patches, hotfixes, atualizações de firmware, assinaturas dos mecanismos de prevenção de intrusão (IPS), bases antivírus, filtros de conteúdo, mecanismos AntiSpam e demais componentes necessários à preservação da segurança e estabilidade da infraestrutura.

Não será admitida a permanência de equipamentos ou softwares classificados pelo fabricante como obsoletos, descontinuados ou sem suporte técnico oficial.

Durante toda a vigência contratual deverão ser fornecidas, sem custos adicionais:

- novas versões de software;
- correções de segurança;
- patches;
- hotfixes;
- atualizações de firmware;
- novas assinaturas de IPS;
- novas assinaturas antivírus;
- novas assinaturas AntiSpam;
- novas bases de reputação;
- novas bases Web Filter.

Nenhum equipamento poderá permanecer com versão considerada obsoleta pelo fabricante.

33. MANUTENÇÃO CORRETIVA

Sempre que identificada qualquer falha capaz de comprometer a disponibilidade ou o desempenho da solução, a CONTRATADA deverá iniciar imediatamente os procedimentos de diagnóstico, isolamento da ocorrência, identificação da causa raiz e adoção das medidas necessárias ao restabelecimento definitivo dos serviços.

Quando a correção exigir substituição de componentes, deverão ser fornecidos equipamentos ou peças com desempenho igual ou superior aos originalmente instalados, mantendo-se integralmente as funcionalidades contratadas.

Todas as ocorrências deverão ser registradas em sistema de gerenciamento de chamados, acompanhadas até sua completa solução e documentadas em relatório técnico encaminhado à fiscalização.

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

Sempre que identificada qualquer falha operacional, a CONTRATADA deverá iniciar imediatamente os procedimentos de diagnóstico.

A manutenção corretiva compreenderá:

- identificação da falha;
- isolamento do problema;
- análise de causa;
- correção definitiva;
- validação do serviço;
- emissão de relatório técnico.

Quando necessário, deverão ser substituídos imediatamente:

- roteadores;
- appliances UTM;
- equipamentos SD-WAN;
- equipamentos ópticos;
- fontes;
- módulos SFP;
- discos SSD;
- componentes internos;
- cabos defeituosos.

Todo equipamento substituído deverá possuir desempenho igual ou superior ao originalmente instalado.

34. SUBSTITUIÇÃO DE EQUIPAMENTOS

A CONTRATADA deverá manter estoque técnico compatível com a criticidade da infraestrutura da SEGUP, assegurando pronta substituição de qualquer equipamento que apresente falha, degradação de desempenho, obsolescência, defeitos recorrentes ou indisponibilidade incompatível com os níveis mínimos de serviço estabelecidos.

Os equipamentos fornecidos em substituição deverão possuir capacidade operacional, desempenho e funcionalidades equivalentes ou superiores aos originalmente instalados, sem qualquer prejuízo ao funcionamento da solução.

A CONTRATADA deverá manter estoque técnico suficiente para atendimento das ocorrências.

A substituição ocorrerá quando houver:

- falha física;
- falha lógica;
- obsolescência;
- defeito recorrente;
- indisponibilidade superior ao SLA;
- recomendação do fabricante.

Os equipamentos substitutos deverão possuir características iguais ou superiores às especificadas neste Termo de Referência.

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

35. GESTÃO DE INCIDENTES

Toda ocorrência operacional deverá ser registrada em sistema informatizado de gerenciamento de serviços, permitindo rastreabilidade completa do atendimento, desde sua identificação até a solução definitiva.

Cada incidente deverá conter informações suficientes para caracterização da ocorrência, incluindo classificação, prioridade, unidade afetada, equipamentos envolvidos, diagnóstico realizado, ações executadas, responsáveis técnicos, horários de atendimento e conclusão, permitindo à fiscalização acompanhar integralmente o ciclo de tratamento dos chamados.

Todo incidente deverá possuir registro formal.

Cada ocorrência deverá conter, no mínimo:

- número do chamado;
- data;
- hora;
- unidade afetada;
- equipamento envolvido;
- descrição;
- classificação;
- prioridade;
- responsável técnico;
- diagnóstico;
- ações executadas;
- horário de encerramento;
- solução aplicada.

A ferramenta deverá manter histórico completo de todos os chamados.

36. GESTÃO DE PROBLEMAS

A CONTRATADA deverá realizar análise permanente das ocorrências registradas, identificando incidentes recorrentes e executando procedimentos de análise de causa raiz, de forma a eliminar definitivamente as origens das falhas e reduzir a reincidência de indisponibilidades.

Sempre que identificadas ocorrências repetitivas, deverá ser elaborado relatório técnico contendo diagnóstico, avaliação dos impactos operacionais, medidas corretivas implementadas, plano preventivo e recomendações para melhoria contínua da infraestrutura.

A CONTRATADA deverá realizar análise permanente dos incidentes recorrentes.

Sempre que houver repetição de falhas deverá ser executada análise de causa raiz.

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

O relatório deverá conter:

- origem;
- causa;
- impacto;
- probabilidade;
- correção definitiva;
- plano preventivo.

37. GESTÃO DE MUDANÇAS

Qualquer alteração na infraestrutura contratada deverá observar processo formal de gerenciamento de mudanças, contemplando planejamento, avaliação dos impactos técnicos, análise dos riscos envolvidos, definição dos procedimentos de implantação e, quando aplicável, plano de reversão.

As mudanças programadas dependerão de autorização prévia da fiscalização da SEGUP, ressalvadas aquelas classificadas como emergenciais e indispensáveis ao restabelecimento imediato dos serviços essenciais, hipótese em que a CONTRATADA deverá comunicar formalmente as medidas adotadas logo após a estabilização da infraestrutura.

Todas as mudanças executadas deverão permanecer registradas para fins de auditoria e rastreabilidade.

Toda alteração na infraestrutura deverá ser previamente documentada.

A solicitação deverá conter:

- descrição da mudança;
- objetivo;
- justificativa;
- impacto esperado;
- riscos;
- plano de implantação;
- plano de reversão;
- cronograma;
- responsáveis.

Nenhuma mudança poderá ser executada sem autorização formal da fiscalização da SEGUP, exceto aquelas necessárias para restabelecimento emergencial dos serviços.

37.1 Classificação das Mudanças

As mudanças serão classificadas em:

- Programadas;
- Emergenciais;

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

- Corretivas;
- Evolutivas;
- Preventivas.

Todas deverão permanecer registradas.

38. CONTINUIDADE OPERACIONAL

Considerando a criticidade dos serviços de segurança pública suportados pela infraestrutura objeto desta contratação, a CONTRATADA deverá adotar mecanismos que assegurem elevados níveis de disponibilidade e continuidade operacional.

A solução deverá incorporar recursos de redundância, recuperação automática de falhas, balanceamento de tráfego, mecanismos de alta disponibilidade, proteção contra indisponibilidades e demais tecnologias capazes de minimizar impactos decorrentes de falhas de equipamentos, enlaces ou componentes da solução.

A solução deverá ser projetada para minimizar indisponibilidades.

A CONTRATADA deverá manter mecanismos que assegurem:

- alta disponibilidade;
- redundância lógica;
- redundância física quando aplicável;
- redundância de equipamentos críticos;
- redundância de enlaces;
- redundância de alimentação elétrica dos appliances compatíveis;
- mecanismos automáticos de recuperação.

39. PLANO DE CONTINGÊNCIA

A CONTRATADA deverá elaborar e manter atualizado Plano de Contingência específico para a infraestrutura da SEGUP, estabelecendo procedimentos destinados ao tratamento de situações de indisponibilidade parcial ou total da solução.

O plano deverá contemplar procedimentos de recuperação para falhas de comunicação, equipamentos de roteamento, plataformas SD-WAN, Firewalls, serviços de mitigação Anti-DDoS, backbone de comunicação, infraestrutura elétrica e demais componentes críticos, definindo responsabilidades, fluxos de comunicação, mecanismos de recuperação, procedimentos de failover e critérios para retorno controlado da operação.

Todas as configurações dos equipamentos deverão possuir cópias de segurança atualizadas, armazenadas de forma protegida e disponíveis para restauração imediata sempre que necessário.

A CONTRATADA deverá elaborar Plano de Contingência específico para a infraestrutura da SEGUP.

O documento deverá contemplar:

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

39.1 Procedimentos de Recuperação

- falha de comunicação;
- falha de roteador;
- falha SD-WAN;
- falha Firewall;
- falha Anti-DDoS;
- indisponibilidade de backbone;
- indisponibilidade elétrica;
- indisponibilidade de equipamentos.

39.2 Procedimentos Emergenciais

Deverão existir procedimentos documentados para:

- troca de equipamentos;
- recuperação de configuração;
- restauração dos serviços;
- ativação de enlaces alternativos;
- failover automático;
- failback controlado.

39.3 Backup das Configurações

Todas as configurações deverão possuir backup automático.

O backup deverá contemplar:

- roteadores;
- SD-WAN;
- Firewalls;
- políticas de segurança;
- VPN;
- objetos;
- usuários;
- certificados;
- regras de NAT;
- regras de QoS.

Os backups deverão permanecer protegidos e disponíveis para restauração imediata.

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

40. TESTES OPERACIONAIS

A CONTRATADA deverá executar periodicamente testes operacionais destinados a validar o funcionamento da infraestrutura, incluindo mecanismos de redundância, failover, recuperação de serviços, desempenho dos enlaces, qualidade da comunicação, políticas de segurança, VPNs, SD-WAN, Firewalls e mecanismos de mitigação de ataques DDoS.

Os resultados obtidos deverão ser documentados e apresentados à fiscalização da SEGUP, permitindo a comprovação da efetividade dos recursos disponibilizados.

A CONTRATADA deverá executar periodicamente testes de:

- failover;
- redundância;
- recuperação;
- disponibilidade;
- desempenho;
- throughput;
- latência;
- QoS;
- VPN;
- Anti-DDoS;
- Firewall;
- SD-WAN.

Os testes deverão ser documentados e submetidos à fiscalização.

41. DOCUMENTAÇÃO OPERACIONAL

Durante toda a vigência contratual, a documentação técnica da solução deverá permanecer permanentemente atualizada, contemplando inventário dos equipamentos, diagramas físicos e lógicos da rede, documentação dos enlaces, endereçamento IP, configurações dos equipamentos, políticas de segurança, procedimentos operacionais, Plano de Contingência, Plano de Recuperação de Desastres e registros das alterações efetuadas na infraestrutura.

Essa documentação deverá permanecer disponível à fiscalização da SEGUP sempre que solicitada.

Durante toda a execução contratual deverão permanecer atualizados:

- inventário dos equipamentos;
- mapa lógico da rede;
- mapa físico da rede;
- endereçamento IP;
- documentação dos enlaces;

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

- configuração dos equipamentos;
- políticas de Firewall;
- políticas SD-WAN;
- procedimentos operacionais;
- Plano de Contingência;
- Plano de Recuperação de Desastres;
- Plano de Gestão de Mudanças.

42. RESPONSABILIDADE OPERACIONAL

A CONTRATADA será integralmente responsável pela operação, administração, gerenciamento, monitoramento, manutenção, atualização tecnológica e suporte técnico de toda a infraestrutura objeto desta contratação emergencial, garantindo que os serviços permaneçam continuamente disponíveis e em conformidade com os níveis mínimos de desempenho, disponibilidade e segurança estabelecidos neste Termo de Referência e no respectivo Acordo de Nível de Serviço (SLA).

Em razão do caráter emergencial da contratação, caberá à CONTRATADA adotar todas as medidas preventivas e corretivas necessárias para evitar interrupções na prestação dos serviços, assegurando a continuidade das comunicações institucionais e a manutenção das atividades essenciais desenvolvidas pela SEGUP, sem qualquer solução de continuidade até a formalização da contratação definitiva.

CENTRO DE OPERAÇÕES DE REDE (NOC), GERENCIAMENTO PROATIVO, PLATAFORMA DE MONITORAMENTO, PORTAL DE GESTÃO, INVENTÁRIO AUTOMATIZADO, DASHBOARDS EXECUTIVOS, RELATÓRIOS GERENCIAIS, ADMINISTRAÇÃO DA SOLUÇÃO SD-WAN E GESTÃO CENTRALIZADA DA INFRAESTRUTURA

43. CENTRO DE OPERAÇÕES DE REDE – NOC

43.1 Objetivo

Considerando que a presente contratação tem por objetivo assegurar a continuidade dos serviços essenciais de comunicação de dados e segurança cibernética da Secretaria de Estado de Segurança Pública e Defesa Social – SEGUP, a CONTRATADA deverá disponibilizar um **Centro de Operações de Rede (Network Operation Center – NOC)** responsável pelo gerenciamento operacional da solução durante toda a vigência contratual.

O NOC constituirá a estrutura central responsável pelo monitoramento permanente da infraestrutura, supervisão dos enlaces de comunicação, acompanhamento do desempenho dos equipamentos, tratamento dos incidentes, gerenciamento da disponibilidade dos serviços e coordenação das ações necessárias ao restabelecimento da operação sempre que identificadas ocorrências que possam comprometer a continuidade dos serviços.

A atuação do Centro de Operações deverá ocorrer de forma preventiva, proativa e corretiva, permitindo a identificação antecipada de degradações de desempenho e reduzindo significativamente o tempo de resposta aos incidentes que afetem a infraestrutura tecnológica da SEGUP.

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

43.2 Regime de Funcionamento

O Centro de Operações deverá permanecer em funcionamento ininterrupto durante toda a execução contratual, operando em regime de **24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, inclusive sábados, domingos e feriados**, dispondo de equipe técnica especializada, ferramentas corporativas de monitoramento e procedimentos operacionais capazes de garantir o atendimento contínuo da infraestrutura contratada.

Toda ocorrência identificada deverá ser registrada, classificada, acompanhada e tratada até sua completa resolução, independentemente do horário de sua ocorrência, não sendo admitida interrupção dos serviços de monitoramento em razão de expediente administrativo.

O Centro de Operações deverá funcionar:

- 24 (vinte e quatro) horas por dia;
- 07 (sete) dias por semana;
- inclusive sábados, domingos e feriados;
- durante toda a vigência contratual.

O ambiente deverá possuir equipe técnica qualificada para monitoramento, diagnóstico, tratamento e acompanhamento integral dos incidentes.

43.3 Competências do NOC

Compete ao NOC exercer a supervisão operacional de toda a infraestrutura objeto desta contratação, realizando monitoramento contínuo dos circuitos de comunicação, equipamentos de rede, plataformas SD-WAN, soluções de segurança perimetral, serviços de mitigação de ataques cibernéticos e demais componentes da arquitetura tecnológica.

Além do monitoramento permanente, o Centro de Operações deverá identificar automaticamente situações de indisponibilidade ou degradação da qualidade dos serviços, iniciar os procedimentos de diagnóstico, executar ações corretivas remotas sempre que possível, coordenar o atendimento presencial quando necessário e acompanhar cada incidente até sua completa solução.

O NOC deverá manter comunicação permanente com a fiscalização da SEGUP, fornecendo informações sobre eventos relevantes, indisponibilidades, ações corretivas executadas e evolução do tratamento dos incidentes, permitindo total rastreabilidade das atividades desenvolvidas.

Compete ao Centro de Operações de Rede:

- monitorar continuamente toda a infraestrutura contratada;
- detectar falhas de forma proativa;
- identificar degradação de desempenho;
- abrir automaticamente chamados técnicos;
- realizar diagnóstico inicial;
- executar ações corretivas remotas;
- coordenar atendimento em campo quando necessário;
- acompanhar integralmente cada incidente até sua solução definitiva;

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

- manter comunicação permanente com a fiscalização da SEGUP.

44. GERENCIAMENTO PROATIVO

A CONTRATADA deverá executar gerenciamento proativo de toda a infraestrutura tecnológica contemplada nesta contratação emergencial, utilizando ferramentas especializadas capazes de identificar tendências de degradação antes que provoquem impactos na continuidade dos serviços institucionais.

Esse gerenciamento deverá compreender análise contínua da utilização dos enlaces, capacidade da infraestrutura, comportamento dos equipamentos, consumo dos recursos computacionais, disponibilidade dos serviços, evolução do tráfego e demais indicadores que permitam antecipar situações de risco operacional.

Sempre que identificadas condições que indiquem possibilidade de saturação, degradação de desempenho, perda de capacidade ou aumento da probabilidade de falhas, a CONTRATADA deverá adotar imediatamente as medidas preventivas necessárias para evitar interrupções nos serviços, comunicando formalmente a fiscalização da SEGUP quando houver necessidade de intervenções planejadas.

O gerenciamento proativo constitui obrigação permanente da CONTRATADA e integra os serviços continuados de operação da solução, não dependendo da abertura prévia de chamados técnicos pela CONTRATANTE.

A CONTRATADA deverá realizar gerenciamento proativo de toda a infraestrutura tecnológica.

O gerenciamento proativo compreende:

- identificação antecipada de falhas;
- análise de tendências;
- monitoramento da capacidade;
- previsão de saturação dos enlaces;
- identificação de degradação de desempenho;
- análise de consumo de recursos;
- análise de disponibilidade;
- recomendações técnicas para expansão da infraestrutura.

A atuação deverá ocorrer antes da interrupção efetiva dos serviços sempre que tecnicamente possível.

45. PLATAFORMA DE MONITORAMENTO

Para garantir adequado acompanhamento operacional da infraestrutura, a CONTRATADA deverá disponibilizar plataforma corporativa de gerenciamento centralizado capaz de consolidar informações de todos os ativos integrantes da solução contratada.

A plataforma deverá permitir visualização em tempo real da operação da rede corporativa, disponibilizando informações sobre disponibilidade dos serviços, desempenho dos enlaces, equipamentos de comunicação, soluções SD-WAN, Firewalls, serviços Anti-DDoS, conexões VPN, utilização da banda, estado operacional dos ativos e demais componentes da infraestrutura.

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

O ambiente deverá possuir arquitetura compatível com soluções corporativas de missão crítica, permitindo correlação automática de eventos, geração de alarmes, acompanhamento histórico do desempenho da infraestrutura, mapas de topologia, indicadores de disponibilidade, emissão de relatórios técnicos e controle de acesso mediante autenticação segura e perfis diferenciados de usuários.

As informações disponibilizadas pela plataforma deverão permanecer acessíveis durante toda a vigência contratual, possibilitando à fiscalização da SEGUP acompanhar continuamente a operação dos serviços contratados.

A solução deverá disponibilizar plataforma única de monitoramento centralizado.

A plataforma deverá possuir arquitetura corporativa e permitir acompanhamento em tempo real de todos os ativos contratados.

Deverá contemplar monitoramento de:

- enlaces de comunicação;
- equipamentos CPE;
- appliances SD-WAN;
- Firewalls UTM/NGFW;
- proteção Anti-DDoS;
- interfaces físicas;
- interfaces lógicas;
- VPNs;
- utilização de banda;
- desempenho das aplicações;
- disponibilidade dos serviços.

45.1 Funcionalidades Mínimas

A plataforma deverá possuir, no mínimo:

- visualização em tempo real;
- atualização automática;
- geração de alarmes;
- mapas de topologia;
- correlação de eventos;
- histórico operacional;
- gráficos de desempenho;
- indicadores de SLA;
- exportação de relatórios;
- perfis de usuários;

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

- trilha de auditoria;
- autenticação segura;
- controle de acesso por perfil.

46. MONITORAMENTO DOS ENLACES

Os circuitos de comunicação utilizados pela SEGUP deverão permanecer sob monitoramento permanente, permitindo acompanhamento em tempo real da qualidade e disponibilidade dos serviços.

A solução deverá acompanhar continuamente indicadores relacionados à disponibilidade dos enlaces, utilização da capacidade contratada, throughput, latência, jitter, perda de pacotes, qualidade da comunicação, utilização por unidade administrativa, comportamento do tráfego por aplicação e demais métricas necessárias à avaliação do desempenho da infraestrutura.

O sistema de monitoramento deverá manter histórico operacional dos indicadores coletados, possibilitando análises comparativas entre diferentes períodos, identificação de tendências e emissão de relatórios que subsidiem a fiscalização contratual.

Os enlaces deverão possuir monitoramento contínuo dos seguintes parâmetros:

- disponibilidade;
- utilização;
- throughput;
- latência;
- jitter;
- perda de pacotes;
- qualidade do circuito;
- utilização por aplicação;
- utilização por unidade;
- utilização por horário.

O sistema deverá permitir análise histórica e comparação entre períodos.

47. MONITORAMENTO DOS EQUIPAMENTOS

Todos os equipamentos integrantes da solução deverão permanecer permanentemente supervisionados durante toda a execução contratual.

O monitoramento deverá abranger o estado operacional dos ativos, utilização dos recursos computacionais, capacidade de processamento, consumo de memória, utilização do armazenamento, temperatura interna, alimentação elétrica, funcionamento das interfaces físicas e lógicas, sessões estabelecidas, disponibilidade das portas de comunicação e demais parâmetros operacionais recomendados pelos respectivos fabricantes.

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

A identificação de qualquer comportamento anômalo deverá gerar registro automático de evento, possibilitando atuação imediata da equipe técnica responsável pela operação da infraestrutura.

Todos os equipamentos deverão ser monitorados continuamente.

Deverão ser acompanhados:

- CPU;
- memória;
- armazenamento;
- temperatura;
- alimentação elétrica;
- interfaces;
- portas;
- utilização;
- sessões;
- estado operacional;
- alarmes do fabricante.

48. MONITORAMENTO DOS FIREWALLS

As soluções de Firewall UTM e Next Generation Firewall (NGFW) deverão permanecer continuamente monitoradas, permitindo acompanhamento permanente de sua capacidade operacional e da efetividade dos mecanismos de proteção da rede corporativa.

O monitoramento deverá contemplar sessões simultâneas, throughput, utilização de processamento, consumo de memória, funcionamento das VPNs, mecanismos de prevenção e detecção de intrusão (IPS/IDS), inspeção de tráfego criptografado, controle de aplicações, filtragem de conteúdo, antivírus, mecanismos AntiSpam, sistemas de reputação, registros de eventos de segurança e demais funcionalidades disponibilizadas pela solução licenciada.

Os eventos classificados como críticos deverão gerar alertas automáticos e integrar os procedimentos de tratamento executados pelo Centro de Operações de Rede.

A solução deverá monitorar permanentemente:

- conexões simultâneas;
- sessões estabelecidas;
- throughput;
- utilização da CPU;
- utilização da memória;
- VPNs;
- IPS;

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

- IDS;
- SSL Inspection;
- Controle de Aplicações;
- Antivírus;
- Web Filter;
- AntiSpam;
- reputação;
- ameaças detectadas;
- bloqueios realizados;
- eventos críticos.

49. MONITORAMENTO DO SD-WAN

A plataforma SD-WAN deverá permanecer sob gerenciamento permanente, permitindo acompanhamento em tempo real do funcionamento dos túneis de comunicação, qualidade dos enlaces, políticas de roteamento inteligente, mecanismos automáticos de failover, balanceamento de carga e desempenho das aplicações corporativas.

O sistema deverá monitorar continuamente indicadores de latência, jitter, perda de pacotes, disponibilidade dos enlaces, utilização das políticas de roteamento, qualidade das aplicações e eficiência dos mecanismos automáticos de seleção dinâmica de caminhos, garantindo o melhor aproveitamento da infraestrutura disponível.

Sempre que identificadas degradações na qualidade da comunicação, a solução deverá executar automaticamente os mecanismos previstos para preservação da continuidade dos serviços.

A plataforma deverá acompanhar permanentemente:

- estado dos túneis;
- disponibilidade dos enlaces;
- failover;
- balanceamento;
- seleção dinâmica de rotas;
- qualidade das aplicações;
- latência;
- jitter;
- perda de pacotes;
- utilização por política;
- utilização por classe de serviço.

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

50. MONITORAMENTO DO SERVIÇO ANTI-DDOS

Os serviços de proteção contra ataques distribuídos de negação de serviço (DDoS) deverão operar continuamente durante toda a vigência contratual, mantendo vigilância permanente sobre o tráfego destinado aos ativos protegidos da SEGUP.

A plataforma deverá identificar automaticamente padrões compatíveis com ataques volumétricos, ataques de reflexão, ataques direcionados às camadas de transporte e aplicação, tentativas de exaustão de banda, ataques aos protocolos de comunicação e demais eventos que possam comprometer a disponibilidade dos serviços institucionais.

Uma vez identificado comportamento malicioso, os mecanismos de mitigação deverão ser acionados automaticamente, preservando a continuidade da comunicação legítima e reduzindo ao máximo os impactos sobre os sistemas corporativos.

Todos os incidentes deverão ser registrados em plataforma de gerenciamento, com emissão de relatórios técnicos contendo a caracterização do evento, período de ocorrência, volume mitigado, medidas adotadas e resultados obtidos, possibilitando o acompanhamento pela fiscalização da SEGUP e subsidiando a gestão da segurança cibernética da infraestrutura contratada.

O sistema deverá identificar automaticamente:

- ataques volumétricos;
- ataques de reflexão;
- ataques DNS;
- SYN Flood;
- UDP Flood;
- ICMP Flood;
- ataques HTTP;
- ataques HTTPS;
- tentativas de exaustão de banda;
- tentativas de indisponibilidade de serviços.

Sempre que identificado evento de segurança, a mitigação deverá ocorrer automaticamente, registrando todas as ações executadas.

51. PORTAL CORPORATIVO DE GESTÃO E GERENCIAMENTO DA SOLUÇÃO

51.1 Portal de Gestão da Infraestrutura

Como parte integrante da solução objeto desta contratação emergencial, a CONTRATADA deverá disponibilizar à Secretaria de Estado de Segurança Pública e Defesa Social – SEGUP um Portal Corporativo de Gestão, acessível por meio de ambiente web seguro, destinado ao acompanhamento operacional, administrativo e técnico dos serviços contratados.

O Portal deverá constituir ferramenta oficial de relacionamento operacional entre a CONTRATADA e a CONTRATANTE, permitindo à fiscalização acompanhar, em tempo real, a disponibilidade da infraestrutura, o desempenho

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

dos serviços, a evolução dos indicadores de qualidade, a execução contratual e o tratamento das ocorrências registradas durante toda a vigência do contrato.

Considerando a criticidade da infraestrutura de comunicação utilizada pela SEGUP, a plataforma deverá permanecer disponível de forma contínua, observando elevados padrões de disponibilidade, segurança da informação, rastreabilidade das operações e integridade dos dados disponibilizados aos usuários autorizados.

O acesso ao ambiente deverá ocorrer exclusivamente mediante mecanismos seguros de autenticação, contemplando comunicação criptografada, controle individual de credenciais, gerenciamento de perfis de acesso, registros de auditoria e demais recursos destinados à proteção das informações operacionais da Administração Pública.

O Portal deverá permanecer permanentemente atualizado, refletindo a situação operacional da infraestrutura contratada e permitindo à fiscalização acompanhar a execução dos serviços independentemente da abertura de solicitações junto à CONTRATADA.

51.2 Funcionalidades da Plataforma de Gestão

A plataforma deverá disponibilizar recursos suficientes para apoiar a fiscalização técnica, administrativa e contratual da SEGUP, permitindo o gerenciamento completo da solução contratada em um único ambiente corporativo.

Deverá possibilitar a abertura, acompanhamento e encerramento de chamados técnicos, permitindo ao usuário acompanhar todas as etapas do atendimento, desde o registro inicial da ocorrência até sua completa resolução, incluindo os registros das atividades executadas, responsáveis pelo atendimento, prazos consumidos, histórico das intervenções realizadas e documentação técnica correspondente.

O ambiente deverá disponibilizar informações atualizadas sobre os Acordos de Nível de Serviço (SLA), possibilitando acompanhamento dos indicadores de disponibilidade, tempos de atendimento, tempos de restabelecimento, desempenho da infraestrutura e cumprimento das metas contratuais estabelecidas neste Termo de Referência.

Também deverá permitir consulta permanente ao inventário dos ativos contemplados na contratação, incluindo enlaces de comunicação, equipamentos de acesso (CPE), dispositivos SD-WAN, Firewalls, equipamentos ópticos, componentes de segurança, licenças, endereçamento IP e demais recursos disponibilizados para atendimento da SEGUP.

A plataforma deverá disponibilizar painéis gerenciais contendo indicadores consolidados da operação, gráficos históricos de utilização da infraestrutura, eventos registrados, ocorrências de segurança, desempenho da rede corporativa, utilização da capacidade instalada, disponibilidade dos serviços, indicadores de tendência e demais informações que auxiliem o gerenciamento contratual.

Deverá ainda permitir a emissão e exportação de relatórios técnicos, administrativos e operacionais em formatos eletrônicos amplamente utilizados pela Administração Pública, incluindo, no mínimo, arquivos PDF e planilhas eletrônicas, possibilitando sua utilização em processos de fiscalização, auditoria, prestação de contas e gestão contratual.

Todos os registros disponibilizados pela plataforma deverão permanecer armazenados durante toda a vigência contratual, preservando histórico suficiente para subsidiar auditorias, análises técnicas e eventual apuração de responsabilidades.

51.3 Controle de Acesso e Perfis de Usuários

A plataforma deverá implementar mecanismo de controle de acesso baseado em perfis de usuários, assegurando que cada agente autorizado da SEGUP possua acesso apenas às funcionalidades compatíveis com suas atribuições institucionais.

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

Os perfis deverão contemplar, no mínimo, permissões destinadas à administração da plataforma, gestão contratual, fiscalização técnica, fiscalização administrativa, operação da infraestrutura, auditoria e consulta, podendo ser criados perfis adicionais sempre que solicitado pela CONTRATANTE.

Cada perfil deverá possuir permissões específicas para visualização, consulta, inclusão, alteração, exportação e administração das informações disponibilizadas pela solução, observando o princípio do menor privilégio e as boas práticas de segurança da informação.

Todas as operações executadas pelos usuários deverão permanecer registradas em trilhas de auditoria, contendo identificação do usuário responsável, data, horário, endereço de acesso, operação executada e demais informações necessárias à rastreabilidade completa das atividades realizadas.

A CONTRATADA deverá garantir a confidencialidade, integridade e disponibilidade das informações armazenadas no Portal, adotando mecanismos de autenticação segura, criptografia de dados, controle de sessões, proteção contra acessos não autorizados e demais recursos compatíveis com ambientes corporativos de missão crítica.

Por se tratar de contratação emergencial destinada à manutenção da infraestrutura crítica da SEGUP, a indisponibilidade do Portal de Gestão não poderá comprometer o atendimento operacional da solução, devendo a CONTRATADA manter procedimentos alternativos que assegurem a continuidade da comunicação com a fiscalização, o registro das ocorrências e o acompanhamento da execução contratual até o restabelecimento integral da plataforma de gerenciamento.

52. GESTÃO DO INVENTÁRIO DA INFRAESTRUTURA TECNOLÓGICA

52.1 Inventário dos Ativos da Solução

Como parte integrante dos serviços de gerenciamento da infraestrutura, a CONTRATADA deverá manter inventário técnico completo, atualizado e permanentemente sincronizado de todos os ativos disponibilizados para execução da presente contratação emergencial.

O inventário deverá contemplar todos os recursos físicos e lógicos que compõem a solução, abrangendo equipamentos de comunicação de dados, dispositivos de borda (CPE), plataformas SD-WAN, equipamentos de segurança perimetral (UTM e NGFW), componentes ópticos, módulos de comunicação, enlaces, licenças, softwares, serviços associados e demais ativos empregados na operação da infraestrutura tecnológica da Secretaria de Estado de Segurança Pública e Defesa Social – SEGUP.

A gestão do inventário deverá ocorrer de forma contínua durante toda a vigência contratual, permitindo o acompanhamento da evolução da infraestrutura, das substituições realizadas, das atualizações tecnológicas implementadas e das intervenções executadas pela CONTRATADA.

Sempre que ocorrer instalação, substituição, remanejamento, atualização, expansão ou retirada de qualquer componente da solução, o inventário deverá ser imediatamente atualizado, assegurando que as informações disponibilizadas à fiscalização reflitam integralmente a configuração operacional existente.

A CONTRATADA será integralmente responsável pela consistência, integridade e atualização das informações registradas, garantindo que o inventário represente fielmente a infraestrutura efetivamente instalada e em operação na SEGUP.

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

52.2 Informações Técnicas dos Ativos

Cada ativo integrante da solução deverá possuir registro individualizado contendo todas as informações necessárias à sua identificação, gerenciamento, manutenção e rastreabilidade operacional.

O cadastro deverá contemplar, no mínimo, identificação única do ativo, fabricante, modelo, número de série, versão de hardware, versão de firmware, versão de software, licenças associadas, endereçamento IP, localização física, unidade administrativa atendida, data de instalação, histórico de substituições, situação operacional, período de garantia, vigência do suporte técnico do fabricante e demais informações técnicas necessárias ao adequado gerenciamento da infraestrutura.

Para os ativos que possuírem configuração lógica, deverão permanecer registrados os parâmetros operacionais relevantes, versões das configurações implantadas, data das últimas alterações, responsável pelas modificações e histórico das intervenções realizadas, permitindo completa rastreabilidade das mudanças ocorridas durante a execução contratual.

Os registros deverão possibilitar a identificação da relação entre equipamentos, enlaces e serviços associados, permitindo visualizar a composição da infraestrutura instalada em cada unidade da SEGUP e sua respectiva interdependência operacional.

52.3 Atualização e Disponibilização das Informações

O inventário deverá permanecer integrado à plataforma corporativa de gerenciamento disponibilizada pela CONTRATADA, permitindo consulta eletrônica permanente pela equipe de fiscalização da SEGUP.

As informações deverão ser atualizadas automaticamente sempre que tecnicamente possível, ou imediatamente após a execução de qualquer intervenção que altere a composição da infraestrutura contratada, vedada a manutenção de registros desatualizados que possam comprometer a fiscalização contratual.

A plataforma deverá permitir consultas por diferentes critérios de pesquisa, emissão de relatórios gerenciais, exportação das informações em formatos eletrônicos amplamente utilizados pela Administração Pública e acompanhamento do histórico completo dos ativos durante toda a vigência do contrato.

52.4 Finalidade do Inventário

O inventário técnico constituirá instrumento oficial de controle patrimonial e operacional da solução contratada, servindo de base para o acompanhamento da execução contratual, fiscalização dos serviços, planejamento das manutenções, controle das substituições de equipamentos, verificação da atualização tecnológica, emissão dos relatórios gerenciais, auditorias técnicas e comprovação da efetiva prestação dos serviços.

Considerando o caráter emergencial da presente contratação, a manutenção de inventário permanentemente atualizado será requisito indispensável para assegurar a continuidade operacional da infraestrutura, a rápida identificação de falhas, a redução do tempo de resposta aos incidentes e o adequado gerenciamento dos ativos críticos que suportam os serviços essenciais prestados pela Secretaria de Estado de Segurança Pública e Defesa Social – SEGUP.

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

53. DASHBOARDS EXECUTIVOS E PAINÉIS GERENCIAIS

53.1 Painéis Executivos de Acompanhamento da Solução

Como parte integrante da plataforma corporativa de gerenciamento da infraestrutura, a CONTRATADA deverá disponibilizar à Secretaria de Estado de Segurança Pública e Defesa Social – SEGUP painéis executivos (dashboards) destinados ao acompanhamento operacional, gerencial e estratégico dos serviços contratados.

Os dashboards deverão consolidar, de forma intuitiva e em tempo real, as principais informações referentes ao desempenho da infraestrutura de comunicação de dados, segurança cibernética e disponibilidade dos serviços, permitindo à fiscalização contratual identificar rapidamente situações que possam comprometer a continuidade operacional da rede corporativa.

Os painéis deverão apresentar interface gráfica responsiva, de fácil interpretação e navegação, possibilitando consultas dinâmicas, filtros por período, unidade administrativa, circuito, equipamento ou serviço, bem como a visualização de informações consolidadas e detalhadas, conforme o perfil de acesso do usuário.

As informações disponibilizadas deverão ser alimentadas automaticamente pela plataforma de gerenciamento, garantindo que os indicadores reflitam permanentemente a situação operacional da infraestrutura contratada, sem necessidade de intervenção manual da equipe técnica da SEGUP.

Os dashboards deverão permanecer acessíveis durante toda a vigência contratual e integrar o conjunto de ferramentas destinadas à fiscalização, gestão do contrato, acompanhamento dos níveis de serviço e apoio à tomada de decisão.

53.2 Indicadores Gerenciais e Operacionais

Os painéis executivos deverão disponibilizar indicadores suficientes para permitir o acompanhamento permanente da qualidade dos serviços prestados, da disponibilidade da infraestrutura e da evolução operacional da solução.

Entre os indicadores mínimos, deverão estar disponíveis informações referentes à disponibilidade global da rede corporativa, disponibilidade individualizada por unidade da SEGUP, disponibilidade dos circuitos de comunicação, desempenho dos enlaces, utilização da capacidade contratada, consumo médio e máximo de banda, utilização por período, comportamento do tráfego e tendências de crescimento da demanda.

Também deverão ser disponibilizados indicadores relacionados à operação do suporte técnico, incluindo quantidade de chamados registrados, ocorrências em atendimento, chamados encerrados, tempos médios de atendimento e de restabelecimento, cumprimento dos Acordos de Nível de Serviço (SLA), histórico de indisponibilidades, incidentes críticos, eventos recorrentes e demais informações necessárias ao acompanhamento da execução contratual.

No âmbito da segurança da informação, os dashboards deverão apresentar informações consolidadas relativas aos eventos de segurança registrados, ameaças identificadas, ataques mitigados pelos mecanismos de proteção cibernética, funcionamento das soluções Firewall UTM/NGFW, serviços Anti-DDoS, disponibilidade das VPNs, estado operacional das políticas de segurança e demais indicadores que permitam avaliar continuamente o nível de proteção da infraestrutura tecnológica da SEGUP.

A plataforma deverá possibilitar análises históricas, comparações entre períodos distintos, identificação de tendências de comportamento da infraestrutura e geração automática de indicadores destinados à gestão contratual e ao planejamento operacional.

53.3 Recursos de Visualização e Análise

Os painéis gerenciais deverão disponibilizar recursos gráficos capazes de representar, de forma clara e objetiva, a situação operacional da infraestrutura contratada, utilizando gráficos estatísticos, séries históricas, mapas operacionais, indicadores consolidados, medidores de desempenho, painéis de disponibilidade e demais elementos visuais compatíveis com ambientes corporativos de gerenciamento de redes.

A solução deverá permitir consultas parametrizadas, aplicação de filtros, exportação das informações em formatos

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

eletrônicos e emissão de relatórios executivos, preservando integralmente os registros históricos utilizados para composição dos indicadores.

Os dados apresentados deverão permanecer armazenados durante toda a vigência contratual, permitindo rastreabilidade completa da execução dos serviços, apoio às atividades de fiscalização, auditoria, medição contratual e elaboração dos relatórios gerenciais exigidos neste Termo de Referência.

53.4 Finalidade dos Dashboards Executivos

Os dashboards executivos constituem instrumento permanente de gestão da infraestrutura tecnológica da SEGUP e têm por finalidade proporcionar à fiscalização contratual visão consolidada do comportamento operacional da solução, permitindo identificar riscos à continuidade dos serviços, acompanhar o desempenho da rede corporativa, avaliar o cumprimento dos níveis de serviço contratados e subsidiar a tomada de decisões relacionadas à operação da infraestrutura.

Considerando o caráter emergencial da presente contratação, os painéis deverão fornecer informações atualizadas em tempo real, permitindo atuação imediata da CONTRATADA diante de qualquer degradação da qualidade dos serviços, indisponibilidade da infraestrutura ou incidente de segurança que possa comprometer o funcionamento dos sistemas institucionais e a continuidade das atividades essenciais desenvolvidas pela Secretaria de Estado de Segurança Pública e Defesa Social – SEGUP.

54. RELATÓRIOS GERENCIAIS

A plataforma deverá gerar relatórios automáticos.

54.1 Emissão e Disponibilização dos Relatórios

A CONTRATADA deverá disponibilizar, como parte integrante da solução de gerenciamento da infraestrutura, mecanismo automatizado para geração e disponibilização de relatórios técnicos, operacionais e gerenciais, destinados ao acompanhamento da execução contratual, fiscalização dos serviços e gestão da infraestrutura tecnológica da Secretaria de Estado de Segurança Pública e Defesa Social – SEGUP.

Os relatórios deverão ser produzidos automaticamente pela plataforma de gerenciamento, utilizando as informações coletadas em tempo real pelos sistemas de monitoramento, possibilitando análise detalhada do desempenho da infraestrutura, da disponibilidade dos serviços e da evolução operacional da solução durante toda a vigência contratual.

A solução deverá permitir emissão programada em periodicidade diária, semanal, mensal, trimestral e anual, bem como geração sob demanda sempre que solicitado pela fiscalização da SEGUP, sem qualquer limitação quanto à quantidade de consultas ou emissões.

Todos os documentos deverão permanecer disponíveis para consulta eletrônica durante toda a vigência contratual, permitindo exportação em formatos compatíveis com os padrões adotados pela Administração Pública.

54.2 Conteúdo dos Relatórios

Os relatórios gerenciais deverão consolidar informações técnicas suficientes para demonstrar a efetiva execução dos serviços contratados e subsidiar o acompanhamento dos indicadores de desempenho previstos neste Termo de Referência.

Deverão contemplar, no mínimo, informações referentes à disponibilidade da infraestrutura, desempenho dos circuitos de comunicação, utilização da capacidade instalada, crescimento do consumo de banda, comportamento do tráfego da rede corporativa, indicadores de desempenho dos equipamentos, histórico de incidentes registrados, eventos operacionais, mudanças realizadas na infraestrutura, manutenções preventivas e corretivas executadas, falhas identificadas, medidas corretivas adotadas, capacidade disponível da solução, utilização dos recursos tecnológicos e recomendações técnicas destinadas à melhoria contínua da operação.

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

Os relatórios também deverão apresentar indicadores consolidados dos níveis de serviço (SLA), demonstrando o desempenho contratual da solução, os tempos de atendimento, os tempos de restabelecimento dos serviços, a evolução da disponibilidade da infraestrutura e os principais eventos que impactaram a operação da rede corporativa da SEGUP.

As informações constantes dos relatórios deverão servir de base para a fiscalização contratual, validação das medições mensais, aplicação dos indicadores de desempenho e acompanhamento da execução do contrato.

Os relatórios deverão conter:

- disponibilidade;
- desempenho;
- utilização;
- crescimento;
- incidentes;
- eventos;
- mudanças;
- manutenções;
- falhas;
- recomendações técnicas;
- indicadores de capacidade.

55. ADMINISTRAÇÃO DA SOLUÇÃO SD-WAN

A administração da infraestrutura SD-WAN será de responsabilidade exclusiva da CONTRATADA durante toda a vigência da contratação emergencial, cabendo-lhe garantir o funcionamento contínuo, seguro e otimizado da arquitetura de comunicação corporativa da SEGUP.

A gestão da solução compreenderá a administração completa das políticas de roteamento inteligente, configuração e manutenção dos túneis de comunicação, gerenciamento das VPNs corporativas, definição e atualização das políticas de priorização de aplicações, otimização automática do tráfego, monitoramento permanente da qualidade dos enlaces, administração dos mecanismos de balanceamento de carga, gerenciamento dos processos de failover e failback, além da implementação de ajustes operacionais necessários para preservar a continuidade dos serviços.

Sempre que identificadas alterações nas condições operacionais da infraestrutura ou degradações capazes de comprometer o desempenho da rede corporativa, a CONTRATADA deverá promover imediatamente os ajustes técnicos necessários, preservando os critérios de disponibilidade, desempenho e segurança estabelecidos neste Termo de Referência.

Todas as alterações de configuração deverão observar os procedimentos de gerenciamento de mudanças previstos na contratação, permanecendo integralmente registradas para fins de auditoria e fiscalização.

Compete à CONTRATADA administrar integralmente a infraestrutura SD-WAN.

As atividades compreenderão:

- criação de políticas;
- alteração de políticas;

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

- gerenciamento dos túneis;
- configuração dos roteamentos;
- gerenciamento das VPNs;
- definição de prioridades;
- otimização do tráfego;
- monitoramento dos enlaces;
- gerenciamento da redundância;
- gerenciamento do balanceamento.

56. GESTÃO CENTRALIZADA DA INFRAESTRUTURA

Toda a infraestrutura objeto desta contratação deverá operar sob plataforma única de gerenciamento centralizado, permitindo administração integrada de todos os equipamentos, enlaces, serviços e componentes tecnológicos disponibilizados para atendimento da SEGUP.

A solução deverá possibilitar gerenciamento remoto dos ativos, provisionamento de configurações, atualização de software e firmware, diagnóstico operacional, administração dos equipamentos de comunicação, gerenciamento das políticas de segurança, controle das versões de configuração, inventário automático da infraestrutura, acompanhamento das alterações realizadas e manutenção do histórico completo das intervenções executadas.

O gerenciamento centralizado deverá permitir atuação remota da equipe técnica da CONTRATADA, reduzindo o tempo de resposta aos incidentes, aumentando a eficiência operacional e minimizando a necessidade de deslocamentos para atendimento presencial, sem prejuízo da realização de intervenções em campo sempre que tecnicamente necessárias.

Considerando a natureza emergencial da contratação, a gestão unificada da infraestrutura deverá assegurar elevada disponibilidade dos serviços, rápida recuperação de falhas e padronização operacional de todos os componentes da solução, contribuindo para a continuidade das atividades críticas desenvolvidas pela SEGUP.

Toda a solução deverá operar sob gerenciamento unificado.

A administração centralizada deverá permitir:

- configuração remota;
- atualização remota;
- gerenciamento remoto;
- diagnóstico remoto;
- inventário automático;
- provisionamento remoto;
- auditoria;
- rastreabilidade;
- controle de versões;

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

- histórico de alterações.

57. AUDITORIA OPERACIONAL

A solução deverá possuir mecanismos permanentes de auditoria operacional capazes de registrar automaticamente todas as atividades administrativas, operacionais e técnicas executadas sobre a infraestrutura contratada.

Os registros deverão abranger qualquer alteração realizada nos equipamentos, políticas de segurança, configurações da rede, plataformas SD-WAN, Firewalls, mecanismos de proteção cibernética, sistemas de gerenciamento e demais componentes da solução, permitindo rastreabilidade integral das operações realizadas durante toda a execução contratual.

Cada evento registrado deverá conter informações suficientes para identificação do responsável pela operação, data e horário da execução, endereço IP de origem, equipamento ou serviço afetado, descrição da alteração realizada, parâmetros modificados, justificativa técnica quando aplicável e resultado da operação executada.

Os registros de auditoria deverão permanecer protegidos contra exclusão ou alteração não autorizada, preservando sua integridade, autenticidade e disponibilidade durante toda a vigência contratual e pelo período legal aplicável, permitindo sua utilização em procedimentos de fiscalização, auditorias internas, órgãos de controle, investigações administrativas e processos de apuração de responsabilidades.

A plataforma deverá disponibilizar mecanismos de consulta, pesquisa e exportação dos registros de auditoria, permitindo à fiscalização da SEGUP acompanhar o histórico completo das atividades executadas sobre a infraestrutura, reforçando os princípios da transparência, rastreabilidade, governança e segurança da informação que orientam a execução desta contratação emergencial.

A solução deverá registrar automaticamente todas as atividades administrativas.

Os registros deverão conter:

- usuário;
- data;
- horário;
- endereço IP;
- operação realizada;
- equipamento alterado;
- configuração modificada.

Os registros deverão permanecer disponíveis durante toda a vigência contratual e pelo período legal aplicável, permitindo rastreabilidade integral das operações.

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

58. INDICADORES DE DESEMPENHO OPERACIONAL

A CONTRATADA deverá acompanhar, no mínimo, os seguintes indicadores (KPIs):

Indicador	Meta Mínima
Disponibilidade da rede	≥ 99,70%
Disponibilidade da plataforma de gerenciamento	≥ 99,90%
Disponibilidade do portal de gestão	≥ 99,90%
Disponibilidade do SD-WAN	≥ 99,90%
Disponibilidade do Firewall UTM/NGFW	≥ 99,90%
Disponibilidade do serviço Anti-DDoS	≥ 99,95%
Tempo de abertura automática de incidente	≤ 5 minutos
Atualização dos dashboards	Tempo real ou intervalo máximo de 5 minutos
Inventário automatizado	Atualização diária ou sob alteração detectada

59. RESPONSABILIDADE DA CONTRATADA

Compete à CONTRATADA assegurar o funcionamento permanente do Centro de Operações de Rede, da Plataforma de Monitoramento, do Portal de Gestão, da Administração Centralizada da solução SD-WAN, dos mecanismos de monitoramento, inventário automatizado, geração de relatórios e dashboards executivos, responsabilizando-se pela continuidade operacional, integridade das informações, disponibilidade dos sistemas de gerenciamento e atendimento aos níveis de serviço estabelecidos neste Termo de Referência.

REQUISITOS DE CIBERSEGURANÇA – FIREWALL UTM/NGFW, IPS, IDS, VPN, CONTROLE DE APLICAÇÕES, WEB FILTER, ANTIVÍRUS, ANTISPAM, INSPEÇÃO SSL, PROTEÇÃO ANTI-DDOS, CRIPTOGRAFIA, ALTA DISPONIBILIDADE, HARDENING, GESTÃO DE CERTIFICADOS, LOGS DE SEGURANÇA E CONFORMIDADE

60. OBJETIVO

A solução deverá incorporar mecanismos avançados de cibersegurança destinados à proteção da infraestrutura de comunicação de dados da Secretaria de Estado de Segurança Pública e Defesa Social – SEGUP, assegurando confidencialidade, integridade, disponibilidade, autenticidade e rastreabilidade das informações trafegadas pela rede corporativa.

Todos os componentes de segurança deverão operar de forma integrada, sob gerenciamento centralizado, permitindo administração unificada das políticas de segurança, monitoramento contínuo dos eventos, resposta automatizada a incidentes e conformidade com a Política de Segurança da Informação da CONTRATANTE.

61. FIREWALL UTM / NGFW

61.1 Requisitos Gerais

Os equipamentos Firewall deverão ser do tipo **Next Generation Firewall (NGFW)**, com funcionalidades integradas de Unified Threat Management (UTM), operando em appliance dedicado ou equipamento virtual homologado pelo fabricante.

A solução deverá possuir gerenciamento unificado das funcionalidades de segurança, permitindo a aplicação de

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

políticas por usuário, aplicação, serviço, dispositivo, endereço IP, grupos ou zonas de segurança.

61.2 Funcionalidades Mínimas

Os equipamentos deverão suportar, simultaneamente:

- Firewall Stateful Inspection;
- Firewall de Próxima Geração (NGFW);
- Controle de Aplicações;
- Sistema de Prevenção de Intrusão (IPS);
- Sistema de Detecção de Intrusão (IDS);
- Antivírus de Gateway;
- AntiSpyware;
- AntiBot;
- AntiSpam;
- Web Filter;
- DNS Security;
- Inspeção SSL/TLS;
- VPN IPsec;
- VPN SSL;
- NAT;
- QoS;
- Alta Disponibilidade (HA);
- Balanceamento de carga;
- Segmentação por zonas;
- Controle por identidade de usuário;
- Integração com serviços de diretório.

62. POLÍTICAS DE FIREWALL

A solução deverá permitir a criação de políticas baseadas em:

- endereço IP;
- sub-redes;
- VLAN;
- usuários;
- grupos;
- aplicações;
- protocolos;
- portas;
- geolocalização;

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

- reputação;
- horários;
- interfaces;
- zonas de segurança.

As regras deverão admitir priorização, comentários, versionamento e histórico de alterações.

63. SISTEMA DE PREVENÇÃO DE INTRUSÃO – IPS

A solução deverá incorporar mecanismo de **Intrusion Prevention System (IPS)** com inspeção em linha (inline), capaz de analisar o tráfego em tempo real e bloquear automaticamente tentativas de exploração de vulnerabilidades.

Deverá contemplar, no mínimo:

- detecção baseada em assinaturas;
- detecção baseada em comportamento;
- proteção contra exploits conhecidos;
- proteção contra ataques de dia zero suportados por inteligência do fabricante;
- atualização automática das assinaturas;
- perfis configuráveis por política;
- exceções controladas;
- geração de alertas e registros.

64. SISTEMA DE DETECÇÃO DE INTRUSÃO – IDS

A solução deverá disponibilizar mecanismo de **Intrusion Detection System (IDS)** para identificação de atividades suspeitas, tentativas de invasão e comportamentos anômalos.

O IDS deverá:

- monitorar o tráfego de rede;
- gerar alertas em tempo real;
- registrar evidências dos eventos;
- classificar a severidade das ocorrências;
- permitir integração com ferramentas de gerenciamento de eventos de segurança (SIEM), quando adotadas pela CONTRATANTE.

65. CONTROLE DE APLICAÇÕES

A solução deverá identificar aplicações independentemente de:

- porta utilizada;
- protocolo;
- endereço IP;
- método de encapsulamento.

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

Deverá possibilitar:

- permitir aplicações;
- bloquear aplicações;
- limitar banda por aplicação;
- priorizar aplicações críticas;
- aplicar políticas por usuário, grupo ou unidade.

A base de aplicações deverá ser mantida permanentemente atualizada pelo fabricante.

66. FILTRAGEM DE CONTEÚDO (WEB FILTER)

A solução deverá possuir mecanismo de filtragem de conteúdo Web baseado em categorias, reputação e análise dinâmica.

Deverá permitir:

- bloqueio de categorias de sites;
- listas de permissão (whitelist);
- listas de bloqueio (blacklist);
- políticas por usuário;
- políticas por grupos;
- políticas por horário;
- inspeção de URLs;
- bloqueio de páginas maliciosas;
- proteção contra phishing;
- proteção contra malware hospedado em páginas web.

67. ANTIVÍRUS DE GATEWAY

O mecanismo antivírus deverá realizar inspeção do tráfego de entrada e saída da rede corporativa.

Deverá suportar inspeção dos principais protocolos utilizados pela solução, identificando e bloqueando códigos maliciosos antes de sua entrega aos usuários.

As bases antivírus deverão permanecer permanentemente atualizadas, de forma automática, durante toda a vigência contratual.

68. ANTISPAM

A solução deverá disponibilizar mecanismos de proteção contra mensagens eletrônicas indesejadas e campanhas maliciosas, quando aplicável ao ambiente contratado.

Os mecanismos deverão contemplar:

- reputação de remetentes;
- listas de bloqueio;
- análise heurística;

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

- detecção de phishing;
- detecção de spoofing;
- proteção contra URLs maliciosas;
- análise de anexos.

69. INSPEÇÃO SSL/TLS

Os equipamentos deverão permitir inspeção de conexões criptografadas mediante políticas definidas pela CONTRATANTE.

A solução deverá:

- suportar inspeção SSL inbound e outbound;
- utilizar certificados digitais específicos para inspeção;
- permitir exclusões por categoria, aplicação ou destino;
- preservar a rastreabilidade das conexões analisadas.

70. REDES PRIVADAS VIRTUAIS – VPN

A solução deverá suportar redes privadas virtuais para comunicação segura entre unidades da SEGUP e acesso remoto autorizado.

Deverá oferecer, no mínimo:

- VPN IPsec Site-to-Site;
- VPN SSL para acesso remoto;
- autenticação multifator quando aplicável;
- criptografia robusta;
- gerenciamento centralizado;
- políticas de acesso por perfil de usuário;
- registro completo das conexões estabelecidas.

71. PROTEÇÃO ANTI-DDOS

A solução deverá incorporar mecanismos permanentes de proteção contra ataques distribuídos de negação de serviço (DDoS), preservando a disponibilidade dos serviços corporativos.

Deverá ser capaz de detectar e mitigar automaticamente:

- ataques volumétricos;
- SYN Flood;
- UDP Flood;
- ICMP Flood;
- DNS Amplification;
- NTP Amplification;

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

- Reflection Attacks;
- HTTP Flood;
- HTTPS Flood;
- ataques às camadas de aplicação.

Sempre que identificado ataque, a solução deverá iniciar automaticamente os mecanismos de mitigação, registrando todas as ações executadas.

72. CRIPTOGRAFIA

Todos os mecanismos criptográficos utilizados deverão adotar algoritmos reconhecidos internacionalmente e considerados seguros pelo estado da técnica.

A solução deverá suportar protocolos seguros para administração, autenticação, comunicação e estabelecimento de túneis VPN, observando as melhores práticas de segurança da informação.

73. ALTA DISPONIBILIDADE

Os equipamentos de segurança deverão suportar operação em Alta Disponibilidade (High Availability – HA), quando aplicável à arquitetura implantada.

A solução deverá permitir:

- redundância ativa/passiva ou ativa/ativa;
- sincronização automática de configurações;
- sincronização de sessões compatível com o equipamento;
- failover automático;
- retorno controlado (failback);
- monitoramento do estado dos nós.

74. HARDENING

Antes da entrada em produção, todos os equipamentos deverão passar por processo de hardening, contemplando, no mínimo:

- remoção de contas padrão;
- alteração de credenciais iniciais;
- desativação de serviços desnecessários;
- restrição de portas administrativas;
- atualização para versões suportadas;
- aplicação das recomendações do fabricante;
- sincronização de horário;
- configuração de logs;
- políticas seguras de autenticação.

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

75. GESTÃO DE CERTIFICADOS DIGITAIS

A solução deverá permitir gerenciamento centralizado dos certificados digitais utilizados pelos componentes de segurança.

Deverá contemplar:

- instalação;
- renovação;
- substituição;
- revogação;
- monitoramento da validade;
- alertas de expiração.

76. LOGS DE SEGURANÇA

Todos os eventos de segurança deverão ser registrados automaticamente.

Os registros deverão conter, no mínimo:

- data;
- hora;
- equipamento;
- usuário;
- endereço IP de origem;
- endereço IP de destino;
- aplicação;
- ação executada;
- política aplicada;
- nível de severidade;
- resultado da operação.

Os registros deverão permanecer protegidos contra alteração e exclusão não autorizada.

77. RETENÇÃO DOS LOGS

Os logs deverão permanecer disponíveis durante toda a vigência contratual e pelo período definido pela CONTRA-TANTE ou pela legislação aplicável.

A solução deverá permitir:

- pesquisa;
- exportação;
- auditoria;
- geração de evidências;
- rastreabilidade completa dos eventos.

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

78. ATUALIZAÇÕES DE SEGURANÇA

Durante toda a execução contratual, a CONTRATADA deverá fornecer, sem ônus adicional:

- atualizações de firmware;
- atualizações de software;
- patches de segurança;
- assinaturas IPS;
- assinaturas IDS;
- bases antivírus;
- bases AntiSpam;
- bases Web Filter;
- inteligência de ameaças disponibilizada pelo fabricante.

As atualizações deverão ser homologadas antes da aplicação em produção, sempre que houver risco de impacto operacional.

79. CONFORMIDADE

A solução deverá atender às diretrizes de segurança da informação estabelecidas pela CONTRATANTE e observar, quando aplicável:

- Lei Federal nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD);
- Lei Federal nº 14.133/2021;
- normas e boas práticas de segurança da informação adotadas pela Administração Pública;
- políticas internas de segurança da SEGUP.

A CONTRATADA deverá manter mecanismos que permitam auditoria, rastreabilidade e comprovação do cumprimento das políticas de segurança implementadas.

80. RESPONSABILIDADE DE SEGURANÇA

Compete à CONTRATADA manter todos os mecanismos de cibersegurança plenamente operacionais, assegurando a atualização tecnológica contínua, a proteção da infraestrutura de comunicação de dados, a disponibilidade dos serviços, a integridade das informações, a confidencialidade dos dados processados e a pronta resposta a incidentes de segurança, observando integralmente os requisitos técnicos, operacionais e de desempenho estabelecidos neste Termo de Referência.

81. OBRIGAÇÕES NA EXECUÇÃO

A CONTRATADA obriga-se a executar integralmente o objeto deste Termo de Referência, observando as disposições da Lei Federal nº 14.133/2021, da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), das normas técnicas aplicáveis, das políticas de segurança da informação da CONTRATANTE e das demais disposições legais pertinentes.

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

81.1 Execução dos Serviços

Compete à CONTRATADA:

I – executar os serviços em estrita conformidade com as especificações técnicas estabelecidas neste Termo de Referência;

II – disponibilizar todos os equipamentos, softwares, licenças, insumos, infraestrutura, materiais, ferramentas e demais recursos necessários à perfeita execução do objeto;

III – garantir o funcionamento ininterrupto da solução durante toda a vigência contratual;

IV – manter equipe técnica especializada em quantidade suficiente para atendimento da demanda contratada;

V – executar integralmente os serviços de instalação, ativação, configuração, integração, testes, homologação, operação assistida, monitoramento, gerenciamento e suporte técnico;

VI – responsabilizar-se por todos os custos diretos e indiretos necessários à execução contratual.

81.2 Equipe Técnica

A CONTRATADA deverá manter equipe técnica qualificada composta por profissionais compatíveis com os serviços contratados.

Os profissionais deverão possuir conhecimento técnico compatível com as tecnologias utilizadas na solução, incluindo comunicação de dados, SD-WAN, Firewall NGFW/UTM, VPN, segurança da informação, redes IP, roteamento, monitoramento e gerenciamento de infraestrutura.

Sempre que solicitado pela fiscalização, deverá ser apresentada a relação atualizada da equipe técnica responsável pela execução contratual.

81.3 Responsabilidade Técnica

A CONTRATADA será integralmente responsável:

- pela qualidade dos serviços;
- pela estabilidade operacional da solução;
- pela segurança lógica da infraestrutura sob sua administração;
- pela atualização tecnológica dos equipamentos fornecidos;
- pela manutenção preventiva e corretiva;
- pelo cumprimento dos níveis mínimos de serviço estabelecidos no SLA.

81.4 Equipamentos

Todos os equipamentos fornecidos deverão:

- estar em condições de uso;
- possuir procedência comprovada;
- estar homologados pela ANATEL, quando aplicável;
- estar em linha de fabricação ou plenamente suportados pelo fabricante durante toda a vigência contratual.

É vedado o fornecimento de equipamentos recondicionados, remanufaturados ou descontinuados sem autorização expressa da CONTRATANTE.

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

81.5 Atualizações Tecnológicas

Compete à CONTRATADA fornecer, sem qualquer custo adicional:

- atualizações de firmware;
- atualizações de software;
- patches;
- correções de segurança;
- novas assinaturas de segurança;
- atualizações de licenciamento;
- novas versões disponibilizadas pelo fabricante compatíveis com a solução implantada.

81.6 Continuidade dos Serviços

A CONTRATADA deverá adotar todas as medidas necessárias para assegurar a continuidade operacional dos serviços, mantendo infraestrutura, equipamentos, enlaces, licenças e equipes suficientes para evitar interrupções indevidas.

Na ocorrência de falhas, deverá iniciar imediatamente as ações de recuperação previstas no Plano de Contingência.

81.7 Suporte Técnico

A CONTRATADA deverá disponibilizar:

- Central de Atendimento;
- Portal Web;
- atendimento telefônico;
- abertura eletrônica de chamados;
- atendimento remoto;
- atendimento presencial quando necessário.

Todos os chamados deverão obedecer aos tempos máximos definidos no SLA.

81.8 Segurança da Informação

Compete à CONTRATADA:

- preservar o sigilo das informações;
- impedir acesso não autorizado;
- proteger credenciais administrativas;
- utilizar conexões seguras;
- adotar mecanismos de criptografia;
- manter registros de auditoria;
- comunicar imediatamente qualquer incidente de segurança.

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

81.9 Confidencialidade

Todas as informações obtidas durante a execução contratual deverão ser consideradas confidenciais.

A CONTRATADA responderá civil, administrativa e criminalmente pela divulgação indevida de informações protegidas.

A obrigação de confidencialidade permanecerá mesmo após o encerramento do contrato.

81.10 LGPD

Caso ocorra tratamento de dados pessoais, a CONTRATADA deverá observar integralmente a Lei Federal nº 13.709/2018.

Compete à CONTRATADA:

- proteger os dados tratados;
- restringir acessos;
- registrar operações de tratamento;
- comunicar incidentes de segurança;
- atender às orientações da CONTRATANTE na qualidade de Controladora dos dados.

81.11 Responsabilidade Trabalhista

Todos os encargos trabalhistas, previdenciários, fiscais, comerciais e tributários decorrentes da execução contratual serão de exclusiva responsabilidade da CONTRATADA, inexistindo vínculo empregatício entre seus empregados e a Administração Pública.

81.12 Responsabilidade Civil

A CONTRATADA responderá integralmente pelos danos causados à Administração ou a terceiros em decorrência de ação ou omissão de seus empregados, prepostos ou subcontratados, sem prejuízo das demais responsabilidades previstas em lei.

81.13 Comunicação com a Fiscalização

Toda comunicação técnica deverá ocorrer por meio formal, utilizando os canais definidos pela CONTRATANTE.

Sempre que solicitado, deverão ser apresentados:

- relatórios;
- evidências;
- logs;
- registros;
- documentação técnica;
- inventários;
- cronogramas;
- planos de ação.

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

82. OBRIGAÇÕES DA CONTRATANTE

Compete à CONTRATANTE:

I – disponibilizar as informações necessárias à execução contratual;

II – designar formalmente Fiscal Técnico, Fiscal Administrativo e Gestor do Contrato;

III – acompanhar e fiscalizar a execução contratual;

IV – comunicar formalmente as ocorrências verificadas;

V – disponibilizar acesso às dependências quando necessário à execução dos serviços;

VI – analisar os relatórios apresentados pela CONTRATADA;

VII – atestar a execução dos serviços efetivamente prestados;

VIII – efetuar os pagamentos na forma prevista no contrato;

IX – aplicar as penalidades cabíveis quando constatado descumprimento contratual;

X – aprovar previamente as janelas de manutenção programadas;

XI – homologar os serviços implantados após a realização dos testes de aceitação;

XII – comunicar à CONTRATADA alterações institucionais que possam impactar a execução contratual.

83. COOPERAÇÃO ENTRE AS PARTES

A CONTRATANTE e a CONTRATADA deverão manter relacionamento baseado na boa-fé objetiva, cooperação, transparência, eficiência e comunicação permanente, visando garantir a continuidade dos serviços essenciais de comunicação e segurança da informação.

84. VEDAÇÕES À CONTRATADA

É vedado à CONTRATADA:

- interromper os serviços sem autorização;
- alterar configurações sem anuência da fiscalização, exceto em situações emergenciais para restabelecimento dos serviços;
- compartilhar credenciais administrativas;
- divulgar informações obtidas durante a execução contratual;
- utilizar equipamentos ou softwares sem licenciamento válido;
- subcontratar integralmente o objeto contratado, sendo admitida apenas a subcontratação parcial, mediante prévia autorização da CONTRATANTE, nos termos estabelecidos neste Termo de Referência;
- utilizar a infraestrutura da CONTRATANTE para fins estranhos ao objeto contratual.

85. RESPONSABILIDADES COMPARTILHADAS

As partes deverão cooperar para:

- assegurar a continuidade dos serviços;
- preservar a disponibilidade da infraestrutura;

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

- garantir a segurança da informação;
- minimizar riscos operacionais;
- promover a melhoria contínua da solução;
- assegurar o cumprimento dos indicadores de desempenho estabelecidos no Acordo de Nível de Serviço (SLA).

86. DISPOSIÇÕES FINAIS DAS OBRIGAÇÕES

O descumprimento das obrigações previstas nesta Seção sujeitará a parte inadimplente às medidas administrativas, contratuais e legais cabíveis, observados o contraditório, a ampla defesa e as disposições da Lei Federal nº 14.133/2021.

FISCALIZAÇÃO DO CONTRATO, GESTÃO CONTRATUAL, MEDIÇÃO DOS SERVIÇOS, CRITÉRIOS DE ACEITAÇÃO, INDICADORES DE DESEMPENHO, GLOSAS POR DESCUMPRIMENTO DO SLA, HOMOLOGAÇÃO E RECEBIMENTO DOS SERVIÇOS

87. DA GESTÃO E FISCALIZAÇÃO DA EXECUÇÃO CONTRATUAL

A execução do Contrato será permanentemente acompanhada, controlada e fiscalizada pela Secretaria de Estado de Segurança Pública e Defesa Social – SEGUP, em conformidade com os arts. 117 a 140 da Lei Federal nº 14.133/2021, mediante designação formal de Gestor do Contrato, Fiscal Técnico, Fiscal Administrativo e, quando necessário, de outros agentes públicos ou equipe de fiscalização especialmente constituída.

A fiscalização contratual será exercida de forma preventiva, orientadora, corretiva e permanente, visando assegurar a adequada execução do objeto, a continuidade dos serviços essenciais, o cumprimento dos Acordos de Nível de Serviço (SLA), a conformidade técnica da infraestrutura implantada, a observância das obrigações contratuais e a correta aplicação dos recursos públicos.

A atuação da fiscalização compreenderá o acompanhamento da implantação da solução, da operação assistida, da execução dos serviços gerenciados, da manutenção preventiva e corretiva, da operação do Centro de Operações de Rede (NOC), da disponibilidade dos enlaces de comunicação, do funcionamento dos equipamentos de segurança cibernética, da plataforma SD-WAN, dos serviços de mitigação de ataques DDoS, da emissão dos relatórios gerenciais e da execução financeira do contrato.

A fiscalização exercida pela CONTRATANTE não exclui nem reduz a responsabilidade exclusiva da CONTRATADA pela perfeita execução do objeto contratado, permanecendo esta integralmente responsável pela qualidade dos serviços, pela disponibilidade da infraestrutura, pela segurança da informação e pelo cumprimento das obrigações assumidas.

88. DO GESTOR DO CONTRATO

O Gestor do Contrato será formalmente designado pela autoridade competente da SEGUP, competindo-lhe coordenar administrativamente a execução contratual, promover a integração entre a fiscalização técnica e administrativa e adotar as providências necessárias para assegurar o cumprimento das disposições contratuais.

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

Constituem, entre outras, atribuições do Gestor do Contrato:

- coordenar a execução administrativa do contrato;
- acompanhar o cumprimento do cronograma físico-financeiro;
- controlar os prazos contratuais e a vigência do ajuste;
- supervisionar a execução orçamentária e financeira;
- consolidar as informações encaminhadas pelos fiscais;
- promover reuniões periódicas de acompanhamento com a CONTRATADA;
- deliberar sobre demandas administrativas relacionadas à execução contratual;
- instruir processos de pagamento;
- propor a aplicação de glosas e penalidades, quando cabíveis;
- acompanhar a gestão dos riscos contratuais;
- encaminhar solicitações de alterações contratuais, apostilamentos ou termos aditivos, quando tecnicamente justificados;
- assegurar que a execução contratual permaneça alinhada às necessidades operacionais da SEGUP.

Durante toda a vigência da contratação emergencial, caberá ao Gestor do Contrato adotar as medidas necessárias para preservar a continuidade dos serviços essenciais, evitando descontinuidade da infraestrutura tecnológica utilizada pelos órgãos integrantes do Sistema Estadual de Segurança Pública.

89. DO FISCAL TÉCNICO

O Fiscal Técnico será responsável pelo acompanhamento permanente da execução operacional da solução, verificando a conformidade técnica dos serviços prestados e o atendimento às especificações estabelecidas neste Termo de Referência.

Compete ao Fiscal Técnico, entre outras atribuições:

- acompanhar a implantação da infraestrutura tecnológica;
- verificar o atendimento das especificações técnicas da solução;
- validar os Acordos de Nível de Serviço (SLA);
- acompanhar a execução das manutenções preventivas e corretivas;
- verificar a operação dos enlaces de comunicação;
- validar o funcionamento dos equipamentos fornecidos;
- acompanhar a operação da plataforma SD-WAN;
- fiscalizar os serviços de Firewall NGFW, VPN, IPS, IDS e Anti-DDoS;
- acompanhar os testes operacionais, funcionais e de contingência;
- analisar os relatórios técnicos emitidos pela CONTRATADA;
- acompanhar incidentes operacionais e eventos críticos;
- validar os indicadores de disponibilidade da infraestrutura;

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

- verificar a atualização tecnológica dos equipamentos;
- conferir os inventários da infraestrutura;
- validar as medições mensais dos serviços executados;
- emitir parecer técnico sobre a conformidade da execução contratual.

Sempre que identificadas não conformidades, o Fiscal Técnico poderá determinar a adoção imediata das medidas corretivas necessárias, comunicando formalmente o Gestor do Contrato.

90. DO FISCAL ADMINISTRATIVO

O Fiscal Administrativo será responsável pelo acompanhamento dos aspectos administrativos, documentais, financeiros e legais da execução contratual, prestando apoio ao Gestor do Contrato na verificação da regularidade da execução.

Compete ao Fiscal Administrativo:

- acompanhar a documentação contratual;
- controlar a vigência do contrato e dos instrumentos acessórios;
- acompanhar a manutenção da garantia contratual, quando exigida;
- verificar a regularidade fiscal, previdenciária e trabalhista da CONTRATADA;
- conferir a documentação apresentada para liquidação da despesa;
- acompanhar o faturamento mensal;
- verificar a conformidade dos documentos fiscais;
- controlar a aplicação de glosas e sanções administrativas;
- manter atualizado o registro das ocorrências administrativas;
- instruir os processos de pagamento;
- acompanhar eventuais pedidos de reajuste, reequilíbrio econômico-financeiro ou alterações contratuais.

91. DAS REUNIÕES DE ACOMPANHAMENTO CONTRATUAL

Durante toda a execução da contratação poderão ser realizadas reuniões técnicas e gerenciais entre representantes da CONTRATANTE e da CONTRATADA, com periodicidade definida pelo Gestor do Contrato ou sempre que houver necessidade operacional.

As reuniões terão como finalidade acompanhar a evolução da execução contratual, avaliar os indicadores de desempenho, verificar o cumprimento dos níveis de serviço, analisar riscos operacionais, tratar ocorrências relevantes, acompanhar os planos de ação, avaliar as manutenções executadas, analisar os relatórios gerenciais e planejar as atividades futuras.

As deliberações deverão ser formalizadas em ata, contendo, no mínimo:

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

- participantes;
- assuntos tratados;
- decisões adotadas;
- responsáveis pela execução das ações;
- prazos estabelecidos;
- pendências identificadas;
- providências futuras.

As atas integrarão o processo de fiscalização contratual.

92. DA MEDIÇÃO DOS SERVIÇOS

A medição dos serviços será realizada mensalmente, considerando a efetiva disponibilização da solução, o desempenho operacional da infraestrutura e o cumprimento das obrigações contratuais assumidas pela CONTRATADA.

A fiscalização avaliará a execução dos serviços com base nas informações obtidas por meio da plataforma de gerenciamento, dos sistemas de monitoramento, dos relatórios operacionais, dos registros do NOC e das demais evidências técnicas produzidas durante o período de referência.

A medição compreenderá, entre outros aspectos:

- disponibilidade da infraestrutura contratada;
- cumprimento dos Acordos de Nível de Serviço (SLA);
- funcionamento dos enlaces de comunicação;
- disponibilidade dos equipamentos instalados;
- operação da solução SD-WAN;
- funcionamento das soluções Firewall NGFW;
- disponibilidade do serviço de mitigação Anti-DDoS;
- monitoramento contínuo da infraestrutura;
- atendimento aos chamados técnicos;
- execução das manutenções preventivas e corretivas;
- entrega dos relatórios obrigatórios;
- atualização dos inventários e registros operacionais.

O resultado da medição servirá de base para emissão do atesto da execução, aplicação de glosas, cálculo da remuneração mensal e avaliação do desempenho contratual.

93. DOS CRITÉRIOS DE MEDIÇÃO DOS SERVIÇOS

A avaliação da execução contratual observará indicadores técnicos e operacionais compatíveis com a natureza dos serviços prestados, abrangendo toda a infraestrutura disponibilizada à SEGUP.

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

Infraestrutura de Comunicação

Serão avaliados, entre outros aspectos:

- disponibilidade dos enlaces de comunicação;
- estabilidade operacional da rede corporativa;
- desempenho da comunicação de dados;
- utilização da largura de banda;
- latência, perda de pacotes e qualidade dos circuitos;
- funcionamento dos mecanismos de redundância.

Equipamentos e Infraestrutura Tecnológica

Serão verificados:

- funcionamento integral dos equipamentos;
- disponibilidade dos ativos;
- atualização tecnológica;
- capacidade operacional instalada;
- integridade das configurações;
- conformidade com as especificações técnicas.

Segurança da Informação

A fiscalização avaliará o funcionamento e a eficácia das soluções de segurança, incluindo:

- Firewall NGFW;
- Sistema de Prevenção de Intrusão (IPS);
- Sistema de Detecção de Intrusão (IDS);
- Redes Privadas Virtuais (VPN);
- mitigação de ataques distribuídos de negação de serviço (Anti-DDoS);
- filtragem de conteúdo (Web Filter);
- mecanismos de proteção antimalware;
- controle de aplicações;
- políticas de segurança implantadas.

Serviços Gerenciados

Também serão considerados:

- qualidade do suporte técnico especializado;
- execução das manutenções preventivas e corretivas;

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

- operação assistida;
- gerenciamento remoto da infraestrutura;
- monitoramento contínuo da solução;
- atuação do Centro de Operações de Rede (NOC);
- atendimento dos prazos estabelecidos para resposta e solução dos chamados.

Os indicadores apurados constituirão referência para avaliação da qualidade da execução contratual, emissão dos atestos mensais, aplicação de glosas, eventual incidência de penalidades e acompanhamento da evolução da prestação dos serviços durante toda a vigência da contratação emergencial.

94. INDICADORES DE DESEMPENHO (KPIs)

Os serviços serão avaliados mediante indicadores objetivos.

Indicador	Meta
Disponibilidade dos enlaces	≥ 99,70%
Disponibilidade do SD-WAN	≥ 99,90%
Disponibilidade do Firewall	≥ 99,90%
Disponibilidade do Anti-DDoS	≥ 99,95%
Atendimento inicial aos chamados críticos	≤ 15 minutos
Restabelecimento de incidente crítico	≤ 4 horas
Atualização das assinaturas de segurança	Conforme fabricante
Entrega dos relatórios mensais	Até o 5º dia útil

95. DAS EVIDÊNCIAS DA EXECUÇÃO CONTRATUAL

95.1 Comprovação da Execução dos Serviços

A CONTRATADA deverá disponibilizar, durante toda a vigência contratual, evidências técnicas suficientes para comprovar a efetiva prestação dos serviços, o cumprimento das obrigações assumidas e a observância dos níveis de desempenho estabelecidos neste Termo de Referência.

As evidências deverão ser produzidas preferencialmente de forma automatizada pelos sistemas de gerenciamento, monitoramento e operação da infraestrutura, permitindo à fiscalização da Secretaria de Estado de Segurança Pública e Defesa Social – SEGUP verificar, de maneira objetiva e rastreável, a execução contratual.

Poderão ser utilizados como elementos comprobatórios, entre outros:

- relatórios gerenciais emitidos automaticamente pela plataforma de gerenciamento;
- dashboards executivos;
- registros de monitoramento da infraestrutura;
- logs operacionais dos equipamentos e sistemas;
- inventário atualizado dos ativos;
- registros dos chamados técnicos;

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

- relatórios de manutenção preventiva e corretiva;
- relatórios de disponibilidade dos enlaces e equipamentos;
- registros operacionais do Centro de Operações de Rede (NOC);
- histórico das atualizações tecnológicas realizadas;
- registros de auditoria;
- demais documentos que evidenciem a execução dos serviços.

Sempre que entender necessário, a fiscalização poderá solicitar informações, documentos ou evidências complementares para validação da execução contratual.

96. DOS CRITÉRIOS DE ACEITAÇÃO DOS SERVIÇOS

Os serviços objeto desta contratação somente serão considerados aceitos quando executados em estrita conformidade com as especificações técnicas, requisitos funcionais, níveis mínimos de desempenho e condições estabelecidas neste Termo de Referência e no Contrato.

A aceitação dependerá da verificação de que a solução permanece integralmente operacional, com disponibilidade compatível com os Acordos de Nível de Serviço (SLA), inexistência de falhas críticas pendentes, documentação técnica atualizada, inventário consistente e pleno funcionamento de todos os componentes da infraestrutura.

A homologação técnica realizada pela fiscalização da SEGUP constitui requisito indispensável para caracterização da conformidade dos serviços, não afastando a responsabilidade da CONTRATADA por defeitos, falhas ocultas ou vícios posteriormente identificados.

97. DA HOMOLOGAÇÃO DA IMPLANTAÇÃO

Concluída a implantação da solução ou de qualquer expansão relevante da infraestrutura contratada, será iniciado processo formal de homologação técnica, destinado a verificar a conformidade da solução com as especificações estabelecidas neste Termo de Referência.

Durante essa etapa, a fiscalização realizará testes técnicos e operacionais destinados a validar o funcionamento integral da solução, incluindo testes funcionais, operacionais, desempenho da rede, redundância dos enlaces, mecanismos de alta disponibilidade, políticas de segurança da informação, serviços SD-WAN, Firewall NGFW, proteção Anti-DDoS, procedimentos de failover, recuperação operacional e demais funcionalidades previstas para a infraestrutura.

Somente após a aprovação integral dos testes será emitido o respectivo Termo de Homologação Técnica, autorizando o início da operação definitiva da solução.

98. DO PROCEDIMENTO DE HOMOLOGAÇÃO

O procedimento de homologação compreenderá avaliação técnica completa da infraestrutura implantada, contemplando, no mínimo:

- inspeção física dos equipamentos instalados;

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

- conferência das configurações implantadas;
- validação das políticas de segurança da informação;
- verificação da operação dos enlaces de comunicação;
- validação da plataforma SD-WAN;
- testes funcionais do Firewall NGFW;
- validação do serviço de mitigação de ataques DDoS;
- conferência da documentação técnica entregue;
- validação do inventário atualizado da infraestrutura;
- análise dos primeiros relatórios operacionais emitidos pela plataforma de gerenciamento.

A homologação poderá ser parcial ou definitiva, conforme o estágio de implantação da solução e a avaliação da fiscalização.

99. DAS NÃO CONFORMIDADES

Sempre que forem identificadas inconformidades durante a implantação, operação, fiscalização ou homologação dos serviços, a CONTRATADA será formalmente notificada para promover as correções necessárias no prazo estabelecido pela fiscalização da SEGUP.

As não conformidades serão classificadas conforme sua criticidade e impacto sobre a continuidade dos serviços, podendo resultar na rejeição parcial ou total da etapa executada, aplicação de glosas, determinação de correções imediatas ou instauração dos procedimentos administrativos cabíveis.

Enquanto permanecerem pendências que comprometam a disponibilidade da infraestrutura, a segurança da solução ou o atendimento dos níveis mínimos de serviço, a Administração poderá deixar de homologar a etapa correspondente, sem prejuízo da aplicação das medidas contratuais cabíveis.

100. OBRIGAÇÕES DA CONTRATADA:

100.1 São obrigações da empresa Contratada:

100.2 A empresa Contratada deve garantir que os ambientes sejam mantidos em perfeitas condições de higiene e segurança durante e após a execução dos serviços.

100.3 Prestar os serviços na forma, no prazo e locais estabelecidos neste Termo de Referência e seus anexos.

100.4 Emitir Nota Fiscal ou recibo e enviá-la a SEGUP, onde informará o número do processo e contrato administrativo, seguindo, após, para os trâmites normais.

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

100.5 Orientar seus empregados para que exerçam comportamento exemplar durante sua permanência no local de trabalho, se portando de forma cordial com as demais pessoas, e ainda a apresentação individual deverá ocorrer dentro dos padrões de postura e higiene exigidos.

100.6 Manter os empregados uniformizados e de forma condizente com os serviços a executar, fornecendo-lhes uniformes em quantidades suficientes para se apresentarem dentro dos padrões recomendáveis, e ainda que estejam os empregados devidamente identificados, através do uso de crachás.

100.7 Prestar todos os esclarecimentos necessários, quando solicitado pelo fiscal do contrato, e ainda atendimento imediato às solicitações encaminhadas.

100.8 Substituir, às suas expensas, os prestadores de serviços, caso não se adequem às exigências do Órgão, ou substituí-los por outros motivos, se for o caso, a fim de que não surjam comprometimentos ao bom andamento dos trabalhos. Caso não se cumpra o exposto exigido neste subitem, o pagamento à empresa poderá não ser suspenso ou mesmo será realizado de forma proporcional, observando as aplicações das sanções previstas.

100.9 Responsabilizar-se pelo transporte de seu pessoal até as dependências do Contratante e vice-versa, por meios próprios, mesmo em caso de paralização dos transportes coletivos.

100.10 A Contratada se responsabilizará por eventuais prejuízos que possa causar ao Contratante, se deixar de cumprir com suas obrigações.

100.11 Reparar ou corrigir, às suas expensas, no todo ou em parte, quaisquer problemas em relação aos serviços previstos em contrato, em que se verifiquem vícios, defeitos ou incorreções.

100.12 Assumir a responsabilidade pelos encargos fiscais e comerciais resultantes dos serviços prestados.

100.13 Havendo atraso em pagamento de fatura por parte do Contratante, decorrentes de circunstâncias diretas, não exime a empresa de promover o pagamento dos empregados nas datas regulamentares.

101. .14 Cumprir rigorosamente o estabelecido neste Termo de Referência e seus anexos.

102. OBRIGAÇÕES DO CONTRATANTE:

102.1 São obrigações do Contratante:

102.2 Caberá a SEGUP fiscalizar de acordo com sua conveniência e no seu exclusivo interesse, o exato cumprimento das cláusulas e condições estabelecidas no Contrato.

102.3 A SEGUP será responsável pelo fornecimento de toda a infraestrutura necessária para instalação e funcionamento dos equipamentos, como local físico, tomadas elétricas (caso a contratada necessite de estabilizador o fornecimento deverá ser realizado pela própria contratada), pontos de acesso à rede.

102.4 Proporcionar as facilidades necessárias visando à execução dos serviços, dentro das normas estabelecidas.

102.5 Exercer permanente fiscalização da execução dos serviços, registrando as ocorrências relacionadas com a execução do objeto contratado, transmitindo aos prestadores as normas, diretrizes e demais determinações que o Órgão expedir, inclusive notificando as imperfeições, falhas e irregularidades constatadas, determinando as medidas corretivas necessárias. Essa fiscalização será efetuada por servidor do Núcleo de Telemática da SEGUP, designado por meio de portaria.

102.6 Efetuar os pagamentos devidos, na forma convencionada no instrumento contratual, dentro do prazo previsto.

Processo: 2026/3271696 | **Sequencial:** 81 | **Autenticação:** 72d3b5be-ae41-46e6-b494-b075fab33221
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:54

102.7 Prestar as informações e os esclarecimentos atinentes ao objeto que venham a ser solicitadas pela Contratada.

102.8 Promover o pagamento na forma e no prazo estipulado em contrato.
102.9 Emissão da Nota de Empenho.

102.10 Fazer o aceite das notas fiscais/recibos, referentes aos serviços prestados, de acordo com o especificado em Termo de Referência e Contrato, para efeito de pagamento.

102.11 Relatar à Coordenadoria de Contratos / Diretoria de Administração e Finanças, quaisquer tipos de ocorrências relacionadas à prestação dos serviços, através de memorando e relatório de fiscalização.

102.12 Quaisquer ocorrências e/ou irregularidades nas prestações dos serviços, será relatada ao fiscal do contrato, que imediatamente entrará em contato com a empresa, visando à equação do problema.

102.13 Sugerir melhorias para melhor execução do contrato.

16. VALIDADE DA PROPOSTA

16.1 As propostas deverão ter validade mínima de 60 (sessenta) dias corridos, a contar da data de abertura das propostas.

17. FISCAL DO CONTRATO E RESPONSÁVEL PELO ACOMPANHAMENTO, TELEFONE E E-MAIL: (91) 98231-7068 – coinfo.nt@segup.pa.gov.br

17.1. O responsável pela verificação do material, pelo atesto das notas ficais, pela fiscalização do contrato e pelos eventuais pedidos de esclarecimentos sobre este termo de referência será efetuado, de segunda-feira a sexta-feira, no horário de 09:00h as 16:00h.

GOVERNO DO ESTADO DO PARÁ
Secretaria de Estado de Segurança Pública

ANEXO II
MODELO DE PROPOSTA COMERCIAL

A SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL

Prezados Senhores,

Apresentamos a V.Sª, nossa proposta de preços de fornecimento de bens_____, pelo preço global de R$__(_____), nos termos do Edital e seus Anexos e conforme especificações abaixo:

Item	Descrição	Marca	Und	Qtde	Valor Unitário	Valor Total

- O prazo de validade da proposta de preços é de 30 (trinta) dias corridos, contados da data da abertura da Dispensa Eletrônica;
- Declaramos que estamos de pleno acordo com todas as condições estabelecidas no Edital e seus Anexos, bem como aceitamos todas as obrigações e responsabilidades especificadas no Termo de Referência;
- Declaramos que nos preços cotados estão incluídas todas as despesas que, direta ou indiretamente, fazem parte do presente objeto, tais como gastos da empresa com suporte técnico e administrativo, impostos, seguros, taxas, ou quaisquer outros que possam incidir sobre gastos da empresa, sem quaisquer acréscimos em virtude de expectativa inflacionária e deduzidos os descontos eventualmente concedidos;
- Caso nos seja adjudicado o objeto da Dispensa Eletrônica, comprometemos a assinar o Contrato no prazo determinado no documento de convocação, e para esse fim fornecemos os seguintes dados:

Razão Social: _____
CNPJ/MF: _____
Endereço:_____

Tel:_____(Conter obrigatoriamente pelo menos uma linha fixa)

Cidade:_____UF:___CEP: _____

SECRETARIA DE SEGURANÇA PÚBLICA E DEFESA SOCIAL

GOVERNO DO ESTADO DO PARÁ

SECRETÁRIA ADJUNTA DE GESTÃO ADMINISTRATIVA
COORDENADORIA DE CONTRATOS

CONTRATO ADMINISTRATIVO Nº XXX/2026-SEGUP/PA

CONTRATO QUE ENTRE SI CELEBRAM O ESTADO DO PARÁ, POR MEIO DA **SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL/SEGUP**, E A EMPRESA **XXXXXXXXXXX**, DA FORMA COMO ABAIXO MELHOR SE INFERE.

O ESTADO DO PARÁ, por meio da **SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL/SEGUP**, com sede nesta cidade, Tv. do Chaco, nº 2271, Bairro: Marco, inscrita no CNPJ/MF sob o nº. 05.054.952/0001-01, neste ato representa da pelo Secretário Adjunto de Gestão Administrativa, **Sr. RENAN HENRIQUE NABOR DE OLIVEIRA**, brasileiro, inscrito sob a matrícula funcional n° 5977679/3, nomeado por Decreto Estadual publicado na página 5, do DOE nº 36.494, doravante denominado **CONTRATANTE**, e a empresa **XXXXXXXXX**, inscrita no CNPJ/MF sob o nº XXXXXXXXX, com sede naXXXXXXXXXXXXX, E-mail:XXXXXXXXXXX, Telefone: XXXXXXXXXXX, neste ato representada pela **Sra.XXXXXXXXXXXXX**, brasileira, CARGO: XXXXXXX, conforme atos constitutivos da empresa ou procuração apresentada nos autos, doravante denominada **CONTRATADA**, tendo em vista o que consta no **Processo Eletrônico n.º 2026/3271696** e em observância às disposições da Lei nº 14.133, de 1º de abril de 2021, e demais legislação aplicável, resolvem celebrar o presente Contrato, decorrente da **DISPENSA ELETRÔNICA Nº XXX/2026 - SEGUP/PA**, mediante as cláusulas e condições a seguir enunciadas.

CLÁUSULA PRIMEIRA – DO OBJETO

1.1. O presente contrato tem como objeto a Contratação Emergencial de Empresa Especializada na Prestação Continuada de Serviços de Comunicação Corporativa de Dados.

1.2. Vinculam esta contratação, independentemente de transcrição:

1.2.1. O Termo de Referência;

1.2.2. O Edital da Dispensa Eletrônica;

1.2.3. A Proposta da Contratada;

1.2.4. Eventuais anexos dos documentos supracitados.

Processo: 2026/3271696 | **Sequencial:** 89 | **Autenticação:** caa1fe29-0e5c-4f22-b4c3-02f798c7e38b
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:57

CLÁUSULA SEGUNDA – DA VINCULAÇÃO AO EDITAL DE LICITAÇÃO

2.1. Este contrato é oriundo da **DISPENSA ELETRÔNICA N° XXX/2026- SEGUP/PA**, referente ao **Processo Eletrônico n.º 2026/3271696**, possuindo fundamentação nas disposições contidas na seguinte legislação: Lei Federal n.º 14.133/21, art. 75, inciso VIII (Lei de Licitações e Contratos Administrativos); Decreto Estadual n. 2.787/22 (institui o Sistema de Dispensa Eletrônica, no âmbito da Administração Pública Estadual Direta, Autárquica e Fundacional); subsidiariamente a Lei n.º 8.078/90 (Dispõe sobre a proteção do consumidor); Lei n.° 13.709/18 (Lei Geral de Proteção de Dados Pessoais - LGPD); e a Portaria nº 074/2026 - GAB/SEGUP, de 12 de janeiro de 2026 (DOE nº 36.496, de 14 de janeiro de 2026), aos quais CONTRATANTE e CONTRATADA estão sujeitas;

2.2. De acordo com a **Portaria nº 071/2026 - GAB.SEC/SEGUP, de 12 de janeiro de 2026 (DOE nº 36.496, de 14 de janeiro de 2026)**, o Secretário Adjunto de Gestão Administrativa tem competência para assinar este Contrato e seus documentos decorrentes em nome desta Secretaria, como Ordenador de Despesas.

CLÁUSULA TERCEIRA – DA VIGÊNCIA E PRORROGAÇÃO

3.1. O presente Contrato terá seu prazo de vigência de **06 (seis) meses**, a contar da data de assinatura do contrato, na forma disposta no art. 75, inciso VIII e art. 105 da Lei Federal n.º 14.133/21;

3.2. O prazo de vigência será prorrogado conforme os termos do art. 75, inciso VIII da Lei Federal n.º 14.133/21.

CLÁUSULA QUARTA - DO PREÇO E DESCRIÇÃO

4.1. O valor global do presente contrato é de **R$ XXXXX**, no qual já estão incluídas todas as despesas especificadas na proposta da CONTRATADA;

4.2. Descrição do objeto conforme especificações abaixo:

ITEM	DESCRIÇÃO	QTD.	VALOR UNITÁRIO	VALOR TOTAL
01	**SERVIÇO DE COMUNICAÇÃO 50 MBPS + UTM SDWAN TIPO B + TIPO E + GERÊNCIA DE REDES**, conforme quantidade, condições e especificações contidas no Termo de Referência, na Proposta da Contratada, no Edital e seus demais anexos.	19 UND	R$ xxx	R$ xxx

02	**SERVIÇO DE COMUNICAÇÃO 500 MBPS + UTM SD-WAN TIPO E + CPE + GERÊNCIA DE REDES + PROTEÇÃO DDOS**, conforme quantidade, condições e especificações contidas no Termo de Referência, na Proposta da Contratada, no Edital e seus demais anexos.	1 UND	R$ xxx	R$ xxx
03	**SERVIÇO DE COMUNICAÇÃO 1 GBPS + UTM SDWAN TIPO F + CPE + GERÊNCIA DE REDES + PROTEÇÃO DDOS**, conforme quantidade, condições e especificações contidas no Termo de Referência, na Proposta da Contratada, no Edital e seus demais anexos.	1 UND	R$ xxx	R$ xxx
VALOR GLOBAL R$ xxxxxxxxxxxxx				

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

CLÁUSULA QUINTA – DA EXECUÇÃO

5.1. DOS PRAZOS:

5.1.1. Ocorrerá mediante emissão de Ordem de Serviço ou instrumento equivalente, compreendendo implantação, configuração, integração, ativação, testes, homologação técnica e operação assistida, conforme este Termo de Referência. A execução deverá ocorrer de forma coordenada com a equipe técnica da SEGUP, preservando a continuidade dos serviços essenciais.

5.2. DO LOCAL:

5.2.1. Os serviços de conectividade, monitoramento de rede (NOC), segurança perimetral, suporte técnico especializado e resolução de incidentes críticos serão prestados de forma contínua e ininterrupta, em regime de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana (24x7x360), observados os prazos do Acordo de Nível de Serviço (SLA) e tempos máximos de atendimento e reparo previstos no Termo de Referência;

5.2.2. As intervenções técnicas presenciais de rotina que dependam de acesso físico às instalações administrativas da SEGUP ocorrerão preferencialmente no horário das 09h às 16h, de segunda a sexta-feira, ressalvadas as janelas programadas de manutenção previamente autorizadas ou situações emergenciais de restauração dos serviços essenciais;

5.3. DAS CONDIÇÕES PARA RECEBIMENTO:

Processo: 2026/3271696 | **Sequencial:** 89 | **Autenticação:** caa1fe29-0e5c-4f22-b4c3-02f798c7e38b
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:57 **Página:** 3/19

5.3.1. A implantação e a ativação deverão ser concluídas no prazo máximo de até **30 (trinta) dias corrido**s. Após a implantação, serão realizados recebimento provisório, inspeção, testes, correção de inconformidades, homologação e recebimento definitivo, conforme os critérios estabelecidos no Termo de Referência.

CLÁUSULA SEXTA – DA GARANTIA CONTRATUAL

6.1. Fica a Contratada obrigada a prestar garantia, nos termos do art. 98 da Lei nº 14.133/21, no percentual de 5% (cinco por cento) do valor inicial do contrato, em uma das modalidades previstas no art. 96, §1, da mencionada lei, ficando retida até o término dos serviços.

CLÁUSULA SÉTIMA – DA SUBCONTRATAÇÃO

7.1. Será permitida a subcontratação parcial de atividades relacionadas à execução do objeto, desde que previamente autorizada pela CONTRATANTE, permanecendo vedada a subcontratação integral.

7.2. A CONTRATADA permanecerá integralmente responsável pelo cumprimento das obrigações contratuais e pela adequada execução dos serviços eventualmente subcontratados.

CLÁUSULA OITAVA – DA ASSISTÊNCIA TÉCNICA E DA GARANTIA DOS EQUIPAMENTOS

8.1. Durante o período contratual, é incumbida à CONTRATADA a responsabilidade de fornecer atendimento abrangente para garantir a operacionalidade contínua dos serviços, abordando necessidades de manutenção, correção e eventual substituição em caso de defeitos identificados;

8.2. Os equipamentos e componentes disponibilizados para a execução dos serviços deverão possuir garantia do fabricante durante toda a vigência contratual, quando aplicável, cabendo à CONTRATADA assegurar sua plena operacionalidade, manutenção, atualização e substituição em caso de falha ou defeito, sem ônus adicional para a CONTRATANTE.

CLÁUSULA NONA – DO PAGAMENTO

9.1. O pagamento será efetuado à Contratada em até **30 (trinta) dias corridos**, após o recebimento e aceitação definitiva do objeto contratado, por parte do servidor designado para

Processo: 2026/3271696 | **Sequencial:** 89 | **Autenticação:** caa1fe29-0e5c-4f22-b4c3-02f798c7e38b
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:57 **Página:** 4/19

proceder ao recebimento e conferência dos materiais, mediante a apresentação das certidões de regularidade com os tributos federais, estaduais e municipais pertinentes, do INSS e FGTS em vigência, do Recibo e/ou Nota Fiscal devidamente atestada para liquidação e pagamento da despesa pela Contratante;

9.1.1. O valor da fatura mensal estará sujeito à aplicação de glosas proporcionais decorrentes do não atendimento aos indicadores de desempenho e metas de disponibilidade estabelecidos no Acordo de Nível de Serviço (SLA) do Termo de Referência, apurados pelo Fiscal Técnico por meio dos relatórios de monitoramento e do Centro de Operações de Rede (NOC), assegurados o contraditório e a ampla defesa;

9.2. O pagamento acima referenciado será creditado em favor do fornecedor, através de ordem bancária, em conta corrente aberta, preferencialmente, no **Banco do Estado do Pará - BANPARÁ**, deixando bem claro pela CONTRATADA os números da respectiva agência e da conta corrente em que deverá ser efetivado o crédito;

9.3. Para fins de pagamento, a CONTRATADA deverá apresentar, juntamente com a Nota Fiscal os seguintes documentos, se exigidos pela CONTRATANTE:

a) Certidão Negativa de Débito do INSS, devidamente atualizada;

b) Certificado de Regularidade com o Fundo de Garantia por Tempo de Serviço - FGTS;

c) Certidão Conjunta de Regularidade com a Fazenda Federal (Quitação de Tributos e Contribuições Federais e Dívida Ativa da União da Fazenda Federal), Estadual e Municipal.

9.4. A não apresentação da Certidão Negativa de Débito do INSS, bem como do Certificado de Regularidade do FGTS e da Certidão Negativa de Débito (CND) relativa aos Tributos Federais, Estaduais e Municipais ou a irregularidade destas, não acarretará retenção do pagamento. Entretanto, a CONTRATADA será comunicada quanto à apresentação de tais documentos em até 30 (trinta) dias, sob pena de rescisão contratual e demais penalidades cabíveis;

9.5. Constatando-se a situação de irregularidade da Contratada, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do Contratante;

9.6. Não havendo regularização ou sendo a defesa considerada improcedente, a Contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à

Processo: 2026/3271696 | **Sequencial:** 89 | **Autenticação:** caa1fe29-0e5c-4f22-b4c3-02f798c7e38b
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:57 **Página:** 5/19

inadimplência da Contratada, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos;

9.7. Persistindo a irregularidade, a Contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à Contratada a ampla defesa e o contraditório;

9.8. Concomitante à notificação à CONTRATADA, para que realize a regularização, a CONTRATANTE oficiará a ocorrência ao INSS, no caso da CND, à Caixa Econômica Federal, no caso do CRF, e à Receita Federal, no caso de CND relativa aos Tributos Federais, Estaduais e Municipais;

9.9. Será rescindido o contrato em execução com a Contratada inadimplente, salvo por motivo de economicidade, segurança nacional ou interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da Contratante;

9.10. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a Contratada não regularize sua situação;

9.11. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável, em especial a prevista no art. 31 da Lei 8.212, de 1993, quando couber;

9.12. Caso o objeto deste Contrato seja recusado e/ou o documento fiscal apresente alguma incorreção, será considerado como não entregue e o prazo de pagamento será contado a partir da data de regularização, observado os prazos dispostos neste Contrato;

9.13. Quaisquer alterações nos dados bancários deverão ser comunicadas à CONTRATANTE, por meio de Carta, ficando sob inteira responsabilidade da CONTRATADA os prejuízos decorrentes de pagamentos incorretos devido à falta de informação;

9.14. Correrão por conta da CONTRATADA o ônus do prazo de compensação e todas as despesas bancárias decorrentes da transferência de crédito;

9.15. A CONTRATANTE efetuará as retenções dos tributos incidentes no faturamento, de acordo com a legislação vigente. O CNPJ, que deverá constar nas Notas Fiscais, deverá ser o mesmo CNPJ que a Contratada utilizou neste Contrato;

9.16. A CONTRATANTE não acatará a cobrança por meio de duplicatas ou qualquer outro título, em bancos ou outras instituições do gênero;

9.17. Os pagamentos efetuados pela CONTRATANTE não isentam a CONTRATADA de

Processo: 2026/3271696 | **Sequencial:** 89 | **Autenticação:** caa1fe29-0e5c-4f22-b4c3-02f798c7e38b
Acessado por: Larissa Coelho Bittencourt (CPF: ***.877.832-**) **em** 03/11/2026 **às** 10:57 **Página:** 6/19

suas obrigações e responsabilidades assumidas;

9.18. A qualquer tempo o órgão Contratante poderá solicitar a apresentação do CRF relativo ao FGTS, bem como, todos os demais documentos constantes da fase de habilitação.

9.19. No caso de eventual atraso de pagamento, desde que a(s) empresa(s) vencedora(s) não tenha(m) concorrido de alguma forma para tanto, fica convencionado que a taxa de atualização financeira devida pelo órgão solicitante, entre a data acima referida e a correspondente ao efetivo adimplemento da parcela, será mediante a aplicação da seguinte fórmula:

EM = I x N x VP

Onde:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela a ser paga; e

I = Índice de atualização financeira = 0,0001644, assim apurado:

$$I = \frac{TX/100}{365} = \frac{6/100}{365} = 0,0001644$$

TX = Percentual da taxa anual = 6%

9.20. Caso haja aplicação de multa, o valor será descontado de qualquer fatura ou crédito existente na Contratante, em favor do fornecedor. Caso o mesmo seja superior ao crédito eventualmente existente, a diferença será cobrada administrativamente ou judicialmente, senecessário;

9.21. Nenhum pagamento será efetuado à participante vencedora enquanto pendente de liquidação, qualquer obrigação financeira, em virtude de penalidade ou inadimplência contratual, sem que isso gere direito a reajustamento de preços.

CLÁUSULA DÉCIMA – DO REAJUSTE DE PREÇOS

10.1. Não haverá reajustamento nos preços propostos.

CLÁUSULA DÉCIMA PRIMEIRA – DO REEQUILIBRIO ECONÔMICO

MINUTA

11.1. Será admitido o requerimento de reestabelecimento do equilíbrio econômico-financeiro, cabendo a CONTRATANTE decidir a respeito no prazo de um mês, passível de prorrogação motivada por igual período, consoante teor do art. 123, p. único, da Lei Federal nº 14.133/21.

CLÁUSULA DÉCIMA SEGUNDA – DAS OBRIGAÇÕES DO CONTRATANTE

12.1. São obrigações do Contratante:

12.1.1. Providenciar a publicação do extrato do Contrato no Diário Oficial do Estado.

12.1.2. Fiscalizar e acompanhar a execução dos serviços constantes no objeto do Contrato;

12.1.3. Promover o recebimento do objeto, rejeitando o que estiver em desacordo com o exigido no Termo de Referência do Edital da **DISPENSA ELETRÓNICA Nº XXX/2026 - SEGUP/PA**;

12.1.4. Efetuar o pagamento do preço ajustado na forma, prazos e condições previstas neste instrumento contratual;

12.1.5. Designar servidor(es) para acompanhar a execução do Contrato;

12.1.6. Comunicar a Contratada toda e qualquer ocorrência relacionada com a execução do presente instrumento contratual;

12.1.7. Exigir o imediato afastamento de qualquer empregado ou preposto da Contratada que não mereça a sua confiança ou embarace a fiscalização ou ainda que se conduza de modo inconveniente ou incompatível com o exercício das funções que Ihe foram atribuídas;

12.1.8. Exigir o cumprimento de todas as obrigações assumidas pelo Contratado, de acordo com o Contrato e demais instrumentos que expressamente se vinculam;

12.1.9. Notificar a Contratada, por escrito, sobre vícios, defeitos ou incorreções verificadas na execução do objeto contratual, para que seja por ela substituído, reparado ou corrigido, no total ou em parte, às suas expensas;

12.1.10. Comunicar a empresa para emissão de Nota Fiscal no que for pertinente 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 dispõe o art. 143 da Lei nº 14.133/21;

12.1.11. Aplicar a Contratada as sanções previstas na lei e neste Contrato;

MINUTA

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

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

CLÁUSULA DÉCIMA TERCEIRA – DAS OBRIGAÇÕES DA CONTRATADA

13.1. A Contratada deve cumprir todas as obrigações constantes neste Contrato e demais instrumentos que expressamente se vinculam, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas:

13.1.1. Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo, quantidades e local constantes no presente instrumento contratual e seus anexos, acompanhado da respectiva nota fiscal/fatura/recibo;

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

13.1.3. Atender às determinações regulares emitidas pelo fiscal ou gestor do contrato ou autoridade superior (art. 137, II, da Lei n.º 14.133/21) e prestar todo esclarecimento ou informação por eles solicitados;

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

13.1.5. Responsabilizar-se pelas despesas de fretes, taxas e eventuais onerações que incidam sobre o objeto contratado;

13.1.6. Responsabilizar-se por quaisquer danos ou prejuízos causados, sejam por dolo ou culpa na execução do Contrato, relacionados com o objeto deste instrumento contratual, indenizando a Contratante, seus servidores e ou terceiros;

MINUTA

13.1.7. Assumir a responsabilidade por todas as providências e obrigações estabelecidas na legislação específica de acidentes de trabalho, quando, em ocorrência da espécie, forem vítimas os seus empregados no desempenho dos serviços ou em conexão com eles, ainda que acontecido nas dependências do Contratante;

13.1.8. Assumir todos os encargos de possível demanda trabalhista, cível ou penal, relacionada a essa contratação, originariamente ou vinculadas por prevenção, conexão ou continência;

13.1.9. Assumir responsabilidade pelos encargos fiscais e comerciais decorrentes da adjudicação que originou o presente Contrato;

13.1.10. Não subcontratar, transferir ou ceder a terceiro, no todo ou em parte, a execução do objeto deste Contrato, salvo a subcontratação parcial expressamente admitida na Cláusula Sétima deste instrumento e previamente autorizada pela CONTRATANTE;

13.1.11. Garantir que a ação ou omissão, total ou parcial, da fiscalização da Contratante, não eximirá a Contratada de total responsabilidade quanto ao cumprimento das obrigações;

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

13.1.13. Indicar preposto para representá-la durante a execução do contrato;

13.1.13.1. A indicação ou a manutenção do preposto da Contratada poderá ser recusada pela Contratante, desde que devidamente justificada, devendo a Contratada designar outro para o exercício da atividade.

13.1.14. Atender às determinações regulares emitidas pelo fiscal do contrato ou autoridade superior, consoante o disposto no art. 137, II, da Lei nº 14.133/21;

13.1.15. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com o Código de Defesa do Consumidor (Lei nº 8.078, de 1990), bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pela Contratante, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida no Edital, o valor correspondente aos danos sofridos;

13.1.16. Não contratar, durante a vigência do contrato, cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente da Contratante ou do fiscal ou gestor do contrato, nos termos do art. 48, parágrafo único, da Lei nº 14.133/21;

13.1.17. Quando não for possível a verificação da regularidade no Sistema de Cadastro de Fornecedores – SICAF, a Contratada deverá entregar ao setor responsável pela fiscalização do contrato, até o dia 30 (trinta) do mês seguinte ao da prestação dos serviços, os seguintes documentos:

13.1.17.1. Prova de regularidade relativa à Seguridade Social;

13.1.17.2. Certidão conjunta relativa aos tributos federais e à Dívida Ativa da União;

13.1.17.3. Certidões que comprovem a regularidade perante a Fazenda Municipal ou Distrital do domicílio ou sede do contratado;

13.1.17.4. Certidão de Regularidade do FGTS – CRF; e

13.1.17.5. Certidão Negativa de Débitos Trabalhistas – CNDT.

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

13.1.19. Promover a guarda, manutenção e tudo o que for necessário à execução do objeto, durante a vigência do contrato;

13.1.20. 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;

13.1.21. Submeter previamente, por escrito, a Contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo ou instrumento congênere;

13.1.22. 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;

13.1.23. 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, consoante o disposto no art. 116, da Lei nº 14.133/21;

MINUTA

13.1.24. Comprovar a reserva de cargos a que se refere ao subitem 13.1.23 acima, no prazo fixado pelo fiscal do contrato, com a indicação dos empregados que preencheram as referidas vagas, conforme disposto no art. 116, parágrafo único. da Lei nº 14.133/21;

13.1.25. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do presente instrumento contratual;

13.1.26. 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, da Lei nº 14.133/21;

13.1.27. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança do Contratante.

CLÁUSULA DÉCIMA QUARTA – DA LEI GERAL DE PROTEÇÃO DE DADOS

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

CLÁUSULA DÉCIMA QUINTA – DAS SANÇÕES ADMINISTRATIVAS

15.1. Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, a Contratada que:

a) Der causa à inexecução parcial do contrato;

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

c) Der causa à inexecução total do contrato;

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

e) Apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;

f) Praticar ato fraudulento na execução do contrato;

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

h) Praticar ato lesivo previsto no art. 5º, da Lei nº 12.846, de 1º de agosto de 2013.

15.2. Serão aplicadas a Contratada que incorrer nas infrações acima descritas as seguintes sanções:

a) Advertência, quando o contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §2º, da Lei nº 14.133/21);

b) Impedimento de licitar e contratar: quando praticadas as condutas descritas nas alíneas "b", "c" e "d" do item 15.1, sempre que não se justificar a imposição de penalidade mais grave (art. 156, § 4º, da Lei nº 14.133/21);

c) Declaração de inidoneidade: quando praticadas as condutas descritas nas alíneas "e", "f", "g" e "h" do item 15.1, bem como nas alíneas "b", "c" e "d" que justificarem imposição de penalidade mais grave (art. 156, §5º, da Lei nº 14.133/21).

d) Multa:

d.a.) moratória de 0,5% (meio por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 10 (dez) dias;

d.b) compensatória de 10% (dez por cento) sobre o valor total do contrato, no caso de inexecução total do objeto;

d.c.) O atraso injustificado da prestação dos serviços, conforme prazo estipulado no Edital e seus anexos, autoriza a Administração a promover a extinção do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe, art. 137, I, da Lei n. 14.133/21.

15.3. A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado a CONTRATANTE (art. 156, §9º, da Lei nº 14.133/21);

15.4. Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa (art. 156, §7º, da Lei nº 14.133/21);

15.5. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação (art. 157, da Lei nº 14.133/21);

15.6. A sanção de impedimento de licitar e contratar impedirá o responsável de licitar e contratar no âmbito da Administração Pública direta e indireta do Estado do Pará;

15.7. A duração da sanção de declaração de inidoneidade para licitar ou contratar observará o prazo previsto no art. 156, § 5º, da Lei Federal nº 14.133/21;

MINUTA

15.8. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pela Contratante a Contratada, além da perda desse valor, a diferença será cobrada judicialmente (art. 156, §8º, da Lei nº 14.133/21);

15.9. Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente, em prazo estipulado pela Administração Pública, a contar da data do recebimento da comunicação enviada pela autoridade competente;

15.10. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no **caput** e parágrafos do art. 158 da Lei nº 14.133/21, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

15.11. Na aplicação das sanções serão considerados (art. 156, §1º, da Lei nº 14.133/21):

a) a natureza e a gravidade da infração cometida;

b) as peculiaridades do caso concreto;

c) as circunstâncias agravantes ou atenuantes;

d) os danos que dela provierem para o Contratante;

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

15.12. Os atos previstos como infrações administrativas na Lei nº 14.133/21, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846/13, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei (art. 159);

15.13. A personalidade jurídica da Contratada poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia (art. 160, da Lei nº 14.133/21);

15.14. O Contratante deverá, no prazo máximo 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela

MINUTA

aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (CNEP), instituídos no âmbito do Poder Executivo Federal. (Art. 161, da Lei nº 14.133/21);

15.15. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133/21;

15.16. Os débitos do contratado para com a Administração contratante, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes deste mesmo contrato ou de outros contratos administrativos que o contratado possua com o mesmo órgão ora contratante, na forma da Instrução Normativa SEGES/ME nº 26, de 13 de abril de 2022.

CLÁUSULA DÉCIMA SEXTA – DA EXTINÇÃO CONTRATUAL

16.1. O contrato se extingue quando cumpridas as obrigações de ambas as partes, ainda que isso ocorra antes do prazo estipulado para tanto;

16.2. Se as obrigações não forem cumpridas no prazo estipulado, a vigência ficará prorrogada até a conclusão do objeto, caso em que deverá a Administração providenciar a readequação do cronograma fixado para o contrato;

16.2.1. Quando a não conclusão do contrato referida no item anterior decorrer de culpa da CONTRATADA:

a) ficará ela constituída em mora, sendo-lhe aplicáveis as respectivas sanções administrativas;

b) poderá a Administração optar pela extinção do contrato e, nesse caso, adotará as medidas admitidas em lei para a continuidade da execução contratual.

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

16.3.1. A extinção nesta hipótese ocorrerá na próxima data de aniversário do contrato, desde que haja a notificação da Contratada pela Contratante nesse sentido com pelo menos 2 (dois) meses de antecedência desse dia;

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

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

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

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

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

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

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

16.6.2. Relação dos pagamentos já efetuados e ainda devidos;

16.6.3. Indenizações e multas.

16.7. A extinção do contrato não configura óbice para o reconhecimento do desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório (art. 131, *caput,* da Lei n.º 14.133/21).

CLÁUSULA DÉCIMA SÉTIMA – DOTAÇÃO ORÇAMENTÁRIA

17.1. Os recursos orçamentários necessários para atender às despesas decorrentes deste Contrato constam do orçamento aprovado da CONTRATANTE, como a seguir especificado:
06.126.1510.8993 - Gerenciamento do Sistema Integrado de Segurança Pública e Defesa Social - SIEDS
Fonte 01500000001
Natureza 339040

CLÁUSULA DÉCIMA OITAVA – DA APROVAÇÃO DA MINUTA

18.1. A minuta deste Contrato foi aprovada pela Consultoria Jurídica da SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA E DEFESA SOCIAL - SEGUP/FESPDS conforme **Parecer Jurídico N° 276/2026-CONJUR**, consoante com o art. 53, da Lei n.º 14.133/21.

MINUTA

CLÁUSULA DÉCIMA NONA – DO CONTROLE E FISCALIZAÇÃO DA EXECUÇÃO

19.1. O acompanhamento e a fiscalização da execução do contrato consistem na verificação da conformidade da prestação dos serviços e da alocação dos recursos necessários, de forma a assegurar o perfeito cumprimento do ajuste, devendo ser exercidos por um ou mais representantes da Contratante, especialmente designados;

19.2. O representante da Contratante deverá ter a experiência necessária para o acompanhamento e controle da execução dos serviços e do contrato;

19.3. A verificação da adequação da prestação do serviço deverá ser realizada com base nos critérios previstos no Termo de Referência;

19.4. O fiscal ou gestor do contrato, ao verificar que houve subdimensionamento da produtividade pactuada, sem perda da qualidade na execução do serviço, deverá comunicar à autoridade responsável para que esta promova a adequação contratual à produtividade efetivamente realizada, respeitando-se os limites de alteração dos valores contratuais previstos na legislação;

19.5. O representante da Contratante deverá promover o registro das ocorrências verificadas, adotando as providências necessárias ao fiel cumprimento das cláusulas contratuais;

19.6. O descumprimento total ou parcial das demais obrigações e responsabilidades assumidas pela(s) contratada(s) ensejará a aplicação de sanções administrativas, previstas neste instrumento contratual e na legislação vigente, podendo culminar em rescisão contratual;

19.7. A Contratante reserva-se o direito de recusar-se a atestar a Fatura/Nota Fiscal se, no ato da apresentação, os serviços executados não estiverem de acordo com a descrição apresentada e aceita;

19.8. A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade da(s) contratada(s), inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica em corresponsabilidade da Contratante ou de seus agentes e prepostos, conforme versa a legislação vigente.

CLÁUSULA VIGÉSIMA – DOS CASOS OMISSOS

20.1. Os casos omissos serão decididos pelo Contratante, segundo as disposições contidas na Lei nº 14.133/21, e demais normas federais aplicáveis e, subsidiariamente, segundo as

disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

CLÁUSULA VIGÉSIMA PRIMEIRA – DAS ALTERAÇÕES

21.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 14.133/21;

21.2. A Contratada é obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato;

21.3. Registros que não caracterizam alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do art. 136 da Lei nº 14.133/21.

CLÁUSULA VIGÉSIMA SEGUNDA – DA PUBLICAÇÃO

22.1. O presente Contrato será publicado sob forma de extrato no Diário Oficial do Estado do Pará,no prazo máximo de 10 (dez) dias contados da data de sua assinatura, de conformidade com o que dispõe o Art. 28, § 5º, da Constituição Estadual.

22.2. Incumbirá a Contratante divulgar o presente instrumento no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no art. 94 da Lei 14.133/21.

CLÁUSULA VIGÉSIMA TERCEIRA – DAS DISPOSIÇÕES FINAIS

23.1. E por assim acordarem, as partes declaram aceitar todas as disposições estabelecidas neste Contrato que, lido e achado conforme, vai assinado em 02 (duas) vias, pelos representantes e testemunhas a seguir.

CLÁUSULA VIGÉSIMA QUARTA – DO FORO

24.1. É competente o Foro da Justiça Estadual, Estado do Pará, com renúncia expressa de qualquer outro por mais privilegiado que seja para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não puderem ser compostos pela conciliação, conforme art. 92, §1º, da Lei nº 14.133/21.

Belém/PA, XX de XXXXX de 2026.

MINUTA

SECRETARIA DE SEGURANÇA PÚBLICA E DEFESA SOCIAL

GOVERNO DO ESTADO DO PARÁ

SECRETÁRIA ADJUNTA DE GESTÃO ADMINISTRATIVA
COORDENADORIA DE CONTRATOS

RENAN HENRIQUE NABOR DE OLIVEIRA
SECRETÁRIO ADJUNTO DE GESTÃO ADMINISTRATIVA
CONTRATANTE

XXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXX
CONTRATADA

TESTEMUNHAS:

1. _____ 2. _____
CPF: CPF:

MINUTA