TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS
Av. André Araújo, S/N - Bairro Aleixo - CEP 69060-000 - Manaus - AM - www.tjam.jus.br

ESTUDO TÉCNICO PRELIMINAR - TJ/AM/SETIC/DVITIC

Responsáveis pela elaboração:

Diogo Mendonça de Sousa

Rodrigo dos Santos Marinho

Contato: (92) 99239-1948

Número de identificação do ETP: 2671070.

Categoria do Objeto: Serviço de Comunicação de Dados; **CATMAT/CATSER:** 26476, 27014, 27014 e 448242.

1 PLANO DE CONTRATAÇÕES ANUAL - PCA

1.1 O objeto da pretensa contratação está previsto no Plano de Contratações Anual (PCA) de 2026, conforme **RESOLUÇÃO Nº 30, DE 11 DE NOVEMBRO DE 2025,** disponibilizado no painel *BI* disponível NESTE LINK, sob os códigos **SETIC-2026-80, SETIC-2026-71, SETIC-2026-73 e SETIC-2026-74**, totalizando **R$ 9.045.275,44** de recurso disponível, conforme o quadro abaixo:

Código PCA	Código SIASG	Descrição	Grupo	Valor estimado no PCA/2026
SETIC-2026-71	448242	Aquisição de switches, roteadores e GBICs	3	R$ 3.195.500,00
SETIC-2026-73	27014	Serviço de prevenção, detecção, gestão e resposta a incidentes, avaliação de vulnerabilidades e riscos.	4	R$ 1.000.000,00
SETIC-2026-74	27014	Serviço de monitoramento e gerenciamento de infraestrutura de TIC	4	R$ 1.000.000,00
SETIC-2026-80	26476	Serviços de telecomunicações de MÉDIA capacidade para interligação suplementar/redundante das unidades do TJAM em Manaus e nas comarcas do interior do Estado do amazonas.	1 e 2	R$ 3.849.775,44
		Total estimado para o objeto		**R$ 9.045.275,44**

2 DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1 O Tribunal de Justiça do Estado do Amazonas (TJAM) necessita assegurar a continuidade, a disponibilidade e a segurança das comunicações de dados que interligam suas unidades na capital e no interior do Estado, além de aprimorar o monitoramento de sua infraestrutura de Tecnologia da Informação e Comunicação (TIC), em conformidade com as diretrizes nacionais de governança e segurança da informação no Poder Judiciário.

2.2 Atualmente, parte desses serviços é atendida por meio do Contrato Administrativo nº 006/2021-FUNJEAM, celebrado com a operadora OI S.A., o qual alcançará o limite legal máximo de prorrogação em fevereiro de 2026, conforme informado no Ofício nº 143 (SEI nº 2188174), tornando-se juridicamente improrrogável. Nesse contexto, torna-se indispensável a instauração de novo procedimento de contratação para substituir esse contrato, de modo a garantir a continuidade dos serviços de comunicação de dados essenciais ao funcionamento das unidades jurisdicionais e administrativas.

2.3 Ademais, embora o TJAM possua outro contrato vigente com a operadora SIDI (Contrato Administrativo nº 046/2023-TJ), a Resolução CNJ nº 370/2021 e as boas práticas de gestão de continuidade exigem a contratação de mais de uma operadora, com redes/backbones distintos, a fim de viabilizar efetiva resiliência e redundância dos serviços de comunicação de dados, prevenindo riscos operacionais decorrentes de falhas sistêmicas ou indisponibilidades parciais de provedores.

2.4 A necessidade de implantação de serviços de monitoramento e gestão de eventos por meio de NOC (Network Operations Center) e SOC (Security Operations Center) decorre de determinação expressa do Conselho Nacional de Justiça (CNJ), conforme consta do Ofício nº 205 – PRES/SGTJ (SEI nº 1535205), emitido em resposta ao Pedido de Providências nº 0007771-53.2023.2.00.0000. O referido ofício registra que a contratação desses serviços será precedida da elaboração de Estudo Técnico Preliminar (ETP), com vistas à inclusão da demanda no Plano de Contratações Anual de 2025, e destaca a relevância estratégica do tema para a continuidade de negócio e o fortalecimento da segurança da informação no âmbito do TJAM.

2.5 Portanto, a necessidade em questão consiste em:

2.5.1 Contratar uma ou duas operadoras para prestação de serviços de comunicação de dados do tipo transporte via fibra óptica, que não utilizem a rede, backbone ou enlaces da operadora SIDI, garantindo a continuidade do serviço atualmente prestado pela OI (Contrato nº 006/2021-FUNJEAM) e atendendo aos requisitos de alta disponibilidade, segurança, resiliência e redundância demandados pelo TJAM para suas atividades finalísticas e administrativas.

2.5.2 Adquirir e instalar switches gerenciados de distribuição, capazes de selecionar dinamicamente o melhor caminho de rede para o tráfego de dados, considerando parâmetros de desempenho, segurança e requisitos de negócios, de modo a otimizar a experiência de usuários e a eficiência operacional, maximizando a utilização da largura de banda e minimizando latência.

2.5.3 Implantar serviços de monitoramento e gestão de eventos 24x7x365 da infraestrutura de TIC do TJAM, por meio de NOC e SOC, garantindo não apenas a supervisão contínua dos novos links a serem contratados, mas também dos equipamentos adquiridos, promovendo governança efetiva de redes e segurança da informação, conforme preceituam a Resolução CNJ nº 468/2022, a Resolução TJAM nº 64/2023 e a mencionada determinação do CNJ.

2.6 A contratação proposta está fundamentada no interesse público de assegurar a prestação jurisdicional sem interrupções, com segurança da informação adequada, atendimento contínuo à sociedade e eficiência na utilização de recursos tecnológicos e financeiros, nos termos da Lei nº 14.133/2021, Resolução CNJ nº 468/2022, Resolução CNJ nº 370/2021 e Resolução TJAM nº 64/2023.

3. UNIDADE DEMANDANTE

3.1. Secretaria de Tecnologia da Informação e Comunicação (SETIC) do TJAM.

4. REQUISITOS DA CONTRATAÇÃO

4.1 Trata-se da formação de Ata de Registro de Preços (ARP) para viabilizar a:

4.1.1 Contratação de uma ou duas operadoras para prestação de serviços de comunicação de dados do tipo transporte via fibra óptica, que não utilizem a rede, backbone ou enlaces da operadora SIDI, garantindo a continuidade do serviço atualmente prestado pela OI (Contrato nº 006/2021-FUNJEAM) e atendendo aos requisitos de alta disponibilidade, segurança, resiliência e redundância demandados pelo TJAM para suas atividades finalísticas e administrativas.

4.1.2 Aquisição e instalação de switches gerenciados de distribuição, capazes de selecionar dinamicamente o melhor caminho de rede para o tráfego de dados, considerando parâmetros de desempenho, segurança e requisitos de negócios, de modo a otimizar a experiência de usuários e a eficiência operacional, maximizando

a utilização da largura de banda e minimizando latência.

4.1.3 Contratação de serviços de monitoramento e gestão de eventos 24x7x365 da infraestrutura de TIC do TJAM, por meio de NOC e SOC, garantindo não apenas a supervisão contínua dos novos links a serem contratados, mas também dos equipamentos adquiridos, promovendo governança efetiva de redes e segurança da informação, conforme preceituam a Resolução CNJ nº 468/2022 e a Resolução TJAM nº 64/2023.

4.2 Sugere-se que a licitação seja realizada na Modalidade Pregão, na forma Eletrônica, tipo Menor Preço por Grupo, mediante sistema de registro de preços, considerando-se os seguintes grupos:

4.2.1 Grupo 1: Serviço de Comunicação de Dados a ser prestado na cidade de Manaus

4.2.2 Grupo 2: Serviço de Comunicação de Dados a ser prestado nas comarcas do interior do Estado do Amazonas

4.2.3 Grupo 3: Fornecimento e instalação de equipamentos na cidade de Manaus

4.2.4 Grupo 4: Serviço de NOC/SOC

4.3 Os eventuais acionamentos dos Grupos 1, 2 e 4 resultarão em contratações de natureza contínua, pois os itens desses grupos constituem serviços que visam atender a demanda do TJAM de forma permanente e contínua, por mais de um exercício financeiro.

4.3.1 A duração inicial desses contratos será de 12 meses, podendo ser prorrogados sucessivamente, respeitada a vigência máxima decenal, conforme Art. 107 da Lei Federal n.° 14.133/2021.

4.4 Os eventuais acionamentos do Grupo 3, por sua vez, resultarão em contratações por escopo, pois esse grupo resume-se a aquisição e implantação de equipamentos e infraestrutura de rede LAN, além de serviços associados à instalação e configuração.

4..4.1 A duração desses contratos será de 36 meses, podendo ser prorrogados, desde que justificadamente, pelo prazo necessário à conclusão do objeto, conforme Art. 6º, XVII, da Lei Federal n.° 14.133/2021.

4.4.2 Os equipamentos adquiridos devem atender a critérios de sustentabilidade, conforme orientações do *Guia Prático de Critérios de Sustentabilidade para Compras no TJAM*.

4.4.3 A contratada deverá transferir conhecimento técnico à equipe do TJAM, incluindo capacitação sobre a operação e manutenção dos equipamentos e sistemas adquiridos.

4.5 Qualificação técnica:

4.5.1 Grupos 1 e 2:

4.5.1.1 Atestado (s) fornecido (s) por Pessoa Jurídica de Direito Público ou Privado, comprovando prestação de serviços análogos a tecnologia MPLS ou de Transporte de Dados, não sendo aceitos links de internet ou links de dados destinados tão somente a efetuar interligação entre os clientes e o backbone da licitante para fornecimento de internet.

4.5.1.2 As licitantes deverão comprovar estarem devidamente autorizadas pela Agência Reguladora (ANATEL) para prestar o serviço constante do objeto, conforme normas daquela Agência, para explorar os serviços objeto destes grupos.

4.5.1.3 As licitantes deverão comprovar possuir autorização da Amazonas Energia para uso e compartilhamento de infraestrutura de postes.

4.5.2 Grupo 3 - Atestado (s) fornecido (s) por Pessoa Jurídica de Direito Público ou Privado, comprovando aptidão para a prestação dos serviços e fornecimento de produtos em características, quantidades e prazos compatíveis com o objeto deste grupo, com as seguintes características mínimas:

4.5.2.1 Serviços comprovadamente bem-sucedidos em características e quantidades compatíveis com o objeto contratado, incluindo a implementação de uma solução de gerenciamento unificada de rede LAN e WLAN, garantindo uma conectividade eficiente em todos os ambientes previstos no contrato.
4.5.2.2 A comprovação de capacidade técnica se aplica a todos os itens da contratação, englobando a implementação de uma solução de controle de acesso abrangente, que assegure a segurança e a gestão eficaz dos dispositivos e usuários conectados à rede, bem como a conformidade com os requisitos de segurança estabelecidos.
4.5.2.3 O licitante deverá comprovar ser uma empresa autorizada a comercializar produtos e serviços do fabricante Aruba;

4.5.3 Grupo 4 - Atestado (s) fornecido (s) por Pessoa Jurídica de Direito Público ou Privado, comprovando a prestação de serviços em ambientes corporativos de porte médio à grande, com no mínimo 1.000 ativos, que englobem no mínimo o seguinte escopo de trabalho:

4.5.3.1 Serviços de Monitoramento de ataques cibernéticos.

4.5.3.2 Serviços de Gestão de Vulnerabilidades.

4.5.3.3 Serviços de Teste de Invasão.

4.5.3.4 Serviços de Teste de Email Phishing.

4.5.3.5 Serviços de Resposta a Incidentes Cibernéticos.

5. LEVANTAMENTO DE MERCADO E JUSTIFICATIVA DA ESCOLHA DO TIPO DE SOLUÇÃO A CONTRATAR

5.1. O mercado nacional oferece soluções consolidadas para cada uma das necessidades identificadas no **item 2 do ETP**:

5.1.1 Continuidade e redundância da comunicação de dados (2.1, 2.2 e 2.3): A análise de fornecedores indica ampla oferta de serviços de transporte de dados baseados em **fibra óptica e tecnologia MPLS**, já amplamente utilizados em órgãos federais e estaduais. Exemplos: **Polícia Federal** (pregão para rede multisserviços IP/MPLS), **CONAB** (edital prevendo rede MPLS em Grupo específico) e tribunais regionais como TRT-17 e TRT-7, que estruturaram contratações similares. Esses casos demonstram que a solução adotada pelo TJAM encontra respaldo em práticas de mercado e que a segmentação por grupos (Manaus e Interior) amplia a competitividade e viabiliza a contratação de fornecedores regionais para localidades interioranas.

5.1.2 Modernização da rede LAN com switches Aruba e gestão centralizada (2.5.2). O levantamento revelou que diversos órgãos públicos já adotam **switches Aruba** integrados ao **Aruba Central** como plataforma de gerenciamento unificado. Casos como a **PRODAM-SP**, a **Justiça Federal no Ceará** e o próprio **PNCP** demonstram a viabilidade de padronização tecnológica, com vantagens claras em simplificação da gestão, redução de falhas e integração nativa com a solução já implantada no TJAM (Contrato Administrativo nº 001/2025). Esse alinhamento atende à exigência do item 2.5.2, que demanda equipamentos capazes de otimizar desempenho, segurança e uso eficiente da largura de banda.

5.1.3 Monitoramento contínuo e segurança da informação (2.4 e 2.5.3): A Resolução CNJ nº 370/2021 e o Ofício nº 205 – PRES/SGTJ obrigam a implantação de **NOC e SOC 24x7**, reforçando a necessidade de gestão proativa da infraestrutura. O levantamento identificou o uso do **Zabbix** para monitoramento de rede (NOC) e de ferramentas como **Wazuh** e **Grafana** em SOCs de diversos entes públicos, como o TJPB, o TCU e municípios que contrataram implantação e suporte de Wazuh. Além disso, empresas públicas como a **PRODAM-AM** já oferecem SOC como serviço, validando o modelo proposto. Essa tendência confirma que o TJAM acompanha diretriz nacional e práticas consolidadas ao adotar ferramentas abertas, auditáveis e economicamente vantajosas para observabilidade e segurança.

5.2. A escolha dos quatro grupos reflete diretamente os aspectos do **item 2 do ETP** e busca atender, de forma integrada, às demandas estratégicas do TJAM:

5.2.1 Grupos 1 e 2 – Conectividade MPLS (capital e interior): garantem a continuidade do serviço atualmente prestado pela OI (Contrato 006/2021-FUNJEAM), já juridicamente improrrogável, e cumprem a exigência de redundância de backbones conforme boas práticas e Resolução CNJ nº 370/2021. O modelo de contratação em grupos distintos é amparado por benchmarks (CONAB, PF, TRTs), que confirmam a maturidade da solução.

5.2.2 Grupo 3 – Switches Aruba com Aruba Central: atende ao requisito de modernização da LAN (item 2.5.2), integrando-se ao sistema já implantado (Contrato 001/2025), evitando soluções heterogêneas e garantindo compatibilidade plena. Além disso, contratações similares em outros órgãos validam o uso do Aruba Central como plataforma unificada, reduzindo TCO e assegurando escalabilidade.

5.2.3 Grupo 4 – Serviços de NOC/SOC: decorre de determinação expressa do CNJ (item 2.4), sendo imprescindível para monitorar não apenas os novos links, mas também os equipamentos adquiridos. A escolha de Zabbix, Wazuh e Grafana como ferramentas padrão garante transparência, auditabilidade e alinhamento com experiências positivas em órgãos como TJPB e GSI/PR, além de evitar custos recorrentes de licenciamento.

5.3. Conclusão

5.3.1 A análise de mercado demonstra que a solução pretendida pelo TJAM encontra **forte paralelo em contratações similares de outros órgãos públicos**, tanto no âmbito federal quanto estadual, o que atesta sua viabilidade técnica e aderência às melhores práticas de governança.

5.3.2 Dessa forma, a contratação dos quatro grupos se justifica como a opção **mais segura, eficiente e estratégica**, pois:

5.3.2.1 garante **continuidade e resiliência da comunicação de dados** (Grupos 1 e 2),

5.3.2.2 promove a **modernização e padronização da infraestrutura de rede LAN** (Grupo 3), e

5.3.2.3 assegura **governança contínua de TIC e segurança da informação** (Grupo 4), em consonância com as exigências legais e normativas estabelecidas pelo CNJ e pelo próprio TJAM.

6. DESCRIÇÃO DA SOLUÇÃO ESCOLHIDA

6.1 Grupo 1 e Grupo 2: Serviços de Comunicação de Dados do tipo transporte via FIBRA ÓPTICA.
6.1.1. Os serviços deverão ser fornecidos por operadora que não utilize a rede, backbone ou enlaces da operadora SIDI, garantindo a continuidade do serviço atualmente prestado pela OI (Contrato nº 006/2021-FUNJEAM) e atendendo aos requisitos de alta disponibilidade, segurança, resiliência e redundância demandados pelo TJAM para suas atividades finalísticas e administrativas.
6.1.2. Os serviços deverão contemplar fornecimento de equipamentos, instalação, configuração, operação, manutenção, suporte e gerência proativa dos serviços contratados.
6.1.3. Todos os equipamentos/acessórios necessários à execução dos serviços exigidos no objeto deste ETP devem ser fornecidos pela CONTRATADA sem ônus para o CONTRATANTE.
6.1.4. O serviço deverá ficar ativo 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, garantindo conectividade ininterrupta às unidades remotas, ou seja, não há procedimento de desconexão.
6.1.5. Os serviços de comunicação de dados deverão ser taxados em valor mensal fixo sem franquia de volume de dados, sem aplicação de políticas de Fair Access Policy (FAP) ou cobrança de tráfego excedente.
6.1.6. Caberá à CONTRATADA elaborar dimensionamento das instalações para cada caso, fornecer os materiais, providenciar documentação pertinente ao transporte de material, efetuar a instalação e manutenção dos equipamentos/acessórios necessários ao perfeito funcionamento de cada link de comunicação.
6.1.7. Nas unidades remotas a implantação do acesso deverá ocorrer através de conexão à interface LAN do equipamento de rede do TJAM, via cabo óptico, twinax ou cabo de rede metálico UTP, conector RJ-45, padrão Cat5 ou Cat6.
6.1.8. O endereçamento IP da interface LAN dos equipamentos de rede do TJAM, bem como as regras de roteamento do link de comunicação, devem ser estabelecidos em conjunto com a equipe técnica da CONTRATANTE.
6.1.9. Todas as especificações SNMP da MIB dos equipamentos utilizados nas pontas do circuito devem estar plenamente disponíveis para consulta pela CONTRATANTE.
6.1.10. O custo do serviço contratado também deverá cobrir todas as despesas de deslocamento, diárias dos funcionários da CONTRATADA se necessário, hospedagem e alimentação da equipe que executará as atividades de instalação e manutenção.

6.1.11. Esses serviços de comunicação de dados serão organizados em grupos da seguinte maneira:

6.1.11.1. Um grupo para capital Manaus, definido como Grupo 1, conforme o quadro abaixo:

GRUPO 1: Serviço de Comunicação de Dados a ser prestado na cidade de Manaus	
ITEM	**DESCRIÇÃO**
1	Serviço mensal de comunicação de dados do tipo transporte via Fibra Óptica com dupla abordagem e velocidade de 10 Gbps para o Concentrador na Sede do TJAM
2	Serviço mensal de comunicação de dados do tipo transporte via Fibra Óptica com velocidade de 1000 Mbps para as unidades descentralizadas do TJAM
3	Serviço mensal de comunicação de dados do tipo transporte via Fibra Óptica com velocidade de 100 Mbps para as unidades descentralizadas do TJAM
4	Serviço de instalação do ponto de acesso.
5	Serviço de remanejamento de ponto de acesso (equipamentos/enlace).

6.1.11.2. Um grupo para o interior do Estado do Amazonas, como forma de aproveitarmos a diversidade de empresas que já atuam de forma consolidada nessas regiões, conforme o quadro abaixo:

GRUPO 2: Serviço de Comunicação de Dados a ser prestado nas comarcas do interior do Estado do Amazonas	
ITEM	**DESCRIÇÃO**
6	Serviço mensal de comunicação de dados do tipo transporte via Fibra Óptica com dupla abordagem e velocidade de 10 Gbps para o Concentrador na Sede do TJAM
7	Serviço mensal de comunicação de dados do tipo transporte via Fibra Óptica com velocidade de 50 Mbps para as unidades descentralizadas do TJAM
8	Serviço de instalação do ponto de acesso.
9	Serviço de remanejamento de ponto de acesso (equipamentos/enlace).

6.1.12 Os endereços das unidades abrangidas nos Grupos 1 e 2 estão nos quadros do Anexo II (SEI nº 2386530).

6.1.13 O escopo de cidades abrangidas no Grupo 2 deverá contemplar no mínimo as cidades já atendidas pelo Contrato Administrativo 046/2023-FUNJEAM, vide Anexo II (SEI nº 2386530).

6.1.14 – Serviço mensal de comunicação de dados via MPLS sobre FIBRA ÓPTICA
6.1.14.1. O serviço consiste no fornecimento de circuitos MPLS, via fibra óptica, para interligar o Datacenter da sede do TJAM, em Manaus, às unidades remotas da CONTRATANTE localizadas na capital e no interior do estado.
6.1.14.2. Os links das unidades remotas deverão ser concentrados na infraestrutura da CONTRATADA e encaminhados, através de backhaul dedicado, até o Datacenter do TJAM.
6.1.14.3. O acesso da CONTRATADA ao Datacenter do TJAM deverá ser implementado exclusivamente em fibra óptica, vedado o uso de rádio.
6.1.14.4. O backhaul dedicado deverá ser dimensionado para suportar, no mínimo, a soma da capacidade total contratada das unidades remotas.
6.1.14.5. A saída para a Internet ocorrerá exclusivamente pela sede do TJAM, em contrato específico. A CONTRATADA deverá encaminhar todo o tráfego das unidades remotas até o concentrador central do TJAM.
6.1.14.6. A CONTRATADA deverá assegurar o sigilo e a inviolabilidade dos dados trafegados em sua rede MPLS.
6.1.15 – Serviço de instalação dos pontos de acesso
6.1.15.1. A CONTRATADA será responsável pela ativação dos circuitos, incluindo eventuais obras civis de pequeno porte (dutos, passagens de cabos, terminações ópticas etc.) até o rack de equipamentos da CONTRATANTE.
6.1.15.2. A infraestrutura necessária para viabilizar a ativação do serviço (lançamento de cabos, conectores, acessórios de fixação e identificação) será de responsabilidade integral da CONTRATADA.
6.1.16 – Serviço de remanejamento de ponto de acesso
6.1.16.1. Caso haja necessidade de mudança de endereço de uma unidade remota ou do concentrador na sede, a CONTRATADA deverá realizar o remanejamento mediante solicitação formal.
6.1.16.2. O prazo máximo para conclusão do remanejamento será de 7 (sete) dias corridos, com indisponibilidade do serviço limitada a 24 (vinte e quatro) horas.

6.1.16.3. Toda a infraestrutura necessária ao funcionamento do serviço no novo endereço será de responsabilidade da CONTRATADA.
6.1.16.4. O novo circuito deverá passar por testes e aceite técnico.
6.1.17. DA APLICAÇÃO DAS SANÇÕES ADMINISTRATIVAS
6.1.17.1 A CONTRATADA fica obrigada a observar as condições de execução do contrato, estando sujeita à avaliação da qualidade dos serviços prestados, segundo os níveis de serviço descritos neste ETP.
6.1.17.2 No caso de atraso injustificado, execução parcial ou inexecução das atividades previstas nos termos citados neste ETP, a CONTRATADA ficará sujeita, sem prejuízo das responsabilidades civil e criminal, ressalvados os casos devidamente justificados e comprovados, a critério da Administração e ainda garantida prévia e ampla defesa, às seguintes cominações administrativas, cumulativamente ou não, com as penalidades previstas neste instrumento:
6.1.17.2.1 Advertência por escrito:
6.1.17.2.1.1 Será aplicada penalidade de advertência no caso de atraso no cumprimento dos prazos para apresentação de uma solução definitiva para o problema com solução provisória, bem como, nos casos de atraso no encaminhamento do diagnóstico da ocorrência e comprovação da correção após a solução definitiva do problema.
6.1.17.2.2 Multa, limitada a 30% (trinta por cento) do valor do contrato, de:
6.1.17.2.2.1. 0,5% (zero vírgula cinco por cento) sobre o valor mensal contratado, por hora ou fração de hora de atraso, nos casos de descumprimento do tempo máximo de atendimento (SLA) previsto para chamados referentes à indisponibilidade do circuito de comunicação (estação remota), limitado a 48 horas.
6.1.17.2.2.2. 2% (dois por cento) sobre o valor global contratado, por dia de atraso, nos casos de descumprimento do prazo previsto para a fase de instalação e ativação da solução de comunicação, limitado a 5 dias.
6.1.17.2.2.3. 3,5% (três vírgula cinco por cento) sobre o valor global contratado, por dia de atraso, nos casos de descumprimento do tempo máximo de atendimento previsto para chamados referentes a falhas no uso dos circuitos de dados ou problemas com impacto que atinjam mais de 10% das unidades remotas contratadas, ainda que estas continuem disponíveis, limitado a 3 dias.
6.1.17.2.2.4 A multa aplicada após regular Processo Administrativo será descontada dos pagamentos eventualmente devidos pelo CONTRATANTE ou ainda, quando for o caso, cobrada judicialmente.
6.1.17.3 As sanções aqui previstas são independentes entre si, podendo ser aplicadas isoladas ou cumulativamente, sem prejuízo de outras medidas cabíveis.

6.1.18. DOS PARÂMETROS DE QUALIDADE DOS SERVIÇOS
6.1.18.1 Na prestação dos serviços, a CONTRATADA obriga-se a atender aos parâmetros mínimos aceitáveis do acordo de nível de serviço (SLA) especificado a seguir, sem que isso isente a CONTRATADA de cumprir todas as demais exigências deste ETP, também passíveis de sanção.

6.1.18.2 DISPONIBILIDADE DO ENLACE: a disponibilidade do serviço indica o percentual de tempo, durante o período de 1 (um) mês de operação, em que um ponto de acesso integrante do serviço permanecer em condições normais de funcionamento.
6.1.18.2.1 No cálculo da disponibilidade serão consideradas todas as interrupções do serviço, conforme ANEXO I, exceto:

6.1.18.2.1.1 As programadas pelo CONTRATANTE ou pela CONTRATADA;

6.1.18.2.1.2 As decorrentes de falha elétrica no local.
6.1.18.2.2. Caso haja necessidade de interrupção dos serviços pela CONTRATADA, inclusive em função de mudança de tecnologia, a CONTRATADA deverá solicitar, por escrito, autorização com antecedência mínima de 5 dias úteis e a janela de interrupção deverá ser acordada com a CONTRATANTE. Havendo autorização para a interrupção, o serviço não será considerado indisponível durante o período indicado. Entretanto, caso a CONTRATADA exceda o período previsto, o serviço será considerado indisponível no tempo excedente.
6.1.18.2.3. O serviço contratado será considerado disponível desde que esteja plenamente funcional e operacional, atendendo a todas as especificações técnicas estabelecidas neste ETP. O serviço não será considerado indisponível em razão de fatos que estejam sob a responsabilidade da CONTRATANTE;
6.1.18.3 RETARDO DA REDE: Deverá atender o disposto no ANEXO I deste ETP;
6.1.18.4 PERDA DE PACOTES: Deverá atender o disposto no ANEXO I deste ETP;
6.1.18.5 TEMPO DE REPARO: a CONTRATADA deverá observar o intervalo de tempo máximo para reparo/restabelecimento de um circuito inoperante, contado da abertura do chamado, verificado conforme os casos abaixo:
6.1.18.5.1. O Tempo de Reparo deverá ser de no máximo 4 (quatro) horas contínuas para as unidades remotas de Manaus.
6.1.18.5.2. O Tempo de Reparo para as unidades remotas do interior do Amazonas deverá ser conforme o quadro abaixo.

Condições de acesso para atendimento presencial	Tempo de reparo máximo
Terrestre	Até 24 horas
Aéreo	Até 48 horas
Terrestre + Fluvial	Até 72 horas
Aéreo + Fluvial	Até 96 horas

6.1.18.5.3. Em todo caso, a CONTRATADA deverá iniciar o atendimento em no máximo 1 (uma) hora.

6.1.18.5.4. Caso a CONTRATADA necessite de acesso físico em local sob a responsabilidade da CONTRATANTE para a reparação ou disponibilização de qualquer serviço e o referido local encontre-se fechado, o prazo para reparação e/ou disponibilização do serviço ficará suspenso até que seja providenciado pela CONTRATANTE o referido acesso, sendo que o prazo começará a contar a partir deste momento;

6.1.18.5.5 - O tempo de reparo deverá atender, no que couber, o disposto no ANEXO I deste ETP;

6.1.19. DOS PARÂMETROS DE GERÊNCIA
6.1.19.1 A CONTRATADA deverá disponibilizar uma Gerência da Rede e Serviços contemplando as áreas funcionais de Gerência de Falhas, Desempenho, Configuração e de Nível de Serviço.
6.1.19.2 Para efeito deste ETP, o serviço de Gerência está dividido em: Gerenciamento Proativo, Chamado Técnico, Portal de Gerência e Relatórios.
6.1.19.3 Gerenciamento proativo:
6.1.19.3.1 A CONTRATADA deverá manter uma infraestrutura própria de gerenciamento de redes e serviços com capacidade para gerenciamento de todos os circuitos e de todos os serviços, independentemente de uma eventual subcontratação.
6.1.19.3.2 Deverá abranger todos os equipamentos, circuitos e serviços, independentemente de suas tecnologias.
6.1.19.3.3 A CONTRATADA é responsável por fornecer, dimensionar e configurar os equipamentos, sistemas e ferramentas necessárias para o provimento da solução de Gerência.
6.1.19.3.4 Qualquer inclusão ou alteração de características técnicas dos circuitos na gerência deverá ser realizado num prazo de 36 (trinta e seis) horas, a partir da implementação da característica técnica ou da ativação do novo circuito.
6.1.19.3.5 A Gerência de Rede e Serviços deverá atuar de forma proativa, antecipando-se aos problemas na rede e garantindo a qualidade do serviço, além da abertura, acompanhamento e fechamento dos chamados técnicos, sempre comunicando a equipe técnica da CONTRATANTE.
6.1.19.3.6 Uma vez detectada e diagnosticada uma falha ou previsão de falha com degradação na qualidade dos serviços, deverão ser realizadas ações corretivas. São exemplos de falhas detectadas pelo monitoramento proativo: taxa de erros acima do limite, intermitências, quedas de circuitos, circuito inativos e interfaces não ativas (down).
6.1.19.3.7 Além da correção de falhas ou da previsão de falhas, é necessário o monitoramento contínuo do desempenho, permitindo detectar e diagnosticar antecipadamente indisponibilidade, acima do acordado no nível de serviço.
6.1.19.3.8 A Gerência deverá operar 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, todos os dias do ano.
6.1.19.3.9 Os dados deverão ficar armazenados ao longo de todo o contrato. A disponibilização dos dados será realizada on-line, para dados dos últimos 90 (noventa) dias e, acesso sob demanda para dados anteriores a esse período.
6.1.19.3.10 No caso da disponibilização dos dados sob demanda, a CONTRATADA terá o prazo de 3 (três) dias para enviar as informações solicitados.
6.1.19.3.11 Os atendentes da Gerência, responsáveis pela abertura e encerramento dos chamados, deverão ter conhecimento da infraestrutura da CONTRATANTE e só devem encerrar os chamados quando confirmarem a operacionalidade dos serviços com a CONTRATANTE, registrando no sistema o agente da CONTRATANTE que realizou os testes.
6.1.19.3.12 A CONTRATANTE fornecerá todas as informações necessárias, como endereço completo, telefones e contatos em todas as unidades que receberão os serviços, e serão gerenciadas pela CONTRATADA.

6.1.19.3.13 Complementarmente ao gerenciamento da CONTRATADA, será feito um gerenciamento pelos técnicos do NOC/SOC correspondente ao Grupo 4. Para implementação dessa gerência, deverá ser habilitado o protocolo SNMP nos equipamentos, onde será criada a comunidade SNMP com o acesso de leitura liberado para a Gerência do NOC/SOC, independente do gerenciamento realizado pela CONTRATADA.
6.1.19.4 Chamado Técnico:
6.1.19.4.1 A Gerência deverá dar suporte a chamados referentes à recuperação de falhas de circuitos e serviços, configuração de equipamentos, endereçamento, desempenho e segurança.
6.1.19.4.2 A abertura do chamado deverá ser realizada pela equipe de gerência da CONTRATADA, imediatamente após a constatação de defeito ou falha em qualquer circuito ou serviço que esteja em funcionamento.
6.1.19.4.3 Após a abertura do chamado, em um prazo máximo de 20 (vinte) minutos, o atendente responsável pela abertura de chamado deverá entrar em contato com técnico da CONTRATANTE, podendo ser por email, para informar as providências já tomadas e a estimativa para solução do problema.
6.1.19.4.4 Após a abertura do chamado, seja de forma proativa pela gerência ou reativa por chamada telefônica ou meio eletrônico, deve ter prazo máximo SLA acordado para resolução da falha identificada.
6.1.19.4.5 Os circuitos e serviços deverão receber uma identificação única tanto para a CONTRATANTE como para a CONTRATADA, que deverá ser de conhecimento de todos os atendentes da equipe de Gerência, e será utilizada na abertura do chamado técnico pela Gerência Proativa.
6.1.19.4.6 As informações de chamados, que serão visualizadas através do Portal on-line, deverão conter:
6.1.19.4.6.1 Número do Chamado;
6.1.19.4.6.2 Data e Hora da Abertura;
6.1.19.4.6.3 Status (aberto/fechado);
6.1.19.4.6.4 Localidade;
6.1.19.4.6.5 Responsável pela abertura (atendente Contratada);
6.1.19.4.6.6 Descrição do Problema motivador do chamado técnico;
6.1.19.4.6.7 Histórico das ocorrências do chamado (data/hora e descrição).
6.1.19.4.7 As tentativas de contato com os técnicos da CONTRATANTE para aberturas de chamados, recorrências ou encerramento de chamados, que não tenham tido sucesso por ausência dos técnicos, deverão ser registradas no campo “Histórico” do chamado.
6.1.19.4.8 Os chamados técnicos só poderão ser encerrados por um técnico da CONTRATANTE, em conjunto com a Central de Atendimento, que deverá entrar em contato com a CONTRATANTE, para encerrar os chamados solucionados.
6.1.19.4.9 Os técnicos autorizados para o encerramento dos chamados serão informados pela CONTRATANTE, na implantação do serviço.
6.1.19.5 Portal de Gerência
6.1.19.5.1. A visualização das informações deverá ser via WEB, através de protocolo HTTPS.
6.1.19.5.2. O intervalo de coleta dos dados para exibição das informações deverá ser de, no máximo, 5 minutos, podendo ser configurável.
6.1.19.5.3. A visualização das informações deverá ser em tempo real, apresentando no mínimo as funcionalidades listadas nos itens abaixo:
6.1.19.5.3.1. Alertas em caso de falhas e anormalidade dos circuitos, com grau de criticidade.
6.1.19.5.3.2. Status de todos os elementos que compõem a topologia da rede para a prestação dos serviços.
6.1.19.5.3.3. Visualização da utilização de banda dos circuitos, pelo menos, diário e mensal, com a opção de consulta de dados históricos.
6.1.19.5.3.4. Visualização do tempo de resposta dos circuitos, em tempo real, com opção de consulta de dados históricos.
6.1.19.5.3.5. Visualização dos chamados registrados, abertos e encerrados, dentro do prazo contratual, por data ou circuito, permitindo acesso ao detalhamento dos chamados.
6.1.19.6 Relatórios
6.1.19.6.1 O acompanhamento da qualidade dos serviços da rede, acompanhamento dos chamados e do SLA estabelecido será feito através de relatórios disponibilizados pela CONTRATADA, no Portal de Gerência, para consulta diária, mensal ou sob demanda.
6.1.19.6.2 Mensalmente, ao encaminhar suas faturas, a CONTRATADA deverá também apresentar um relatório à CONTRATANTE, e torná-lo disponível no Portal, para fins de comprovação de atendimento do acordo de nível de serviço contratado, onde estejam apurados os seguintes itens:
6.1.19.2.1 Nome da Contratante;
6.1.19.6.2.2 Designação do circuito;
6.1.19.6.2.3 Localidade do circuito;
6.1.19.6.2.4 Número de chamados do período, por localidade;
6.1.19.6.2.5 Tempo de reparo de cada chamado no período, por localidade;
6.1.19.6.2.6 Disponibilidade apurada por localidade;
6.1.19.6.3 Os relatórios abaixo poderão ser visualizados on-line com os dados em tempo real ou gerados sob demanda para períodos anteriores a 90 dias. Para fins destes relatórios deverá ser considerado o mês normal, ou seja, com todos os dias que o compõe:
6.1.19.6.3.1 Relatórios de Disponibilidade: devem ser emitidos mensalmente e apresentar informações diária, semanal e mensal.
6.1.19.6.3.2 Relatórios de Tráfego: relatórios diários que apresentam o tráfego de todos os circuitos, com suas séries históricas, fornecendo subsídios para analisar o desempenho e as tendências de aproveitamento dos recursos da rede. Devem demonstrar informações da banda utilizada e do volume de tráfego.
6.1.19.6.3.3 Relatório de Acompanhamento dos Chamados: relatório diário com todas as informações relativas ao chamado como data, hora, identificação do elemento (circuito ou equipamento), descrição detalhada do chamado.
6.1.19.6.3.4 Relatórios de Chamados: relatório mensal de chamados abertos e encerrados.
6.1.19.6.3.5 Relatório de Acompanhamento de SLA: descritivo de SLA, contendo para cada circuito as ocorrências de falhas, caso tenham existido e os valores mensais apurados para cada indicador estabelecido no item ACORDO DE NÍVEL DE SERVIÇOS.
6.1.19.6.3.6 Relatório Específico de SLA: relatório de acompanhamento de cada indicador a ser monitorado para o SLA. Estes relatórios devem ser emitidos mensalmente.
6.1.19.6.4 Todos os relatórios digitais deverão permitir o uso de filtros para visualizar as informações: Filtro por período desejado, por localidade.
6.1.19.6.5 Todos os relatórios deverão possibilitar a seleção de datas de início e fim do período a que se referem os dados a serem exibidos.
6.1.19.6.6 A CONTRATADA deverá armazenar todos os dados e informações coletadas durante a vigência do contrato, tais como: dados brutos coletados nos elementos gerenciados, dados sumarizados para confecção de relatórios, acompanhamento dos chamados, acompanhamento da qualidade de serviço, de faturamento, dentre outros. Esses dados deverão ser disponibilizados a CONTRATANTE ao final do contrato.

6.2 Grupo 3: Fornecimento e instalação de equipamentos na cidade de Manaus

6.2.1 Descrição do Objeto: A contratação visa à modernização da infraestrutura de rede LAN do TJAM, abrangendo a aquisição, instalação, configuração e manutenção de equipamentos de rede, além de treinamento técnico e suporte especializado. O objetivo é garantir maior conectividade, segurança e eficiência operacional para todas as unidades judiciais do TJAM.
6.2.2 As especificações técnicas que detalham os bens e serviços objeto deste grupo estão descritos no Anexo III (SEI nº 2386531).

6.2.3. Forma de Acompanhamento do Atendimento aos Prazos de Garantia e Níveis Mínimos de Qualidade Aceitável de Serviços Exigidos (NSE)
6.2.3.1. Os tempos de resposta e de solução para os chamados técnicos abertos serão contados a partir do registro dos mesmos através de contato telefônico ou por outro meio disponível.
6.2.3.2. Quanto aos níveis de SLA:
6.2.3.2.1 Ficam estabelecidos níveis mínimos de serviço a serem cumpridos pela CONTRATADA, com mensuração consolidada mensal e emissão de relatórios pelos fiscais do contrato para sua aferição:
6.2.3.2.2 O prazo de solução é o período compreendido entre a abertura do chamado pelo Tribunal e a solução efetiva do mesmo.
6.2.3.2.3 A Contratada deverá atender e solucionar todos os chamados, conforme os prazos estabelecidos.
6.2.3.2.4 Os prazos de atendimento definidos pelo Tribunal são os relacionados na tabela a seguir:

Falhas/Serviço	Prazo de Solução
Instabilidade do Sistema	6 Horas Úteis
Resolução de dúvidas de utilização	48 Horas

6.2.3.2.4.1 Na hipótese do descumprimento do nível de qualidade aceitável, o Tribunal poderá aplicar sanções administrativas, conforme tabela abaixo:

Serviço	Falhas	Grau da Infração	Tipo de Multa
Disponibilidade do Sistema	Atraso injustificado na instalação do sistema e habilitação dos usuários entre 6 a 12 horas consecutivas.	Descumprimento de obrigações contratuais, consideradas leves	1
	Atraso injustificado na instalação do sistema e habilitação dos usuários superior a 12 horas consecutivas.	Erros de execução do objeto	2
	Atraso injustificado na instalação do sistema superior a 12 horas consecutivas.	Execução imperfeita do objeto	3
Suporte Técnico	Chamados sem resposta entre 48 a 72 horas.	Descumprimento de obrigações contratuais, consideradas leves	1
	Chamados ao suporte em prazo superior a 72 horas.	Execução imperfeita do objeto	3

6.2.6.2.4.1.1 As penalidades a serem aplicadas pela Contratante estão discriminadas no Anexo V (SEI nº 2389063) deste ETP.

6.2.7 A modernização da rede LAN do TJAM envolve, além da atualização dos ativos de rede, a integração com o sistema de gerenciamento unificado Aruba Central, já devidamente adquirido e implantado por meio do Contrato Administrativo nº 001/2025. Essa solução permite uma administração centralizada, inteligente e em nuvem dos switches da marca Aruba, otimizando as operações da equipe de infraestrutura de TI com maior agilidade, visibilidade e controle.

6.2.7.1 Considerando o elevado número de switches Aruba que compõem o parque tecnológico da instituição, torna-se inviável a gestão individualizada desses equipamentos. A plataforma Aruba Central se mostra, portanto, essencial para a operação eficiente e centralizada da rede, permitindo o gerenciamento de todos os pontos de acesso e switches por meio de uma interface única.

6.2.7.2 Diante disso, é imprescindível que todos os novos switches eventualmente adquiridos ou substituídos sejam integralmente compatíveis com o Aruba Central, garantindo sua gestão plena e nativa pela plataforma já em operação, sem necessidade de soluções paralelas ou adaptações.

6.2.7.3 A adoção e padronização do Aruba Central como solução de gerenciamento de rede traz benefícios significativos para o TJAM, tais como:

6.2.7.3.1 *Gestão simplificada e centralizada*: Através do Aruba Central, todos os switches e demais dispositivos de rede são administrados por meio de um painel único e intuitivo, o que reduz a complexidade operacional e facilita a atuação da equipe técnica.

6.2.7.3.2 *Eficiência operacional e automação*: A plataforma permite automatizar tarefas recorrentes como provisionamento, atualização de firmware, configuração de VLANs e políticas de segurança, reduzindo falhas humanas e otimizando os recursos da equipe de TI.

6.2.7.3.3 *Segurança aprimorada*: Com políticas de segurança unificadas e monitoramento contínuo por meio da plataforma, é possível detectar anomalias, aplicar regras de acesso e garantir uma proteção mais eficaz contra ameaças internas e externas.

6.2.7.3.4 *Melhoria no desempenho da rede*: O Aruba Central permite análise contínua da performance dos switches e pontos de acesso, possibilitando ajustes dinâmicos que otimizam o tráfego de dados e proporcionam uma experiência mais estável e eficiente aos usuários.

6.2.7.3.5 *Redução de equipamentos e simplificação da arquitetura*: A centralização do gerenciamento dispensa a necessidade de múltiplas controladoras físicas, reduzindo pontos de falha, consumo de energia e custos com manutenção.

6.2.7.4 Assim, caberá à CONTRATADA garantir que todos os serviços e equipamentos ofertados no âmbito desta contratação sejam plenamente compatíveis com o sistema Aruba Central, assegurando sua integração à plataforma de gerenciamento já implantada no TJAM.

6.3 Grupo 4: Serviço de NOC/SOC e Resposta a Incidente
6.3.1. ITEM 13 do GRUPO 4 – Serviços Gerenciados de Monitoramento de Ambiente Tecnológico e Segurança da Informação – NOC/SOC
6.3.1.1. Características Gerais:
6.3.1.1.1. O NOC/SOC deverá ser planejado e executado pela CONTRATADA em conformidade com as melhores práticas de gerenciamento de serviços de TIC e de segurança da informação.
6.3.1.1.2. O NOC/SOC deverá operar em regime ininterrupto, com disponibilidade de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, inclusive feriados.
6.3.1.1.3. O NOC/SOC deverá operar remotamente sobre o ambiente da CONTRATANTE.
6.3.1.1.4. A equipe designada pela CONTRATADA deverá ser tecnicamente capacitada e dimensionada para atender integralmente aos requisitos deste ETP.
6.3.1.2. Atividades do NOC/SOC:
6.3.1.2.1. Executar rotinas e procedimentos técnicos diários para prevenir, detectar e tratar incidentes e problemas no ambiente tecnológico da CONTRATANTE, de forma proativa.
6.3.1.2.2. Assegurar que as ferramentas de monitoramento e segurança da informação estejam atualizadas, estáveis e configuradas de forma adequada para manter informações fidedignas do parque tecnológico.
6.3.1.2.3. Promover o Gerenciamento de Incidentes, abrangendo comunicação, identificação, tratamento, resolução e/ou escalonamento de alertas oriundos das ferramentas do NOC (Zabbix) e do SOC (Wazuh/Grafana), integrando as equipes envolvidas.
6.3.1.2.4. Promover o Gerenciamento de Problemas, garantindo análise de causa raiz, tratamento e resolução dos alertas e eventos gerados.
6.3.1.2.5. Realizar abertura e acompanhamento de chamados junto a terceiros contratados pela CONTRATANTE em caso de indisponibilidade ou degradação de serviços, coordenando o processo de atendimento.
6.3.1.2.6. Elaborar e disponibilizar relatórios técnicos periódicos e sob demanda, a partir das informações geradas pelo Zabbix (NOC), Wazuh e Grafana (SOC).
6.3.1.2.7. Atividades de Liberação de Sistemas Críticos:
6.3.1.2.7.1. Executar e/ou acompanhar homologações e liberações de atualizações em sistemas críticos da CONTRATANTE (ex.: Projudi, SAJ, SEI etc.), conforme solicitação.
6.3.1.2.7.2. Documentar em passo a passo os procedimentos realizados, entregando relatório técnico.
6.3.1.2.7.3. Executar tais atividades fora do horário comercial, inclusive em finais de semana, de forma presencial e/ou remota.
6.3.1.2.7.4. A CONTRATADA deverá garantir profissionais disponíveis sempre que comunicada pela CONTRATANTE com antecedência mínima de 12 (doze) horas.
6.3.1.3. Serviços Gerenciados de Monitoramento de Ambiente Tecnológico – NOC:
6.3.1.3.1. Escopo de monitoramento através do Zabbix Community:
6.3.1.3.1.1. Monitoramento de Rede.
6.3.1.3.1.2. Monitoramento de Servidores.
6.3.1.3.1.3. Monitoramento de Ambientes de Nuvem.
6.3.1.3.1.4. Monitoramento de Máquinas Virtuais.
6.3.1.3.1.5. Monitoramento de Aplicativos.
6.3.1.3.1.6. Monitoramento de Bancos de Dados.
6.3.1.3.1.7. Monitoramento de Datacenter.
6.3.1.3.2. Condições de execução (NOC):
6.3.1.3.2.1. O monitoramento deverá ser realizado utilizando exclusivamente o Zabbix Community, instalado no ambiente da CONTRATANTE, cabendo à CONTRATADA sua administração, atualização, manutenção, suporte e operação integral.
6.3.1.3.2.2. O Gerenciamento Técnico e Administrativo do Zabbix, incluindo cadastro de itens, configuração de parâmetros, manutenção preventiva/corretiva e atualização da plataforma, será de responsabilidade exclusiva da CONTRATADA.

6.3.1.3.3 O Anexo IV (SEI nº 2387266) contém informações detalhadas da Infraestrutura e da Topologia de TIC do TJAM.
6.3.1.4. Serviços Gerenciados de Segurança da Informação (SOC):
6.3.1.4.1. Composição dos serviços de administração, instalação, integração, atualização, manutenção, monitoramento, resposta a incidentes e suporte técnico das soluções Wazuh, Graylog e Grafana, abrangendo, mas não se limitando, às seguintes atividades:
6.3.1.4.1.1. Instalação do Wazuh e Gestão de Agentes
6.3.1.4.1.1.1. Realizar a instalação inicial do Wazuh e agentes em todos os servidores, estações de trabalho, ativos de rede e ativos em nuvem do parque tecnológico.
6.3.1.4.1.1.2. Garantir que todos os agentes sejam configurados de forma adequada, reportando ao Wazuh Manager e com logs devidamente coletados.
6.3.1.4.1.1.3. Manter o ciclo de vida dos agentes, realizando atualizações periódicas, reinstalação em caso de falhas e auditoria constante para identificar endpoints sem agente instalado. 6.3.1.4.1.1.4. Promover a integração dos novos ativos ao ambiente monitorado, garantindo que não haja falhas de cobertura.
6.3.1.4.1.2. Administração da Plataforma
6.3.1.4.1.2.1. Verificar diariamente o status do servidor Wazuh Manager, dos Wazuh Indexers e do Wazuh Dashboard, garantindo integridade e disponibilidade da solução.
6.3.1.4.1.2.2. Monitorar conectividade entre agentes e servidor, corrigindo falhas de comunicação e assegurando cobertura integral do parque.
6.3.1.4.1.3. Atualização e Gestão de Regras
6.3.1.4.1.3.1. Acompanhar e aplicar atualizações regulares do Wazuh Ruleset.
6.3.1.4.1.3.2. Customizar regras conforme riscos e particularidades da CONTRATANTE. 6.3.1.4.1.3.3. Criar exceções e ajustes para reduzir falsos positivos, mantendo alta efetividade de detecção.
6.3.1.4.1.4. Monitoramento e Correlação de Eventos (SIEM)
6.3.1.4.1.4.1. Coletar, centralizar e correlacionar eventos de segurança, logs de sistemas operacionais priorizando sistemas, firewalls, switches, servidores de aplicação, ativos em nuvem e serviços críticos.
6.3.1.4.1.4.2. Detectar incidentes como tentativas de intrusão, malware, falhas de autenticação, movimentação lateral, escalonamento de privilégios e acessos não autorizados.
6.3.1.4.1.4.3. Gerar dashboards e relatórios em tempo real, disponibilizando evidências ao SOC e à área de Segurança da Informação.
6.3.1.4.1.5. Resposta a Incidentes e Correção de Eventos Críticos
6.3.1.4.1.5.1. Atuar diretamente no tratamento de incidentes de segurança, seguindo o plano de resposta a incidentes da CONTRATANTE.
6.3.1.4.1.5.2. Executar ações de Active Response, como bloqueio de IPs maliciosos, finalização de processos suspeitos, isolamento de endpoints comprometidos e aplicação de correções emergenciais. Incidentes que demandem investigação aprofundada, análise forense ou resposta emergencial de maior complexidade serão escalados para consumo do banco de horas de resposta a incidentes cibernéticos (6.3.1.4.8).
6.3.1.4.1.5.3. Registrar todas as ocorrências críticas em relatórios técnicos e acionamento de chamados, detalhando medidas de contenção, erradicação e recuperação.
6.3.1.4.1.5.4. Apoiar a área responsável na comunicação e coordenação de resposta a incidentes, garantindo rastreabilidade e documentação completa.
6.3.1.4.1.6. Detecção de Intrusão em Hosts (HIDS)
6.3.1.4.1.6.1. Ativar e monitorar continuamente o File Integrity Monitoring para identificar alterações não autorizadas em arquivos de sistema e aplicações críticas.
6.3.1.4.1.6.2. Validar alertas sobre execução de processos suspeitos, escalonamento de privilégios, instalação de backdoors e alterações em registros críticos do sistema.
6.3.1.4.1.7. Gestão de Vulnerabilidades
6.3.1.4.1.7.1. Executar varreduras periódicas com o módulo de Vulnerability Detection, correlacionando com bancos NVD, CVE e OVAL.
6.3.1.4.1.7.2. Produzir relatórios de vulnerabilidades priorizados por criticidade e apoiar o time de infraestrutura na aplicação dos patches e correções necessárias.
6.3.1.4.1.8. Integração com Inteligência de Ameaças
6.3.1.4.1.8.1. Monitorar e correlacionar eventos com indicadores de comprometimento (IoCs) de Threat Intelligence Feeds.
6.3.1.4.1.8.2. Identificar conexões externas com C2, domínios maliciosos, IPs suspeitos e atividades anômalas de rede.
6.3.1.4.1.9. Monitoramento de Nuvem e Containers
6.3.1.4.1.9.1. Se necessário, configurar e acompanhar monitoramento em AWS, Azure e GCP, avaliando permissões excessivas, acessos administrativos e anomalias.
6.3.1.4.1.9.2. Auditar logs de Docker e Kubernetes, garantindo a integridade de containers e clusters.
6.3.1.4.1.10. Monitoramento de Conformidade e Auditoria
6.3.1.4.1.10.1. Ativar módulos de compliance monitoring para LGPD, ISO 27001 e outras normas aplicáveis.
6.3.1.4.1.10.2. Gerar relatórios periódicos de conformidade para apoiar auditorias internas e externas.
6.3.1.4.1.11. Relatórios e Evidências Operacionais
6.3.1.4.1.11.1. Emitir relatórios diários de incidentes críticos.
6.3.1.4.1.11.2. Emitir relatórios semanais sobre vulnerabilidades e status dos agentes. 6.3.1.4.1.11.3. Emitir relatórios mensais consolidados com indicadores de ameaças detectadas, incidentes tratados, endpoints não conformes e recomendações de melhoria.
6.3.1.4.1.11.4. Registrar todos os eventos relevantes para compor trilhas de auditoria.
6.3.1.4.1.12. Backup e Continuidade
6.3.1.4.1.12.1. Verificar rotinas automáticas de backup da base do Wazuh e validar periodicamente a restauração.
6.3.1.4.1.12.2. Garantir plano de continuidade do monitoramento SIEM, mesmo em caso de falha do servidor principal.
6.3.1.4.1.13. Descoberta e Inventário de Ativos
6.3.1.4.1.13.1. Executar varreduras periódicas para identificar ativos não gerenciados ou sem agente instalado, promovendo sua inclusão imediata no ambiente monitorado.
6.3.1.4.1.13.2. Consolidar inventário atualizado de endpoints, servidores e dispositivos monitorados pelo Wazuh. As informações de inventário geradas por esta e outras soluções serão consolidadas em uma base unificada ou apresentadas de forma integrada no Grafana.
6.3.1.4.2. Composição dos serviços de administração, atualização, manutenção, monitoramento, migração, resposta a incidentes e suporte técnico da solução Graylog, abrangendo, mas não se limitando, às seguintes atividades:
6.3.1.4.2.1. Administração da Plataforma
6.3.1.4.2.1.1. Manter a solução já implementada, assegurando que sua operação esteja em conformidade com as melhores práticas de mercado.
6.3.1.4.2.1.2. Verificar diariamente o status dos servidores de aplicação, banco de dados e indexadores do Graylog, assegurando alta disponibilidade e integridade da solução.
6.3.1.4.2.1.3. Instalar os agentes e monitorar a ingestão de logs, garantindo que todos os ativos de rede, sistemas e serviços (com foco em Active Directory e ambientes Windows) estejam enviando registros em tempo real para o Graylog.
6.3.1.4.2.1.3.1. Se solicitado pela CONTRATANTE, deverá ser realizada a migração dos controles atualmente implementados no Graylog para a plataforma Wazuh, contemplando todas as regras, correlações, alertas, dashboards e relatórios de segurança. A CONTRATADA será responsável por planejar, executar, validar e documentar o processo de migração, garantindo a integridade das informações, a continuidade das operações de monitoramento e a equivalência ou melhoria dos controles existentes.
6.3.1.4.2.1.4. Aplicar atualizações de versão, plugins e correções de segurança da plataforma Graylog, mantendo-a sempre alinhada às boas práticas.
6.3.1.4.2.2. Monitoramento de Eventos de Segurança no AD
6.3.1.4.2.2.1. Monitorar eventos de criação, habilitação, desabilitação e exclusão de usuários no AD, identificando acessos suspeitos ou criação indevida de contas.
6.3.1.4.2.2.2. Acompanhar tentativas de logon local e conexões via RDP, acionando resposta imediata em caso de tentativas repetidas ou fora do horário de expediente.
6.3.1.4.2.2.3. Identificar alterações de senha realizadas por usuários, suporte técnico ou sistemas automatizados, correlacionando com tentativas de acesso maliciosas.
6.3.1.4.2.2.4. Detectar atividades relacionadas a elevação de privilégios ou inclusão de usuários em grupos administrativos, acionando contramedidas imediatas.
6.3.1.4.2.3. Monitoramento de Serviços e Objetos de Sistema
6.3.1.4.2.3.1. Monitorar eventos de instalação de novos serviços, garantindo que somente softwares autorizados sejam executados.
6.3.1.4.2.3.2. Detectar exclusão de objetos críticos em File Servers, correlacionando com tentativas de sabotagem, vazamento ou exclusão indevida de dados.
6.3.1.4.2.3.3. Acompanhar eventos de criação de novas tarefas agendadas, prevenindo uso malicioso de task scheduler para execução de malwares.
6.3.1.4.2.4. Tentativas de Acesso e Falhas de Logon
6.3.1.4.2.4.1. Identificar falhas de logon e tentativas repetidas de acesso a objetos, correlacionando com possíveis ataques de força bruta ou enumeração de contas.
6.3.1.4.2.4.2. Correlacionar eventos de falha de logon com origens geográficas e dispositivos não reconhecidos, gerando alertas automáticos de segurança.

6.3.1.4.2.5. Correlação Avançada e Alertas
6.3.1.4.2.5.1. Configurar alertas no Graylog para eventos críticos como:
6.3.1.4.2.5.1.1. Elevação de privilégios;
6.3.1.4.2.5.1.2. Inclusão de usuários em grupos de administradores;
6.3.1.4.2.5.1.3. Instalação de novos serviços;
6.3.1.4.2.5.1.4. Tentativas de acesso a objetos sensíveis;
6.3.1.4.2.5.1.5. Excesso de falhas de logon.
6.3.1.4.2.5.2. Integrar os alertas do Graylog ao sistema de gestão de incidentes, com abertura automática de chamados para investigação pelo SOC.
6.3.1.4.2.6. Resposta a Incidentes
6.3.1.4.2.6.1. Atuar de forma proativa na correção de eventos críticos detectados no Graylog, como:
6.3.1.4.2.6.1.1. Desabilitar contas comprometidas;
6.3.1.4.2.6.1.2. Bloquear serviços não autorizados;
6.3.1.4.2.6.1.3. Isolar máquinas envolvidas em atividades suspeitas;
6.3.1.4.2.6.1.4. Forçar redefinição de credenciais em caso de comprometimento.
6.3.1.4.2.6.2. Incidentes que demandem investigação aprofundada, análise forense ou resposta emergencial de maior complexidade serão escalados para consumo do banco de horas de resposta a incidentes cibernéticos (6.3.1.4.8).
6.3.1.4.2.6.3. Documentar todas as ações tomadas, mantendo trilhas de auditoria completas. 6.3.1.4.2.6.4. Apoiar a área de Segurança da Informação no ciclo de contenção, erradicação e recuperação dos incidentes.
6.3.1.4.2.7. Relatórios e Evidências Operacionais
6.3.1.4.2.7.1. Gerar relatórios diários de incidentes críticos.
6.3.1.4.2.7.2. Gerar relatórios semanais de tendências, como tentativas de logon, acessos suspeitos e eventos de elevação de privilégios.
6.3.1.4.2.7.3. Gerar relatórios mensais consolidados de indicadores de segurança, estatísticas de alertas e incidentes tratados via Graylog.
6.3.1.4.3. Composição dos serviços de instalação, integração, administração, atualização, manutenção, monitoramento e suporte técnico da solução Grafana, em integração com Wazuh e Graylog, abrangendo, mas não se limitando, às seguintes atividades:
6.3.1.4.3.1. Criação e Gestão de Dashboards
6.3.1.4.3.1.1. Desenvolver dashboards customizados para melhor visualização de métricas de segurança e eventos críticos coletados pelo Wazuh e Graylog.
6.3.1.4.3.1.2. Disponibilizar visões em tempo real para análise de incidentes, tendências de ameaças, vulnerabilidades e status de conformidade.
6.3.1.4.3.1.3. Criar dashboards específicos para áreas distintas (SOC, Segurança da Informação, Infraestrutura), atendendo às necessidades operacionais da CONTRATANTE.
6.3.1.4.3.2. Integração e Monitoramento de Soluções
6.3.1.4.3.2.1. Integrar o Grafana com os dados do Wazuh e Graylog, consolidando alertas e indicadores de forma centralizada.
6.3.1.4.3.2.2. Configurar painéis de correlação entre vulnerabilidades, incidentes e eventos de log, permitindo análise rápida e tomada de decisão.
6.3.1.4.3.2.3. Implementar alarmes e notificações no Grafana para situações críticas, com integração ao sistema de chamados do SOC.
6.3.1.4.3.3. Relatórios Avançados e Visibilidade Estratégica
6.3.1.4.3.3.1. Emitir relatórios executivos com indicadores de performance, tendências de ataques e postura de segurança.
6.3.1.4.3.3.2. Consolidar informações do Wazuh (HIDS, vulnerabilidades, conformidade) e Graylog (logs, tentativas de acesso, elevação de privilégios) em relatórios unificados.
6.3.1.4.3.3.3. Disponibilizar relatórios customizados para apoiar auditorias, reuniões de gestão e processos de tomada de decisão estratégica.
6.3.1.4.4. Franquia 40 horas para Resposta Proativa a Incidentes de Segurança
6.3.1.4.4.1. Composição dos Serviços Gerenciados de Red Team Proativo (Avaliação Contínua da Postura de Segurança): Estes serviços têm como objetivo principal avaliar proativamente a postura de segurança da CONTRATANTE, identificar e validar vulnerabilidades antes de um incidente, simulando ataques realistas para fortalecer as defesas.
6.3.1.4.4.1.1. Testes de Invasão de Rede Externa (Perímetro Internet): Trimestral.
6.3.1.4.4.1.2. Testes de Invasão de Rede Interna: Semestral.
6.3.1.4.4.1.3. Testes de Email-Phishing: Semestral.
6.3.1.4.4.1.4. Password & Credential Assessment: Mensal.
6.3.1.4.4.1.5. As análises e testes serão realizados tanto por meio de ferramentas automatizadas quanto com atuação de equipe especializada de Red Team.
6.3.1.4.4.1.6. As vulnerabilidades identificadas por estes serviços e por outras ferramentas (Wazuh, OpenVAS/Greenbone, Trivy, OWASP ZAP) deverão ser registradas e publicadas em um sistema WEB centralizado, com acesso seguro, criptografado e devidamente autenticado. Cada vulnerabilidade registrada no sistema deverá estar acompanhada das informações necessárias para a sua adequada correção.
6.3.1.4.4.2. Composição dos serviços gerenciados de gestão de vulnerabilidades, riscos e conformidade de infraestrutura e aplicações web (OpenVAS/Greenbone Vulnerability Management, Trivy, OWASP ZAP e Wazuh):
6.3.1.4.4.2.1. Realizar análise contínua de até 500 servidores, ativos de rede, ativos de segurança e recursos em cloud computing, utilizando OpenVAS/Greenbone e Trivy para identificação e priorização de vulnerabilidades.
6.3.1.4.4.2.2. Executar varredura de até 50 (cinquenta) aplicações web por meio do OWASP ZAP, permitindo monitoramento contínuo e detecção de vulnerabilidades específicas.
6.3.1.4.4.2.3. Consolidar relatórios priorizados por criticidade, abrangendo servidores, ativos críticos, perímetro Internet e aplicações web. Todas as vulnerabilidades serão reportadas e gerenciadas através do sistema WEB centralizado (6.3.1.4.4.1.6).
6.3.1.4.4.2.4. Possibilidade de Utilização de Solução Própria da CONTRATADA para Análise de Vulnerabilidades:
6.3.1.4.4.2.4.1 É facultado à CONTRATADA, mediante prévia aprovação da CONTRATANTE, utilizar solução própria que otimize o processo de análise de vulnerabilidades em servidores, ativos de rede, ativos de segurança, recursos em cloud computing e aplicações web, desde que esta solução atenda integralmente ao escopo e entregue os mesmos resultados esperados dos serviços descritos nos itens 6.3.1.4.4.2.1 e 6.3.1.4.4.2.2 e que não gere custo adicional à CONTRATANTE.
6.3.1.4.5. Composição dos serviços de administração, atualização, manutenção, monitoramento e suporte técnico da solução Kaspersky Security Center (KSC)
6.3.1.4.5.1. Verificar o status do Servidor de Administração do Kaspersky Security Center, por meio da geração de relatórios e painéis para certificar-se do correto funcionamento dos servidores de rede.
6.3.1.4.5.2. Acompanhar diariamente as atualizações das bases de antivírus e módulos de proteção no KSC, assegurando que todos os endpoints recebam as últimas definições. 6.3.1.4.5.3. Monitorar os logs e alertas de segurança no KSC, com especial atenção às detecções do antivírus e de outros módulos de proteção. Em caso de incidentes não solucionados automaticamente, acionar através de chamados.
6.3.1.4.5.4. Identificar, nos relatórios do KSC, equipamentos com módulos de proteção desativados (ex.: File Anti-Virus, Web Anti-Virus, Network Attack Blocker), enviando comandos de ativação e aplicando correções necessárias.
6.3.1.4.5.5. Gerar relatórios semanais do KSC contendo estatísticas de atualização, detecção de ameaças e conformidade dos endpoints.
6.3.1.4.5.6. Realizar a limpeza e ajustes manuais de computadores que apresentem registros duplicados (ex.: IPs ou nomes duplicados) no banco de dados do KSC.
6.3.1.4.5.7. Verificar a execução dos backups automáticos da base de dados do KSC, programados periodicamente, garantindo que sejam concluídos com sucesso.
6.3.1.4.5.8. Realizar varreduras de descoberta de rede no KSC, com a finalidade de identificar computadores não gerenciados ou desprovidos de antivírus, promovendo sua integração ao ambiente. As informações de inventário geradas serão consolidadas em uma base unificada ou apresentadas de forma integrada no Grafana (conforme 6.3.1.4.1.13.2).
6.3.1.4.5.9. Enviar pacotes de atualização de software, patches e definições de segurança para os clientes que estiverem desatualizados.
6.3.1.4.5.10. Gerar relatórios mensais com os quantitativos de endpoints que apresentaram problemas críticos e que demandaram tratamento por meio de chamados técnicos.
6.3.1.4.6. Monitoramento da solução Aruba ClearPass
6.3.1.4.6.1. Monitorar os logs, alertas e eventos de autenticação e autorização no ClearPass, com atenção especial a falhas de login, tentativas de acesso indevido e dispositivos não conformes às políticas de segurança.
6.3.1.4.6.2. Identificar nos relatórios do ClearPass os dispositivos que não estejam em conformidade (ex.: endpoints sem antivírus atualizado, sem patches de sistema ou com configurações de segurança inadequadas), aplicando políticas de quarentena ou restrição de acesso.
6.3.1.4.6.3. Gerar relatórios semanais do ClearPass, com estatísticas de acessos permitidos, negados e dispositivos colocados em quarentena, consolidando a visibilidade do ambiente. 6.3.1.4.6.4. Realizar scans e varreduras de rede (profiling) utilizando os recursos nativos do ClearPass, com a finalidade de identificar dispositivos não autorizados, IoT não gerenciados ou endpoints sem conformidade, aplicando as devidas políticas de segurança. As informações de inventário e

profiling geradas serão consolidadas em uma base unificada ou apresentadas de forma integrada no Grafana (conforme 6.3.1.4.1.13.2).
6.3.1.4.6.5. Gerar relatórios mensais consolidados contendo os quantitativos de acessos bem-sucedidos, falhas de autenticação, incidentes de não conformidade e dispositivos bloqueados, com indicadores de desempenho do NAC.
6.3.1.4.7. Canal de Atendimento
6.3.1.4.7.1. Deverá ser disponibilizado um Canal de Atendimento em regime integral de 24 (vinte e quatro) horas em 7 (sete) dias na semana e em feriados.
6.3.1.4.7.2. O Canal de Atendimento deverá ser implementado por meio de ferramentas de comunicação disponibilizadas pela CONTRATADA de modo a garantir a disponibilidade de contato, sendo, no mínimo:
6.3.1.4.7.2.1. Via plataforma Google Meet.
6.3.1.4.7.2.2. Via aplicativo WhatsApp.
6.3.1.4.7.2.3. Via E-mail.
6.3.1.4.7.2.4. Via telefone, com a disponibilização de 2 (dois) números de contato.
6.3.1.4.7.2.5. Outros canais de comunicação poderão ser também disponibilizados pela CONTRATADA, desde que com a anuência da CONTRATANTE e sem prejuízo ao regime de atendimento especificado neste ETP.
6.3.1.4.8. Serviços de Resposta a Incidentes Cibernéticos, Investigação, Mitigação e Análise Forense (Banco de Horas). Estes serviços complementam as ações de resposta automatizadas/de primeiro nível das ferramentas (Wazuh, Graylog), sendo acionados para incidentes que demandem investigação aprofundada, contenção manual complexa, erradicação, recuperação emergencial, análise forense ou validação pós-incidente. 6.3.1.4.8.1. Consistem em serviços de preparação, detecção, análise, contenção, erradicação, recuperação em situação emergencial e em pós-incidente, por meio de banco de horas de 800 (oitocentas) horas a serem consumidas durante a vigência contratual, sob demanda da CONTRATANTE, bem como:
6.3.1.4.8.1.1. Recomendação de medidas para mitigação dos ataques e ameaças detectadas (adequação de regras de firewall, proteção de endpoint, atualização de sistema operacional, dentre outros).
6.3.1.4.8.1.2. Apoio na implementação de ações de remediação e/ou mitigação de vulnerabilidades de segurança da informação.
6.3.1.4.8.1.3. Assessoria na aplicação de atualizações de segurança no ambiente, quando pertinente.
6.3.1.4.8.1.4. Assessoria para restauração do ambiente ao seu estado normal de operação. 6.3.1.4.8.1.5. Definir, propor e executar uma estratégia para a mitigação e contenção do ataque. 6.3.1.4.8.1.6. Investigar e identificar no ambiente alvo ameaças persistentes ou vulnerabilidades passíveis de exploração, propondo soluções para a sua mitigação e, quando possível, realizar o tratamento das ameaças identificadas.
6.3.1.4.8.1.7. Identificar as vulnerabilidades exploradas pelo atacante que permitiram o comprometimento do ambiente.
6.3.1.4.8.1.8. Monitorar o ambiente, após a sua restauração, para identificar e conter novos ataques.
6.3.1.4.8.1.9. Responder a eventuais novos ataques cibernéticos.
6.3.1.4.8.2. Composição dos Serviços Gerenciados de Red Team Pós-Incidente: Estes serviços são acionados no contexto de resposta a incidentes, com foco na validação da remediação, identificação de vulnerabilidades persistentes após um comprometimento e avaliação da resiliência do ambiente após um ataque.
6.3.1.4.8.2.1. Teste de invasão do perímetro Internet e identificação de vulnerabilidades persistentes no ambiente.
6.3.1.4.8.2.2. Serviços de Password Assessment, para identificação de credenciais frágeis de usuário e senha de domínio AD, potencialmente exploradas por atacantes e utilizadas para comprometer o ambiente.
6.3.1.4.8.3. Demandas de Atividades:
6.3.1.4.8.3.1. A CONTRATANTE, para demandar a contratação das horas, deverá emitir Ordem de Serviço contendo as atividades a serem executadas pela CONTRATADA, total de horas estimadas para a execução de cada atividade.
6.3.1.4.8.3.2. Os projetos que se utilizam das 800 (oitocentas) horas poderão ter suas atividades gerais estimadas:
6.3.1.4.8.3.2.1. Serviços de preparação, detecção, análise, contenção, erradicação, recuperação em situação emergencial e em pós-incidente: 500 (quinhentas) horas.
6.3.1.4.8.3.2.2. Serviços de recomendações, apoio, assessoria e investigação: 300 (trezentas) horas.
6.3.1.4.8.3.3. Por se tratarem de atividades de segurança da informação onde o escopo do projeto não pode ser definido, tendo em vista que a motivação é futura, é permitido à CONTRATANTE redimensionar a estimativa de horas alocada para as atividades gerais acima descritas, desde que justificadas em Ordem de Serviço.

7. DA NECESSIDADE DE FORMALIZAÇÃO DE CONTRATO

7.1 Os eventuais acionamentos dos Grupos 1, 2 e 4 resultarão em contratações de natureza contínua, pois os itens desses grupos constituem serviços que visam atender a demanda do TJAM de forma permanente e contínua, por mais de um exercício financeiro.

7.1.1 A duração inicial desses contratos será de 12 meses, podendo ser prorrogados sucessivamente, respeitada a vigência máxima decenal, conforme Art. 107 da Lei Federal n.° 14.133/2021.

7.2 Os eventuais acionamentos do Grupo 3, por sua vez, resultarão em contratações por escopo, pois esse grupo resume-se a aquisição e implantação de equipamentos e infraestrutura de rede LAN, além de serviços associados à instalação e configuração.

7.2.1 A duração desses contratos será de 36 meses, podendo ser prorrogados, desde que justificadamente, pelo prazo necessário à conclusão do objeto, conforme Art. 6º, XVII, da Lei Federal n.° 14.133/2021.

8. ESTIMATIVAS DAS QUANTIDADES PARA A CONTRATAÇÃO

GRUPO 1: Serviço de Comunicação de Dados a ser prestado na cidade de Manaus				
ITEM	**DESCRIÇÃO**	**UND.**	**Quantidade Mínima**	**Quantidade Total**
1	Serviço mensal de comunicação de dados do tipo transporte via Fibra Óptica com dupla abordagem e velocidade de 10 Gbps para o Concentrador na Sede do TJAM	ponto	1	1
2	Serviço mensal de comunicação de dados do tipo transporte via Fibra Óptica com velocidade de 1000 Mbps para as unidades descentralizadas do TJAM	ponto	1	4
3	Serviço mensal de comunicação de dados do tipo transporte via Fibra Óptica com velocidade de 100 Mbps para as unidades descentralizadas do TJAM	ponto	9	9
4	Serviço de instalação do ponto de acesso.	und.	11	14
5	Serviço de remanejamento de ponto de acesso (equipamentos/enlace).	und.	11	14

GRUPO 2: Serviço de Comunicação de Dados a ser prestado nas comarcas do interior do Estado do Amazonas				
ITEM	**DESCRIÇÃO**	**UND.**	**Quantidade Mínima**	**Quantidade Total**
6	Serviço mensal de comunicação de dados do tipo transporte via Fibra Óptica com dupla abordagem e velocidade de 10 Gbps para o Concentrador na Sede do TJAM	ponto	1	1
7	Serviço mensal de comunicação de dados do tipo transporte via Fibra Óptica com velocidade de 50 Mbps para as unidades descentralizadas do TJAM	ponto	20	49
8	Serviço de instalação do ponto de acesso.	und.	21	50
9	Serviço de remanejamento de ponto de acesso (equipamentos/enlace).	und.	21	50

Grupo 3: Fornecimento e instalação de equipamentos na cidade de Manaus				
ITEM	**DESCRIÇÃO**	**UND.**	**Quantidade Mínima**	**Quantidade Total**
10	Switch gerenciado de distribuição (para unidades com alto tráfego de dados)	und.	1	4
11	Interface 10g ethernet para longa distância	und.	18	72
12	Instalação de switch gerenciado	serviço	1	4

GRUPO 4: Serviço de NOC/SOC e Resposta a Incidente				
ITEM	**DESCRIÇÃO**	**UND.**	**Quantidade Mínima**	**Quantidade Total**
13	Monitoramento e gestão de eventos da infraestrutura de TIC do TJAM, em regime 24x7x365, através da implantação de NOC (Network Operations Center) e SOC (Security Operations Center)	serviço	1	1
14	Resposta a Incidentes Cibernéticos, Investigação, Mitigação e Análise Forense de Incidentes de Segurança	hora	100	800

9. ESTIMATIVA DE PREÇOS OU PREÇOS REFERENCIAIS

GRUPO 1: Serviço de Comunicação de Dados a ser prestado na cidade de Manaus (12 meses)						
ITEM	**DESCRIÇÃO**	**Quantidade Mínima**	**Quantidade Total**	**VL UNIT.**	**VL MENSAL**	**VALOR TOTAL**
1	Serviço mensal de comunicação de dados do tipo transporte via Fibra Óptica com dupla abordagem e velocidade de 10 Gbps para o Concentrador na Sede do TJAM	1	1	R$ 58.332,50	R$ 58.332,50	R$ 699.990,00
2	Serviço mensal de comunicação de dados do tipo transporte via Fibra Óptica com velocidade de 1000 Mbps para as unidades descentralizadas do TJAM	1	4	R$ 7.500,00	R$ 30.000,00	R$ 360.000,00
3	Serviço mensal de comunicação de dados do tipo transporte via Fibra Óptica com velocidade de 100 Mbps para as unidades descentralizadas do TJAM	9	9	R$ 1.083,30	R$ 9.749,70	R$ 116.996,40
4	Serviço de instalação do ponto de acesso.	11	14	R$ 100,00	-	R$ 1.400,00
5	Serviço de remanejamento de ponto de acesso (equipamentos/enlace).	11	14	R$ 100,00	-	R$ 1.400,00
					TOTAL DO GRUPO	**R$ 1.179.786,40**

GRUPO 2: Serviço de Comunicação de Dados a ser prestado nas comarcas do interior do Estado do Amazonas (12 meses)						
ITEM	**DESCRIÇÃO**	**Quantidade Mínima**	**Quantidade Total**	**VL UNIT.**	**VL MENSAL**	**VALOR TOTAL**
6	Serviço mensal de comunicação de dados do tipo transporte via Fibra Óptica com dupla abordagem e velocidade de 10 Gbps para o Concentrador na Sede do TJAM	1	1	R$ 58.332,50	R$ 58.332,50	R$ 699.990,00
7	Serviço mensal de comunicação de dados do tipo transporte via Fibra Óptica com velocidade de 50 Mbps para as unidades descentralizadas do TJAM	20	49	R$ 3.333,33	R$ 163.333,17	R$ 1.959.998,04
8	Serviço de instalação do ponto de acesso.	21	50	R$ 100,00	-	R$ 5.000,00
9	Serviço de remanejamento de ponto de acesso (equipamentos/enlace).	21	50	R$ 100,00	-	R$ 5.000,00
					TOTAL DO GRUPO	**R$ 2.669.988,04**

Grupo 3: Fornecimento e instalação de equipamentos na cidade de Manaus (36 meses)						
ITEM	**DESCRIÇÃO**	**UND.**	**Quantidade Mínima**	**Quantidade Total**	**VL UNT.**	**VALOR TOTAL**
10	Switch gerenciado de distribuição (para unidades com alto tráfego de dados)	und.	1	4	R$ 120.296,00	R$ 481.184,00
11	Interface 10g ethernet para longa distância	und.	18	72	R$ 19.763,00	R$ 1.422.936,00
12	Instalação de switch gerenciado	serviço	1	4	R$ 2.716,00	R$ 10.864,00
					TOTAL DO GRUPO	**R$ 1.914.984,00**

GRUPO 4: Serviço de NOC/SOC e Resposta a Incidente (12 meses)							
ITEM	**DESCRIÇÃO**	**UND.**	**Quantidade Mínima**	**Quantidade Total**	**VL UNT.**	**VL MENSAL**	**VALOR TOTAL**
13	Monitoramento e gestão de eventos da infraestrutura de TIC do TJAM, em regime 24x7x365, através da implantação de NOC (Network Operations Center) e SOC (Security Operations Center)	serviço	1	1	R$ 122.151,67	R$ 122.151,67	R$ 1.465.820,02
14	Resposta a Incidentes Cibernéticos, Investigação, Mitigação e Análise Forense de Incidentes de Segurança	hora	100	800	R$ 275,00	-	R$ 220.000,00
						TOTAL DO GRUPO	**R$ 1.685.820,02**

10. JUSTIFICATIVA PARA PARCELAMENTO OU NÃO DA CONTRATAÇÃO

10.1 Cada grupo deverá possuir vencedor único para todos os itens, uma vez que os bens e serviços pretendidos em cada grupo estão intrinsecamente relacionados. A adjudicação dos itens, dentro do mesmo grupo, para empresas diferentes poderia resultar na aquisição de soluções incompatíveis, o que acarretaria prejuízo a CONTRATANTE.

11. CONTRATAÇÕES CORRELATAS/INTERDEPENDENTES

11.1 As contratações oriundas dos eventuais acionamentos do:

11.1.1 Grupo 1 e Grupo 2: servirão para substituir o Contrato Administrativo nº 006/2021 e suplementar o Contrato Administrativo nº 046/2023;

11.1.2 Grupo 3: Suplementar o Contrato Administrativo nº 001/2025;

11.1.3 Grupo 4: Gerenciar a execução das contratações oriundas dos Grupos 1, 2 e 3.

12. RESULTADOS PRETENDIDOS

12.1 Assegurar a interligação ininterrupta entre a sede e as unidades do TJAM, na capital e no interior, com alta disponibilidade, baixa latência e redundância de backbones, evitando riscos de descontinuidade do serviço jurisdicional.

12.2 Substituir e expandir switches de distribuição por equipamentos da marca Aruba, plenamente integrados ao **Aruba Central**, garantindo maior desempenho, segurança, escalabilidade e facilidade de gestão centralizada.

12.3 Implementar serviços de NOC utilizando o **Zabbix Community**, com acompanhamento contínuo de links, servidores, bancos de dados, aplicações e datacenter, assegurando resposta rápida a falhas e anomalias.

12.4 Operacionalizar o SOC com uso das ferramentas **Wazuh** e **Grafana**, viabilizando detecção de ameaças, correlação de eventos, análise de comportamento anômalo e emissão de alertas tempestivos, em conformidade com diretrizes do CNJ.

12.5 Disponibilizar equipe e horas técnicas especializadas para investigação, contenção, mitigação e análise forense de incidentes, promovendo maior resiliência cibernética e reduzindo o tempo de indisponibilidade em situações de crise.

12.6 Simplificar a gestão de redes e segurança por meio de plataformas unificadas (Aruba Central, Zabbix, Wazuh, Grafana), evitando soluções fragmentadas, reduzindo TCO (Custo Total de Propriedade) e otimizando recursos humanos e financeiros.

12.7 Atender às Resoluções do CNJ (nº 370/2021 e nº 468/2022) e às normativas internas do TJAM, garantindo governança, rastreabilidade e alinhamento com os padrões nacionais de segurança da informação.

12.8 Entregar conectividade estável, desempenho otimizado e menor tempo de resposta para magistrados, servidores e jurisdicionados, resultando em maior eficiência nos serviços judiciais e administrativos.

13. PROVIDÊNCIAS PARA ADEQUAÇÃO DO AMBIENTE DO ÓRGÃO

13.1 Não há necessidade de adequação do ambiente das unidades para a implantação da solução.

14. IMPACTOS AMBIENTAIS

14.1 Aplicar, no que couber, a Resolução CNJ nº 400 de 16 de junho de 2021 que dispõe sobre a política de sustentabilidade no âmbito do Poder Judiciário.

15. SERVIÇOS DE MANUTENÇÃO E ASSISTÊNCIA TÉCNICA

15.1 Grupos 1 e 2: Caso haja a necessidade de realizar manutenção preventiva da solução, a CONTRATADA deverá formalizar via e-mail, à FISCALIZAÇÃO, com no mínimo dois dias úteis de antecedência da data proposta para a realização do serviço e que deverá ser autorizada pela CONTRATANTE.

15.2 Grupo 3

15.2.1. Toda a solução deste Grupo deverá considerar período de garantia por um prazo de 36 (trinta e seis) meses para a solução como um todo (hardware e software), exceto para os switches, que deverão ter sua garantia do tipo lifetime, extensível pelo período mínimo de 05 anos após o end of sales do equipamento;
15.2.2. Conforme disposto na lei 14.133/2021, Art. 40, inciso V, alínea a) (V - atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho), todos os itens deverão ser da marca Aruba.
15.2.3. Os chamados serão abertos juntamente a autorizada oficial do fabricante no Brasil através de ligação telefônica no idioma português, website e e-mail durante a vigência da garantia. O suporte deverá ser na modalidade de 24x7 (24 horas por dia, 7 dias por semana) durante o prazo de garantia;
15.2.4. Durante o prazo de garantia, deve ser possível realizar a atualização de sistema operacional dos equipamentos para obter novas funcionalidades e correção de bugs;
15.2.5. Em caso de defeitos de fabricação, a garantia deve incluir envio de peças ou equipamentos de reposição até o local onde o equipamento está instalado, obedecendo a modalidade NBD (Next Business Day).

16. DECLARAÇÃO DE VIABILIDADE (OU NÃO) DA CONTRATAÇÃO

16.1 Considerando todo o exposto, esta Secretaria de Tecnologia da Informação e Comunicação declara que a formação de ARP para prestação de serviços de comunicação de dados, NOC/SOC e Resposta a Incidente, assim como fornecimento e instalação de equipamentos de rede, é não só viável, mas indispensável para o TJAM manter a alta disponibilidade, segurança e continuidade de suas operações, em consonância com as exigências regulatórias e a criticidade de suas atividades.

17. OBRIGAÇÕES PERTINENTES À LEI GERAL DE PROTEÇÃO DE DADOS

17.1 O objeto desta contratação, por si só, não está diretamente vinculada à Lei Geral de Proteção de Dados (LGPD). Portanto, esta aquisição não exige cláusulas específicas de proteção de dados.

18. MAPEAMENTO DE RISCOS

FASE: ESTUDO TÉCNICO PRELIMINAR											
ID	**Risco**	**Causa (Devido a)**	**Evento (Poderá ocorrer)**	**Consequência (O que poderá levar a)**	**Prob.**	**Impacto**	**Nível**	**Resposta**	**Medidas Preventivas**	**Medidas de Contingência**	**Respo**
R1	Interrupção de conectividade entre capital e interior	Não contratação dos Grupos 1 e 2 (MPLS) após o término do contrato atual	Indisponibilidade de links de backup de baixa capacidade.	Eliminação formal da redundância de comunicação, com aumento do risco operacional em caso de falha do link principal — mas sem impacto relevante adicional, visto que a atual capacidade já não atende adequadamente.	Alta	Baixo	Médio	Aceitar/Mitigar	Priorizar a contratação de novos links com capacidade adequada, evitando manutenção de circuitos obsoletos.	Em caso de falha do link principal, readequar o tráfego via provedores alternativos	Al Adminis SET
R2	Incompatibilidade tecnológica na LAN	Aquisição de switches de fabricantes distintos sem integração ao Aruba Central	Incompatibilidade com sistema de gerenciamento unificado já implantado	Perda de eficiência na gestão de rede, aumento de custos e risco de falhas	Média	Alto	Alto	Evitar	Garantir aquisição apenas de switches Aruba compatíveis	Realocação de equipamentos não integráveis e aquisição emergencial de modelos compatíveis	SET
R3	Vulnerabilidade cibernética não detectada	Ausência de contratação do SOC (Grupo 4)	Ameaças não monitoradas ou incidentes não tratados tempestivamente	Ataques cibernéticos com perda de dados, indisponibilidade ou vazamento de informações sensíveis	Alta	Alto	Crítico	Mitigar	Implantar SOC 24x7 com Wazuh e Grafana	Acionamento emergencial de força-tarefa de segurança e apoio externo	Al Adminis SET

FASE: ESTUDO TÉCNICO PRELIMINAR											
ID	**Risco**	**Causa (Devido a)**	**Evento (Poderá ocorrer)**	**Consequência (O que poderá levar a)**	**Prob.**	**Impacto**	**Nível**	**Resposta**	**Medidas Preventivas**	**Medidas de Contingência**	**Respo**
R4	Indisponibilidade de sistemas críticos	Ausência de monitoramento contínuo (NOC – Grupo 4)	Falhas de rede/servidores não detectadas a tempo	Indisponibilidade de serviços como SEI, Projudi e e-SAJ	Alta	Alto	Crítico	Mitigar	Manter monitoramento 24x7 via Zabbix Community	Reconfiguração emergencial manual, mobilizando equipe interna	Al Adminis SET
R5	Descumprimento de normativas CNJ	Não implantação de NOC/SOC conforme Ofício nº 205-PRES/SGTJ e Res. CNJ nº 370/2021	Irregularidade administrativa e descumprimento de determinação nacional	Sanções administrativas, apontamentos em auditorias e risco à governança de TIC	Média	Alto	Alto	Evitar	Assegurar contratação em conformidade com exigências do CNJ	Justificar formalmente à Corregedoria/CNJ eventual atraso	Al Admini
R6	Aumento de custos operacionais	Falta de padronização e gestão unificada de rede	Manutenção fragmentada e uso de múltiplas controladoras	Aumento do TCO (Total Cost of Ownership) e desperdício de recursos públicos	Média	Médio	Médio	Mitigar	Padronizar em Aruba Central e switches Aruba	Readequação contratual ou migração gradual para padrão definido	SET
R7	Atraso na implantação dos serviços	Processo de contratação não concluído em tempo hábil	Sobreposição de contratos antigos com término de vigência	Descontinuidade operacional, necessidade de contratação emergencial mais onerosa	Alta	Médio	Alto	Transferir/mitigar	Planejamento antecipado, cronograma de implantação alinhado	Formalização de aditivo emergencial/dispensa justificada	Al Admini

NÍVEL DE RISCO

Alto: Obrigatoriedade de tratamento do risco por meio de ação, monitoramento, e controle efetivo.

Moderado: Recomendável o tratamento do risco por meio de ação, monitoramento, e controle.

Baixo: Não há obrigatoriedade de tratamento do risco, cabendo uma reavaliação no ciclo posterior e/ou decisão da alta direção do TJAM quanto à emissão de ação, após a análise do tema em questão.

Baixo	**Menor e/ou igual a 5.**
Moderado	**Entre 6 e 9.**
Alto	**Maior que 9.**

Manaus- AM, data registrada no sistema.

Diogo Mendonça de Sousa
Diretor de Infraestrutura de TIC
Secretaria de Tecnologia da Informação e Comunicação - SETIC
(assinado digitalmente)

Documento assinado eletronicamente por **DIOGO MENDONCA DE SOUSA**, **Diretor(a)**, em 21/01/2026, às 13:53, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tjam.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2671070** e o código CRC **B65262AD**.