



TRIBUNAL REGIONAL ELEITORAL DO PARÁ
Rua João Diogo 288 - Bairro Campina - CEP 66015-902 - Belém - PA
ESTUDOS TÉCNICOS PRELIMINARES
(ETP SERVIÇOS - TIC)

1. DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO (obrigatório)

Fundamentação: Descrição da necessidade da contratação, considerado o problema a ser resolvido sob a perspectiva do interesse público (inciso I do § 1º do art. 18 da Lei 14.133/2021 e art. 11, inciso I da IN SGD/ME 94/2022).

1.1. Descrição da necessidade

1.1.1. Sobre o detalhamento da necessidade de uma nova visão sobre segurança da informação e defesa cibernética com adoção de inteligência artificial generativa e nova arquitetura de malha

O Tribunal Regional Eleitoral do Pará (TRE-PA) é o órgão do Poder Judiciário Federal responsável pela gestão, organização e fiscalização do processo democrático no estado do Pará. Sua missão institucional é garantir a legitimidade do processo eleitoral e o livre exercício do direito de votar e ser votado, fundamentais para a manutenção do Estado Democrático de Direito.

Para o desempenho adequado de suas funções e a resiliência de serviços essenciais, como o cadastro de eleitores e a apuração de resultados, o Tribunal conta com uma infraestrutura tecnológica capilarizada, composta por 101 Zonas Eleitorais e diversas unidades judiciárias distribuídas por todo o território paraense, contando ainda com serviços hospedados em Data Center Tier 3, localizado na Sede do Tribunal, e Serviços em Nuvem.

Diante da crescente digitalização e da sofisticação das ameaças digitais, a Justiça Eleitoral do Pará necessita de serviços especializados e ininterruptos de suporte em segurança da informação e operação de infraestrutura crítica. Tais serviços são pilares indispensáveis para assegurar a confidencialidade, integridade e disponibilidade dos dados sob custódia do Tribunal, garantindo a conformidade com a Lei Geral de Proteção de Dados (LGPD) e a proteção dos ativos tecnológicos contra riscos cibernéticos que possam comprometer a soberania dos pleitos eleitorais e a confiança da sociedade.

Nesse panorama, a infraestrutura da Justiça Eleitoral do Pará reflete o cenário de crescente complexidade enfrentado pelas organizações modernas, onde a segurança cibernética em ambientes híbridos torna-se um desafio central. Os dados não estão mais confinados a um Data Center local; eles residem em plataformas de nuvem, são acessados em trabalho remoto e por meio de dispositivos móveis (BYOD). Essa dissolução do perímetro de rede tradicional torna obsoletos os modelos tradicionais de segurança baseados em confiança perimetral.

Neste contexto, surge a arquitetura Zero Trust (ZTA), ou "Confiança Zero", tornando-se fundamental para a proteção de dados nas organizações. A ZTA abandona a ideia de um "limite de confiança" ou "borda de rede" segura, partindo do princípio "nunca confie, sempre verifique" (never trust, always verify). Em vez de confiar implicitamente na localização da rede, a ZTA foca na identidade (de usuários e dispositivos), nos ativos e nos recursos. Isso exige a verificação explícita e contínua de cada solicitação de acesso, independentemente da origem, o que é essencial para proteger ambientes distribuídos e mitigar riscos de forma eficaz.

Contudo, a implementação prática dessa filosofia esbarra em um desafio histórico: as abordagens de segurança típicas são construídas em produtos pontuais especializados operando em silos para defender ativos de maneira reativa e especializada, o que aumenta os custos, cria regiões de "sombra" ou mesmo "sobreposição" de funcionalidades e deixa lacunas consideráveis na cobertura e na visibilidade. As abordagens tradicionais para arquitetura de segurança foram projetadas para uma geração anterior de computação na qual tínhamos controle físico sobre praticamente tudo.

Agora, como mencionado, os ativos digitais estão amplamente espalhados por muitos locais e muitas nuvens, portanto, precisamos de uma nova abordagem para exercer o controle em ambiente distribuído. Por isso, o modelo de silos é inadequado para a natureza rápida e distribuída da maioria das organizações modernas. Defender um ambiente computacional moderno requer uma nova abordagem que trate a segurança como um ecossistema, e não como uma coleção de soluções isoladas.

Na visão do Gartner, as organizações que adotarem uma arquitetura de malha de segurança cibernética (CSMA) para integrar ferramentas de segurança, de modo que funcionem juntas como um ecossistema, reduzirão o impacto financeiro de incidentes de segurança individuais em 90%, em média.

Uma arquitetura de malha de segurança cibernética (CSMA) é um ecossistema colaborativo de ferramentas e controles para proteger uma empresa moderna e distribuída. Ele se baseia em uma estratégia de integração de ferramentas de segurança distribuídas e combináveis, centralizando os dados e o plano de controle para obter uma colaboração mais eficaz entre as ferramentas. Os resultados incluem recursos aprimorados para detecção, respostas mais eficientes, políticas consistentes, postura e gerenciamento de playbook e controle de acesso mais adaptável e granular - todos os quais levam a uma melhor segurança. Um CSMA promove composição, escalabilidade e interoperabilidade.

No mundo dinâmico de computação distribuída de hoje, silos desconectados de ferramentas de segurança são insuficientes. Ao mesmo tempo, os líderes e gestores públicos de segurança e gerenciamento de riscos estão procurando maneiras de obter mais benefícios de seus investimentos existentes. Os esforços de consolidação dos fornecedores de segurança são promissores em algumas áreas, contudo os benefícios e resultados financeiros e de eficiência operacional dependem muito de uma visão integrada, conectada e de um ecossistema consolidado trazendo uma única abordagem adotada.

Os líderes e gestores públicos de segurança cibernética estão procurando maneiras de aumentar a eficiência de suas operações, reduzir a carga sobre sua equipe e responder com mais eficácia às ameaças e aos requisitos e oportunidades de negócios. A visão clara e objetiva do CSMA – Cybersecurity Mesh Architecture tem quatro camadas fundamentais para permitir que controles de segurança distintos funcionem juntos e facilitem sua configuração e gerenciamento, conforme exibem as Figuras 1, a seguir.

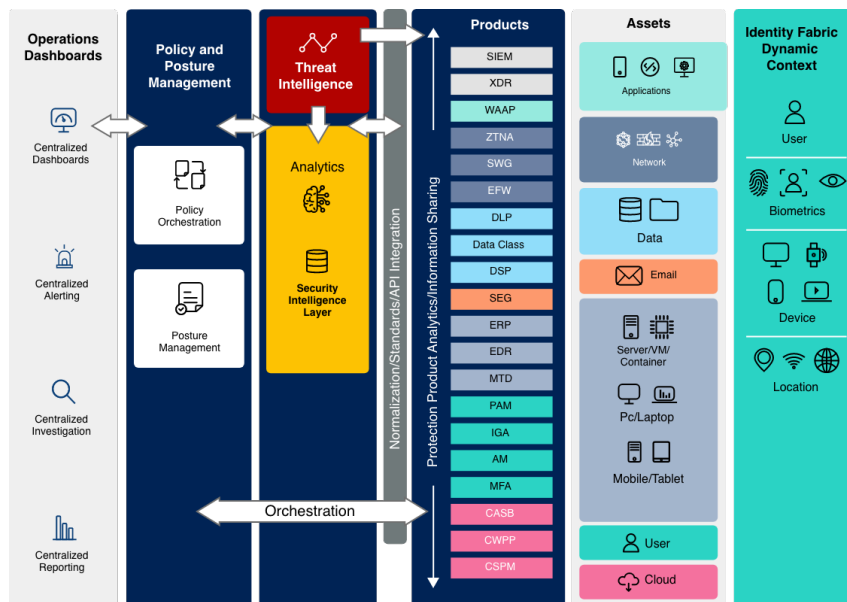


Figura 1 - Leveraging Cybersecurity Mesh Architecture

A figura anterior, "Figura 2 - Leveraging Cybersecurity Mesh Architecture", detalha a visão do Gartner para a arquitetura de malha de segurança cibernética (CSMA). Ela ilustra como controles de segurança distintos podem funcionar juntos como um ecossistema colaborativo, superando o modelo tradicional de silos. Conforme descrito no ETP, essa arquitetura se baseia em quatro camadas fundamentais: (1) a Estrutura de Identidade ("Identity Fabric"), que fornece contexto dinâmico sobre ativos, usuários e dispositivos; (2) a Política Consolidada ("Policy and Posture Management"), que utiliza esse contexto para orquestrar regras de forma centralizada; (3) a Análise e Inteligência de Segurança ("Analytics" e "Threat Intelligence"), que processa dados dos diversos "Products" (ferramentas como SIEM, XDR, WAF); e (4) os Painéis Consolidados ("Operations Dashboards"), que unificam a visualização, alertas e investigação. A interoperabilidade entre essas camadas e os produtos é viabilizada por uma base de integração ("Normalization/Standards/API Integration" e "Information Sharing"), permitindo que a segurança atue como um ecossistema adaptativo e não como uma coleção de ferramentas isoladas.

Para construir uma arquitetura de malha de segurança cibernética (CSMA), os gestores públicos de segurança responsáveis e a CONTRATADA devem:

- Consolidar as ferramentas de segurança existentes para um maior alinhamento com os princípios do CSMA, explorando as opções de integração pré-construídas, onde agregam valor aos casos de uso existentes.
- Reduzir o tempo de valorização ao buscar um CSMA implantando plataformas de segurança consolidadas, sempre que possível.
- Obter todos os recursos flexíveis que suportam metas de longo prazo, fazendo investimentos direcionados na construção das quatro camadas fundamentais de um CSMA: análise e inteligência de segurança, estrutura de identidade, política consolidada, postura e gerenciamento de playbook e painéis consolidados.
- Planejar aumentar os investimentos em tecnologias independentes de análise de segurança, avaliando soluções emergentes que aplicam princípios de dados e análise às informações de segurança.
- Investir em recursos profissionais altamente especializados de forma a permitir o estudo, planejamento, implantação e a operação desta nova visão de cibersegurança e defesa cibernética.

Além disso, para potencializar as novas abordagens e modelos de trabalho, as organizações precisam fazer uso intensivo de Inteligência Artificial Generativa e automatização de processos de trabalho. No mundo dinâmico de hoje, os líderes de segurança procuram aumentar a eficiência, reduzir a carga sobre suas equipes e responder às ameaças crescentes com mais eficácia. A IA Generativa, quando integrada aos processos de trabalho existentes, atua como um componente capaz de multiplicar resultados e diminuir prazos das entregas. Ela pode analisar vastos volumes de dados de telemetria, identificar padrões de ameaças complexas que passariam despercebidos, automatizar respostas a incidentes em tempo real e sugerir políticas de acesso repetitivas, adaptativas e granulares.

Portanto, em resposta direta à obsolescência do modelo tradicional de segurança em silos e alinhado a esta visão estratégica, a presente contratação define como um de seus objetivos fundamentais a adoção e a operacionalização da arquitetura de malha de segurança cibernética (CSMA). O objetivo é substituir a abordagem reativa e fragmentada por um ecossistema de defesa verdadeiramente integrado, colaborativo e adaptativo, capaz de proteger os ativos da organização no complexo ambiente distribuído atual.

Em suma, a transição do Justiça Eleitoral do Pará para um modelo de Confiança Zero (Zero Trust) e uma Arquitetura de Malha de Segurança Cibernética (CSMA) — potencializados pelo uso de Inteligência Artificial Generativa — não é apenas uma mudança de ferramentas, mas uma mudança de paradigma operacional que depende intrinsecamente do fator humano especializado. A eficácia dessa nova visão está diretamente condicionada ao desenvolvimento e à alocação de equipes técnicas de alta senioridade, capazes de gerir a complexidade de um ambiente híbrido e descentralizado, paradigma para o qual o Tribunal está gradualmente migrando nos últimos anos. Portanto, a presente contratação, ao focar na disponibilização de perfis profissionais especializados e em indicadores de resultados (NMS), constitui o meio viabilizador para que o Tribunal abandone a defesa reativa em silos e alcance um ecossistema de proteção de dados verdadeiramente adaptativo, resiliente e alinhado aos desafios cibernéticos contemporâneos.

1.1.2. Sobre a necessidade de Contratação de Serviços Continuados de Suporte em Segurança Cibernética e Operação de Infraestrutura Crítica para o TRE-PA

A crescente adoção de tecnologias voltadas à digitalização de processos e à implementação de sistemas informatizados — como a computação em nuvem (cloud) e a Inteligência Artificial Generativa — embora ofereça benefícios de escalabilidade e eficiência, amplia significativamente a superfície de ataque. Nesse cenário, as equipes de segurança da informação enfrentam ambientes híbridos onde os dados extrapolam o perímetro tradicional do datacenter. A utilização de IA Generativa, por exemplo, introduz novos vetores de risco, como o Shadow AI, o vazamento de informações sensíveis em modelos de linguagem e a execução de ataques de engenharia social altamente sofisticados. Tais fatores elevam os desafios para a efetiva proteção de dados, exigindo monitoramento constante e especializado para garantir a resiliência cibernética em infraestruturas complexas e distribuídas, ponto considerado crítico para a Justiça Eleitoral do Pará.

De modo a assegurar os princípios garantem que o acesso às informações seja restrito a usuários autorizados, que os dados não sejam alterados indevidamente e que os sistemas e informações estejam acessíveis quando necessário (Confidencialidade, Integridade e Disponibilidade, respectivamente), é essencial o investimento em infraestrutura de segurança cibernética robusta e resiliente. Essa infraestrutura deve incluir componentes como segurança de perímetro de rede, monitoramento de ameaças, gerenciamento de exposição cibernética, controle de acesso, ecossistema de proteção de dados (backup), mecanismos de resposta a incidentes, dentre outros, todos operando em alta disponibilidade e preparados para resistir a falhas e ataques cibernéticos.

Considerando, porém, que a segurança cibernética não é uma atividade fim do TRE-PA, ou seja, não está diretamente ligada à sua missão principal de condução de eleições, o Tribunal opta por não sobrecarregar sua estrutura interna, buscando soluções externas para atingir seus objetivos sem comprometer o desempenho nas atividades principais. Neste contexto, a Secretaria de Tecnologia da Informação do TRE-PA possui quadro de pessoal especializado para execução dos serviços de Suporte Técnico/Operacional aos usuários de TIC. O quadro atual da Coordenadoria de Gestão de Segurança da Informação e Infraestrutura de Datacenter - CGSI/STI dispõe de apenas 5(once) servidores, sendo 2(dois) analistas e 3(três) técnicos de apoio especializado — tecnologia da informação, os quais

possuem diversas responsabilidades diárias relacionadas ao gerenciamento dos serviços disponibilizados por esta Secretaria na área de segurança cibernética, elaboração de contratações e fiscalização de contratos de TIC correlatos; não existindo dessa forma ociosidade por parte da equipe. Resta claro que a quantidade de servidores da CGSI/STI mostra-se insuficiente para absorver as inúmeras complexas atividades operacionais existentes nesta área, assim como a consecução de novas demandas, como implantação de novos sistemas de segurança cibernética, o que pode comprometer a eficácia da estratégia de defesa cibernética do Tribunal.

Em adição, importa destacar que, no contrato atual do Tribunal, cujo objeto versa sobre contratação de equipe dedicada à atividades de infraestrutura (CT N° 28/2020), o pagamento dos serviços se dá por meio de um rol de tarefas e respectivas atividades em suporte de TIC descritas no documento intitulado “Catálogo de Serviços”, onde foram estabelecidos a complexidade, o prazo de solução e a quantidade de Unidades de Serviços Técnicos (UST), valor de referência obtido no certame e usado para pagamento de todos dos serviços faturados. Entretanto, verificou-se, ao longo da execução do contrato atual, que a condução deste modelo vem se mostrando complexo e oneroso operacionalmente à fiscalização, composta por servidores, razão pela qual se justifica a mudança no modelo de terceirização para a modalidade de Serviços continuados de suporte e operação de segurança da informação, com remuneração por Valor Fixo Mensal, vinculada ao atendimento de Níveis Mínimos de Serviços (NMS), em detrimento ao modelo atual.

Deste modo, o modelo de prestação continuada de serviços, com pagamento fixo mensal vinculado a níveis mínimos de serviço, mostra-se mais adequado ao atendimento das necessidades do Tribunal, na medida em que exige disponibilidade operacional compatível com a criticidade do ambiente, inclusive com atuação presencial quando tecnicamente necessária.

Dessa forma, pretende-se, em consonância com a legislação vigente, manter os servidores do quadro efetivo do TRE-PA, predominantemente, nas implantação e supervisão das políticas de Segurança da Informação e privacidade de dados, enquanto a equipe de colaboradores executam as atividades operacionais e executivas correlatas de forma indireta, mediante contratação, conforme dispõe o Item 13.3 do Anexo I (Modelo de Contratação de Serviços de Operação de Infraestrutura e Atendimento ao Usuário de TIC) da Portaria SGD/MGI n° 1.070/2023:

13. Aspectos de segurança da informação

[...]

13.3. As ações das categorias de segurança da informação, bem como da categoria de banco de dados, devem necessariamente ser supervisionadas por servidor ou equipe do órgão ou entidade.

Deste modo, para suprir as necessidades das atividades mencionadas, o TRE-PA visa a contratação de uma empresa especializada na prestação de serviços técnicos de segurança da informação. Essa contratação tem como objetivo garantir a proteção dos dados e sistemas do TRE-PA, aumentar o grau de maturidade e resiliência cibernética, atender às exigências legais e suprir demandas que surgirem da relação cada vez mais estreita entre os processos eleitorais e a tecnologia da informação e comunicação (TIC).

1.2. Motivação/justificativa

A Secretaria de Tecnologia da Informação do TRE-PA sustenta diversas plataformas e sistemas que são disponibilizados aos usuários internos e externos por meio de portais e sistemas acessíveis via internet. Esses sistemas desempenham um papel essencial na interação com o público, incluindo os serviços prestados ao jurisdicionado e a execução de eleições. A infraestrutura tecnológica é a base para essa dinâmica, garantindo que a interação com a população ocorra de forma eficiente e segura, principalmente por meio de canais online. No entanto, essa dependência da tecnologia também expõe o TRE-PA a diversos riscos cibernéticos, como acesso indevido a informações confidenciais e a indisponibilidade dos sistemas devido a ataques maliciosos, executados por hackers ou grupos com interesses diversos. Além disso, existe o risco de ataques orquestrados por organizações de estados-nação, que podem visar infraestruturas críticas dos órgãos públicos com o intuito de desestabilizar suas operações e comprometer a segurança nacional.

Diante desse cenário, especialmente com o uso de dados pessoais e informações sensíveis em muitos desses sistemas, a proteção dessas informações se torna um desafio ainda mais relevante. A entrada em vigor da Lei Geral de Proteção de Dados (LGPD - Lei n° 13.709/2018), juntamente com o Plano de Dados Abertos (PDA) e o Marco Civil da Internet (Lei n° 12.965/2014), estabelece um rigoroso conjunto de regras sobre o acesso e o uso correto dessas informações pessoais. Essas regulamentações definem diretrizes para segurança no ambiente de Tecnologia da Informação, visando a proteção e privacidade dos dados, além de preverem sanções para as instituições que não as cumpram, incluindo multas consideráveis. Nesse contexto, é fundamental que o TRE-PA invista em ferramentas e recursos tecnológicos de segurança da informação, bem como em recursos humanos e treinamentos especializados, para proteger os dados e atender às exigências legais.

Por outro lado, a transformação digital e o avanço tecnológico no Poder Judiciário foram acelerados pela publicação da Resolução n° 370, de 08 de janeiro de 2021, que estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação (ENTIC-JUD). Com isso, torna-se essencial o fortalecimento das medidas de segurança cibernética, considerando que a crescente digitalização dos processos judiciais e a adoção de tecnologias emergentes aumentam a exposição a ameaças, como ransomware, vazamento de dados e ataques de negação de serviço (DDoS). É, portanto, fundamental implementar processos robustos de segurança, que envolvem o uso e a manutenção contínua de ferramentas avançadas de monitoramento, controle de acesso e gestão de vulnerabilidades, a fim de proteger os ativos críticos e garantir a continuidade das operações judiciais.

Adicionalmente, a pandemia de Covid-19 impulsionou a adoção do trabalho remoto, impactando diretamente a operação dos datacenters. Tradicionalmente, esses centros possuíam limites físicos bem definidos, centralizando o armazenamento e processamento de dados. Contudo, a necessidade de trabalho remoto aumentou a dependência de soluções em nuvem, VPNs e acesso a recursos distribuídos. Essa descentralização exige uma abordagem mais flexível para a continuidade dos negócios, ao mesmo tempo em que traz novos desafios de gerenciamento e segurança da informação.

O TRE-PA, assim como outros órgãos públicos, enfrenta os desafios impostos pela transformação digital, o trabalho remoto e adoção gradual de tecnologias de nuvem, que ampliam a superfície de ataque e tornam a segurança cibernética uma prioridade. O surgimento constante de vulnerabilidades, as ameaças como o roubo de informações sensíveis e o aumento da incidência de ataques de ransomware exige a adoção de medidas preventivas e corretivas adequadas.

Conforme o Tribunal de Contas da União (TCU) apontou no Acórdão 4.035/2020-TCU-Plenário, relatado pelo Ministro Vital do Rêgo, é crucial que o governo dê atenção especial aos riscos cibernéticos. O TCU realizou um levantamento com o objetivo de avaliar a governança e gestão de segurança da informação e cibernética na Administração Pública Federal (APF), considerando aspectos legislativos, normativos e de responsabilidade.

Nesse contexto, é vital que o TRE-PA reforce a governança e a gestão da segurança da informação e invista na contratação de serviços especializados, por meio da alocação de equipes de segurança cibernética. Esses profissionais, servidores e colaboradores, são essenciais para a detecção, identificação, prevenção e resposta a ataques cibernéticos, assegurando a proteção dos sistemas do Tribunal e garantindo a continuidade das operações.

Nesse contexto, é vital que o TRE-PA reforce a governança e a gestão da segurança da informação e invista na contratação de serviços especializados de segurança cibernética, estruturados por níveis mínimos de serviço e perfis profissionais mínimos necessários à execução. Esses profissionais, aliados à força de trabalho dos servidores, são essenciais para a detecção, identificação, prevenção e resposta a ataques cibernéticos, assegurando a proteção dos sistemas do Tribunal e garantindo a continuidade das operações.

Deste modo, o TRE-PA incluiu em seu Plano Anual de Contratações a contratação de serviços especializados em segurança cibernética, visando fortalecer a resiliência de sua infraestrutura tecnológica, bem como para garantir a conformidade com as normas e regulamentações vigentes. Esse investimento permitirá ao Tribunal adotar uma estrutura de segurança sólida, alinhada às melhores práticas e às exigências legais, protegendo seus dados e sistemas contra ameaças cibernéticas e cumprindo as recomendações do TCU e do Conselho Nacional de Justiça (CNJ).

Ademais, o Tribunal Regional Eleitoral do Pará - TRE/PA, no Biênio 2023-2023, tem buscado constantemente aprimorar a maturidade em Segurança da Informação por meio do fortalecimento da Governança, Gestão e Operação de Segurança e Proteção de Dados. Neste sentido, destaca-se o Planejamento Estratégico da Justiça Eleitoral do Pará 2021-2026, que consiste na construção coletiva das diretrizes estratégicas, responsáveis pelo norteamento da atuação do Tribunal, possui como um dos seus eixos estratégicos o Fortalecimento da estratégia nacional de TIC e de proteção de dados, cujo Índice de cumprimento de requisitos de Proteção de Dados mede o percentual de cumprimento da implantação dos requisitos relacionados à Proteção e Segurança de Dados. As ações mais recentes do Tribunal incluem a atualização da Política de Segurança da Informação (PSI), a normatização de documentos complementares, e a revisão contínua de processos de trabalho, a disseminação da cultura sobre Segurança da Informação e privacidade de dados, assim como a contratação de inúmeras soluções de datacenter e ferramentas de detecção de novas ameaças, em conformidade à Resolução CNJ N° 396 de 07/06/2021 - Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).

Contudo, considerando a crescente importância dos sistemas e serviços de TI para a transformação digital das organizações e o desenvolvimento constante de novas ameaças cibernéticas, é essencial evoluir continuamente e aprimorar os mecanismos de segurança, bem como desenvolver equipes cada vez mais eficazes.

Para tanto, a Estratégia Nacional de Cibersegurança JE (2021 a 2024 TSE e TREs), evento 1370070, encaminhada pelo Ofício-Circular GAB-DG nº 254/2021 (processo SEI 0008549-27.2021.6.14.8000), que traz as seguintes recomendações quanto à estruturação de equipes mínimas para o suporte de infraestrutura de soluções de segurança cibernética âmbito da Justiça Eleitoral:

[...] há necessidade de se criar equipes dedicadas ao tema de segurança da informação, em modelo similar ao adotado pelos bancos e instituições financeiras. Devem ser formadas e desenvolvidas equipes dedicadas ao emprego de técnicas de defesa e ataque para criação de medidas de segurança computacional. Isso implica mudanças no organograma dos órgãos da Justiça Eleitoral, com a criação de cargos e setores específicos, bem como integração de ações de segurança cibernética nas unidades funcionais já constituídas. O objetivo desse eixo é, fundamentalmente, ter um panorama contínuo e dedicado sobre o assunto. (grifo nosso)

No contexto de cibersegurança, convém detalhar que a Política de Segurança da Informação da Justiça Eleitoral (TSE, 2021) prevê: (i) a criação de Comissão de Segurança da Informação; (ii) a designação de Gestor de Segurança da Informação; e (iii) a formação de Equipe de Tratamento de Incidentes em Redes de Computadores (ETIRs). Ainda assim, observa-se que atividades específicas ou rotineiras, tais como análise de riscos, manutenção do sistema de gestão de segurança da informação (SGSI), definição e acompanhamento de indicadores de desempenho (KPIs), realização de campanhas de conscientização, assessoramento em segurança da informação ao encarregado pelo tratamento de dados pessoais, resposta a auditorias internas e externas, dentre outras, não foram distribuídas como atribuições específicas a componente algum da estrutura funcional. Tais lacunas na designação de responsabilidades justificam a existência de equipes formalmente designadas e dedicadas, nos Tribunais Regionais Eleitorais, ao tratamento da segurança cibernética. (grifo nosso)

Neste contexto, a atual equipe de segurança cibernética do TRE-PA, composta pelos servidores da STI (Coordenadoria de Gestão da Segurança da Informação e Infraestrutura de Data Center), e o modelo de contratação vigente, focado na aquisição de produtos e serviços de operação e gestão da segurança cibernética, não são suficientes para acompanhar a velocidade com que surgem novas ameaças e com que o mercado de segurança evolui e lança novos produtos. Cumpre esclarecer que atualmente, a referida Coordenadoria é composta por duas unidades (Seção de Defesa Cibernética - SDC e Seção de Soluções Corporativas - SSC) cujas responsabilidades de operação e gestão da segurança do tribunal é desempenhadas por apenas 5 (cinco) servidores, distribuídos conforme Figura 2, a seguir:

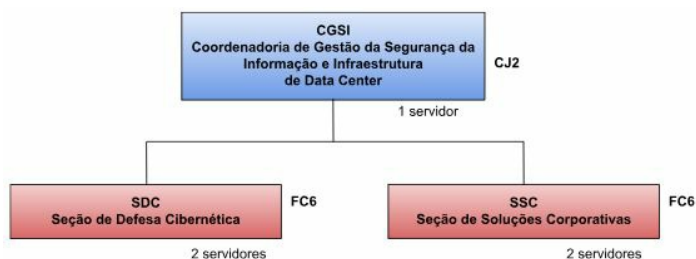


Figura 2 - Estrutura da Coordenadoria de Gestão da Segurança da Informação e Infraestrutura de Data Center

Para tanto, o fato que justifica a necessidade de nova contratação, é que as atividades operacionais relativas a esses serviços de operação de soluções de segurança da informação e proteção de dados, manutenção e suporte da infraestrutura de datacenter requerem, para sua execução, profissionais especializados e em quantidade adequada às exigências do Tribunal. Conforme demonstrado, o caso concreto da CGSI/STI/TRE-PA, o reduzido quadro de servidores efetivos alocados nas Unidades Técnicas, mostra-se insuficiente para execução das atividades mencionadas. Devido ao volume e complexidade das atividades, ante à realidade do quadro de servidores efetivos reduzido, as tarefas tanto do Coordenador quanto de servidores que compõe as unidades estão mais relacionadas ao exercício dos papéis e das ações de planejamento, definição, coordenação, supervisão, gestão e controle das atividades de implantações de soluções contratadas em âmbito institucional. Em virtude disso, são perfeitamente compreensíveis as decisões institucionais, com devido amparo legal, que verificam a terceirização das atividades operacionais como a melhor estratégia para a execução e o fornecimento desses serviços de Tecnologia da Informação.

Dentre outras, merecem destaque as seguintes vantagens e benefícios da contratação dos serviços de TIC em questão:

- as unidades pode desobrigar-se da operacionalização e da execução das atividades de demanda, suporte e rotinas técnicas que não são seu core business;
- larga possibilidade de obtenção de profissionais especializados na execução dessas atividades de complexidade alta;
- maior flexibilidade quanto à alocação daqueles profissionais especializados envolvidos na execução dos serviços;
- alcance maior de redução de custos econômico-financeiros, operacionais, administrativos, relacionados, inclusive, a instalações físicas, a treinamento e capacitação, a gestão de pessoal, entre outros.

Reforça esse entendimento o Decreto nº 9.507, de 21 de setembro de 2018, que dispõe sobre a execução indireta, mediante a contratação de serviços pela Administração Pública Federal direta, autárquica e fundacional e dá outras providências. No art. 2º desse decreto, foi atribuída a competência, à época, ao Ministro do Planejamento, Desenvolvimento e Gestão, atual, Ministro da Economia, para estabelecer os serviços que serão preferencialmente objeto de execução indireta mediante contratação. Nessa esteira, o então Ministro do Planejamento, Desenvolvimento e Gestão publicou a Portaria 443, de 27 de dezembro de 2018, estabelecendo que os serviços de tecnologia da informação e prestação de serviços de informação serão preferencialmente objeto de execução indireta, conforme observa-se do excerto a seguir:

“Portaria nº 443, de 27 de dezembro de 2018. Estabelece os serviços que serão preferencialmente objeto de execução indireta, em atendimento ao disposto no art. 2º do Decreto nº 9.507, de 21 de setembro de 2018. Art. 1º No âmbito da administração pública federal direta, autárquica e fundacional, serão preferencialmente objeto de execução indireta, dentre outros, os seguintes serviços: XXIII - serviços de tecnologia da informação e prestação de serviços de informação;” (Grifo nosso)

Dessa forma, o TRE-PA estará melhor preparado para enfrentar os desafios impostos pela digitalização e pela evolução constante das ameaças cibernéticas, com uma abordagem proativa e eficiente na proteção de seus ativos tecnológicos e na preservação da segurança dos dados sensíveis.

1.3. Identificação das necessidades não tecnológicas ou de negócio

1.3.1. A presente contratação deverá prover serviços continuados de suporte especializado e operação de segurança cibernética em **3º nível de atendimento**, atuando como escalão superior de resposta e consultoria técnica avançada para as necessidades da **Justiça Eleitoral do Pará**, compreendendo as seguintes atividades e condições gerais:

- a) Assegurar o suporte técnico de alta especialização para a proteção dos ativos digitais, atuando na resolução de incidentes complexos e na elevação dos níveis de resiliência e disponibilidade, além de prover suporte consultivo na evolução das arquiteturas de segurança (**Zero Trust** e **CSMA**) do Tribunal;
- b) Garantir que as definições de alta complexidade técnica da **Política de Segurança da Informação (PSI)** sejam traduzidas em controles efetivos e configurações avançadas nos ativos de segurança do TRE-PA;
- c) Promover a maturidade institucional por meio da gestão avançada de vulnerabilidades, realizando análises profundas de riscos, threat hunting (busca proativa de ameaças) e a projeção de melhorias estruturais no ecossistema de segurança;
- d) Atuar como ponto focal no pronto restabelecimento dos serviços de TIC em casos de crises cibernéticas, coordenando tecnicamente o gerenciamento de mudanças críticas e problemas complexos relacionados à infraestrutura de segurança;
- e) Garantir o suporte especializado de última instância para a estrutura de monitoramento (SOC), realizando a análise forense e o tratamento de incidentes

de segurança que exijam conhecimentos avançados além dos níveis operacionais básicos;

- f) Operacionalizar ações estratégicas de gestão da postura de segurança, garantindo que as ferramentas de defesa estejam integradas de forma ecossistêmica e eficiente;
- g) Elevar a confiabilidade técnica dos sistemas eleitorais e judiciários, garantindo que a camada mais profunda de defesa cibernética esteja preparada para enfrentar ameaças persistentes avançadas (APTs);
- h) Prover subsídios técnicos detalhados para a tomada de decisão da gestão, assegurando que o tratamento de dados pessoais e sensíveis ocorra sob os mais rigorosos controles de proteção, em conformidade com a **LGPD** e normas do TSE.

A contratação de equipes de segurança cibernética visa atender a demandas estratégicas e operacionais relacionadas à proteção dos ativos digitais do Tribunal. Para garantir a segurança contínua das informações e a integridade dos sistemas, a solução deve atender às seguintes necessidades:

- a) **Prover equipes especializadas de segurança cibernética com atuação contínua**, garantindo a proteção contra ameaças digitais emergentes e o monitoramento proativo de incidentes de segurança.
- b) **Oferecer suporte especializado para mitigação de riscos e resposta rápida a incidentes**, garantindo a continuidade das atividades críticas do Tribunal, minimizando o tempo de indisponibilidade dos serviços e os impactos operacionais.
- c) **Atender a requisitos regulatórios e boas práticas de segurança cibernética**, incluindo conformidade com normas legais e regulamentações específicas, além de aderir a políticas internas de segurança da informação, como Res. CNJ N° 396/2021, LGPD e outras diretrizes relevantes.
- d) **Prover relatórios e auditorias periódicas sobre o desempenho das atividades de segurança**, identificando pontos de melhoria e ações preventivas, além de garantir a transparência e rastreabilidade dos serviços prestados.
- e) **Implementar uma estratégia de prevenção e monitoramento contínuo**, incluindo a detecção e resposta a incidentes, para minimizar os impactos de ataques cibernéticos e outros riscos, tais como phishing, ransomware, vazamento de dados e acessos não autorizados.
- f) **Garantir a integração das equipes de segurança com outros setores de TIC e operacionais do Tribunal**, promovendo uma abordagem coordenada entre a segurança cibernética e as operações de TI para garantir uma gestão integrada e eficiente.
- g) **Estabelecer um plano de contingência e recuperação de incidentes cibernéticos**, com procedimentos claros para resposta e recuperação de desastres, assegurando a rápida retomada dos serviços críticos em caso de compromissos de segurança.
- h) **Promover o uso de ferramentas e soluções tecnológicas avançadas**, como sistemas de detecção e resposta a intrusões (IDS/IPS), análise de tráfego de rede, e soluções de monitoramento e correlação de eventos (SIEM), para garantir uma segurança cibernética robusta e proativa.
- i) **Assegurar a disponibilidade de suporte técnico especializado contínuo, para acompanhamento integral de eventos relacionados a possíveis incidentes**, para acompanhamento integral de eventos relacionados a possíveis incidentes e a execução contínua das atividades de segurança, garantindo que eventuais ameaças sejam tratadas imediatamente, sem comprometer a operação do Tribunal.
- j) **Fornecer consultoria e suporte estratégico em segurança cibernética**, ajudando o Tribunal a adotar práticas de segurança inovadoras e acompanhar a evolução das ameaças digitais, além de revisar e fortalecer as políticas de segurança existentes.
- k) **Alterar o modelo de contratação do serviço**, cuja contratação deve ser baseada no modelo de pagamento fixo mensal, vinculada ao atendimento de níveis mínimos de serviços previamente estabelecidos, conforme quantidades e perfis profissionais mínimos previstos em ordens de serviço. Esse modelo garante previsibilidade orçamentária e assegura que os serviços sejam prestados de maneira contínua e eficiente, conforme os parâmetros definidos pelo Tribunal.

1.4. Identificação das necessidades tecnológicas

A contratação de equipes de segurança cibernética exige que essas equipes sejam responsáveis pela operação e gestão de diversas tecnologias essenciais para garantir a segurança e continuidade das atividades no Tribunal. As necessidades tecnológicas incluem:

- a) **Ferramentas de monitoramento e gerenciamento de incidentes de segurança (SIEM)**: A equipe será responsável por operar e monitorar as ferramentas existente no Tribunal, utilizadas para detectar, correlacionar e responder a incidentes de segurança em tempo real, garantindo uma vigilância contínua do ambiente de TI.
- b) **Infraestrutura para detecção e resposta a intrusões**: As equipes alocadas terão a responsabilidade de gerenciar as soluções de NDR, configurando-as, e/ou realizando ajustes, quando for o caso, e monitorando-as para detectar e bloquear tentativas de intrusão, assegurando a integridade da infraestrutura digital.
- c) **Plataforma de gestão de vulnerabilidades**: A equipe será responsável por operar as ferramentas de gestão de vulnerabilidades, realizando varreduras regulares, classificando vulnerabilidades e recomendando ou aplicando as correções necessárias para mitigar os riscos.
- d) **Soluções de controle de acesso privilegiado (PAM)**: A operação e manutenção das soluções PAM estarão sob a responsabilidade da equipe, garantindo o controle rigoroso dos acessos privilegiados a sistemas críticos e monitorando as atividades realizadas por usuários gestores dos ativos de missão crítica.
- e) **Tecnologias de proteção contra ransomware e malwares avançados**: A equipe irá configurar, monitorar e operar as ferramentas de proteção contra ransomware e outras ameaças avançadas, utilizando inteligência artificial e técnicas preditivas para antecipar e mitigar ataques.
- f) **Ferramentas de segurança para ambientes de nuvem e multi-nuvem**: A equipe será encarregada de gerenciar a segurança dos dados e sistemas em ambientes de computação on-premise e em nuvem, configurando as políticas de segurança e garantindo a conformidade com os padrões de proteção de dados.
- g) **Processo de backup e recuperação de dados**: A operação das soluções de backup automatizado será responsabilidade da equipe, assegurando que as rotinas de backup sejam executadas e que os dados possam ser recuperados rapidamente em caso de incidentes.
- h) **Soluções de criptografia de dados em trânsito e em repouso**: A equipe deverá implementar e gerenciar as soluções de criptografia, assegurando que os dados estejam protegidos durante a transmissão e armazenamento, evitando acessos não autorizados.
- i) **Implementação e operação de ambiente seguro para desenvolvimento e testes**: A equipe será responsável por criar e gerenciar ambientes controlados para realização de testes de segurança e simulação de ataques, assegurando que as configurações de segurança sejam testadas antes de serem implementadas.
- j) **Capacitação e treinamentos contínuos em segurança cibernética**: A equipe de segurança deverá também participar de programas contínuos de capacitação e webinars, garantindo que estejam atualizados com as melhores práticas e novas ameaças emergentes.
- k) **Ferramentas de automação para resposta a incidentes (SOAR)**: A operação de ferramentas de automação para a resposta a incidentes estará sob a responsabilidade da equipe, permitindo ações rápidas e automáticas na mitigação de ameaças.
- l) **Plataformas de controle e proteção de endpoints (EDR/XDR)**: A equipe será responsável pela gestão e monitoramento das soluções EDR, garantindo a proteção dos dispositivos finais (endpoints) contra possíveis ameaças e ataques.
- m) **Ferramentas de gestão de logs e auditoria**: A equipe operará e gerenciará as ferramentas de registro e auditoria de atividades, assegurando que todas as ações no ambiente de TI sejam rastreadas e monitoradas para garantir transparência e segurança.

Com a operação dessas tecnologias, as equipes de segurança cibernética contratadas serão essenciais para garantir a proteção e a continuidade dos serviços do Tribunal Regional Eleitoral, atuando de forma proativa na prevenção e mitigação de ameaças.

1.5. Consequências da não contratação do Serviço

A não contratação dos serviços especializados de segurança cibernética pode resultar em diversas consequências graves para o Tribunal, comprometendo a integridade, a disponibilidade e a confidencialidade das informações.

Conforme mencionado, visto que, no quadro funcional da CGSI/STI, não há servidores especializados em quantidade suficiente para a adequada prestação dos serviços em questão, torna-se necessária a imediata alocação dos serviços demandados. Essa alocação é essencial para garantir o bom andamento dos serviços do TRE-PA. Além disso, a ausência de uma equipe especializada, na quantidade suficiente para resposta aos incidentes de segurança cibernética pode acarretar:

- **Comprometimento da Disponibilidade dos Sistemas Eleitorais e Administrativos:** A interrupção de serviços essenciais pode impactar diretamente a realização de eleições, o processamento de dados eleitorais e administrativos, prejudicando a transparência e confiabilidade dos processos.
- **Risco de Manipulação de Informações Sensíveis:** Sem mecanismos eficazes de proteção, dados críticos podem ser alterados indevidamente, comprometendo a integridade e autenticidade de documentos e registros judiciais.
- **Maior Exposição a Ameaças e Ataques Cibernéticos:** A falta de monitoramento e resposta a incidentes pode tornar o Tribunal um alvo fácil para ataques como ransomware, phishing e negação de serviço (DDoS), aumentando significativamente os riscos operacionais.
- **Violação de Normas e Regulamentações de Segurança:** A não conformidade com normativas como a Lei Geral de Proteção de Dados (LGPD) e a ISO/IEC 27001 pode resultar em sanções legais, multas elevadas e restrições operacionais.
- **Dificuldade na Recuperação de Dados e Continuidade das Operações:** A ausência de uma estrutura de segurança robusta pode impedir a rápida restauração de sistemas e informações após um incidente, aumentando os prejuízos institucionais.
- **Perda de Confiança da Sociedade e dos Órgãos de Controle:** Incidentes de segurança podem prejudicar a imagem da organização, comprometendo a confiança do público e de parceiros institucionais, além de gerar desgaste junto a órgãos de controle e auditoria.
- **Aumento dos Custos Operacionais e de Recuperação:** A falta de prevenção e mitigação de riscos pode levar a gastos emergenciais elevados com recuperação de dados, substituição de equipamentos e contratação de consultorias especializadas para remediação dos danos.
- **Impedimento de Adoção de Novas Tecnologias:** A insegurança no ambiente digital pode limitar a modernização dos serviços, inviabilizando a implementação de soluções inovadoras para otimizar processos e melhorar o atendimento à sociedade.

Em caso de incidentes, a falta desses serviços pode acarretar graves consequências para toda a infraestrutura de informática que depende deles, resultando em falhas catastróficas nos equipamentos do datacenter. Essas falhas causariam perdas físicas e paralisariam parte essencial dos serviços prestados à sociedade, colocando em risco tanto as atividades meio quanto as atividades finalísticas do Tribunal.

Diante desses riscos, a contratação de uma equipe especializada em segurança cibernética torna-se essencial para garantir a proteção dos ativos digitais, a continuidade dos serviços prestados e a conformidade com as normas e regulamentações vigentes.

1.6. Análise da contratação anterior ou a série histórica, se houver.

Atualmente, o Tribunal Regional Eleitoral do Pará (TRE-PA) mantém dois contratos ativos que fornecem mão de obra para áreas correlatas ao objeto desta contratação, notadamente para a Coordenadoria de Segurança da Informação (CGSI/STI) e a Coordenadoria de Suporte e Redes (CORSUP):

1) Contrato (CTO) nº 28/2020:

- **Objeto:** "FORNECIMENTO DE SERVIÇOS ESPECIALIZADOS DE SUPORTE ÀS EQUIPES DE GESTÃO DE INFRAESTRUTURA TECNOLÓGICA [...] PRESTADOS POR MEIO DE UNIDADES DE SERVIÇOS TÉCNICOS – UST."
- **Modalidade e Vigência:** Contrato focado em entregas de serviços (Unidade de Serviço Técnico), é utilizado para atividades de defesa cibernética e gestão de serviços corporativos. Este modelo não se adequa à necessidade de prestação continuada de serviços com atendimento a níveis mínimos de serviço, prontidão operacional e disponibilização de perfis profissionais mínimos compatíveis com a criticidade do ambiente.
- **Alocação:** Este é o principal contrato utilizado para alocar colaboradores nas equipes de gestão de serviços corporativos e defesa cibernética (CGSI/STI), atualmente com 6(seis) colaboradores. A medição por UST é orientada à entrega de serviços/produtos específicos (conforme catálogo), e não à alocação de postos fixos.

2) Contrato (CTO) nº 121/2022:

- **Objeto:** "CONTRATAÇÃO DE SERVIÇOS ESPECIALIZADOS NA ÁREA DE TECNOLOGIA DA INFORMAÇÃO PARA ATIVIDADES DE SUPORTE TÉCNICO À INFRAESTRUTURA DE TIC, MEDIANTE ALOCAÇÃO DE POSTOS DE TRABALHOS, COM DESCONTO POR NÍVEIS MÍNIMOS DE SERVIÇO"
- **Modalidade e Vigência:** Prestação por alocação de Postos de Trabalho com medição por Nível Mínimo de Serviço (NMS). A vigência do Contrato nº 121/2022 por 12 (doze) meses, até 01/08/2026.
- **Alocação:** Conforme verificado, este contrato aloca 3 (três) postos de trabalho para a CGSI/STI.

O TRE-PA utiliza atualmente dois modelos distintos de contratação para áreas de infraestrutura e segurança: um focado em entregas (CTO 28/2020 por UST) e outro focado em disponibilidade de pessoal (CTO 121/2022 por Posto de Trabalho). Não obstante o CTO 121/2022 possua previsão para serviços de suporte técnico à infraestrutura de TIC, mediante alocação de Postos de Trabalhos, o referido contrato possui apenas 3(três) cargos cedidos à CGSI/STI, não possuindo possibilidade de acréscimo para novos postos de trabalho para **segurança da informação e proteção de dados**. O quadro do item 3.5.2 detalha a força de trabalho do Contratos atuais, os cargos e respectivas quantidades.

Diante da insuficiência de pessoal dos contratos vigentes e da impossibilidade de aditar o contrato de postos de trabalho existente, a realização de um novo processo licitatório emerge como a única solução viável para suprir a carência de pessoal técnico especializado, garantindo a **execução continuada das atividades de segurança da informação e proteção de dados**.

2. REQUISITOS NECESSÁRIOS E SUFICIENTES À ESCOLHA DA SOLUÇÃO DE TIC

Fundamentação: descrição dos requisitos da contratação contendo de forma detalhada, motivada e justificada, inclusive quanto à forma de cálculo, o quantitativo de bens e serviços necessários para a sua composição (inciso III do § 1º do art. 18 da Lei 14.133/2021 e art. 11, inciso I da IN 94/2022).

2.1. Natureza do objeto

2.1.1. Os serviços a serem contratados são passíveis de execução indireta, pois enquadram-se nos pressupostos do Decreto n.º 9.507/2018 e da IN SEGES nº 5/2017, constituindo-se em atividades materiais acessórias, instrumentais ou complementares à área de competência legal do órgão licitante, não inerentes às categorias funcionais abrangidas por seu respectivo plano de cargos.

2.1.2. Os serviços objeto desta contratação são caracterizados como comuns, nos termos do art. 6º, inciso XIII, da Lei 14.133/2021, por possuir especificações usuais do mercado, que permitem a fixação de padrões de qualidade e de desempenho para o referido serviço. Nesse sentido, a classificação alinha-se ao disposto no item 2.1.5 do Anexo A da Portaria SGD/MGI nº 1.070/2023 (alterada pela Portaria SGD/MGI nº 6.680/2024), bem como ao art. 2º, inciso XXXII, da Instrução Normativa SGD/ME nº 94/2022.

2.1.3. Dessa forma, a classificação apresentada se adequa perfeitamente ao objeto em questão, levando em consideração sua natureza explicitamente definida neste ETP, bem como os padrões de desempenho estabelecidos nos Níveis Mínimos de Serviços.

2.1.4. O objeto é identificado na Classificação do Catálogo de Serviços (CATSER) pelo seguinte código:

- 27014 - SERVIÇOS DE GERENCIAMENTO DE INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (TIC)

2.1.5. A contratação apresenta padrões de desempenho e qualidade que podem ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado.

2.1.5.1. Principais atividades relacionadas à contratação:

- Projetar, operar, administrar e manter o conjunto de soluções, ferramentas, softwares e hardwares que compõe o ambiente de segurança de TIC da contratante;
- Tratar incidentes, problemas, requisições e mudanças relacionados ao ambiente de segurança de TIC da contratante;
- Realizar configurações, alterações, automações e otimizações no ambiente de segurança de TIC da contratante;
- Realizar testes de vulnerabilidades dos sistemas e serviços de TIC da contratante, identificando os riscos e sugerindo ações para o devido tratamento;
- Apoiar na elaboração e manutenção da política de segurança da contratante;
- Apoiar na elaboração e manutenção do plano de continuidade de negócio da contratante;
- Apoiar na elaboração e manutenção do plano de gerenciamento de risco da contratante;
- Manter o ambiente sempre atualizado observando as orientações previstas no gerenciamento de mudanças;
- Acompanhar fornecedores de serviço caso necessário;
- Elaborar e manter atualizada a documentação de todo o ambiente.

2.1.5.2. Maiores informações sobre as atividades relacionadas à contratação serão detalhadas no Capítulo 6 - Descrição da Solução.

2.2. Necessidade continuada da solução

(X) SIM () NÃO

O serviço é classificado como continuado devido à sua essencialidade, uma vez que a manutenção da segurança cibernética constitui necessidade permanente e prolongada para a sustentação administrativa e finalística deste Órgão. A interrupção dessas atividades por mais de um exercício financeiro comprometeria severamente a prestação do serviço público e a integridade dos processos eleitorais, resultando em prejuízo direto à missão institucional do TRE-PA. Tal enquadramento fundamenta-se no art. 15 da Instrução Normativa SEGES/MP nº 05/2017, ratificada pela Instrução Normativa SEGES/ME nº 98/2022, que caracteriza a natureza contínua de serviços cuja paralisação coloque em risco o cumprimento do interesse público.

A contratação observará pagamento fixo mensal, vinculado ao atendimento dos níveis mínimos de serviço estabelecidos, com unidade de medida mensal, nos termos do modelo adotado para serviços continuados de operação de infraestrutura e segurança cibernética.

Deste modo, os serviços são classificados como essenciais, pois fornecem o suporte indispensável à execução das atividades finalísticas da Justiça Eleitoral do Pará. A interrupção, mesmo que temporária, desses serviços (como monitoramento de incidentes ou gestão de vulnerabilidades) exporia os sistemas eleitorais e os dados sensíveis (incluindo proteção de dados pessoais) a riscos operacionais e de integridade inaceitáveis.

A modalidade de fornecimento continuado, com vigência plurianual, é a que melhor se adequa ao objeto, pois assegura a estabilidade e a permanência das ações preventivas e corretivas. Isso é indispensável para garantir a Confidencialidade, Integridade e Disponibilidade (CID) dos ativos de informação, protegendo o Tribunal contra um cenário de ameaças digitais complexo e em constante evolução.

Em virtude da criticidade da segurança cibernética para a missão institucional do TRE-PA, a necessidade desta solução é estratégica e permanente, justificando plenamente sua classificação como serviço continuado nos termos da legislação vigente, como suporte essencial às atividades finalísticas do Tribunal Regional Eleitoral. A vigência plurianual se mostra mais vantajosa, pois assegura a continuidade da proteção dos sistemas e dados sensíveis e sistemas críticos que suportam as atividades eleitorais, garantindo a integridade, confidencialidade, disponibilidade, confiabilidade e segurança dos processos que são essenciais ao cumprimento da missão institucional do Tribunal.

2.2.1. Vigência plurianual

O objeto da contratação se estende necessariamente por mais de um ano?

(X) SIM () NÃO

Justificativa: A contratação de equipes especializadas em segurança cibernética é classificada como de natureza continuada, pois se estende por mais de um ano e decorre de necessidades permanentes ou prolongadas da atividade administrativa do órgão, conforme o art. 6º, inciso XV, da Lei 14.133/2021. Este serviço envolve a manutenção e disponibilização contínua de recursos e serviços essenciais ao Tribunal, assegurando a sustentação da infraestrutura tecnológica e dos sistemas computacionais, além de identificar e mitigar ameaças digitais. A interrupção ou descontinuidade desses serviços pode resultar em prejuízos operacionais e no agravamento de riscos reputacionais e legais para o Tribunal, especialmente em casos de ataques cibernéticos, falhas de segurança ou vazamento de dados pessoais, o que comprometeria a imagem institucional, bem como a confiança da sociedade nos processos eleitorais e nas atividades do órgão.

Nesse contexto, a vigência plurianual é mais vantajosa, considerando os aspectos técnicos e de negócio identificados neste Estudo Técnico Preliminar. Além disso, o objeto da contratação abrange serviços especializados de segurança digital, cuja continuidade é imprescindível para o Tribunal Regional Eleitoral do Pará (TRE-PA). Dada a necessidade de aumentar a resiliência e maturidade em Segurança da Informação e garantir a integridade, disponibilidade e confiabilidade dos serviços prestados, o estabelecimento de um contrato de longo prazo se faz necessário.

Essa análise está alinhada à dinâmica contínua e crescente das necessidades tecnológicas do órgão, que demanda uma solução de longo prazo para garantir a estabilidade operacional e a evolução alinhada às inovações do setor. A vigência plurianual mostra-se vantajosa considerando a necessidade de planejamento estratégico a médio e longo prazo, proporcionando estabilidade financeira, previsibilidade orçamentária e permitindo uma gestão mais eficaz dos recursos, além de estabelecer um relacionamento sólido com o provedor de serviços em nuvem, favorecendo a continuidade do suporte técnico e atualizações conforme as demandas emergentes.

Essa abordagem proporciona não apenas uma gestão eficiente dos recursos financeiros, mas também permite adaptações contínuas, melhorias tecnológicas e níveis consistentes de qualidade e suporte ao longo do período contratual, otimizando assim a relação custo-benefício.

2.2.2. Regime de Execução: Empreitada por Preço Global.

Justificativa: Considerando a forma de pagamento prevista no modelo da *Portaria SGD/MGI nº 1.070/2023*, qual seja pagamento por valor fixo mensal, em que os custos finais dos serviços para o contrato todo são estimados com melhor precisão, pode-se classificar o regime de execução como “empreitada por preço global”, embora o pagamento venha a ser efetuado em parcelas mensais.

2.3. Adoção do Sistema de Registro de Preços – SRP?

() Sim (X) Não

Não será realizado o Registro de Preços para o objeto deste Estudo Técnico Preliminar (ETP). A contratação será contemplada mediante Pregão Tradicional.

2.4. Admissão ou não de subcontratação do objeto contratual

() SIM (X) NÃO

Não será admitida a subcontratação para a contratação.

2.5. Exigência de amostra/prova de conceito

() SIM (X) NÃO

O Objeto da Contratação não vincula à necessidade de apresentação de amostra/prova de conceito.

2.6. Garantia, manutenção e assistência técnica

() Sim () Não (**X**) Não se aplica

2.6.1. A CONTRATADA deverá assegurar a garantia técnica da execução dos serviços de suporte e operação de segurança da informação e defesa cibernética, durante toda a vigência do contrato, incluindo eventuais prorrogações, respondendo pela qualidade, disponibilidade e conformidade das atividades prestadas.

2.6.2. A garantia técnica compreende a correção tempestiva, sem ônus para a CONTRATANTE, de quaisquer falhas, erros ou deficiências identificados nos serviços prestados, procedimentos executados ou artefatos entregues pela CONTRATADA, abrangendo, entre outros: a) Erros ou falhas de configuração, monitoramento ou resposta a incidentes de segurança cibernética, decorrentes de ação ou omissão da CONTRATADA; b) Imperfeições operacionais que comprometam a disponibilidade, a integridade, a confidencialidade ou a autenticidade das informações e sistemas do TRE-PA; c) Ausência, inconsistência, atraso ou má-qualidade na entrega de relatórios, artefatos técnicos, registros de auditoria ou qualquer documentação obrigatória, conforme definido neste Termo de Referência; d) Qualquer outra ocorrência que afete a eficácia das medidas de segurança da informação ou a continuidade dos serviços críticos sob responsabilidade da CONTRATADA, ou que não atenda aos padrões e Níveis Mínimos de Serviço (NMS) estabelecidos.

2.6.3. As demandas de serviços em garantia serão formalizadas pela CONTRATANTE por meio de Ordem de Serviço (OS) específica, ou outro documento hábil, na qual deverão constar os prazos de início e de término do atendimento, que também estarão sujeitos à aferição de NMS.

2.6.4. O controle das demandas de execução de garantia técnica e de manutenção corretiva será realizado pelo sistema informatizado de gerenciamento de serviços da CONTRATANTE.

2.6.5. A execução de serviços em garantia técnica pela CONTRATADA não afasta a aplicação de penalidades e de outras sanções previstas neste Termo de Referência, conforme o caso.

2.6.6. Os serviços em garantia técnica deverão, durante todo o período de execução contratual, ser registrados no sistema informatizado, cabendo à CONTRATADA a obrigação de manter base histórica dos dados sobre a execução dos referidos serviços.

2.6.7. Em nenhuma hipótese, será objeto de faturamento o serviço executado a partir de acionamento de garantia técnica, devendo ser efetuado sem qualquer ônus para a CONTRATANTE, seja financeiro ou de atraso na prestação de outro(s) serviço(s).

2.6.8. Durante a execução da garantia técnica, todas as despesas com a equipe necessária para o atendimento (incluindo deslocamentos, se aplicável) serão custeadas integralmente pela CONTRATADA.

2.6.9. As atividades oriundas de garantia técnica poderão ser realizadas pelos profissionais alocados na equipe mínima de referência, cabendo à CONTRATADA gerenciar a execução para que não haja comprometimento das demais Ordens de Serviço em curso ou descumprimento dos NMS estabelecidos.

2.7. Garantia de execução contratual

(X) SIM () NÃO

2.7.1. Será exigida a garantia contratual da execução, nos termos do art. 96 da Lei 14.133/2021, no percentual de 5% do valor contratado e de acordo com a condições devidamente especificada no Termo de Referência, tendo em vista o valor estimado da contratação ser de monta considerável, bem como aos riscos inerentes à solução contratada para o Tribunal, conforme estabelecido no mapa de gerenciamento de risco.

2.8. Requisitos de capacitação

() SIM () NÃO (**X**) NÃO SE APLICA

2.8.1. Não faz parte do escopo da contratação o fornecimento de capacitação técnica direcionada aos servidores do TRE-PA. No que tange à necessidade de capacitação e atualização contínua da equipe terceirizada de segurança cibernética (citada no item 1.4), ressalta-se que, em estrita observância ao item 10.6.3 do Anexo A da Portaria SGD/MGI nº 1.070/2023, é de responsabilidade integral e exclusiva da CONTRATADA manter sua equipe técnica devidamente treinada. Os custos com a capacitação de seus profissionais deverão estar contemplados no BDI ou encargos da própria empresa, sendo expressamente vedado qualquer repasse direto de custos de treinamento ao Tribunal ou pedido de reembolso a este título, conforme estabelecido no Termo de Referência.

2.9. Requisitos legais

2.9.1. O processo de contratação deve estar aderente à seguinte legislação, sem prejuízo de outras normas aplicáveis:

- Lei nº 14.133, de 1º de abril de 2021, Nova Lei de Licitações e Contratos, que estabelece normas gerais de licitação e contratação para as Administrações Públicas diretas, autárquicas e fundacionais da União, Estados, Distrito Federal e Municípios.
- Portaria SGD/MGI nº 1.070, de 1º de junho de 2023 (alterada pela Portaria SGD/MGI nº 6.680/2024), que estabelece modelo de contratação de serviços de operação de infraestrutura e atendimento a usuários de Tecnologia da Informação e Comunicação, no âmbito dos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.
- Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.
- Resolução CNJ nº 468 de 15/07/2022, Dispõe sobre diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação pelos órgãos submetidos ao controle administrativo e financeiro do Conselho Nacional de Justiça (CNJ).
- Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).
- LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018).
- Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor)
- Portaria SGD/MGI nº 852, de 28 de maio de 2023, que dispõe o Programa de Privacidade e Segurança da Informação.
- **Instrução Normativa GSI/PR nº 5**, de 30 de agosto de 2021, Dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal.
- Norma Complementar nº 14/IN01/DSIC/SCS/GSIPR, Estabelece os princípios, diretrizes e responsabilidades relacionados à segurança da informação para o tratamento da informação em ambiente de computação na nuvem.
- Resolução TSE nº 23.702, de 9 de junho de 2022, Dispõe sobre a Política de Governança das contratações na Justiça Eleitoral e dá outras providências.
- Resolução CNJ nº 400, de 16 de junho de 2021, que dispõe sobre a política de sustentabilidade no âmbito do Poder Judiciário.
- Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, Dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional.
- Resolução CNJ nº 370/2021, institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD).
- Resolução CNJ nº 396, de 7 de junho de 2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).
- Resolução TSE nº 23.644, de 1º de julho de 2021, Dispõe sobre a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral.
- ABNT NBR ISO/IEC 27017 de 07/2016. Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação com base ABNT NBR ISO/IEC 27002 para serviços em nuvem
- PORTARIA PRESIDÊNCIA CNJ Nº 140 DE 22 DE ABRIL DE 2024. Determina a implementação do método de autenticação do tipo Múltiplo Fator de Autenticação (MFA) como requisito funcional para acesso a sistemas judiciais sensíveis.

2.10. Requisitos temporais

Deverão ser observados, na fase de execução contratual, os seguintes requisitos e restrições temporais:

- A vigência do contrato iniciar-se-á a partir da data de sua assinatura, momento em que terá início a Fase de Implantação, com duração prevista de 30 (trinta) dias corridos. Durante este período, a CONTRATADA obriga-se a absorver as tecnologias, metodologias, processos de trabalho e a infraestrutura necessários à realização dos serviços.
- O contrato terá vigência inicial de 36 (trinta e seis) meses, contados a partir da data de sua assinatura, podendo ser prorrogado por períodos sucessivos até o limite de 10 (dez) anos, nos termos dos arts. 106 e 107 da Lei nº 14.133/2021, condicionada à existência de créditos orçamentários e ao interesse da Administração.
- O evento de Início da Operação (Assunção dos Serviços) corresponde ao primeiro dia subsequente ao término da Fase de Implantação, momento em que a CONTRATADA assume integralmente a responsabilidade operacional dos serviços de segurança cibernética e infraestrutura do Tribunal. Somente a partir deste marco a CONTRATADA fará jus ao faturamento da Parcela Fixa Mensal vinculada aos NMS, que será calculada de forma proporcional (pró-rata) caso o primeiro mês de operação efetiva não seja completo.
- A contagem dos prazos obedecerá à seguinte regra: os prazos de cunho administrativo (como a Fase de Implantação e apresentação de documentos) serão contados em dias corridos; já os prazos operacionais de mobilização, atendimento e entrega de soluções (SLA) ocorrerão de forma contínua e sob demanda, sendo contados rigorosamente nas métricas (horas ou dias) definidas de forma individualizada em cada Ordem de Serviço (OS) e no Catálogo de Serviços do TRE-PA.
- A partir da assinatura do contrato, a CONTRATADA deverá indicar formalmente um preposto no prazo de até 10 (dez) dias úteis. A documentação da equipe técnica a ser habilitada para a prestação dos serviços deverá ser apresentada até 5 (cinco) dias antes do término da Fase de Implantação.
- O licitante selecionado deve fornecer suporte técnico contínuo durante todo o período contratual, garantindo disponibilidade de pessoal qualificado. A resolução de incidentes de segurança cibernética deverá ser tempestiva para não prejudicar os indicadores de proteção de dados, cumprindo rigorosamente os prazos definidos no Acordo de Nível de Serviço estabelecido na seção CRITÉRIOS DE MEDIÇÃO E PAGAMENTO.
- A descrição e os tipos de serviços constantes no Catálogo de Serviços poderão sofrer ajustes de acordo com a necessidade do Tribunal ao longo da execução do contrato, a fim de melhorar os processos, a comunicação e a resposta a novas ameaças cibernéticas.

2.11 Requisitos de Segurança da Informação e Privacidade

2.11.1. O fornecimento do serviço a ser contratado deverá, no que couber, atender às seguintes normas internas de proteção e dados e privacidade do Tribunal:

- Política de Segurança da Informação da Justiça Eleitoral, instituída por meio da Resolução Nº 23.644/2021, assim como a Resolução TRE -PA n.º 5.699/2021 que institui a Política de Privacidade e Proteção de Dados;
- Lei Nº 13.708, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais;
- PORTARIA Nº 22804/2024 - Dispõe sobre as regras e os procedimentos para Desenvolvimento Seguro de Software do Tribunal Regional Eleitoral do Pará.
- PORTARIA Nº 22805/2024- Dispõe sobre as regras e os procedimentos para gerenciamento de backup e restauração de dados no âmbito da rede corporativa de dados do Tribunal Regional Eleitoral do Pará.
- PORTARIA Nº 22806/2024 - Institui regras para a Gestão de Identidade e o Controle de Acesso Físico e Lógico ao ambiente cibernético do Tribunal Regional Eleitoral do Pará.
- PORTARIA Nº 22807/2024- Estabelece a Política de Uso Aceitável dos Recursos de Tecnologia da Informação no Tribunal Regional Eleitoral do Pará.
- PORTARIA Nº 22808/2024 - Institui norma de gerenciamento contínuo de vulnerabilidades no âmbito do TRE-PA.
- PORTARIA Nº 22809/2024- Dispõe sobre as regras e os procedimentos para a realização da gestão e monitoramento de registro de atividades (logs) no ambiente computacional do Tribunal Regional Eleitoral do Pará.
- PORTARIA Nº 22810/2024 - Institui norma de configuração segura de ambientes, referente à Política de Segurança da Informação da Justiça Eleitoral.
- PORTARIA Nº 22811/2024- Dispõe sobre as regras e os procedimentos para gestão de riscos de segurança da informação do Tribunal Regional Eleitoral do Pará.

2.11.2. O Termo de Referência deve conter, no que couber ao objeto contratado, requisitos e obrigações de privacidade e segurança da informação, devendo o órgão ou entidade empregar, conforme critérios próprios, aqueles requisitos que forem imprescindíveis, considerando a legislação vigente e os riscos de privacidade e segurança da informação.

2.11.2.1. A solução deverá estar alinhada, na medida do possível, com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14 de agosto de 2018). Em especial, aos princípios de segurança (Art. 6º, inciso VII) e prevenção (Art. 6º, inciso VIII).

2.11.2.2. A CONTRATADA deverá assegurar que possui total conhecimento da Lei nº 13.709 de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais) e que em toda sua prestação de serviço respeitará o regramento nela preconizado, especialmente quando algum preposto eventualmente tiver acesso a informações que contenham dados pessoais.

2.11.3. DA CONDUTA E DO SIGILO DAS INFORMAÇÕES

2.11.3.1. A CONTRATADA estará compelida a obedecer à Política de Segurança da Informação da Justiça Eleitoral ([RESOLUÇÃO TSE Nº 23.644/2021](#)), assim como as Normas Complementares de Segurança da Informação instituídas no âmbito do TRE-PA, e não divulgar, sem autorização, as informações restritas ou confidenciais de propriedade do Órgão, em conformidade com as condições abaixo. Para tanto, a empresa deverá assinar o Termo de Compromisso de Sigilo e entregar juntamente com a documentação exigida (5 dias úteis a contar da assinatura) e, seus empregados, o Termo de Ciência do Compromisso de Sigilo e TERMO DE RESPONSABILIDADE devidamente assinados, conforme modelos disponibilizados do Termo de Referência (os termos dos empregados deverão ser entregues até a data da apresentação de cada empregado no TRE-PA);

2.11.3.2. As informações a serem tratadas de forma sigilosa, restrita e confidencialmente são aquelas que, por sua natureza, são consideradas como de interesse restrito ou confidencial e não podem ser de conhecimento de terceiros, como por exemplo:

- Programas de computador, seus códigos-fonte e códigos-objeto, bem como suas listagens e documentações;
- Toda a informação relacionada a programas de computador existentes ou em fase desenvolvimento no âmbito da instituição e rotinas desenvolvidas por terceiros, incluindo fluxogramas, estatísticas, especificações, avaliações, resultado de testes, arquivo de dados, versões "beta" de quaisquer programas, etc.;
- Documentos relativos à lista de usuários do Secretaria de Tecnologia da Informação (STI) e seus respectivos dados, armazenados sob qualquer forma;
- Metodologias e ferramentas de serviços, desenvolvidas pela STI; e
- Parte ou totalidade dos modelos de dados que subsidiam os sistemas de informações da STI, sejam eles executados interna ou externamente.

2.11.3.3. Em caso de dúvida acerca da confidencialidade de determinada informação, a CONTRATADA não deverá divulgar a mesma, até que venha a ser expressamente autorizado, por escrito, por meio eletrônico ou impresso, pelo do Secretário da STI;

2.11.3.4. Em hipótese alguma se interpretará o silêncio da STI como liberação de qualquer dos compromissos ora assumidos;

2.11.3.5. A CONTRATADA obriga-se expressamente a:

- Preservar a integridade e guardar sigilo das informações de que fazem uso, bem como zelar e proteger os respectivos recursos de processamento de informações;
- Cumprir a política de segurança, sob pena de incorrer nas sanções disciplinares e legais cabíveis;
- Utilizar os sistemas de informação e os recursos a eles relacionados somente para os fins previstos pelas normas de segurança em vigor;
- Manter o caráter sigiloso das senhas de acesso, aos recursos e sistemas da STI;
- Não compartilhar, sob qualquer forma, informações confidenciais com outros que não tenham a devida autorização de acesso;
- Responder por todo e qualquer acesso aos recursos de informática e dados da STI, bem como pelos efeitos desses acessos efetivados através do seu

código de identificação ou outro atributo utilizado para esse fim;

- Respeitar a proibição de usar, inspecionar, copiar ou armazenar programas de computador, lista de usuários e seus respectivos dados, cadastros e afins, modelos, etc;
- Devolver, ao término da prestação dos serviços, inclusive, suas notas pessoais sob qualquer forma, se houver matéria sigilosa relacionada com a STI, registros de documentos de qualquer natureza que tenham sido usados, criados ou tenham estado sob seu controle; e
- Cumprir as dispositivos instituídos pelo o Código de Conduta e Integridade do Tribunal Regional Eleitoral do Pará

2.11.3. A licitante deve ainda observar, no mínimo, os requisitos de privacidade e segurança da informação, além daqueles constantes nos templates de artefatos da contratação disponibilizados pela SGD em parceria com a AGU:

2.11.3.1 a contratação deve estar alinhada às normas correlatas publicadas pelo Gabinete de Segurança Institucional da Presidência da República - GSI/PR, a exemplo da IN GSI/PR nº 5, de 30 de agosto de 2021, que dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal;

2.11.3.2. a solução deve estar em conformidade com a Política de Segurança da Informação da Justiça Eleitoral.

2.11.3.3. todas as informações consideradas sensíveis pelo TRE-PA deverão ser resguardadas por parte da CONTRATANTE não sendo permitido, em hipótese alguma, o compartilhamento, cópia, retirada, reprodução, carga, levantamento, entre outros, de informações oriundas dos usuários da solução ou de sistemas informatizados institucionais sem a devida autorização prévia e expressa por parte da autoridade competente do TRE-PA.

2.11.3.4. a propriedade intelectual e os direitos autorais dos dados e informações e qualquer tipo de trabalho relacionado às demandas da CONTRATANTE, serão de sua titularidade. A CONTRATADA deve-se abster de divulgar ou repassar quaisquer dados ou informações, salvo se expressamente autorizado pela CONTRATANTE.

2.11.3.5. a CONTRATADA deverá assinar Termo de Compromisso de Manutenção de Sigilo e os respectivos funcionários alocados ao contrato deverão assinar Termo de Ciência, cujo prazo de entrega ao CONTRATANTE será de 5(cinco) úteis após a assinatura do CONTRATO.

2.11.3.6. a CONTRATADA deverá apresentar, na reunião inicial, relação nominal dos profissionais envolvidos na execução do contrato que terão acesso às informações do CONTRATANTE, se for o caso, bem como os referidos Termos de Ciência assinados. Caberá ao preposto alocado ao contrato manter esta lista atualizada sempre que um novo profissional necessitar de acesso às informações tratadas.

2.11.3.7. cumprir a Política de Segurança da Informação da CONTRATANTE (Política de Segurança da Informação da Justiça Eleitoral - Resolução Nº 23.644), assim como a Resolução TRE -PA n.º 5.699/2021 que institui a Política de Privacidade e Proteção de Dados.

2.11.3.8. assumir responsabilidade sobre todos os possíveis danos físicos e/ou materiais causados à CONTRATANTE, advindos de imperícia, negligência, imprudência ou desrespeito às normas de segurança.

2.11.3.9. não veicular publicidade acerca dos serviços contratados, sem prévia e formal autorização por parte da CONTRATANTE.

2.11.3.10. comunicar formal e imediatamente à CONTRATANTE qualquer ponto de fragilidade percebido que exponha a confidencialidade, integridade ou disponibilidade das informações e do serviço CONTRATADO.

2.11.3.11. A CONTRATADA deve garantir que a operação em ambientes de nuvem e o uso de Inteligência Artificial Generativa sigam protocolos rigorosos de proteção de dados. É vedada a inserção de dados pessoais sensíveis da Justiça Eleitoral do Pará em modelos de linguagem públicos (LLMs) sem anonimização prévia. O gerenciamento de credenciais e chaves criptográficas deve seguir o princípio do privilégio mínimo, com auditoria completa de logs de acesso.

2.12. Requisitos sociais, ambientais e culturais

2.121. Os serviços devem estar aderentes às seguintes diretrizes sociais, ambientais e culturais:

- Durante a execução de tarefas no ambiente do CONTRATANTE, os colaboradores da empresa fornecedora deverão observar, no trato com os servidores e o público em geral, a urbanidade e os bons costumes de comportamento, tais como: asseio, pontualidade, cooperação, respeito mútuo, discrição e zelo com o patrimônio público. Deverão ainda portar identificação pessoal, de acordo com as normas internas das instituições.
- Os produtos gerados em função da prestação dos serviços, bem como todas as documentações, deverão ser entregues no idioma português do Brasil (pt-BR), com exceção de termos técnicos usuais que poderão ser apresentados em língua estrangeira.
- E ainda com o objetivo de promover uma relação contratual responsável e alinhada com os princípios de sustentabilidade, respeito aos direitos humanos, valorização da cultura e ética empresarial deverá observar na execução do objeto (sempre que couber) os seguintes requisitos:
 - o Responsabilidade Social: a) Observar e respeitar os direitos humanos, garantindo igualdade de oportunidades e não-discriminação em todas as suas atividades. b) Promover a diversidade e a inclusão, valorizando a equidade de gênero, etnia, idade, orientação sexual e demais características individuais. c) Estimular a contratação de mão de obra local e a capacitação de profissionais da região, contribuindo para o desenvolvimento econômico e social.
 - o Sustentabilidade Ambiental: a) Adotar práticas sustentáveis em suas operações, promovendo a economia de recursos naturais, a redução da emissão de gases de efeito estufa e o uso eficiente de energia. b) Gerenciar de forma adequada os resíduos gerados durante a prestação dos serviços, priorizando a coleta seletiva, a reciclagem e a destinação correta. c) Respeitar e adotar normas ambientais vigentes, visando à preservação dos ecossistemas e à mitigação de impactos ambientais adversos.
 - o Preservação Cultural: a) Respeitar e valorizar a diversidade cultural local, observando as tradições, costumes e patrimônio histórico. b) Promover ações que valorizem a cultura regional.
 - o Transparência e Ética: a) Cumprir rigorosamente as leis, regulamentos e normas éticas relacionadas à prestação dos serviços, garantindo a integridade e a transparência em todas as atividades. b) Assegurar a confidencialidade das informações do Tribunal e dos dados dos usuários, implementando medidas adequadas de segurança da informação.
- A CONTRATADA deverá adotar práticas de sustentabilidade ambiental na execução do objeto, observando, no que couber, as diretrizes do Guia Nacional de Contratações Sustentáveis, elaborado pela Câmara Nacional de Sustentabilidade da Controladoria Geral da União/Advocacia Geral da União, bem como as disposições da Instrução Normativa SLTI/MP nº 1/2010 e do Decreto nº 7.746/2012, da Casa Civil, da Presidência da República.

2.13. Critérios e práticas de sustentabilidade

De forma geral, os serviços contratados, sempre que possível, deverão ser executados em conformidade com as orientações e normas voltadas para a sustentabilidade ambiental, em especial as contidas no art. 6º da Instrução Normativa/SLTI/MPOG nº 01, de 19 de janeiro de 2010 e no Decreto nº 7.746/2012, da Casa Civil, da Presidência da República, no que couber.

2.14. Requisitos da Arquitetura Tecnológica

2.14.1. A solução ou serviço contratado deverá atender integralmente aos requisitos de arquitetura tecnológica que serão detalhados a seguir e ao longo do ciclo de vida completo do objeto contratado.

4.14.1.1. A adoção de tecnologias, arquiteturas ou procedimentos alternativos, deverá ser previamente autorizada pela Contratante. Na ausência de tal autorização, a CONTRATADA está proibida de implementar arquiteturas, scripts, componentes, processos ou tecnologias diferentes das especificadas pela Contratante ou existentes na infraestrutura do Tribunal.

4.14.1.2. A CONTRATADA deverá utilizar os padrões de arquitetura definidos pelo Tribunal, além de realizar recomendações e análises dessas arquiteturas para aprimorar a segurança de ativos de infraestrutura e aplicações. As avaliações deverão estar alinhadas às melhores práticas e frameworks de segurança da informação, como o CIS Controls, o NIST Cybersecurity Framework e as diretrizes do OWASP, aplicando, quando for o caso, metodologia DevSecOps para a integração contínua de segurança ao desenvolvimento e operação dos sistemas.

4.14.1.3 Os serviços prestados pela CONTRATADA devem ser compatíveis com as tecnologias de hardware, software, linguagem de programação, interfaces, entre outros, utilizadas pelo CONTRATANTE, considerando as versões atualmente em uso.

2.14.2. Recomenda-se que os licitantes realizem a vistoria prévia ao processo licitatório, a fim de conhecer o parque tecnológico do Tribunal e obter informações detalhadas sobre a infraestrutura existente. Essa vistoria permite que os licitantes tenham uma visão mais precisa das necessidades e requisitos específicos da organização, facilitando a elaboração de propostas alinhadas com as demandas reais.

2.14.3. Durante a vistoria, os licitantes podem ter a oportunidade de avaliar a atual arquitetura de TI, a rede de comunicação, os sistemas e aplicativos em uso, bem como a infraestrutura de segurança existente. Essa análise detalhada possibilita uma compreensão mais completa do ambiente de segurança cibernética do Tribunal, permitindo que os licitantes adequem suas propostas de acordo com as características e exigências específicas do Tribunal.

2.14.4. Além disso, a vistoria prévia também proporciona aos licitantes a chance de esclarecer dúvidas, obter informações adicionais e interagir diretamente com os responsáveis pela área de tecnologia do Tribunal. Essa troca de informações contribui para um melhor entendimento das expectativas da organização e permite que os licitantes ofereçam propostas mais personalizadas e alinhadas com as necessidades reais do TRE-PA.

2.15. Requisitos de Projeto e Implementação

2.15.1. Não se aplica, pois não há fase de projeto ou implementação de uma nova solução, uma vez que o objeto está relacionado à contratação de serviços.

2.16. Requisitos de implantação

2.16.1. A descrição detalhada da implantação eficaz dos serviços especializados de segurança cibernética, incluindo todas as etapas, requisitos e procedimentos necessários para assegurar a qualidade e a conformidade do processo, está disponível no Catálogo de Serviços da Contratante, servindo como referência oficial para a execução das atividades contratadas. Esses requisitos visam garantir que a implantação dos serviços de segurança cibernética ocorra de forma estruturada, eficiente e alinhada às necessidades e normas da Contratante.

2.17. Requisitos de experiência profissional

2.17.1. A equipe responsável pela execução do objeto deve ser composta por profissionais qualificados e capacitados na área de segurança da informação e defesa cibernética, de acordo com os requisitos estabelecidos neste ETP. A qualificação da equipe é de extrema importância para garantir a excelência na prestação dos serviços e a obtenção dos resultados esperados.

2.17.2. A empresa fornecedora dos serviços de segurança cibernética deve dispor de profissionais especializados e com experiência comprovada na implementação, operação e gestão de soluções de segurança da informação. Esses profissionais devem possuir conhecimento técnico aprofundado em ferramentas e tecnologias de segurança, além de experiência prática na proteção de infraestruturas críticas, análise de ameaças e resposta a incidentes.

2.17.3. É essencial que a equipe tenha as competências e habilidades necessárias para lidar com a complexidade e as demandas específicas do ambiente em que serão executadas as tarefas. Isso inclui o domínio das tecnologias e metodologias de segurança cibernética, a capacidade de solucionar problemas de forma eficiente, a habilidade de comunicação e trabalho em equipe, bem como a capacidade de se adaptar a novas situações e cumprir prazos estabelecidos.

2.17.4. A equipe deve manter-se constantemente atualizada em relação às tendências e ameaças emergentes no cenário de segurança cibernética, participando de treinamentos, certificações e eventos técnicos da área. A adoção de uma abordagem proativa e adaptativa garantirá a efetividade na prestação dos serviços e a proteção contínua dos ativos da organização.

2.16.5. Deste modo, é imprescindível que a equipe de segurança cibernética seja composta por profissionais altamente capacitados, experientes e certificados, assegurando a excelência dos serviços prestados e o cumprimento das exigências técnicas e estratégicas da contratante *definidos no ETP e Termo de Referência*.

2.18. Requisitos de formação da equipe

2.18.1. Os serviços deverão ser prestados por profissionais devidamente qualificados, cujos perfis (incluindo formação acadêmica, experiência profissional e certificações técnicas mínimas obrigatórias) devem atender rigorosamente aos requisitos previstos no item 3.7 do ETP e Anexo IX - Equipe Técnica e Qualificação Profissional para a Execução dos Serviços do TR.

2.19. Requisitos de metodologia de trabalho

2.19.1. Todo o processo de sustentação dos serviços, objeto da contratação, será acompanhada e supervisionada por servidores do TRE-PA.

2.19.2. O início da execução dos serviços está condicionada ao recebimento pelo Contratado de Ordem de Serviço (OS) emitida pela Contratante.

2.19.3. A execução dos serviços contratados pressupõe a existência dos seguintes papéis e responsabilidades:

- **FISCAL DE CONTRATO:** Integrante do setor requisitante que exercerá função operacional de acompanhar e fiscalizar a execução do contrato, relatando os fatos à autoridade competente; anotar as ocorrências em registro próprio; e determinar a regularização de faltas ou defeitos observados.
- **GESTOR DE CONTRATO:** Integrante da Secretaria de Tecnologia da Informação (STI) do TRE, exercerá função de supervisão, o acompanhamento, a fiscalização e a intervenção na execução contratual, de tal forma que garanta a fiel observância das cláusulas contratuais e a perfeita realização do objeto.

2.19.4. O encaminhamento formal de demandas deverá ser realizado sempre por escrito, utilizando o e-mail corporativo com formalização de documentos via SEI.

2.19.5. A execução dos serviços está condicionada ao recebimento de Ordem de Serviço (OS) pela Contratada emitida pela Contratante.

2.19.6. A OS indicará o serviço (e demais informações consideradas essenciais) que deverá ser prestado.

2.19.7. A execução do serviço deverá ser acompanhada pelo representante informado pela Contratada, que dará ciência de eventuais acontecimentos à Contratante.

2.19.8. O horário regular de prestação dos serviços deverá ocorrer entre 8h e 17 horas em dias úteis, ou de acordo com a escala a ser definida conforme orientações do CONTRATANTE.

2.19.8.1. Poderá ser exigida a disponibilização dos perfis profissionais mínimos em horários distintos e em dias não úteis, especialmente em período eleitoral ou diante de incidentes críticos. Para acionamentos de emergência fora do horário regular (8h às 17h), a CONTRATADA deverá garantir o início do atendimento remoto ou presencial em, no máximo, 2 (duas) horas, conforme a criticidade definida no Plano de Resposta a Incidentes da Justiça Eleitoral do Pará.

2.19.9. Quando demandado por Ordem de Serviço, os serviços relacionados ao objeto principal serão executados por meio de atuação presencial na sede do TRE-PA, conforme exigido pela natureza das atividades e pela criticidade do ambiente, cabendo à contratada a gestão da equipe necessária ao cumprimento das ordens de serviço e dos níveis mínimos de serviço.

2.19.9.1. Para todos os serviços definidos na Contratação, considera-se necessária, para a adequada execução do objeto, a disponibilidade de profissionais com os perfis mínimos exigidos, inclusive com atuação presencial quando a natureza da atividade, a proteção dos ativos críticos ou o tempo de resposta assim o exigirem.

2.19.9.2. Conforme necessidade da administração, poderá ser necessário deslocamento dos colaboradores do Contrato para outras unidades do TRE-PA, como Cartórios Eleitorais e Postos de Atendimento Eleitoral, objetivando o atendimento de atividades relacionados ao suporte aos Sistemas Operacionais, endpoints de segurança cibernética instalados nas unidades do Tribunal. Além disso, existe a possibilidade de deslocamento dos colaboradores da contratada para outras unidades da federação, para participação em reuniões técnicas ou testes em campo que demandem a participação e apoio técnico da Contratada, especialmente no período eleitoral, cujos custos deverão estar incluídos no valor global da proposta, conforme estimativa (série histórica) detalhado no item 3.9.5.2 deste ETP.

2.19.10. Atendendo ao item 12. VERIFICAÇÃO DA QUALIDADE DOS SERVIÇOS, do ANEXO A da Portaria SGD/MGI nº 1.070/2023, serão definidos no Instrumento de Medição para verificação da qualidade dos níveis esperados da prestação do serviço e respectivas adequações de pagamento, conforme descrito a seguir:

12.1. A verificação da qualidade constitui-se em procedimento indispensável para a fiscalização e a gestão de contratos de serviços da Administração Pública. Proporciona a devida verificação da medida em que o que está sendo entregue ao longo do contrato efetivamente corresponde ao resultado esperado (ou planejado). Nesse sentido, indicadores de níveis de serviços devem ser definidos para todo e qualquer contrato de operação de infraestrutura e atendimento a usuários de TIC, observando-se um conjunto mínimo de indicadores capaz de assegurar a efetiva prestação de serviço com a qualidade esperada.

2.19.10.1. O gerenciamento dos níveis de serviço representa uma relação entre um provedor de serviço e um cliente, determinando critérios de aferição de resultados da contratação, definindo, em bases compreensíveis, tangíveis, objetivamente observáveis e comprováveis, os níveis esperados de qualidade da prestação do serviço e respectivas adequações de pagamento.

2.19.10.2. A CONTRATADA obriga-se a atender os parâmetros mínimos aceitáveis definidos pela equipe de planejamento da contratação, as quais também são passíveis de sanção em caso de descumprimento deste acordo.

2.19.11. Para a execução do objeto desse Termo de Referência serão utilizados os seguintes mecanismos de comunicação:

FUNÇÃO DE COMUNICAÇÃO	DOCUMENTO	EMISSION	DESTINATÁRIO	FORMATO	PERIODICIDADE
1. Autorizar a execução de prestação dos Serviços	Ordem de Serviço	Contratante – Gestor do Contrato e Fiscal Requisitante	Contratada	Eletrônico	Sob demanda
2. Registro das reuniões realizadas entre a CONTRATANTE e a CONTRATADA	Ata de Reunião	Contratante	Contratada	Eletrônico	A cada reunião
3. Registro/Resposta de cada solicitação de suporte técnico feito pela CONTRATANTE	Relatório de Atendimento Técnico	Contratada	Contratante	Eletrônico	Após cada Chamado
4. Dirimir dúvidas e prestar esclarecimentos acerca de itens presentes no contrato firmado	Ofício pela Contratada e Ofício ou Chamado pela Contratante	Contratada ou Contratante	Contratada ou Contratante	Eletrônico com confirmação de recebimento	Sob demanda
5. Confirmação da conclusão do atendimento ou chamado(s) técnico(s)	“De acordo” da conclusão de chamado ou atendimento técnico	Fiscal Técnico	Contratada	Eletrônico com confirmação de recebimento	Sob demanda
6. Acusar o recebimento provisório do objeto da contratação	Termo de Recebimento Provisório	Fiscal Técnico	Gestor do Contrato	Formato Digital (SEI)	Sob demanda
7. Acusar o Recebimento Definitivo do objeto da contratação	Termo de Recebimento Definitivo	Gestor do Contrato / Contratante	Contratada	Formato Digital (SEI)	Sob demanda
8. Comunicar autorização para faturamento	Autorização para faturamento	Gestor do Contrato / Contratante	Contratada	Eletrônico com confirmação de recebimento e/ou carta registrada	Sob demanda
9. Receber notas fiscais/fatura	Nota Fiscal/Fatura	Contratada	Fiscal Administrativo (Contratante)	Papel e/ou meio eletrônico com confirmação de recebimento	Sob demanda
10. Comunicar pagamento	Notificação de pagamento	Gestor do Contrato / Contratante	Contratada	Eletrônico com confirmação de recebimento	Sob demanda

Tabela 1 - Mecanismos de comunicação da Contratação

2.20. Da participação de consórcios

2.20.1. Não será permitida a participação de empresas em consórcio, pois a natureza do objeto não enseja a necessidade da previsão da formação em consórcio por si, uma vez que o objeto consiste no fornecimento de solução de TIC cuja logística não se apresenta como complexa para fornecimento, ou seja, uma única revenda detém em seu portfólio de serviço condições de atender as demandas previstas, sem a necessidade de se consorciar com outra empresa para conseguir atender o objeto na sua completude. Desse modo, não há situação fática que comprove a necessidade da previsão do uso do instituto do consórcio no presente processo.

2.21. Da participação de pessoa física

2.21.1. Não será permitida a participação de pessoas físicas, pois a presente contratação exige estrutura mínima da contratada, incluindo estrutura administrativa, instalações e equipe de profissionais ou corpo técnico para a execução do objeto incompatíveis com a natureza profissional da pessoa física (art. 4º da IN SEGES/ME nº 116/2021).

2.22. Da participação de cooperativas

2.22.1. Não será permitida a participação de cooperativas, tendo em vista que os serviços que tratam o objeto, presumem subordinação e exigem especialização técnica específica, o que incompatibiliza a natureza cooperativista, conforme preconiza a Lei nº 14.133, de 1º de abril de 2021, que rege as licitações e contratos no âmbito público brasileiro.

2.23. Indicação de marcas ou modelos

() SIM () NÃO (X) NÃO SE APLICA

Não se aplica ao objeto da Contratação.

2.24. Vedação de marcas, modelos ou produtos

() SIM () NÃO (X) NÃO SE APLICA

Não se aplica ao objeto da Contratação.

2.25. Necessidade de transição contratual

2.25.1 Estratégia de Continuidade da Solução em Caso de Interrupção Contratual

Para garantir a continuidade da execução contratual, deverá haver monitoramento permanente do contrato, registrando todas as ocorrências e controlando possíveis riscos que comprometam a prestação dos serviços. A equipe de Planejamento da Contratação define a estratégia de continuidade dos serviços especializados de segurança cibernética em caso de interrupção contratual. As seguintes ações deverão ser adotadas:

EVENTO	EFEITO	CAUSAS	CONTROLES ATUAIS	AÇÕES DE CONTINUIDADE / RESPONSÁVEIS
Encerramento por abandono, inadimplimento ou incapacidade da empresa contratada em fornecer o serviço.	Falha na operação de monitoramento e proteção cibernética, comprometendo a disponibilidade dos sistemas essenciais e aumentando a exposição a ataques.	Falta de profissionais especializados disponíveis no mercado para atendimento aos perfis profissionais exigidos, comprometimento da contratada na execução do contrato.	Aplicação de sanções contratuais e monitoramento contínuo do cumprimento das obrigações.	Acompanhar a execução contratual e a qualidade dos serviços prestados de indicadores definidos. Responsáveis: Fiscal Técnico e Administrativo.

Tabela 2 - Estratégia de Continuidade da Solução em Caso de Interrupção Contratual

2.25.2 Estratégia de Independência do TRE-PA com Relação à Empresa Contratada

A contratação de serviços de segurança cibernética será baseada em padrões de mercado, garantindo que não haja dependência de um fornecedor específico. Dessa forma, o TRE-PA poderá buscar outros prestadores de serviço em caso de necessidade de transição contratual. As seguintes estratégias deverão ser adotadas:

EVENTO	EFEITO	CAUSAS	CONTROLES ATUAIS	ESTRATÉGIA DE INDEPENDÊNCIA / RESPONSÁVEIS
Interrupção ou fim do suporte contratado.	Redução da capacidade de resposta a incidentes e aumento do risco cibernético. Sobrecarga de atividades nos servidores dedicados à gestão de segurança da informação do Tribunal.	Fim do contrato ou inexecução/descontinuidade do serviço por parte do fornecedor.	Monitoramento da vigência da contratação e prazos relacionados à prorrogação.	Planejamento de uma nova contratação e análise de fornecedores alternativos. Implementação de uma base de conhecimento interna sobre procedimentos e soluções para continuidade. Transferência de conhecimento durante a contratação. Responsáveis: Fiscal Técnico e Administrativo.
Inexecução parcial da contratação.	Impacto na continuidade dos serviços de segurança cibernética e aumento do risco cibernético.	Divergências na execução do contrato.	Monitoramento contínuo da conformidade contratual.	Aplicação de sanções e adoção de medidas corretivas. Manutenção de documentação detalhada das exigências contratuais e obrigações da empresa contratada. Transferência de conhecimento durante a contratação. Responsável: Fiscal Técnico.
Fim da vigência do contrato.	Necessidade de nova contratação para evitar descontinuidade dos serviços.	Término do prazo de execução contratual.	Planejamento antecipado para a substituição e transição dos serviços contratados.	Abertura de novo processo de contratação com antecedência mínima de 6 meses. Manutenção de uma estratégia de contingência baseada na retenção de conhecimentos essenciais. Transferência de conhecimento durante a contratação. Responsáveis: Fiscal Técnico e Administrativo.

Tabela 3 - Estratégia de Independência do TRE-PA com Relação à Empresa Contratada

2.25.2.1. Transferência de conhecimento durante a contratação.

a) Durante a vigência da contratação a CONTRATADA fica obrigada ao repasse de conhecimento de:

- Tecnologias envolvidas na contratação;
- Metodologias envolvidas na contratação;
- Processos;

b) A transmissão de conhecimento deverá ser realizada aos usuários replicadores dentro da TI por meio de:

- Documentação dos processos;
- Documentação das dos procedimentos operacionais padrões;
- Cartilhas, webinar, vídeos institucionais;
- Palestras, workshops;
- Treinamento aos usuários replicadores;

c) Relatórios e Documentação

A CONTRATADA deve apresentar, por seus representantes, os seguintes relatórios para acompanhamento dos serviços conforme descrito na tabela abaixo:

RELATÓRIO	CONTEÚDO	PRAZO DE ENTREGA A CONTRATANTE
Relatório de ocorrências	Relatório preliminar com as informações básicas, após ocorrência de qualquer irregularidade no ambiente da CONTRATANTE.	Até duas horas, com atualizações periódicas até que a ocorrência esteja solucionada e; No dia subsequente, deve apresentar relatório revisado/definitivo.
Relatório Diário	Relatório de passagem de turno com informações sobre a execução dos serviços, todas as ocorrências/incidentes do turno, ou qualquer outra irregularidade ou atividade realizada.	Diário, conforme horários a serem definidos pela CONTRATANTE.

Relatório semanal de Serviços e Ocorrências	Relatório com informações sobre a execução dos serviços e resumo das ocorrências da semana, especialmente das mudanças	Semanalmente às segundas-feiras, contendo as informações referentes ao período de segunda-feira anterior a domingo.
Relatório mensal para controle de licenças	Relatório mensal para controle de licenças dos softwares dos ambientes e suas respectivas versões.	Até as 18h00 do dia 15 do mês subsequente à prestação do serviço.
Relatório mensal para controle de Ativos de TIC	Inventário atualizado para controle dos ativos de TIC sob a responsabilidade da CONTRATADA	Até as 18h00 do dia 15 do mês subsequente à prestação do serviço.
Relatório mensal dos níveis de serviços	Relatório com informações sobre os indicadores/metade de níveis de serviços alcançados para cada célula com gráficos, planilhas, estatísticas e informações de evolução dos indicadores/ serviços, recomendações de melhorias técnicas e administrativas para o próximo período e demais informações relevantes para a gestão contratual.	Até as 18h00 do dia 15 do mês subsequente à prestação do serviço.
Planilha Mensal de Indicadores	Contendo indicadores/metade de níveis de serviços alcançados para cada célula refletindo no faturamento (quando houver ocorrência de glosa).	Até as 18h00 do dia 3 do mês subsequente à prestação do serviço.
Documentação das atividades	Documentos operacionais e demais documentos descritivos dos processos, atividades e rotinas sob sua responsabilidade.	Atualização constante, sempre que ocorrerem alterações e; Revisão periódica sob demanda da CONTRATANTE.

Tabela 4 - Relatórios e documentos relacionados à transferência de conhecimentos.

Observações:

- 1) Os relatórios devem ser assinados pelo(s) representante(s) da CONTRATADA e entregues em meio eletrônico e/ou magnético, nas versões editável e não editável, mediante depósito em "Repositório de Documentos" a ser definido pela CONTRATANTE.
- 2) Na eventualidade de indisponibilidade de acesso ao repositório poderá ser entregue em meio papel devidamente assinado pelos representantes da CONTRATADA e/ou por outro meio definido pela CONTRATANTE.
- 3) A Planilha Mensal de Indicadores (alínea 6 da tabela acima) deverá ser entregue, obrigatoriamente, em meio papel, devidamente assinada pelo(s) representante(s) da CONTRATADA e da CONTRATANTE em função de que servem de base à verificação dos valores mensais a serem pagos à CONTRATADA.
- 4) Os relatórios de gerenciamento e acompanhamento dos serviços não são passíveis de remuneração (emissão de OS).
- 5) A CONTRATADA obriga-se a manter atualizada a documentação de arquitetura 'As-Built' de todo o ambiente de segurança da informação. No encerramento do contrato, o pagamento da última fatura ficará condicionado à entrega final desta documentação e à realização de um workshop técnico de transição para a equipe de servidores do TRE-PA

2.25.3 Ações para Transição Contratual

O TRE-PA manterá o monitoramento constante do contrato, garantindo o armazenamento de dados, registros e documentos gerados durante a execução dos serviços. As seguintes ações serão adotadas para garantir uma transição eficaz:

ID	AÇÃO	RESPONSÁVEL	INÍCIO	FIM
01	Realizar reunião inicial de alinhamento (Kick-off) com a nova contratada sobre a execução dos serviços de segurança cibernética, definindo interlocutores e matriz de responsabilidades.	Gestor do Contrato e Empresa Contratada	Até 5 dias após a assinatura do contrato	Até a apresentação e aprovação do plano de execução.
02	Mapeamento de Processos Críticos (De-Para) <i>Realizar o inventário dos scripts e automações existentes no modelo UST atual e documentar sua migração para os playbooks dos perfis profissionais mínimos. A nova contratada deverá, nos primeiros 60 dias (Fase de Inserção), homologar a efetividade das rotinas de segurança legadas, garantindo que a mudança da métrica de pagamento não gere descontinuidade na vigilância dos ativos críticos.</i>	Fiscal Técnico e Equipe de Planejamento (Atual e Nova Contratada)	Imediato após Reunião Inicial	Até 30 dias (Fim da Fase de Implantação)

Tabela 5 - Ações para Transição Contratual

2.25.4 Ações para Encerramento Contratual

Durante a vigência do contrato, o TRE-PA implementará ações de controle para assegurar o adequado encerramento dos serviços. As seguintes ações serão adotadas:

Id	AÇÃO	RESPONSÁVEL	INÍCIO	FIM
01	Validar a entrega das versões finais dos serviços, produtos alvos, scripts, arquivos de configuração e outras documentações pertinentes à contratação	Gestor do Contrato	Após a assinatura do contrato	Ao término do contrato
02	Transferência final de conhecimentos sobre a execução e a manutenção da Solução de Tecnologia da Informação e Comunicação	Gestor do Contrato	Após a assinatura do contrato	Ao término do contrato
03	Devolução de recursos materiais	Não se aplica. Pela natureza do contrato, não há necessidade do TRE-PA disponibilizar recursos de TI para a contratada.	Após a assinatura do contrato	Ao término do contrato
04	Revogação de perfis de acesso. Credenciais administrativas devem ser revogadas.	Gestor do Contrato com apoio do Fiscal Técnico	Após a assinatura do contrato	Ao término do contrato

05	Eliminação de dados armazenados	Gestor do Contrato	Após a assinatura do contrato	Ao término do contrato
06	Realizar o encerramento administrativo do contrato	Gestor do Contrato	5 (cinco) dias antes do final do contrato	Ao término do contrato

Tabela 6 - Ações para Encerramento Contratual

2.25.5. Direitos de propriedade intelectual

Todas as informações, imagens e documentos a serem manuseados e utilizados são de propriedade do CONTRATANTE, não podendo ser repassadas, copiadas, alteradas ou absorvidas pela CONTRATADA sem expressa autorização da CONTRATANTE, de acordo com Termo de Compromisso de Manutenção de Sigilo e Termo de Ciência, a ser firmado entre a CONTRATADA e seus empregados, disponibilizada cópia à CONTRATANTE.

A CONTRATADA deverá entregar para o CONTRATANTE toda e qualquer documentação produzida decorrente da instalação da solução de TI, objeto desta CONTRATAÇÃO, bem como, cederá ao CONTRATANTE, em caráter definitivo e irrevogável, o direito patrimonial e a propriedade intelectual dos resultados produzidos durante a vigência do contrato e eventuais aditivos, entendendo-se por resultados quaisquer estudos, relatórios, especificações, descrições técnicas, protótipos, dados, bancos de dados, esquemas, plantas, desenhos, diagramas e documentação, em papel ou em qualquer forma ou mídia.

Para fins de prevenção à dependência tecnológica (Vendor Lock-in) e garantia da continuidade do negócio, define-se que integram o patrimônio intelectual do **CONTRATANTE** todos os artefatos de configuração e inteligência cibernética desenvolvidos ou customizados durante a vigência contratual. Isso abrange, taxativamente:

- 1) **Regras de Correlação e Detecção:** Códigos, queries e lógicas implementadas em ferramentas de SIEM/XDR;
- 2) **Automação:** Playbooks, scripts (Python, PowerShell, etc.), conectores e fluxos de trabalho criados para orquestração de resposta (SOAR);
- 3) **Observabilidade e monitoramento:** Painéis (Dashboards), relatórios customizados e parsers de logs;
- 4) **Documentação Operacional:** Runbooks técnicos e bases de conhecimento de incidentes. Fica vedada à **CONTRATADA** a utilização de códigos proprietários fechados, criptografados ou ofuscados na camada de configuração dessas ferramentas que impeçam a leitura, manutenção ou migração futura por parte da equipe do Tribunal ou de terceiros

Todos os artefatos de inteligência cibernética, incluindo regras de correlação no SIEM, scripts em Python/PowerShell e playbooks de SOAR, são de propriedade exclusiva do **TRE-PA**. A CONTRATADA deve entregar esses códigos em formato aberto, legível e extensamente documentado, sendo **expressamente vedado** o uso de bibliotecas proprietárias fechadas ou técnicas de ofuscação que impeçam a manutenção futura por outra empresa ou pelo próprio Tribunal.

2.26. Tratamento diferenciado para ME e EPP

Esta contratação não se enquadra nos benefícios da Lei Complementar nº 123/2006 e do Decreto 8.538/15, devido o valor total estimado de cada item ser superior a R\$ 80.000,00 (oitenta mil reais).

2.27. Das reservas de vagas

2.27.1. Possibilidade de participação de egressos na execução do Contrato a ser firmado, conforme determina o Decreto Federal n.º 9.450/2018 e a Resolução TRE/PA n.º 5.434/2018

() SIM (X) **NÃO**

A utilização de egressos do sistema penal encontra alguns entraves para este contrato, quais sejam:

- a) Em relação à possibilidade de contratação de Egressos do Sistema Penal, conforme determina o Decreto Federal n.º 9.450/2018 e a Resolução TRE/PA n.º 5.434/2018, informamos que este contrato envolve parcela variável referente a atividades que ensejam viagens para outros municípios do Estado, ou até outros Estados da Federação, motivo este pelo qual não seria indicado aos egressos.
- b) Ademais, considerando que a contratação envolve atividades de operação a sistemas com acesso privilegiado, que apresentam informações sensíveis e dados de pessoa natural (eleitores), a exemplo do sistema ELO e ACESSONET, entendemos que esta contratação específica também não se enquadraria, a priori, na hipótese de utilização de candidatos do sistema penal (Res. TRE-PA 5.434/2019, Art. 4º Parágrafo Único).
- c) Por fim, cumpre destacar o alto grau de especialização do serviço a ser contratado.

2.27.2. Da reserva de vagas para pessoas em condição de vulnerabilidade (Resolução CNJ 497/2023)

A Resolução CNJ 497/2023 não é aplicável à presente contratação, pois o contrato resultante da Licitação contará com número de colaboradores inferior 25.

2.28. Outros Requisitos Aplicáveis

Vistoria

2.28.1. A avaliação prévia do local de execução dos serviços é imprescindível para o conhecimento pleno das condições e peculiaridades do objeto a ser contratado, sendo assegurado ao interessado o direito de realização de vistoria prévia, acompanhado por servidor designado para esse fim, de segunda à sexta-feira, das 08:00 horas às 17:00 horas.

2.28.1.1. Para a vistoria, o representante legal da empresa ou responsável técnico deverá estar devidamente identificado, apresentando documento de identidade civil e documento expedido pela empresa comprovando sua habilitação para a realização da vistoria.

- Local da vistoria: A vistoria ocorrerá no Edifício Sede do TRE-PA e seus respectivos prédios Anexos, localizado na Rua João Diogo 288, Campina, CEP 66015-902, Belém-PA.

2.28.2. Serão disponibilizados data e horário diferentes aos interessados em realizar a vistoria prévia.

2.28.3. Por meio da vistoria serão apresentados às licitantes:

- a) Ambientes Físicos: Os locais onde os serviços serão prestados, incluindo o Datacenter e as instalações das equipes da Coordenadoria de Gestão da Segurança da Informação e Infraestrutura de Data Center (CGSI).
- b) Infraestrutura de Datacenter: O ambiente de servidores, a solução de virtualização e os subsistemas de controle e operação que hospedam os sistemas críticos do TRE-PA.
- c) Softwares de Segurança Cibernética: O conjunto de soluções, ferramentas e softwares que compõem o ambiente de segurança da informação do Tribunal, tais como:

- d) Firewall de Próxima Geração (NGFW) e Firewall de Aplicação Web (WAF).
- e) Ferramentas de segurança para ambientes de nuvem e de microsegmentação.
- f) Sistemas de Monitoramento e Observabilidade: As ferramentas de monitoramento e gerenciamento de incidentes de segurança (SIEM), gestão de logs e auditoria, e as plataformas de detecção de intrusão (NDR) utilizadas pela Justiça Eleitoral do Pará.
- g) Processos de Backup e Continuidade: A solução de backup e restauração de dados em uso e os procedimentos para garantir a continuidade dos serviços essenciais.
- h) Ambiente e Metodologias de Trabalho: Os processos atuais estão focados em gestão de incidentes, resposta a ameaças e apoio à infraestrutura e operação de desenvolvimento seguro (DevSecOps).

2.28.4. Caso o licitante opte por não realizar a vistoria, deverá prestar declaração formal assinada pelo responsável técnico do licitante acerca do conhecimento pleno das condições e peculiaridades da contratação.

2.28.5. A não realização da vistoria não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes dos locais da prestação dos serviços, devendo o contratado assumir os ônus dos serviços decorrentes.

2.28.6. A fim de mitigar a assimetria informacional e garantir a isonomia, a Justiça Eleitoral do Pará disponibilizará aos licitantes que realizarem a vistoria técnica (ou participarem da sessão pública) os seguintes dados mínimos consolidados, resguardado o sigilo necessário:

- a) Inventário quantitativo de ativos de rede e segurança (Firewalls, WAF, IPS, etc.) com versões de firmware;
- b) Topologia lógica simplificada do ambiente de rede e nuvem;
- c) Volumetria média mensal de incidentes de segurança registrados nos últimos 12 meses;
- d) Relação de ferramentas de segurança atualmente em operação (catálogo de software).

3. ESTIMATIVA DA DEMANDA - QUANTIDADE DE BENS E SERVIÇOS (VOLUMETRIA)

Esta seção detalha a volumetria integral do ambiente tecnológico e de serviços do TRE-PA, abrangendo desde o atendimento a 101 Zonas Eleitorais e aproximadamente 1.580 usuários até a gestão de mais de 1.500 ativos, bem como a série histórica de chamados relacionados à equipe atual, fundamentando o dimensionamento estratégico de 9 perfis profissionais especializados para a gestão de TIC, sustentação da segurança da informação e proteção de dados.

3.1. A quantidade de serviços/perfis, deve observar os descritos na tabela abaixo:

ITEM	DESCRIÇÃO DA ATUAÇÃO	ID	CBO DE REFERÊNCIA	PERFIL	CÓDIGO	QUANTIDADE DE PROFISSIONAIS
1 – Serviços técnicos especializados de atendimento ao usuário de TIC	Profissional com responsabilidade de coordenar e gerenciar a atuação dos demais técnicos de suporte e de manutenção, garantindo a adequada prestação dos serviços, bem como controlando e planejando operacionalmente as ações da equipe. Presta também apoio à tomada de decisão do órgão auxiliando na prospecção de soluções de suporte ao usuário, fornecimento de informações táticas e operacionais e proposição de ações de aprimoramento dos serviços de suporte ao usuário.	1.1	1425-25	Gerente de suporte técnico de tecnologia da informação	GERSUP	1
	Profissional responsável por assegurar a prestação de serviços de segurança da informação, incluindo o monitoramento e tratamento de incidentes, ações preventivas, implantação e monitoramento de controles de segurança, realização dos diferentes testes e inspeções de segurança, presta serviços de controle de segurança preventivo e reativo relacionados aos diferentes ativos da infraestrutura, bem como apoia na implementação das ações técnicas previstas na política de segurança.	1.2	2123-20	Administrador em segurança da informação - Sênior	ASEG-03	3
		1.3	2123-21	Administrador em segurança da informação - Pleno	ASEG-02	2
		1.4	2123-22	Administrador em segurança da informação - Júnior	ASEG-01	3
TOTAL						9

Tabela 7. Quantidade de Perfis associados ao serviço.

3.1.1. A definição e o dimensionamento dos perfis profissionais para a presente contratação fundamentam-se estritamente nas diretrizes da Portaria SGD/MGI nº 1.070/2023 (atualizada pelas Portarias nº 6.680/2024 e nº 6.055/2025), que padroniza o modelo de contratação de serviços de operação de infraestrutura de TIC no Poder Executivo Federal, utilizado como referência integral para a presente contratação. A adoção de um quadro composto por 9 (nove) profissionais — distribuídos entre Gerente de Suporte Técnico (GERSUP) e Administradores de Segurança da Informação (ASEG Júnior, Pleno e Sênior) — garante que o serviço contratado possua a qualificação técnica padronizada, com base nas competências (ITIL, COBIT, NIST, MITRE ATT&CK, CIS Controls) exigidas pelo órgãos órgãos de controle (CNJ e TCU) para o cumprimento das exigências da Resolução CNJ Nº 396, de 07 de junho de 2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).

3.1.2. Esse dimensionamento pautou-se no histórico de consumo de chamados de incidente/requisição para a área de segurança cibernética do Tribunal, assegurando que a futura contratada disponha da capacidade operacional mínima necessária para cumprir rigorosamente os Níveis Mínimos de Serviço (NMS), afastando a métrica de mero esforço (UST) e focando na efetiva proteção e disponibilidade do ambiente. A escolha de diferentes níveis de senioridade e especialização é justificada pelo nexo de causalidade direto com a alta complexidade e criticidade da infraestrutura tecnológica do TRE-PA.

3.1.3. O perfil estratégico GERSUP é vital para a gestão dos recursos, governança e interlocução em crises cibernéticas. A exigência de perfis Sênior e Pleno (ASEG-03 e ASEG-02) reflete a necessidade imperativa de implementar arquiteturas avançadas de segurança, como a Cybersecurity Mesh Architecture (CSMA) e Zero Trust, além de realizar a engenharia de detecção (SIEM/SOAR), caça a ameaças e o enrijecimento (hardening) contra incidentes destrutivos, como o ransomware; **exigências a serem atendidas com profissionais adequados para as atividades em tela, sem que ocorra desvio de função profissional por perfis estranhos às atividades de Segurança Cibernética e Infraestrutura.** Por fim, a base operacional formada pelos perfis Júnior (ASEG-01) assume a gestão de identidades (IAM) e a triagem ágil de alertas, formando um ecossistema de defesa escalonado e capaz de assegurar a conformidade com a Lei Geral de Proteção de Dados (LGPD) e com as resoluções do Conselho Nacional de Justiça (CNJ).

3.2. Metodologia de cálculo da volumetria estimada

3.2.1. A definição da volumetria estimada para a presente contratação pautou-se nos parâmetros técnicos e metodológicos propostos pela Portaria SGD/MGI nº 1.070/2023, sendo dimensionada para refletir a necessidade de proteção contínua dos ativos digitais da Justiça Eleitoral do Pará. O quantitativo considerado adequado para a execução dos serviços de 3º nível de atendimento fundamentou-se, essencialmente, nos seguintes pilares:

- a) Análise do histórico e contratos vigentes: Avaliação da execução contratos atuais (Vide item 1.6) para identificar lacunas e oportunidades de melhoria na alta especialização em segurança, visando o desenvolvimento da maturidade em frameworks CIS Controls v8, NIST e MITRE ATT&CK;
- b) Levantamento volumétrico de demandas das equipes: Análise técnica do histórico de chamados e incidentes complexos que exigiram intervenção de última instância, desconsiderando-se, para fins de dimensionamento desta equipe, as demandas de média e alta complexidade típicas de 3º nível;
- c) Inventário e Complexidade do Ambiente: Mapeamento da infraestrutura híbrida (Infraestrutura crítica, Data Center Tier 3 e Nuvem) e da capilaridade das 101 Zonas Eleitorais, considerando a criticidade dos serviços e a necessidade de conformidade com a LGPD e as regulamentações do TSE e CNJ.

3.2.2. Este dimensionamento visa garantir que o suporte especializado possua a senioridade necessária para a sustentação de arquiteturas modernas, como a Malha de Segurança Cibernética (CSMA) e o modelo Zero Trust, assegurando a resiliência operacional do Tribunal.

3.2.3. Para determinar a quantidade adequada de profissionais, foram considerados ainda os seguintes fatores:

a) Inventário, Complexidade da Infraestrutura de TIC, frequência de incidentes e requisitos de compliance.

- Número total de servidores físicos e virtuais, ativos de rede, firewalls e dispositivos de segurança.
- Quantidade de aplicações críticas em operação e sua dependência de monitoramento contínuo.
- Estimativa de acessos internos e externos aos sistemas institucionais.
- Principais Cargas de Trabalho e Indicadores Operacionais.
- Frequência de varreduras de vulnerabilidades e tempo necessário para mitigação.
- Número de logs e eventos gerados por ferramentas de monitoramento e detecção de ameaças (SIEM, IDS/IPS, firewalls, etc.).
- Quantidade de solicitações de gerenciamento de acessos privilegiados e concessão de credenciais.
- Normas, Regulamentações e Requisitos de Compliance

b) Adesão às diretrizes do CIS Controls v8, NIST Cybersecurity Framework, ISO/IEC 27001 e ISO/IEC 27035 (gestão de incidentes).

- Quantidade de controles do catálogo de serviço aplicados em atendimento às exigências da Lei Geral de Proteção de Dados (LGPD) para controle de acesso e proteção de informações sensíveis.
- Quantidade de controles aplicados em conformidade com requisitos de auditoria e monitoramento contínuo de segurança cibernética.
- Modelos de Serviços e Cobertura Necessária

c) Necessidade de suporte presencial 8x5 para resposta a incidentes e mitigação de riscos emergentes.

- Operação de diferentes frentes, como monitoramento de ameaças, análise de vulnerabilidades, resposta a incidentes, inteligência cibernética e auditoria de segurança.
- Ajustes sazonais na demanda, considerando plantões eventuais para mudanças de infraestrutura, participação em eleições oficiais e suplementares, auditorias internas e externas, e períodos de alta atividade judicial.

3.2.4. Com base nesses fatores, a estimativa da volumetria foi calculada a partir da combinação de indicadores históricos, projeções de crescimento da infraestrutura *on premise* e nuvem, bem como a necessidade de aumento de governança e resiliência operacional. A definição do quantitativo de profissionais foi estruturada com base em perfis especializados para diferentes níveis de atuação (estratégico, tático e operacional), considerando o quantitativo mínimo de referência atualmente em atuação, garantindo a proteção eficaz dos ativos digitais do Tribunal.

3.3. Análise dos contratos atuais

3.3.1. Para efeito de memória de cálculo foi seguida a orientação de Portaria SGD/MGI nº 1.070/2023:

“10.7.2.1. Orienta-se que o dimensionamento para a estimativa inicial das equipes e a seleção dos perfis profissionais que balizarão a formação do preço de referência considere o histórico de quantitativo de pessoal dos contratos atual e anteriores e/ou o quantitativo de servidores que atuam nos serviços de operação de infraestrutura e atendimento a usuários de TIC.”

3.3.2. Atualmente os serviços são mantidos por meio do Contratos nº 28/2020 e nº 121/2022, que possuem em seu escopo perfis e serviços de atendimento a usuários de TIC e de operação de infraestrutura de TIC do TRE-PA. O quantitativo descrito na tabela abaixo, mostra a atual equipe no atendimento aos serviços objeto destas contratações, servindo como um dos parâmetros de dimensionamento:

FORÇA DE TRABALHO ATUAL		
CONTRATO	DESCRIÇÃO	QUANTIDADE
28/2020	COORDENADOR DE TECNOLOGIA DA INFORMAÇÃO	1
	TÉCNICO EM INFORMÁTICA	2
	ANALISTA DE SUPORTE COMPUTACIONAL - PLENO / ADMINISTRADOR EM SEGURANÇA DA INFORMAÇÃO	2
	ANALISTA DE SISTEMAS OPERACIONAIS	1
121/2022	ANALISTA DE SUPORTE OPERACIONAL	3
TOTAL		9

Tabela 8 - Força de Trabalho atual - CTO Nº 28/2020 e CTO nº 121/2022 alocada na CGSI/STI

3.3.3. Conforme orienta a Portaria SGD/ME no 1.070/2023, essas informações são importantes para auxiliar no dimensionamento dos serviços e, consequentemente, dos perfis profissionais necessários para as categorias de serviços.

3.3.4. O(s) Contrato(s) atual(is) mantiveram uma equipe média de 9 profissionais ao longo dos últimos anos. Com a possibilidade de reestruturação do processo em nova contratação a equipe de planejamento ajustou a senioridade dos perfis mantendo o quantitativo mínimo de profissionais em 9 (nove), necessários à contratação. Tal definição considera a implementação e revisão de processos, a otimização de recursos e a implementação de automações pela nova contratada, ressaltando-se que as estimativas realizadas não configuram alocação de postos de trabalho com dedicação exclusiva.

3.3.5. Em se tratando de contratação de serviços, com execução orientada para alcançar níveis de serviço, a CONTRATADA poderá investir no aumento da sua produtividade, adotando providências de melhoria da gestão dos processos operacionais que encontrem sob a sua responsabilidade, adotando as melhores práticas, racionalizando métodos e processos que transformem, implementem, agreguem valor as atividades, atuando em conformidade com orientações governamentais, entre outros fatores diretamente relacionados à gestão de TIC, direcionando-os sempre para o aumento da qualidade do ambiente tecnológico da CONTRATANTE.

3.3.6. Nos termos da Portaria SGD/MGI nº 1.070/2023 (item 10.7.2.6), a estrutura inicialmente definida pode sofrer ajustes durante o período de execução contratual, mediante prévia comunicação à empresa CONTRATADA, permitindo que ela possa se adaptar à nova estrutura e a dinâmica da necessidade do TRE-PA ao longo da execução contratual.

3.3.7. No que tange a atuação dos perfis de 3º Nível da contratação, cumpre destacar a mudança dos perfis operacionais de infraestrutura para atendimento específico de atividades da área de segurança da informação e gestão de infraestrutura. Esta proposta de reestruturação de perfis, visa atender demandas relacionadas às tendências tecnológicas, de conformidade e o aumento da complexidade de tarefas de proteção de dados, ante à necessidade de migração para ambientes de cloud.

3.3.8. Adicionalmente, foram consideradas no Estudo Técnico as melhorias contínuas e automações previstas pela Portaria SGD MGI no 1.070/2023, além de um benchmarking com práticas do setor para validar a necessidade de profissionais com relação à especificidade e senioridade. Dessa forma, entende-se que a estimativa de profissionais proposta atenderá minimamente à demanda, mantendo a eficiência operacional alinhada às melhores práticas de operação de infraestrutura de TIC, segurança da informação e defesa cibernética.

3.3.9. Vale ressaltar que os ambientes de TIC encontram-se disponíveis e operacionais com a equipe de profissionais mantida pelo contrato atual, atendendo os níveis mínimos de serviços exigidos e com satisfação adequada dos usuários e dos gestores de TI do TRE-PA. Dessa forma, a equipe de planejamento entende não haver necessidade de alteração substancial no quantitativo e perfis estimados, ressaltados os ajustes consolidados na tabela do item 3.1.

3.4. Levantamento do Histórico de Chamados

3.4.1. Conforme estabelecido na Portaria SGD/MGI nº 1.070, de 1º de junho de 2023, a análise de dados históricos confiáveis são pressupostos fundamentais para a correta aplicação do modelo de estimativa de demanda. O levantamento do histórico de chamados tem como objetivo reunir e analisar registros de requisições de serviço, incidentes e requisições de mudança direcionados à equipe atual de operação de segurança cibernética, manutenção da infraestrutura de Datacenter e atendimento a usuários de TIC. O período mínimo considerado para essa análise foi de **12 meses (setembro/2024 a setembro/2025)**, cuja série histórica foi levantada por meio da ferramenta de Gerenciamento de Serviços de TI utilizada no TRE-PA.

3.4.2. Na contratação CTO nº 28/2020, baseada em Unidade de Serviços Técnico (UST), as atividades são classificadas como solicitações **rotineiras**, solicitações por **demandas** e **suporte**. Tarefas **rotineiras** são atividades operacionais recorrentes e predefinidas para manter a infraestrutura e os serviços; **demandas** referem-se a solicitações específicas dos usuários por novos serviços ou acessos, enquanto **suporte** envolve a resolução de incidentes e problemas para restaurar a operação normal dos serviços de TI.

3.4.3. Além disso, cada chamado relacionado à demanda é categorizado como **requisição de serviço**, que é uma solicitação formal de um usuário para um serviço padrão, como criação de conta ou acesso a sistemas. A categoria **incidente**, está relacionada à interrupção ou degradação não planejada de um serviço de TI, exigindo ação corretiva para restauração. A **manutenção** refere-se a atividades planejadas para preservar ou melhorar a infraestrutura e evitar falhas futuras. Neste contexto, existe a classificação de **incidente de segurança**, relacionado a um tipo específico de incidente associado a violações de políticas de segurança, tentativas de acesso não autorizado, comprometimento de dados ou atividades maliciosas que possam ameaçar a integridade, confidencialidade ou disponibilidade dos sistemas e informações. Os chamados relacionados à segurança cibernética e infraestrutura de Data Center são recepcionados pela Central de Atendimento ao Usuário, onde são classificados e priorizados ao 3º Nível (CGSI/STI).

3.4.4. Nestes termos, a utilização do registro histórico de chamados permite a obtenção dos dados qualitativos e quantitativos sobre os serviços prestados, auxiliando no correto dimensionamento dos serviços a serem contratados e na definição dos perfis profissionais necessários à equipe dedicadas à infraestrutura e segurança cibernética do Tribunal. Esse levantamento contribui para a justificativa do quantitativo máximo de profissionais requeridos para a prestação adequada dos serviços especializados de segurança cibernética. Além disso, outros fatores, como os níveis mínimos de serviço estabelecidos no escopo da contratação, também exercem influência direta no dimensionamento da equipe necessária. Dessa forma, a análise histórica de chamados é etapa essencial para garantir a alocação adequada de recursos e a eficiência da execução das atividades a serem contratadas.

3.4.5. Os quadros a seguir apresentam as estatísticas e volume de chamados tratados pela Coordenadoria de Gestão de Segurança da Informação e Infraestrutura de Datacenter durante período de Setembro de 2024 a Setembro de 2025, segmentados por unidade: Defesa Cibernética e Serviços Corporativos.

a) Histórico de Chamados Atendidos pela Seção de Defesa Cibernética (SDC) - período 2024/2025

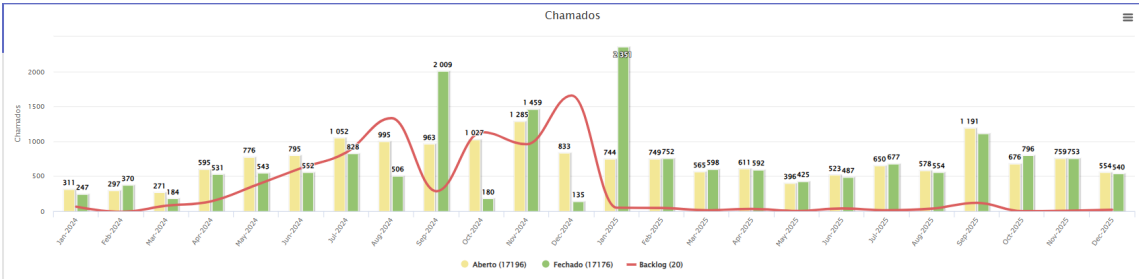


Figura 3 - Fila de chamados atendidos pela Seção de Defesa Cibernética (SDC) - 2024 e 2025



Figura 4 - Quantidade de chamados por categoria



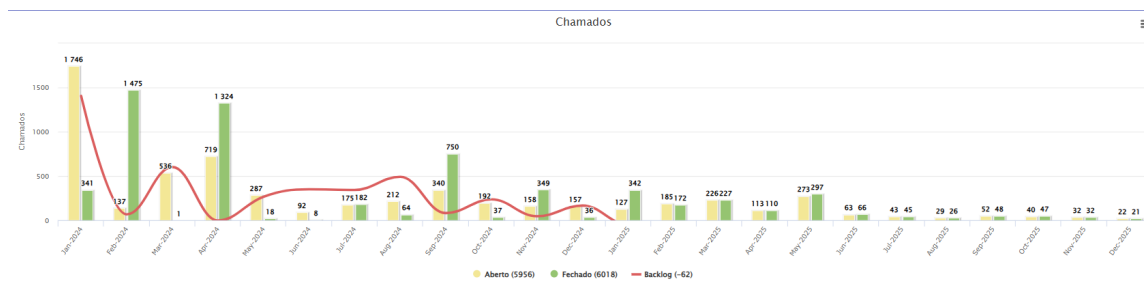


Figura 7 - Fila de chamados atendidos pela Seção de Soluções Corporativas (SSC) - 2024 e 2025

Top 5 - Chamados por Categoria

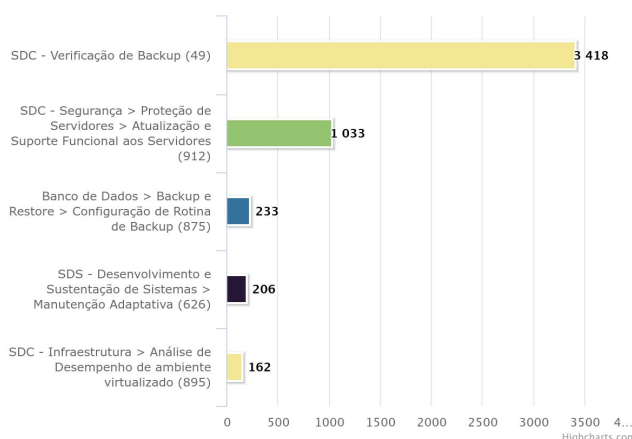


Figura 8 - Quantidade de chamados por categoria

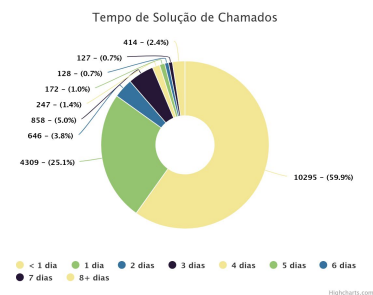


Figura 9 - Tempo de solução

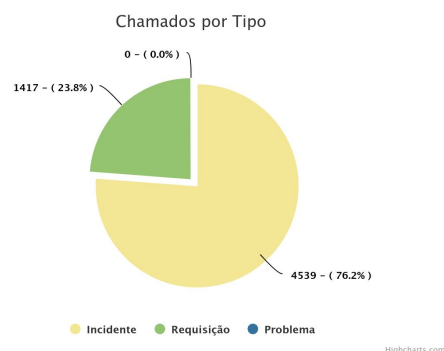


Figura 10 - Quantidade de chamados por categoria

Catego	2024												2025											
	jan.-24	Feb-24	mar.-24	Apr-24	May-24	jun.-24	jul.-24	Aug-24	Sep-24	Oct-24	nov.-24	Dec-24	jan.-25	Feb-25	mar.-25	Apr-25	May-25	jun.-25	jul.-25	Aug-25	Sep-25	Oct-25	nov.-25	Dec-25
Aberto (□)	1.746	137	536	719	287	92	175	212	340	192	158	157	127	185	226	113	273	63	43	29	52	40	32	22
Fechado (□)	341	1.475	1	1.324	18	8	182	64	750	37	349	36	342	172	227	110	297	66	45	26	48	47	32	21

Tabela 10 - Histórico de chamados SDC 2024/2025

3.5. Ambiente Tecnológico do TRE-PA

3.5.1. Esta seção descreve o Ambiente Tecnológico do TRE-PA. Informações detalhadas sobre o parque computacional de TIC, topologia de rede, soluções de segurança e versões de ferramentas, modelos de servidores, fabricante/versões banco de dados, entretanto, não serão incluídos neste ETP por se tratarem de informações de natureza estratégica do órgão. Maiores detalhes poderão ser repassados somente durante a vistoria, após a assinatura de termo de manutenção de sigilo e de responsabilidade por parte das empresas interessadas no certame (Item 10.2.4.2 da Portaria SGD/MGI nº 1.070/2023).

3.5.2. O "Levantamento do ambiente" detalha a dimensão e complexidade da infraestrutura do TRE-PA, permitindo à licitante dimensionar corretamente a proposta comercial, com base no levantamento do ambiente computacional, assim como em outras informações relevantes como a descrição das atividades por meio do catálogo de serviços, volumetria histórica de chamados, locais de prestação, perfis exigidos, Níveis Mínimos de Serviços (NMS), dentre outros elencados neste ETP. Com esses dados e os detalhes sensíveis liberados apenas na vistoria técnica, a empresa estima seus custos com precisão para garantir o cumprimento dos prazos e metas de serviço (NMS).

3.5.3. Neste contexto, a CONTRATADA deverá estar apta a prestar os serviços de suporte e manutenção continuada no ambiente tecnológico do Tribunal, visando a proteção de dados e a disponibilidade dos ativos de TIC descritos na tabela (não exaustiva) a seguir.

3.5.4. A tabela abaixo detalha o ambiente tecnológico do TRE-PA:

ID	DESCRIÇÃO
AMBIENTE TECNOLÓGICO	

1	Zonas Eleitorais	A Justiça Eleitoral do Pará atende a 101 zonas eleitorais.
2	Usuários de Computador	O ambiente corporativo possui aproximadamente 1.580 usuários, entre magistrados, servidores, requisitados estagiários e colaboradores.
3	Conectividade - Link Internet	A instituição conta com 4 links de internet para redundância e performance.
4	Conectividade - Link com TSE	Existem 2 links dedicados de comunicação com o Tribunal Superior Eleitoral.
5	Aplicações Críticas	Aproximadamente 80 aplicações críticas em operação demandam monitoramento contínuo de segurança.
6	Volume de Requisições	Média mensal de 80.000.000 de requisições aos sistemas institucionais.
7	Volume de Tráfego de Dados	Volume de acessos internos e externos estimado em ~10TB por mês.
8	Centro de Dados - Datacenter TIER 3	A instituição possui 1 Datacenter com certificação TIER 3.
9	Centro de Dados - Infra Nuvem	Utilização de 1 infraestrutura de nuvem complementar ao datacenter físico.
10	Servidores de Rede	Existência de 4 servidores físicos dedicados à rede.
11	Nós de Hiperconvergência	A infraestrutura conta com 10 nós físicos de hiperconvergência.
12	Storage SAN	No momento, não há Storage SAN dedicado (valor 0).
13	Capacidade de Processamento	Capacidade total de processamento em produção de 984.32 GHz.
14	Memória RAM Total	Aproximadamente 10TB de memória RAM em todo o ambiente de produção.
15	Armazenamento On-Premise	Capacidade de armazenamento local (produção) de aproximadamente 500TB.
16	Armazenamento em Nuvem	Capacidade de armazenamento em nuvem (produção) de aproximadamente 2TB.
17	Soluções de Backup em Disco	A instituição possui 3 soluções de repositório backup baseadas em disco, com capacidade total de 600TB
18	Soluções de Backup em Nuvem	O Tribunal possui 3 buckets ou instâncias de backup em nuvem S3, com capacidade total de 60TB
19	Robô de Backup / Biblioteca de Fitas LTO	1 robô de backup para armazenamento em fita ou mídia física com armazenamento em cofre externo
20	Servidores Físicos (Windows)	3 servidores físicos operando com sistema operacional Windows.
21	Servidores Físicos (Linux)	Nenhum servidor físico operando exclusivamente com Linux (valor 0).
22	Virtualização (VMWare)	Utilização de 10 hosts no clusters/instâncias VMWare.
23	Virtualização (Nutanix)	No momento, não há utilização de Nutanix (valor 0).
24	Outras Virtualizações	Não há outras plataformas de virtualização em uso (valor 0).
25	Servidores Virtuais Windows	Aproximadamente 50 servidores virtuais operando com Windows.
26	Servidores Virtuais Linux	80 servidores virtuais operando com Linux (incluindo bancos de dados).
27	Cluster Kubernetes	A instituição opera 8 clusters Kubernetes para microsserviços (desenvolvimento, homologação e produção)
28	Aplicações Containerizadas	Total de 200 aplicações rodando em formato de containers.
29	IaaS (Nuvem Pública)	1 provedor de IaaS (Azure/Amazon/Google Cloud) em uso.
30	SaaS (Office 365 / Google Workspace)	1.580 usuários suportados em modelo SaaS.
31	Visualização de Mapas (Google Maps)	1 serviço de visualização de mapas integrado.
32	Firewall de Borda/Perímetro (Físico)	4 firewalls de borda para proteção do perímetro.
33	Firewall Departamental	106 Firewalls utilizados nos cartórios eleitorais e itinerantes para proteção de dados e conexão VPN.
34	Serviço de VPN	1 serviço de VPN para acesso remoto seguro.
35	Portal de Aplicações	1 portal unificado de acesso remoto às aplicações.
36	Certificados Digitais A3	Gestão de aproximadamente 450 certificados digitais tipo A3.
37	Gestão de Ativos (Desktops)	Inventário de TIC cobrindo 1.500 desktops/notebooks.
38	Gestão de Ativos (Servidores)	Inventário de TIC cobrindo 80 servidores
39	Software de Backup	1.300 licenças de software de backup gerenciadas.
40	Antimalware (EDR/XDR) - Desktops	Proteção para 1450 estações de trabalho (valor para desktops).
41	Antimalware (EDR/XDR) - Servidores	Proteção para 80 servidor (conforme dado da planilha).
42	Antispam /Anti-Phishing	1 solução de proteção de correio eletrônico (Antispam / Anti-Phishing).
43	NDR (Ambiente Virtualizado)	1.480 sensores de detecção e resposta de rede (NDR).
44	Endpoint Privilege Manager	Licenças para gestão de privilégios em estações de trabalho.
45	Firewall de Aplicação (WAF)	2 Appliances Virtuais de solução de WAF para proteção de aplicações web.
46	SIEM / Solução de Logs	1 plataforma centralizada para agregação e gestão de eventos e logs de segurança.
47	Gestão de Vulnerabilidades	Cobertura de até 500 dispositivos na solução de gerenciamento.
48	Auditoria de Dados Não Estruturados	1 solução para auditoria e proteção de arquivos e dados em modo SaaS.
49	PAM (Privileged Access Management)	1 solução de gestão de acessos privilegiados implementada.
50	Software para Cópia e Recuperação de Dados	1 Solução para cópia e recuperação de dados baseada em software.
51	Servidores DNS	4 Servidores DNS internos
52	Domínios LDAP	O Tribunal possui 2 (dois) domínios de serviços de diretório.
53	Banco de Dados SGBD	2 instâncias de Produção de Homologação
54	Quantidade média de tráfego mensal das aplicações	~ 1.8 TB
55	Média mensal do total de requisições das aplicações	~ 35 (trinta e cinco) milhões de requisições.

Tabela 11 - Levantamento do Ambiente Computacional do TRE-PA

3.5.5. A tabela anterior apresenta o inventário sintético e a volumetria dos principais ativos e soluções que compõem o ambiente tecnológico da Justiça Eleitoral do Pará, sem mencionar, por motivos de segurança, detalhes técnicos como tecnologias específicas e versões. Este quadro detalha quantitativos de infraestrutura (como servidores físicos, infraestrutura virtualizada e de nuvem), volumetria de usuários e zonas eleitorais, bem como a relação das principais ferramentas de segurança da informação e proteção de dados atualmente em uso (tais como Firewall, WAF, SIEM, EDR/XDR, NDR, PAM e soluções de gestão de vulnerabilidades). O objetivo desta lista é fornecer aos licitantes uma visão macro da complexidade do ambiente que será atendido pelos serviços objeto desta contratação.

3.5.6. Verifica-se do ambiente a ser suportado a complexidade tecnológica, bem como os volumes não desprezíveis de serviços prestados pela STI para os usuários e a fim de suportar as atividades finalísticas do TRE-PA. Logo, entende-se que os serviços prestados pela futura contratada são críticos e essenciais para o Tribunal e tomar por base os parâmetros do contrato atual representam uma aproximação adequada para fins de dimensionamento de recursos a serem alocados.

3.5.7. Ademais, a estimativa dos serviços foi dimensionada a partir da análise de todos os dados já apontados neste documento, em especial no histórico de execução do atual contrato, a perspectiva de ampliação da quantidade dos serviços executados, a necessidade de modificação dos níveis de serviço para obtenção de serviços com mais qualidade, a quantidade estimada de usuários dos serviços, atendendo às diretrizes da Portaria SGD/MGI no 1.070/2023.

3.5.8. Nos termos da Portaria SGD/MGI no 1.070/2023, a estrutura inicialmente definida pode sofrer ajustes durante o período de execução contratual, mediante prévia comunicação à empresa contratada, permitindo que ela possa se adaptar à nova estrutura. Isso tudo para garantir eventuais oscilações do total de usuários a serem atendidos e do tamanho/complexidade da infraestrutura a ser suportada. Situação que não é incomum num ambiente distribuído e diverso como o do TRE-PA.

3.5.9. Nesse sentido, a presente contratação engloba perfis para atender a reestruturação das equipes, níveis de serviços, com capacidade de implementar controles de segurança, garantir a disponibilidade e operação do ambiente, bem como atender normas afetas aos serviços atendimento a usuários e sustentação de infraestrutura de TIC do TRE-PA.

3.6. Nexo de Causalidade e Justificativa de Senioridade dos Perfis

3.6.1. A complexidade crescente das ameaças cibernéticas e a rigorosa necessidade de conformidade legal, notadamente com a Lei Geral de Proteção de Dados (LGPD) e a Resolução CNJ N° 396/2021, impõem que a estratégia de defesa do TRE-PA evolua de uma postura reativa para um modelo preditivo e inteligente, conforme previsto neste ETP.

3.6.2. O dimensionamento do quantitativo de 9 (nove) perfis profissionais mínimos necessários à execução, somado ao aumento da complexidade das atividades de segurança cibernética, à série histórica de chamados (cerca de 13.900 anuais) e volumetria de ativos (mais de 1.500 ativos e 240 máquinas virtuais), reflete, fundamentalmente, a necessidade de **elevação do nível de senioridade e especialização** da força de trabalho em relação aos Contratos anteriores (28/2020 e 121/2022).

3.6.3. A nova contratação exige a implementação e operação de arquiteturas avançadas, como a *Cybersecurity Mesh Architecture* (CSMA) e *Zero Trust Architecture* (ZTA), além da gestão de incidentes críticos (como *ransomware* e vazamento de dados) sob os frameworks NIST CSF 2.0 e CIS Controls v8.

3.6.4. Dessa forma, os serviços que outrora eram absorvidos por colaboradores de suporte genérico ou de infraestrutura básica agora exigem perfis dedicados à Engenharia de Detecção (SIEM/SOAR), Caça a Ameaças (*Threat Hunting*), Análise de Malware (EDR/NDR) e Governança de Acessos Privilegiados (PAM). A tabela abaixo materializa o nexo de causalidade (De > Para) que justifica o nível de senioridade exigido para os perfis profissionais que compõem a contratação.

Perfis Anteriores (Operação Tradicional - Contratos 28/2020 e 121/2022)	Perfis da Nova Contratação (Defesa Cibernética Avançada - ETP Atual)	Justificativa Técnica para a Senioridade Exigida no Novo Cenário
Coordenação de Suporte Técnico / Gestão de SLA Básica	1x Gerente de Infraestrutura de TI (GERINF)	Alta Senioridade para a liderança da equipe técnica e governança dos serviços de TIC. O perfil deve aplicar frameworks COBIT para assegurar o alinhamento estratégico e gestão de riscos, além de ITIL para garantir a eficiência operacional, a melhoria contínua e o cumprimento dos níveis de serviço (SLA/NMS) no âmbito do TRE-PA.
Analistas de Segurança (Foco em Antivírus e regras de Firewall de Borda)	3x Administrador em Segurança da Informação Sênior (ASEG-03)	Alta Senioridade (N3 / Threat Hunting): O ambiente migrou para detecção avançada. O perfil Sênior é exigido para operar orquestração e automação (SOAR), correlacionar logs complexos no SIEM, criar regras e playbooks baseadas no MITRE ATT&CK e desenvolver processos de análise forense em casos de intrusão. O perfil Sênior é essencial para manter baselines de segurança (CIS Benchmarks), garantir a imutabilidade de backups, gerir cofres de senhas (PAM) e garantir recuperação de desastres (Disaster Recovery).
Analistas de Suporte (Tratamento de tickets rotineiros de bloqueios/acessos)	2x Administrador em Segurança da Informação Pleno (ASEG-02)	Média Senioridade (N3 / Resposta a Incidentes): Atuam na contenção imediata de incidentes, gestão do ciclo de vida de vulnerabilidades (Gap Analysis proativo) e operação de plataformas de proteção de endpoints (EDR), garantindo o cumprimento rígido de Níveis Mínimos de Serviço (NMS).
Técnicos de Monitoramento de Rede (NOC) e Suporte N1	3x Administrador em Segurança da Informação Júnior (ASEG-01)	Senioridade Inicial Especializada (N3 / IAM): Shift do monitoramento de disponibilidade (NOC) para monitoramento de segurança baseado em análise comportamental. Realizam a gestão de identidade (IAM), gestão de acessos privilegiados, configuração de perfis (VPN, certificados digitais) de triagem inicial de alertas de EPM/EDR, separando falsos positivos e aplicando playbooks básicos de contenção antes do escalonamento.

Tabela 12 - Nexo de causalidade (De > Para) que justifica o nível de senioridade.

3.6.5. A exclusão de indicadores de atendimento genérico ao usuário final (*Help Desk* básico) e a concentração das métricas na eficácia do tratamento de vulnerabilidades, MTTR (Tempo Médio de Resposta) e prevenção a ataques tornam inviável a execução contratual por profissionais de baixa qualificação técnica. A exigência dos 9 perfis (com predominância de profissionais Sênior e Pleno) é condição para operar o atual parque tecnológico complexo do TRE-PA e resguardar os dados custodiados pelo Tribunal.

3.7. Qualificação Técnica necessária à Contratação

3.7.1. A definição da experiência profissional e das competências técnicas para esta contratação observa as diretrizes de experiência mínima e o enquadramento dos perfis da Portaria SGD/MGI n° 1.070/2023. Tal parametrização garante que a equipe técnica possua senioridade e especialização compatíveis com a criticidade dos ativos e a complexidade do ambiente tecnológico do TRE-PA, conforme detalhado na seção 3.6 anterior.

3.7.2. A alocação de profissionais com os níveis de senioridade propostos (Júnior, Pleno e Sênior) justifica-se pela necessidade de escalonamento técnico em incidentes críticos, garantindo que a **Justiça Eleitoral do Pará** disponha de suporte especializado para a manutenção da disponibilidade, integridade e confidencialidade dos seus dados e sistemas.

3.7.3. Os perfis foram projetados para atender à alta criticidade do ambiente, exigindo-se competências que abrangem desde o monitoramento ostensivo de segurança até a execução de contramedidas em incidentes complexos. A qualificação técnica deve assegurar a plena operação das ferramentas de proteção de borda, gestão de identidades e auditoria de dados, competências estas essenciais para neutralizar vetores de risco e garantir a sustentabilidade dos serviços críticos e a proteção de dados sensíveis sob custódia da Justiça Eleitoral do Pará.

3.7.4. A definição dos perfis profissionais e suas respectivas qualificações técnicas fundamenta-se na complexidade do ambiente tecnológico da Justiça Eleitoral do Pará, garantindo a execução dos serviços por perfis técnicos altamente especializado. Esta especificação visa assegurar que a contratada aloque competências compatíveis com as exigências de segurança da informação e proteção de dados mapeadas na fase de planejamento. Tais requisitos são essenciais para a mitigação de riscos operacionais e para o suporte à continuidade dos sistemas críticos do Tribunal.

3.7.5. A exigência de qualificações técnicas rigorosas atua como um filtro de exequibilidade na fase aberta, obrigando as licitantes a precificarem suas propostas com base no real valor de mercado dos especialistas em segurança da informação e proteção de dados, o que previne lances inexequíveis que possam comprometer a execução contratual.

3.7.6. Quando do início da execução do Contrato, a CONTRATADA deverá comprovar, dentre os integrantes de suas equipes, o atendimento aos requisitos de formação acadêmica, experiência profissional, certificações e conhecimentos, conforme descrito nos itens a seguir. Maiores detalhes sobre prazos e etapas serão discriminados no Termo de Referência.

a) Requisitos de formação acadêmica

ITEM	PERFIL PROFISSIONAL	FORMAÇÃO ACADÊMICA	COMPROVAÇÃO
Serviços técnicos especializados de operação de infraestrutura de TIC	Gerente de suporte técnico de tecnologia da informação	Ensino superior completo na área de TIC ou equivalente, acrescido de curso de pós-graduação/especialização na área de TIC, com no mínimo 360 h/a.	a) Diploma reconhecido pelo MEC para o ensino superior completo; b) Diploma emitido por instituição reconhecida pelo MEC para cursos de pós-graduação/especialização.
	Administradores de Segurança da Informação - Sêniores		
	Administradores de Segurança da Informação - Pleno	Ensino superior completo na área de TIC ou equivalente	
	Administradores de Segurança da Informação - Junior		

Tabela 13 - Requisitos de formação acadêmica

b) Experiência Profissional

ITEM	PERFIL PROFISSIONAL	TEMPO DE EXPERIÊNCIA	COMPROVAÇÃO
Serviços técnicos especializados de operação de infraestrutura de TIC	Gerente de suporte técnico de tecnologia da informação	Possuir experiência mínima de 6 (seis) anos de experiência na área de Tecnologia da Informação, com no mínimo 3 (três) anos de experiência em coordenação e/ou supervisão e/ou gerência na área de atendimento ao usuário de TIC (service desk / suporte, etc).	a) Carteira assinada, acompanhada de declaração de atividades do último empregador; b) Contrato de prestação de serviços de pessoa física ou pessoa jurídica da qual seja sócio, acompanhada de declaração de atividades do último contratante.
	Administradores de Segurança da Informação - Sêniores	Experiência mínima de 4 (quatro) anos em funções de segurança da informação, administrando soluções como Gestão de UTM, Gestão de Antivírus e Antispam, Cofre de Senha, Monitoramento e Gestão de Firewall de aplicação (WAF), desenvolvimento de projetos e relatórios de segurança da informação.	
	Administradores de Segurança da Informação - Pleno	Experiência mínima de 3 (anos) anos em funções de segurança da informação.	
	Administradores de Segurança da Informação - Junior	Experiência mínima de 2 (dois) anos na área de Segurança da Informação.	

Tabela 14 - Requisitos de experiência profissional

c) Requisitos específicos

ITEM	PERFIL PROFISSIONAL	QUALIFICAÇÃO TÉCNICA	
		Experiência/Qualificação	Certificações Exigidas
Serviços técnicos especializados de operação de infraestrutura de TIC	Gerente de suporte técnico de tecnologia da informação	Possuir experiência mínima 6 (seis) anos na área TIC e 3 (três) anos em coordenação de equipes de infraestrutura de TI. E possuir experiência em: gerenciamento e coordenação de equipes de infraestrutura de TI; Possuir experiência em projetos de infraestrutura de TI, incluindo especificação, desenho, projeto de arquiteturas de infraestrutura de TI; Administração de equipes de 1º e 2º nível; gerenciamento e administração de ambientes de atendimento.	Possuir as seguintes certificações (ou certificações superiores): ITIL foundation v4 (ou superior) e COBIT 5 foundation (ou superior)
	Administradores de Segurança da Informação - Sêniores	Ampla domínio em Segurança da Informação e Proteção de Dados, integração contínua e segurança aplicada à infraestrutura de TI. Conhecimento em: Sistemas Operacionais Windows e Linux. Ferramentas de versionamento, fusão (merge), revisão e gerenciamento de código-fonte. Plataformas de integração, teste contínuo e pipelines de CI/CD. Gerenciamento de mudanças, aprovações de liberação e automação de deploys. Segurança da informação aplicada a ambientes de automação, com base em normas e frameworks (ISO, NIST, CIS Controls, LGPD). Gestão de vulnerabilidades, identidades e acessos, com uso de ferramentas especializadas (Tenable, CyberArk, Varonis). Tecnologias de virtualização, backup e gestão de endpoints (VMware, Veeam, Trend, Ivanti). Monitoramento de ameaças, resposta a incidentes e threat intelligence (ex.: MITRE ATT&CK, SOC assessments, Google Security Operations). Fundamentos de pentest e ethical hacking para validação de segurança em ambientes automatizados.	Possuir ao menos cinco das seguintes certificações (ou certificações superiores): CompTIA Security+, CompTIA Pentest+, CySA+ (CompTIA), ECSA - Ec-Council Security Analyst (Ec-Council), GAWN - GIAC Assessing Wireless Networks (SANS), GCIA - GIAC Certified Intrusion Analyst (SANS), GPEN - GIAC Penetration Tester (SANS), SSCP - Systems Security Certified Practitioner (ISC²), Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP), Systems Security Certified Practitioner (SSCP), OSCP - Offensive Security Certified Professional, OSCE - Offensive Security Certified Expert, OSEE - Offensive Security Exploitation Expert, DCPT - DESEC Certified Penetration Tester, ECIH - Ec-Council Certified Incident Handler, CND - Certified Network Defender, CEH v10 ou superior - Certified Ethical Hacker, ECSA - Ec-council Certified Ethical Analyst, CPENT - Certified Penetration Testing Professional, LPT - Licensed Penetration Tester, CCNA v4, Varonis Cloud Data Defense Certification - Varonis, Varonis Data Defense Certification, Varonis Certified Administrator - DatAdvantage - Varonis, VCA: DatAdvantage for Microsoft 365, Introduction to Citrix Infrastructure Protection (ICIP) - OPSWAT Academy, Veeam Backup & Replication v12.3: Configure, Manage, and Recover (VMCE), Blue Team: Cybersecurity Network Security Expert - Acadi TI, Veeam Backup & Replication v12.3: Configure, Manage, and Recover (VMCE), F5 Certified Administrator (F5201 - TMOS Administration), Certified Kubernetes Administrator.

Administradores de Segurança da Informação - Pleno	Amplo domínio em Segurança da Informação e Proteção de Dados. Conhecimento em: Administração e configuração de soluções de segurança de borda e endpoint (Firewalls, EDR/XDR, Antispam). Operação de ferramentas de gestão de vulnerabilidades e execução de rotinas de hardening em servidores Windows e Linux. Monitoramento de eventos de segurança em plataformas SIEM e suporte na resposta a incidentes cibernéticos. Gestão de identidades e acessos em ambientes híbridos (Active Directory e Azure AD/Google Workspace). Conhecimento prático em normas de segurança e privacidade, com foco na ISO/IEC 27001, ISO/IEC 27002 e nos requisitos da LGPD aplicados ao setor público. Operação de soluções de backup e replicação de dados para garantia da continuidade de negócios. Noções de arquitetura Zero Trust e segurança de aplicações web (WAF).	Possuir ao menos três das seguintes certificações (ou certificações superiores): COBIT 5 Foundation, ITIL ® 4 Foundation, ISFS - Information Security Foundation based on ISO/IEC 27002 (EXIN), ISMAS - Information Security Management Advanced based on ISO/IEC 27002 (EXIN), ISMES - Information Security Management Expert based on ISO/IEC 27002 (EXIN), Security+ (CompTIA), Certified Information Systems Security Professional (CISSP), Systems Security Certified Practitioner (SSCP), Introduction to Critical Infrastructure Protection (ICIP), EXIN Information Security Management, LPT – Licensed Penetration Tester, CCNA v4, Varonis Cloud Data Defense Certification - Varonis, Varonis Data Defense Certification, Varonis Certified Administrator - DatAdvantage - Varonis, VCA: DatAdvantage for Microsoft 365;
Administradores de Segurança da Informação - Junior	Conhecimentos fundamentais em segurança da informação e administração de infraestrutura de TI. Inclui: Redes de computadores, protocolos e serviços. Sistemas operacionais Windows e Linux aplicados à segurança. Soluções de Endpoint Security para proteção de estações de trabalho e servidores. Práticas de hardening, gestão de vulnerabilidades e aplicação de patches. Administração e monitoramento de infraestrutura e serviços. Fundamentos de governança e boas práticas de TI (ISO 27001/27002, LGPD, ITIL, COBIT, CIS Controls). Gestão de Identidade e Administração de usuários no AD e Nuvem	Possuir ao menos uma das seguintes certificações (ou certificações superiores): ITIL 4 Foundation, Framework CIS Controls v8 Linux LPIC-1 ou superior;

Tabela 15 - Requisitos específicos de certificações

Nota: Conforme o Anexo I, item 9.4.4, alínea "d", da Portaria SGD/MGI nº 1.070/2023, a norma não estabelece detalhamento ou exigência absoluta e inflexível de certificações para todos os perfis, mas determina que elas devem ser exigidas "sempre que couber". De acordo com as diretrizes do modelo, e em observância ao art. 16, inciso II, alíneas "f" e "g", da Instrução Normativa SGD/ME nº 94/2022, cabe à equipe de planejamento de cada órgão definir, para cada categoria de serviço, os requisitos exatos de experiência profissional, formação acadêmica e certificações necessários para assegurar a qualidade dos serviços. A própria Portaria 1.070/2023 (Anexo I, item 10.6.2) reconhece que ambientes tecnológicos que exijam determinadas certificações ou habilidades técnicas específicas para a sua operacionalização geralmente demandam profissionais com níveis de senioridade mais altos, como Pleno ou Sênior. Neste sentido, as exigências escolhidas nesta seção, com relação à formação acadêmica e certificações profissionais de mercado, tomaram por base a complexidade do ambiente tecnológico descrito no ETP e o nível de conhecimento e excelência adequado para o atingimento dos Níveis Mínimos de Serviço previstos na contratação. Ressalta-se que a comprovação das certificações será exigida apenas quando do início da execução contratual, sendo expressamente vedada a sua exigência prévia na fase de licitação, conforme determina o art. 5º, inciso VII, da referida IN SGD/ME nº 94/2022.

3.8. Locais e Endereços da prestação dos serviços

3.8.1. Para todos os serviços definidos neste ETP, considera-se necessária, para a consecução do objeto, a disponibilidade operacional dos perfis mínimos exigidos, inclusive com atuação remota ou presencial quando tecnicamente justificada pelo CONTRATANTE na Ordem de Serviço. Maiores informações sobre a modalidade de prestação dos serviços serão detalhadas no Termo de Referência.

3.8.2. O atendimento aos chamados ocorre de forma predominantemente **presencial na Sede** do TRE-PA e na **modalidade remota** às Zonas Eleitorais. Entretanto, conforme necessidade da administração, poderá ser necessário deslocamento dos colaboradores para outras unidades do TRE-PA, como Cartórios Eleitorais e Postos de Atendimento Eleitoral (todos os endereços estão publicados no Portal [Infozonas TRE-PA](#)), objetivando o atendimento de atividades relacionados ao suporte computacional das unidades do Tribunal; nos casos de Eleições Gerais, Municipais e/ou suplementares.

3.3.3.1. Todas as informações sobre as Zonas Eleitorais do TRE-PA como o endereço, região de abrangência e composição podem ser obtidas no Sítio Internet do TRE-PA:
https://apps2.tre-pa.jus.br/apex/r/apex_app/infozonas/zonas/

3.8.3. Ademais, existe a possibilidade de deslocamento dos perfis profissionais da contratada para outras unidades da federação (Outros Tribunais Regionais Eleitorais e TSE), para participação em projetos nacionais, reuniões técnicas, Teste Público de Segurança (TSE) ou testes em campo que demandem os serviços da Contratada, especialmente no período eleitoral.

3.8.4. O tópico a seguir exibe a série histórica de deslocamentos do(s) Contrato(s) atual(is) para efeito de estimativas da proposta comercial da Licitante.

3.9.5. Histórico de diárias, passagens e Acionamentos Excepcionais Fora do Horário Regular (Horas Extraordinárias)

3.9.5.1. As tabelas a seguir exibem o histórico detalhado de deslocamentos realizados no contrato anterior, refletindo a capilaridade e eventualidade de atendimentos nas localidades descritas nos itens 3.9.2/3.9.3, sendo essenciais para o correto provisionamento de custos operacionais da contratada. Os dados exibem a quantidade de diárias no período, valor passagens aéreas, os destinos cobertos e respectivos valores de diárias. Tais dados permitem o dimensionamento estimado de diárias e passagens necessárias ao suporte técnico de segurança da informação e proteção de ativos previstos na contratação. A análise deste retrospecto é obrigatória para a formulação da proposta comercial, garantindo a cobertura de manutenções preventivas e corretivas presenciais, quando necessário. Assim, assegura-se a conformidade com as exigências de disponibilidade e integridade dos dados conforme previsto neste ETP.

3.9.5.2. DA LOGÍSTICA DE DESLOCAMENTO E SÉRIE HISTÓRICA

3.9.5.2.1. Para viabilizar a execução continuada das atividades de **segurança da informação e proteção de dados** em toda a jurisdição da **Justiça Eleitoral do Pará**, a CONTRATADA deverá assegurar o suporte técnico presencial nas Zonas Eleitorais e demais unidades do Tribunal sempre que a natureza do incidente ou a indisponibilidade de acesso remoto seguro assim o exigir.

3.9.5.2.2. Conforme vedação normativa estabelecida no inciso V do art. 5º da Instrução Normativa SGD/ME nº 94/2022, a Administração **não realizará reembolso ou pagamento avulso** por despesas operacionais com deslocamento, passagens, hospedagens ou transporte da equipe. O modelo de execução adotado pressupõe o pagamento fixo mensal atrelado exclusivamente ao cumprimento de resultados e aos Níveis Mínimos de Serviços (NMS).

3.9.5.2.3. Com o objetivo de conferir transparência e permitir a justa elaboração da proposta comercial pelas licitantes, apresenta-se abaixo a **série histórica de deslocamentos** realizados no último biênio 2024/2025:

Valor em diárias faturados pela Contratada	Diárias	Passagens (aéreas)	Destino
R\$ 2.964,49	3,5	R\$ 1.690,79	Brasília/DF
R\$ 2.180,81	7,5	--	Monte Alegre/PA
R\$ 726,92	2,5	--	São Paulo/SP
R\$ 2.782,28	6,5	R\$ 774,91	Santarém/PA
R\$ 21.928,18	38,5	R\$ 9.321,00	Prainha/PA, Brasília/DF, Santarém/PA e Conceição do Araguaia/PA
DIÁRIAS E PASSAGENS - 2025			
Valor em diárias faturados pela Contratada	Diárias	Passagens (aéreas)	Destino
R\$ 1.308,48	4,5	--	Breu Branco/PA e Conceição do Araguaia/PA
R\$ 3.713,09	4,5	R\$ 2.088,40	Recife/PE

	Diárias	Valor em diárias faturados pela Contratada	Passagens (aéreas)
2024	58,5	R\$ 30.582,68	R\$ 11.786,70
2025	9	R\$ 5.021,57	R\$ 2.088,40
TOTAL	67,5	R\$ 35.604,25	R\$ 13.875,10

Tabela 16 - Histórico de diárias e passagens aéreas

3.9.5.2.4. Ressalta-se que os dados da série histórica acima possuem caráter **meramente informativo e subsidiário**. Tais registros servem exclusivamente como parâmetro para que a licitante projete sua logística, estime a frequência de viagens e precifique o risco operacional, que é integralmente da CONTRATADA.

3.9.5.2.5. A partir dessa análise, cabe à empresa embutir no **valor fixo mensal** todos os custos decorrentes de deslocamentos eventuais necessários para garantir a resiliência e a pronta resposta a incidentes de segurança cibernética em qualquer ponto do estado do Pará, não cabendo pleitos de reequilíbrio econômico-financeiro sob a alegação de desconhecimento da necessidade logística.

3.9.5.3. Em complemento, a tabela de Horas Extraordinárias, a seguir, apresenta o histórico de acionamentos excepcionais realizados fora do horário regular de expediente nos anos de 2024 e 2025, decorrentes de atividades críticas de manutenção, janelas de atualização ou resposta a incidentes de segurança da informação. Esta volumetria retroativa é indispensável para que as licitantes estimem o impacto financeiro relativo aos adicionais extraordinários e encargos sociais em sua proposta comercial, garantindo o suporte ininterrupto à infraestrutura de proteção de dados da Justiça Eleitoral do Pará em regimes de sobreaviso ou intervenções emergenciais. Conforme verificado, em razão da extensão dos horários de funcionamento do Tribunal, existe um aumento significativo de acionamentos excepcionais, fora do horário regular, em função do acompanhamento do processo eleitoral, especialmente devido aos plantões no período de setembro a novembro do ano eleitoral.

HISTÓRICO DE HORAS EXTRAORDINÁRIAS		
ANO	2024 (Ano eleitoral)	2025 (Ano não eleitoral)
QTDE	1.274	237,6
VALOR TOTAL	R\$ 179.125,07	R\$ 34.548,06

Tabela 17 - Histórico de Horas Extraordinárias executadas (Referência: valor total em diárias executados - CTO 28/2020)

3.9.5.4. A atuação nesses dias e horários excepcionais está estabelecida em duas modalidades de prestação de serviços:

- **EVENTUAL** (atendimento presencial em regime de plantão): serviços executados em eventos excepcionais ou em períodos específicos, previamente combinados e informados, em horários excepcionais, fora do horário normal de expediente (finais de semana e feriados), de acordo com as necessidades eventuais e janelas de manutenção autorizada, não havendo ônus adicional ao CONTRATANTE relativo a essa disponibilização.
- **PROGRAMADA**: quando necessário, atualizações e manutenções em serviços e ativos de TIC deverão ser realizadas em horários excepcionais como madrugadas, finais de semana e feriados, mediante prévio agendamento ou programação por parte dos responsáveis, a fim de não comprometer os serviços contratados. O atendimento presencial poderá ser solicitado em horários fora do expediente normal (inclusive sábados, domingos e feriados), desde que com aviso prévio por parte do CONTRATANTE, não havendo ônus adicional ao CONTRATANTE relativo a essa disponibilização.

3.9.5.5. Conforme igualmente pontuado para a necessidade de deslocamentos, cumpre salientar, que no modelo da Portaria 1.070/2023, a Administração não realiza o pagamento avulso ou reembolso individualizado de horas extras. A contratação é baseada em um pagamento fixo mensal atrelado exclusivamente ao cumprimento de resultados e Níveis Mínimos de Serviços (NMS). Cabe à licitante prever e embutir os custos com jornadas extraordinárias diretamente no Módulo (Composição da Remuneração) de sua proposta. A contratada assume todo o risco operacional, arcando com o ônus financeiro associado à execução de horas extras, eventuais e programadas. Dessa forma, a administração pública garante previsibilidade orçamentária, enquanto a empresa possui total autonomia e responsabilidade pela escala de sua equipe. Logo, a média histórica de execução de Horas Extraordinárias foi reproduzida neste ETP para conhecimento da licitante quanto a estimativa de proposta comercial.

4. ANÁLISE COMPARATIVA DE SOLUÇÕES E LEVANTAMENTO DE MERCADO

Fundamentação: análise comparativa de soluções, que deve considerar, além do aspecto econômico, os aspectos qualitativos em termos de benefícios para o alcance dos objetivos da contratação, observando o que dispõe as alíneas do inciso II do art. 11, da IN 94/2022 (inciso V do § 1º do art. 18 da Lei 14.133/2021 e Art. 11, inciso II da IN 94/2022).

4.1. Avaliação das Diferentes Soluções Disponíveis no Mercado e que Atendam aos Requisitos do Projeto (Levantamento das alternativas)

Preliminarmente, informo que foram levadas em consideração as orientações contidas nos Modelos, Diretrizes e Orientações para Contratação de Soluções de TIC, disponíveis nos seguintes links:

- [Modelos, Diretrizes e Orientações para Contratação de Soluções de TIC](#).
- [Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação - MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO](#).
- [Catálogos de Soluções de TIC com Condições Padronizadas publicados pelo Órgão Central do SISP](#), onde verificou-se que a solução escolhida não possui item presente, dentre os itens encontrados no referido catálogo (§ 2º do art. 43 da Lei nº 14.133/2021).
- [Modelos da Lei 14.133/21 para bens e serviços de TIC da Advocacia-Geral da União](#).

Deste modo, para elaboração do ETP foram consideradas as orientações para Contratação de bens e serviços de Tecnologia da Informação e Comunicação (TIC), disponíveis no Portal Governo Digital, do **Ministério da Gestão e da Inovação em Serviços Públicos** (disponível em <https://www.gov.br/governodigital/pt-br/contratacoes>). No referido site é possível encontrar as recomendações e diretrizes para o processo de contratação de soluções de TIC. Neste portal, também estão disponíveis Guias, Modelos e Diretrizes para Contratações de Solução de TIC de caráter geral e por temas, onde é possível verificar as boas práticas do governo federal na administração e contratação de recursos de TIC. Deste modo, **ratificamos que na elaboração do Estudo Preliminar, Termo de Referência e demais documentos de planejamento da contratação para a solução pretendida, foram observados os guias, manuais e modelos publicados pelo Órgão Central do SISP.** (IN SGD nº 94/2022, art. 8º, §2).

Também foi consultada a base do Portal de Compras (disponível no endereço <https://www.comprasgovernamentais.gov.br/>) e do PNCP (<https://www.gov.br/pncp/pt-br>), que reúnem diversos outros pontos de pesquisa, como o sistema Comprasnet, o Pannel de Compras (<https://paineldecompras.economia.gov.br/>), o Pannel de Preços (<https://paineldeprecos.planejamento.gov.br/>), consulta a Contratações publicadas e Atas de

Registro de Preços, os quais apresentam dados estruturados de contratações realizadas pelos órgãos da Administração Pública Federal. Essas contratações representam o resultado de uma avaliação das contratações de Soluções de TI pelos Órgãos e Entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) do Governo Federal e encontram-se catalogadas e categorizadas por subconjunto de bens e serviços.

Ainda, no âmbito da Administração Pública Federal, foi consultado o Portal da Transparência mantido pela Controladoria-Geral da União (<http://www.portaltransparencia.gov.br/contratos/>), através da pesquisa disponível nas opções “Consulta Detalhada” e após em “Contrato” e também por meio do campo “Busca específica”.

Com relação às diretrizes e recomendações do Conselho Nacional de Justiça (CNJ), convém registrar que o Guia de Contratações de STIC do Poder Judiciário, anexo da Resolução CNJ nº 468/22, serviu de fonte de consulta para este ETP. De igual modo, a Plataforma de Governança Digital Colaborativa do Poder Judiciário (Connect-Jus) foi consultada para verificação da existência e adoção de soluções similares por órgãos do Poder Judiciário.

Outra forma de pesquisa se deu por meio da verificação dos contratos dos órgãos pertencentes ao Poder Executivo Federal, por meio de sites de busca, avaliando também como estão se posicionando acerca desse tipo de demanda por solução de TI. Neste caso foram pesquisadas as seguintes palavras chaves: renovação garantia, licenciamento Firewall. Nesse contexto, a partir da definição dos requisitos e dos métodos de pesquisa supracitados, a Equipe de Planejamento da Contratação identificou as alternativas de mercado destacadas neste Estudo Técnico Preliminar.

Destaca-se que, na consulta ao PNCP na data de 25/02/2025, não foi encontrada IRP de objeto semelhante para participação, provavelmente em razão das especificidades do objeto.

4.2. Disponibilidade de solução similar (alínea a)

Soluções contratadas por órgãos da Administração Pública: foram encontradas as seguintes contratações recentes, similares aos Serviços Gerenciados de Segurança da Informação a serem aqui contratados, com seus respectivos objetos e condições gerais de contratação:

ÓRGÃO	PREGÃO/CONTRATO OU INEXIGIBILIDADE	OBJETO
Conselho Nacional de Justiça – CNJ	Pregão Eletrônico nº 3/2021	Contratação de Serviços Gerenciados de Segurança da Informação, incluindo Serviços de Administração, Operação e Atendimento a Requisições, Gestão de Vulnerabilidades de Ataques Cibernéticos e Testes de Invasão
Tribunal de Justiça do Estado de São Paulo - TJSP	Pregão Eletrônico nº 0290/2018	Contratação de serviço contínuo especializado de SOC (<i>security Operation Center</i> ou Centro de Operações de Segurança), no intuito de garantir a segurança das informações digitais inseridas nos sistemas da CONTRATANTE, além de propiciar ambiente técnico adequado para a continuidade da atividade fim do Tribunal de Justiça de São Paulo.
Ministério Público do Distrito Federal e Territórios – MPDFT	Pregão Eletrônico nº 73/2021	Contratação de empresa especializada para o fornecimento de solução de gestão e correlação de eventos de segurança da informação (SIEM) e gestão da resposta a incidentes de segurança da informação (SOAR) e demais serviços associados.
Supremo Tribunal de Justiça – STJ	Pregão Eletrônico nº 43/2021	Contratação de empresa especializada em segurança cibernética para prestação de Serviços Gerenciados de Segurança da Informação, em regime de dedicação exclusiva de mão de obra, envolvendo consolidação e visibilidade de eventos de segurança, administração, operação, análise, monitoramento e respostas a incidentes de segurança da informação.
Tribunal de Justiça do Rio de Janeiro – TJRJ	Pregão Eletrônico nº 50/2022	Contratação de Serviços Gerenciados de Segurança da Informação (GSTI) para implantação e execução de serviços de segurança da informação, cibernética, privacidade e proteção de dados, incluindo instalação, licenças, administração, supervisão e operação das ferramentas de segurança de informação e de outras ferramentas relacionadas à segurança da informação.
Tribunal de Justiça de Minas Gerais – TJMG	Pregão Eletrônico nº 208/2023	Serviços gerenciados de segurança cibernética (<i>managed security services</i> – MSS), de natureza continuada, remotos e presenciais, em níveis estratégico, tático e operacional, com fornecimento de equipe técnica especializada, ferramentas, processos e transferência de conhecimento.
Tribunal de Justiça do Estado da Bahia	Pregão Eletrônico nº 048/2024	Contratação de Serviços Gerenciados de Segurança da Informação com Central de Operações de Segurança (Security Operations Center – SOC) no modelo Software as a Service (SaaS), incluindo Gestão de Vulnerabilidades, Gestão de Incidentes, Monitoramento e Visibilidade de ataques Cibernéticos, Testes de Invasão, Simulação de ataques relacionados à Segurança Digital, para o Tribunal de Justiça do Estado da Bahia - TJBA, conforme exigências estabelecidas neste documento e seus anexos.
TRIBUNAL REGIONAL ELEITORAL DE PERNAMBUCO	Pregão Eletrônico nº 036/2024	Contratação de serviço de suporte à infraestrutura de TIC do TRE de Pernambuco em apoio às equipes de gestão da Coordenadoria de Segurança da Informação e Infraestrutura.
FUNDAÇÃO OSWALDO CRUZ	Contrato nº 44/2025	Contratação emergencial de serviços técnicos especializados em operação de infraestrutura, segurança da informação e atendimento à usuários de Tecnologia da Informação e Comunicação.
ADVOCACIA-GERAL DA UNIÃO	CONTRATO ADMINISTRATIVO Nº 021/2024	Contratação de solução de tecnologia da informação e comunicação de prestação de serviços de atendimento ao usuário de TIC e de operação de infraestrutura de TIC, para atendimento da Advocacia Geral da União (AGU).

Tabela 18 - Disponibilidade da solução em outros órgãos da administração pública

4.3. Alternativas do mercado (alínea b)

4.11.1. A **Súmula nº 269 do Tribunal de Contas da União (TCU)** estabelece que, nas contratações para a prestação de serviços de tecnologia da informação, a remuneração deve estar vinculada a resultados ou ao atendimento de níveis de serviço. Admite-se o pagamento por hora trabalhada ou por posto de serviço somente quando as características do objeto não permitirem outra forma, hipótese em que a excepcionalidade deve estar prévia e adequadamente justificada nos respectivos processos administrativos.

4.11.2. Além disso, o **Acórdão nº 1508/2020 - TCU - Plenário** determinou que a Unidade de Serviços Técnicos (UST) não deve ser utilizada em contratações públicas **sem padronização**. O Tribunal constatou deficiências na estimativa de preços da UST, dimensionamento baseado em parâmetros injustificados e ausência de memória de cálculo para os pesos utilizados nos contratos avaliados. Portanto, a UST não pode ser adotada como métrica ou unidade de medida **sem a devida padronização e justificativas técnico-econômicas**.

4.11.3. Dessa forma, após levantamento de mercado e em consonância com a Súmula nº 269 e o Acórdão nº 1508/2020 do TCU, as boas práticas indicam que as contratações de serviços de tecnologia da informação devem priorizar modelos de remuneração baseados em resultados ou no cumprimento de níveis de serviço

previamente estabelecidos. Com base nestes pressupostos, compreendemos que a utilização de métricas como a UST deve ser evitada na proposta da nova contratação, a menos que haja padronização e justificativas técnicas adequadas que assegurem a eficiência e a economicidade da contratação.

4.4. Existência de software público (<http://www.softwarepublico.gov.br>) ou software de governo (alínea c)

() SIM () NÃO (X) NÃO SE APLICA

4.5. Políticas, modelos e padrões de governo (alínea d)

Não se aplica, pois o objeto não consiste na aquisição e desenvolvimento de Software.

4.6. Necessidades de adequação do ambiente (alínea e)

As necessidades de adequação do ambiente estão descritas no item 7.1 deste ETP.

4.7. Diferentes modelos de prestação do serviço (alínea f)

De forma geral, os diferentes modelos de prestação do serviço foram demonstrados no item "4.12. Identificação e descrição das soluções".

4.8. Diferentes tipos de solução (alínea g)

De forma geral, os diferentes modelos de prestação do serviço foram demonstrados no item "4.12. Identificação e descrição das soluções".

4.9. Contratação como aquisição de bens x como serviço (alínea h)

() SIM () NÃO (X) NÃO SE APLICA (trata-se de contratação de serviços de TIC, não se aplica a contratação de bens para a demanda apresentada)

4.10. Ampliação x Substituição da solução implantada (alínea i)

() SIM () NÃO (X) NÃO SE APLICA (conforme demonstrado neste ETP, a proposta de nova contratação não prevê a ampliação, mas a substituição da solução atualmente implantada)

4.11. Diferentes métricas de prestação do serviço e de pagamento (alínea j)

4.11.1. A execução das atividades especializadas de segurança cibernética ocorrerá sob o regime de pagamento mensal (parcela fixa) e por resultados (sob demanda), estando estritamente vinculada ao cumprimento das metas estabelecidas nos Níveis Mínimos de Serviço (NMS). Este modelo de aferição observa as diretrizes da Portaria SGD/MGI nº 1.070/2023, garantindo a entrega de valor e a eficiência operacional no âmbito da Justiça Eleitoral do Pará.

4.11.2. Os prazos e métricas definidos serão contabilizados a partir do registro formal da demanda ou incidente pela Contratante, mediante abertura de chamado na Central de Serviços de TI. A contagem do tempo de solução está condicionada à disponibilização integral das informações necessárias para o diagnóstico, análise e tratamento da ocorrência por parte da equipe técnica da Contratada.

4.11.3. Os NMS constituem regras objetivas de controle que estipulam os patamares mínimos de qualidade e desempenho. A aplicação destes indicadores visa:

- Assegurar que os serviços de segurança da informação alcancem os níveis de eficácia e satisfação pretendidos;
- Fomentar a melhoria contínua dos processos de proteção de dados e defesa cibernética;
- Prover mecanismos robustos para o monitoramento e fiscalização técnica da execução contratual;
- Permitir o redimensionamento dos pagamentos (glosas) em função dos resultados efetivamente obtidos e da conformidade com os SLAs.

4.11.4. Na seleção dos indicadores que compõem este Termo de Referência, foram priorizadas métricas de criticidade técnica para a infraestrutura de Data Center. Em consonância com a estratégia de contratação, optou-se pela exclusão dos indicadores de atendimento genérico ao usuário final (Help Desk básico), focando a atuação da Contratada em atividades de nível N2 e N3 especializadas em segurança da informação.

Ao se selecionar dos indicadores de Portaria SGD/MGI nº 1.070/2023 para os NMS, foram incluídos os seguintes indicadores de atendimento ao usuário:

(I) QUANTIDADE DE CHAMADOS (REQUISIÇÃO E INCIDENTES) ATENDIDOS DENTRO DO PRAZO	
Tópico	Descrição
Finalidade	Apurar a quantidade de chamados (requisições e incidentes) atendidos dentro do prazo estabelecido no Catálogo de Serviços, assegurando a agilidade e a eficácia do atendimento.
Meta a cumprir	IACP ≥ 95%
Instrumento de medição	Sistema de Gerenciamento de Serviços de TI (ITSM) utilizado pelo Tribunal Regional Eleitoral do Pará, por meio da extração de relatórios analíticos.
Forma de acompanhamento	A aferição será realizada mensalmente, de forma automatizada, por meio de relatórios extraídos da ferramenta de ITSM que registrem o ciclo de vida de cada chamado, desde sua abertura até o seu encerramento.
Periodicidade	Mensal.
Mecanismo de Cálculo (métrica)	$IACP = \frac{TCA}{TCS} \times 100$ Onde: ACP – Índice de Atendimento de Chamados no Prazo; TCS – Total de Chamados Solucionados dentro do prazo no período de aferição; TCA – Total de Chamados com prazo de solução expirado no período de aferição (inclui os chamados abertos em períodos anteriores e cujo prazo de solução se encerrou no período de aferição).
Observações	Obs1: O prazo de atendimento e solução de cada tipo de chamado está definido no Catálogo de Serviços Apêndice II do Termo de Referência. Obs2: A contagem do tempo de atendimento será pausada quando a solução do chamado depender de uma ação do usuário ou de outra área do TRE-PA, e será retomada quando a pendência for solucionada, conforme registrado na ferramenta de ITSM.
Início de Vigência	A partir do primeiro dia do mês subsequente ao início da prestação dos serviços.
Faixas de ajuste no pagamento e Sanções	Para valores do indicador IACP apurados mensalmente: - IACP ≥ 95%: Pagamento integral (100%) do valor mensal referente aos serviços. - 90% ≤ IACP < 95%: Aplicar-se-á glosa de 1% sobre o valor da fatura mensal. - 85% ≤ IACP < 90%: Aplicar-se-á glosa de 2% sobre o valor da fatura mensal. - IACP < 85%: Aplicar-se-á glosa de 3% sobre o valor da fatura mensal, além da abertura de processo administrativo para apuração de responsabilidade e possível aplicação de outras sanções contratuais, dada a criticidade para a operação da Justiça Eleitoral do Pará.

Tabela 19 - QUANTIDADE DE CHAMADOS (REQUISIÇÃO E INCIDENTES) ATENDIDOS DENTRO DO PRAZO

(2) AFERIR O GRAU DE SATISFAÇÃO DOS USUÁRIOS SOBRE O SERVIÇO PRESTADO	
Tópico	Descrição
Finalidade	Aferir a percepção técnica e estratégica dos Gestores de Sistemas e membros da Alta Administração da Justiça Eleitoral do Pará sobre a eficácia dos controles de segurança e o suporte especializado prestado.
Meta a cumprir	Média de satisfação $\geq 4,0$ (em uma escala de 1 a 5), o que equivale a 80% de satisfação.
Instrumento de medição	A medição será realizada por meio de formulário específico enviado mensalmente aos Gestores de TI e donos de processos de negócio (Alta Administração). A pesquisa focará na confiança sobre o ambiente de segurança e na qualidade das entregas técnicas.
Forma de acompanhamento	A aferição será realizada mensalmente, consolidando os dados extraídos da ferramenta de ITSM. A equipe de fiscalização contratual realizará auditorias por amostragem nas respostas para verificar a consistência e a fidedignidade das avaliações, garantindo a eficácia do indicador.
Periodicidade	Mensal.
Mecanismo de Cálculo (métrica)	O indicador será calculado pela média aritmética simples das notas atribuídas pelos usuários nas pesquisas de satisfação respondidas dentro do período de aferição. $ISU = \frac{\text{Total de Pesquisas Respondidas} \sum (\text{Notas da Pesquisa})}{\text{Total de Pesquisas Respondidas}}$ Onde: ISU – Indicador de Satisfação do Usuário; $\sum$ (Notas da Pesquisa) – Somatório de todas as notas atribuídas pelos usuários (de 1 a 5) no período; Total de Pesquisas Respondidas – Quantidade total de pesquisas que foram respondidas no período.
Observações	Obs1: A pesquisa de satisfação utilizará uma escala de 1 a 5, onde 1 representa "Totalmente Insatisfeito" e 5 representa "Totalmente Satisfeito". Obs2: Para que o indicador seja considerado válido no mês, é necessário que haja uma taxa de resposta de, no mínimo, 60% do total de pesquisas enviadas. Caso a taxa de resposta seja inferior, a CONTRATADA será notificada para que promova ações de incentivo à participação dos usuários, sem prejuízo da aplicação das faixas de ajuste.
Início de Vigência	A partir do primeiro dia do mês subsequente ao início da prestação dos serviços.
Faixas de ajuste no pagamento e Sanções	Para valores do indicador ISU apurados mensalmente: - $ISU \geq 4,0$: Pagamento integral (100%) do valor mensal referente aos serviços. - $3,5 \leq ISU < 4,0$: Aplicar-se-á glosa de 0,5% sobre o valor da fatura mensal. - $3,0 \leq ISU < 3,5$: Aplicar-se-á glosa de 1% sobre o valor da fatura mensal. - $ISU < 3,0$: Aplicar-se-á glosa de 1,5% sobre o valor da fatura mensal. A reincidência por 3 (três) meses consecutivos ou 5 (cinco) alternados dentro de um período de 12 meses ensejará a abertura de processo administrativo para aplicação de sanções mais severas, conforme previsto no Termo de Referência e no Contrato item 13.2.

Tabela 20 - AFERIR O GRAU DE SATISFAÇÃO DOS USUÁRIOS SOBRE O SERVIÇO PRESTADO

(3) EFICÁCIA NO TRATAMENTO DE CHAMADOS (REQUISIÇÕES, INCIDENTES E INCIDENTES DE SEGURANÇA)	
Tópico	Descrição
Finalidade	Apurar a eficácia da CONTRATADA na resolução de chamados, garantindo que as soluções aplicadas para as demandas de segurança da informação e proteção de dados sejam definitivas e evitem a reincidência de problemas, garantindo que as ameaças sejam detectadas e respondidas dentro dos tempos ótimos de MTTD (Tempo Médio de Detecção) e MTTR (Tempo Médio de Resposta).
Meta a cumprir	$\geq 98\%$
Instrumento de medição	A medição será realizada por meio da ferramenta de Gerenciamento de Serviços de TI (ITSM) utilizada pela Justiça Eleitoral do Pará, que registra e monitora todo o ciclo de vida dos chamados.
Forma de acompanhamento	A aferição será realizada mensalmente pela equipe de fiscalização do contrato, através da extração e análise de relatórios gerados pela ferramenta de ITSM. Serão realizadas auditorias periódicas por amostragem para verificar a correta classificação e o tratamento dado aos chamados reabertos.
Periodicidade	Mensal.
Mecanismo de Cálculo (métrica)	O indicador será calculado pela seguinte fórmula: $ETC(\%) = ((\text{Total de chamados atendidos} - \text{Total de chamados reabertos}) / \text{Total de chamados atendidos}) \times 100.$ Onde: ETC – Eficácia no Tratamento de Chamados. Total de chamados atendidos – Quantidade total de chamados (requisições, incidentes e incidentes de segurança) fechados com solução dentro do período de aferição. Total de chamados reabertos – Quantidade de chamados que, após terem sido fechados, foram reabertos pelo usuário ou pela equipe de fiscalização por não terem tido a sua causa raiz efetivamente solucionada.

Observações	Obs. 1: Consideram-se atendidos os chamados fechados com solução. Não devem ser considerados os chamados fechados sem solução, como, por exemplo, chamados duplicados, cancelados pelo usuário ou encerrados por falta de resposta do demandante.
	Obs. 2: Um chamado será considerado reaberto se o mesmo problema ou solicitação original voltar a ocorrer e for reportado pelo usuário dentro de 5 (cinco) dias úteis após o seu encerramento.
	Obs. 3: Segregação por Criticidade - Para fins de aferição deste indicador, os incidentes classificados como 'Críticos' (ex: indisponibilidade de sistemas eleitorais, detecção de ransomware, exfiltração de dados) terão peso diferenciado. A meta de 98% de eficácia aplica-se globalmente, contudo, para incidentes 'Críticos', a tolerância para reabertura de chamados ou falha na contenção é zero, sujeitando a CONTRATADA às sanções máximas previstas no IMR, dada a natureza sensível das operações da Justiça Eleitoral.
	Obs. 4: A eficácia será considerada nula (reabertura compulsória) para incidentes de segurança onde a CONTRATADA não comprove o cumprimento dos tempos de resposta (MTTR) definidos no Catálogo de Serviços, independentemente da solução técnica aplicada.
Início de Vigência	A partir do primeiro dia do mês subsequente ao início da prestação dos serviços.
Faixas de ajuste no pagamento e Sanções	Para valores do indicador ETC apurados mensalmente: - ETC $\geq$ 98%: Pagamento integral (100%). - 95% $\leq$ ETC < 98%: Glosa de 2,5% sobre o valor da fatura mensal. - 90% $\leq$ ETC < 95%: Glosa de 3% sobre o valor da fatura mensal. - ETC < 90%: Glosa de 5% sobre o valor da fatura mensal. A reincidência por 3 (três) meses consecutivos ou 5 (cinco) alternados ensejará a abertura de processo administrativo para aplicação de sanções contratuais mais severas.

Tabela 21 - EFICÁCIA NO TRATAMENTO DE CHAMADOS (REQUISIÇÕES, INCIDENTES E INCIDENTES DE SEGURANÇA)

(4) EFICÁCIA EM MANUTENÇÃO PERIÓDICA DA INFRAESTRUTURA	
Tópico	Descrição
Finalidade	Apurar a aderência da CONTRATADA ao cronograma e escopo das manutenções preventivas e periódicas programadas para a infraestrutura de TI, visando a proatividade na segurança da informação e na sustentação do ambiente que suporta a proteção de dados da Justiça Eleitoral do Pará, mitigando riscos de falhas e incidentes.
Meta a cumprir	$\geq$ 95%
Instrumento de medição	A medição será realizada por meio de relatórios de planejamento e execução de manutenções, evidências de conclusão (logs, registros de sistemas, formulários de manutenção) e acompanhamento do cronograma de atividades, a serem fornecidos pela CONTRATADA.
Forma de acompanhamento	A aferição será realizada mensalmente pela equipe de fiscalização do contrato, através da análise dos relatórios e evidências entregues pela CONTRATADA, comparando o planejado com o executado. Serão realizadas auditorias por amostragem para verificar a correta execução e os resultados das manutenções.
Periodicidade	Mensal. O indicador será calculado pela seguinte fórmula:
Mecanismo de Cálculo (métrica)	$PCMP (\%) = (\text{Número de Manutenções Preventivas Realizadas Conforme Cronograma e Escopo} / \text{Número Total de Manutenções Preventivas Programadas}) \times 100$
	Onde: PCMP – Percentual de Conformidade da Manutenção Preventiva.
	Número de Manutenções Preventivas Realizadas Conforme Cronograma e Escopo – Quantidade de manutenções preventivas e periódicas que foram executadas integralmente dentro do prazo estabelecido e de acordo com o escopo técnico definido para o período de aferição.
	Número Total de Manutenções Preventivas Programadas – Quantidade total de manutenções preventivas e periódicas planejadas para o período de aferição, conforme cronograma acordado.
Observações	Obs. 1: Considera-se "realizada conforme cronograma e escopo" a manutenção que foi iniciada e concluída dentro das datas previstas e que atendeu a todas as etapas e procedimentos técnicos definidos previamente. Obs. 2: Qualquer alteração no cronograma ou escopo das manutenções deve ser formalmente justificada pela CONTRATADA e aprovada pela CONTRATANTE com antecedência mínima de 5 (cinco) dias úteis. A ausência de aprovação implicará na não conformidade para fins de cálculo do indicador.
Início de Vigência	A partir do primeiro dia do mês subsequente ao término do período de estabilização.
Faixas de ajuste no pagamento e Sanções	Para valores do indicador PCMP apurados mensalmente: - PCMP $\geq$ 95%: Pagamento integral (100%). - 90% $\leq$ PCMP < 95%: Glosa de 2,5% sobre o valor da fatura mensal. - 85% $\leq$ PCMP < 90%: Glosa de 3% sobre o valor da fatura mensal. - PCMP < 85%: Glosa de 5% sobre o valor da fatura mensal. A reincidência por 3 (três) meses consecutivos ou 5 (cinco) alternados ensejará a abertura de processo administrativo para aplicação de sanções contratuais mais severas.

Tabela 22 - EFICÁCIA EM MANUTENÇÃO PERIÓDICA DA INFRAESTRUTURA

(5) VINCULAÇÃO DA RESOLUÇÃO DE REQUISIÇÕES DE SERVIÇO À BASE DE CONHECIMENTO	
Tópico	Descrição
Finalidade	Aferir a cobertura dos padrões de atendimento registrados na base de conhecimento
Descrição	Uma base de conhecimento auxilia o times de atendimento – N1 e N2 – na busca por informações, propõe resoluções para problemas relacionados aos serviços/produtos, acelera as soluções e a entrega de serviços, ajuda a configurar recursos quando necessário e traz outras informações relevantes para a função da Central de Serviços de TI. Portanto, é necessário um indicador que registre se as soluções encontradas para os chamados possuem como fonte a base de conhecimento, o que denota a importância de atualização constante das informações existentes na base de conhecimento.
Meta a cumprir	60% do total de chamados fechados na Central de Serviços de TI (N1) possuem vinculação à base de conhecimento - $\uparrow$ Quanto maior melhor
Instrumento de Medição	Software ITSM
Forma de acompanhamento	Pelo fiscal do contrato, consulta relatório mensal do Software ITSM
Periodicidade	Mensal
Mecanismo de cálculo	$= (\text{Total de requisições com resolução vinculada à base de conhecimento} / \text{Total de requisições resolvidas}) \times 100$

Observações	1. Ao longo da contratação, é natural o aumento do percentual de vinculação dos chamados à base de conhecimento, por isso, a meta tem como caráter o mínimo aceitável para o início do contrato.	
Faixa no ajuste no pagamento	Percentual de chamados fechados sem vinculação à base de conhecimento (%)	Decréscimo na Fatura Mensal (%)
	1% a 15%	não haverá desconto
	16% a 25%	1%
	26% a 35%	2%
	36% a 45%	5%
Sanções	Ver item 13.2. SANÇÕES ADMINISTRATIVAS	

Tabela 23 - VINCULAÇÃO DA RESOLUÇÃO DE REQUISIÇÕES DE SERVIÇO À BASE DE CONHECIMENTO

(6) EFICÁCIA NO TRATAMENTO DE VULNERABILIDADES CRÍTICAS E ALTAS (ITV)	
Tópico	Descrição
Finalidade	Apurar a eficácia da CONTRATADA no cumprimento dos prazos de correção de vulnerabilidades técnicas com níveis de severidade "Crítico" e "Alto", visando mitigar riscos de exploração e garantir a proteção de dados do TRE-PA.
Descrição	
Meta a cumprir	ITV = 100% (Zero vulnerabilidades críticas ou altas fora do prazo de correção estabelecido).
Instrumento de medição	Software de Gestão de Vulnerabilidades e sistema de ITSM utilizados pelo Tribunal Regional Eleitoral do Pará.
Forma de acompanhamento	A aferição será realizada mensalmente pela unidade de Defesa Cibernética e pela fiscalização do contrato, mediante extração de relatórios das ferramentas de varredura que indiquem a idade das vulnerabilidades abertas.
Periodicidade	Mensal.
O indicador expressa o percentual de vulnerabilidades críticas e altas tratadas dentro do prazo:	
$ITV = \left(\frac{VCP}{VTP} \right) \times 100$	
Mecanismo de Cálculo (métrica)	Onde: ITV: Índice de Tratamento de Vulnerabilidades; VCP: Quantidade de vulnerabilidades (CVEs) Críticas e Altas cujo tratamento foi concluído dentro do prazo ou que possuem renúncia aprovada; VTP: Total de vulnerabilidades Críticas e Altas identificadas cujos prazos de correção expiraram no período de aferição.
Observações	Obs1: Os prazos de correção seguem o Anexo I da Portaria 22808/2024: Crítico (até 15 dias) e Alto (até 30 dias). Obs2: Vulnerabilidades com "solicitação de renúncia" formalmente aceita pelo Secretário de TI não serão contabilizadas como atraso para fins deste indicador.
Início de Vigência	A partir do primeiro dia do mês subsequente ao término do período de estabilização.
Faixas de ajuste no pagamento e Sanções	Para valores do indicador ITV apurados mensalmente:
	• ITV = 100%: Pagamento integral (100%).
	• $95\% \leq ITV < 100\%$: Glosa de 2% sobre o valor da fatura mensal.
	• $90\% \leq ITV < 95\%$: Glosa de 4% sobre o valor da fatura mensal.
	• $ITV < 90\%$: Glosa de 5% sobre o valor da fatura mensal e abertura de processo administrativo.

Tabela 24 - EFICÁCIA NO TRATAMENTO DE VULNERABILIDADES CRÍTICAS E ALTAS (ITV)

(7) EFICÁCIA NA PROTEÇÃO CONTRA RANSOMWARE E INTEGRIDADE DE BACKUP	
Tópico	Descrição
Finalidade	Garantir a disponibilidade e integridade dos dados da Justiça Eleitoral por meio da execução rigorosa de backups e testes de restauração, assegurando a proteção contra ataques de ransomware e outras ameaças cibernéticas.
Descrição	O gerenciamento de backup e restauração deve garantir que as cópias de segurança sejam realizadas de forma íntegra, criptografada e em mídias distintas, incluindo cópias offline ou em locais externos. O indicador monitora a taxa de sucesso das rotinas programadas e a eficácia dos testes de restauração mensais, fundamentais para mitigar riscos de sequestro de dados e garantir a disponibilidade da informação.
Meta a cumprir	I-BACKUP $\geq$ 98% e Tolerância Zero para falhas em sistemas críticos.
Instrumento de medição	Relatórios automáticos da solução de backup e restauração, logs de auditoria de sistemas, e Relatórios de Testes de Restauração (RTR) validados mensalmente.
Forma de acompanhamento	Aferição mensal realizada pela fiscalização do contrato mediante análise dos logs de sucesso/falha das rotinas agendadas e conferência das evidências de testes de restauração realizados em ambiente segregado.
Periodicidade	Mensal.

O indicador é a média percentual de sucesso entre backups realizados e testes de restauração:

$$I - BACKUP = \left(\frac{B_{suc} + T_{suc}}{B_{prog} + T_{prog}} \right) \times 100$$

Mecanismo de Cálculo (métrica)

Onde:

B_{suc} : Total de rotinas de backup executadas com sucesso no período;

T_{suc} : Total de testes de restauração realizados com sucesso (conforme plano);

B_{prog} : Total de backups programados no período;

T_{prog} : Total de testes de restauração previstos no Plano de Gerenciamento.

Observações	Obs 1: Conforme Art. 20, ao menos uma cópia deve ser offline (não endereçável pelo SO) para proteção contra ransomware. Obs 2: Falhas de backup em sistemas "Críticos" (ex: Sistemas Eleitorais) devem ser remediadas imediatamente e reportadas em até 2 horas. Obs 3: A contagem de falhas exclui indisponibilidades causadas por queda de energia no Data Center ou falhas de hardware do Tribunal, desde que devidamente comprovadas.
Início de Vigência	A partir do primeiro dia do mês subsequente ao término do período de estabilização.
Faixas de ajuste no pagamento e Sanções	Para valores do indicador I-BACKUP apurados mensalmente: • $I-BACKUP \geq 98\%$: Pagamento integral (100%). • $95\% \leq I-BACKUP < 98\%$: Glosa de 2,5% sobre a fatura mensal. • $90\% \leq I-BACKUP < 95\%$: Glosa de 4% sobre a fatura mensal. • $I-BACKUP < 90\%$ ou falha total em restauração crítica: Glosa de 5% sobre a fatura mensal e abertura de processo administrativo.

Tabela 25 - EFICÁCIA NA PROTEÇÃO CONTRA RANSOMWARE E INTEGRIDADE DE BACKUP

4.12. Identificação e descrição das soluções

4.12.1. A fase de identificação das soluções buscou mapear no mercado de Tecnologia da Informação as alternativas capazes de suprir a necessidade de suporte técnico especializado em segurança da informação e proteção de dados para este Tribunal. O foco da análise recaiu sobre modelos que garantissem não apenas a execução de tarefas operacionais, mas a resiliência cibernética contínua e a conformidade com a LGPD e as resoluções do CNJ.

4.12.2. Para a prospecção das soluções, foram considerados os modelos de prestação de serviços baseados em métricas de esforço (como alocação de Posto de Trabalho e Unidade de Serviço Técnico - UST) e modelos baseados em resultados (Valor Fixo Mensal com NMS). A avaliação pautou-se na busca pela solução que oferecesse o melhor equilíbrio entre eficácia técnica, eficiência administrativa e segurança jurídica, considerando a criticidade do ambiente tecnológico da Justiça Eleitoral do Pará, especialmente em períodos de pleitos eleitorais.

4.12.3. Em observância ao Guia de Contratações de TIC do Poder Judiciário e à Portaria SGD/MGI nº 1.070./2023, a equipe de planejamento priorizou a identificação de soluções que utilizassem perfis profissionais padronizados e metodologias de gerenciamento de serviços reconhecidas internacionalmente (como o framework NIST e CIS Controls). A seguir, detalham-se as alternativas identificadas e a análise comparativa que fundamentou a escolha da solução de referência para esta contratação.

4.12.4. O quadro a seguir apresenta as principais soluções disponíveis no mercado para a contratação em tela.

Id	Descrição da solução (ou cenário)
1	Solução 1 – Postos de trabalho ou Posto de Serviço nas dependências do Órgão Contratante. Análise: Modelo de contratação em que o Contratante responsável pela gerência dos profissionais e suas entregas, definindo os quantitativos de profissionais necessários na execução dos serviços conforme suas especialidades e com dedicação exclusiva ao atendimento das demandas do contratante. Além da Gestão dos postos centralizada pelo contratante, a fiscalização técnica e o pagamento é simplificado. No posto de trabalho de forma pura, não se tem garantia de entrega. O pagamento se dá em razão da disponibilidade do profissional pela Contratada. Existe o risco de pagamento por postos para execução de atividades estranhas ao objeto contratado. Características do modelo: - Menor esforço na fiscalização técnica; - Risco de a lista de atividades não abranger todas as possibilidades possíveis para atendimento adequado às necessidades; - Risco de dimensionamento incorreto por parte da Contratada, em função da lista extensa de atividades previstas para execução; - Presença do paradoxo lucro-incompetência, ou seja, remuneração fixa mesmo que a produtividade possa ser menor do que esperado; Este modelo de contratação é vedado pela Resolução Nº 468 de 15/07/2022, Art. 8º, inciso IX, salvo os casos justificados mediante a comprovação obrigatória de resultados compatíveis com o posto previamente definido. Esta norma dispõe sobre diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação pelos órgãos submetidos ao controle administrativo e financeiro do Conselho Nacional de Justiça, e proíbe a contratação de serviços contínuos com dedicação exclusiva de mão de obra por meio de postos de trabalho, exceto em casos devidamente justificados e aprovados pela autoridade competente. A vedação busca evitar o risco de des controle nos gastos públicos e de práticas ineficazes, promovendo uma gestão mais eficiente dos contratos de terceirização. A Resolução incentiva a contratação com base em resultados e não em alocação de mão de obra, o que fomenta a adoção de melhores práticas de gestão de contratos no setor público. Considerando ainda as disposições da Portaria SGD/MGI no 1.070/2023, a contratação de serviços de operação de infraestrutura e atendimento a usuários de Tecnologia da Informação e Comunicação deverá ser realizada por meio de modelo de pagamento fixo mensal, vinculada exclusivamente ao atendimento de níveis mínimos de serviços previamente estabelecidos. Assim sendo, o modelo não se configura como postos de trabalho. A solução 1 – Dessa forma, uma vez que o modelo de Posto de Trabalho/Serviço é baseado no esforço, a equipe de planejamento da contratação conclui que a presente alternativa é inviável e não está em conformidade com as orientações da Portaria SGD/MGI no 1.070/2023 e nem do TCU, uma vez que se busca uma prestação de serviços baseada em resultados ou ao atendimento de níveis mínimos de serviço.

2	Solução 2 – Por Métrica de Unidade de Serviços Técnicos (UST) Descrição: Modelo de contratação no qual o prestador de serviços fica responsável pela gerência dos profissionais e suas entregas, adequando seu quadro de profissionais de acordo com as necessidades para o cumprimento dos entregáveis solicitados pelo CONTRATANTE. É um modelo com pagamento vinculado a cada atividade prevista no catálogo de serviços, de acordo com a matriz de complexidade e tempo necessário para a execução de cada uma delas. Esta métrica pressupõe a abertura de Ordens de Serviço (OS) com base nas tarefas/atividades de TIC a serem executadas, nos resultados esperados, nos padrões de qualidade exigidos, cabendo à Contratada cumprir as atividades solicitadas, à medida em que são demandadas. Este modelo exige um elevado nível de maturidade do CONTRATANTE e uma elevada carga de trabalho para a gestão e fiscalização do CONTRATO, uma vez que para o sucesso da execução, é necessária a existência de um catálogo de serviço fixo, base histórica que reflita a realidade do atendimento da área de TIC e uma equipe capaz de fiscalizar a prestação dos serviços de forma consistente, pois demanda a análise e verificação do atendimento, prazo de execução, entregáveis e o custo efetivo para cada uma das micro atividades existentes no catálogo, na quantidade de vezes em que elas ocorreram. Além disso, o modelo pode gerar uma distorção entre o esforço despendido e o valor efetivo para a realização da tarefa, e como consequência gerar gastos excessivos ao erário público ou até privação da execução de algumas demandas. A remuneração da contraprestação baseada em entregas vinculadas à quantidade de incidentes e problemas foi objeto de análise do Tribunal de Contas da União que através da representação TC 014.760/2018-5. O Acórdão nº 2.037/2019 - TCU - Plenário e o Acórdão nº 1508/2020-TCU-Plenário faz uma série de ressalvas quanto à utilização do modelo: • A métrica UST deve ser evitada para a contratação de serviços de suporte contínuo de infraestrutura de TI; • Avaliar, durante o planejamento da contratação do serviço de TI, alternativas à métrica UST, bem como documentar as justificativas da escolha; e • Os serviços especificados no Catálogo de Serviços devem estar diretamente vinculados aos resultados esperados da contratação, não se permitindo o pagamento individualizado por serviços intermediários. A análise do TCU deixou claro que quanto maior o caos, maior seria a quantidade de USTs e, conseqüentemente, maior a remuneração da empresa prestadora dos serviços. Por isso, a adoção do modelo de contratação pura e simplesmente por entregáveis não se demonstra uma escolha viável. Diante do exposto, considerando que o mesmo não atende às recomendações legais para a contratação de serviços de suporte contínuo de Infraestrutura de TI, conclui-se que essa alternativa não é uma opção viável para o atendimento da presente demanda.
3	Solução 3 – Valor fixo mensal vinculado ao atendimento de Níveis Mínimos de Serviço (NMS) Este modelo é o recomendado pela Portaria SGD/MGI no 1.070/2023, no âmbito dos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação – SISF – do Poder Executivo Federal, e é de utilização obrigatória para contratação de serviços de infraestrutura e atendimento a usuários de TI. O modelo consiste na contratação de serviços de TI realizada por meio de modelo de pagamento fixo mensal, vinculado exclusivamente ao cumprimento dos NMS definidos com aplicação redutores no faturamento, por meio de glosas, pelo não cumprimento dos NMS. O modelo não se configura como de dedicação exclusiva de mão de obra, contratação por homem/hora, nem por postos de trabalho. Nesta métrica é criado um catálogo de serviço com os respectivos NMS, bem como indicadores de desempenho e qualidade, definidos em contrato, que deverão ser observados. O modelo busca a eficiência, uma vez que a empresa contratada buscará ser eficiente para garantir a remuneração máxima contratada. O modelo observa as práticas de gerenciamento de serviços descritas na série ABNT 20.000:2020 e as práticas ágeis de DevSecOps. Os serviços estão relacionados à segurança da informação, intercomunicação e rede de comunicação de dados, bancos de dados, servidores de rede, sistemas operacionais, sistemas de backup, recursos de armazenamento de dados, monitoramento e gerenciamento operacional. A definição do valor de referência e do valor máximo da contratação utiliza a pesquisa salarial de preços e fator-k. O modelo busca vincular a execução dos serviços a critérios objetivos de qualidade e resultados, bem como prover maior previsibilidade do cronograma físico e financeiro da execução contratual e maior transparência dos custos associados para o órgão contratante. Esse modelo tem como desvantagem não permitir variações do volume de demandas, ou seja, caso haja redução do volume de demandas, não haverá redução da parcela fixa, a Administração terá um custo maior pelos mesmos serviços e pagará pela ociosidade da demanda contratada e não utilizada. Embora a legislação permita ajustar os contratos administrativos à demanda, esse instrumento não tem por objetivo ser utilizado de forma corriqueira e sim em situações excepcionais e de modo a não desvirtuar a obrigação do gestor público em planejar adequadamente as contratações que realiza. Este modelo tem ainda como desvantagem: a contratada é quem define o quantitativo de profissionais para demanda. O modelo é de utilização obrigatória para a contratação de serviços de operação de infraestrutura e atendimento a usuários de tecnologia da informação e comunicação. A Solução 3 apresenta-se como uma alternativa tecnicamente viável para a presente contratação, em razão das justificativas e escopos definidos pela norma. Além disso, atende às recomendações legais e estabelece padrões de qualidade e indicadores de fácil mensuração com vistas ao ganho na qualidade e na produtividade dos serviços, facilidade de custeamento e orçamentação e simplificação da gestão e fiscalização do contrato. Não obstante o TRE-PA não integre a estrutura do Poder Executivo Federal, mas sim a do Poder Judiciário, a equipe de planejamento optou por utilizar a modelagem referida na Portaria nº 1.070/2023.

Tabela 26 - Identificação das soluções disponíveis no mercado

4.13. Análise Comparativa das Soluções

4.13.1. A Instrução Normativa 94 de 23 dezembro de 2022/SGD/ME no inciso II do art. 11, estabelece a análise comparativa de soluções como obrigatório.

4.13.2. Para tanto, consiste em análise crítica das diferentes soluções levantadas, considerando, além do seu aspecto econômico, os aspectos qualitativos em termos de benefícios para o alcance dos objetivos da contratação. Todavia, considerando que a contratação segue o modelo estabelecido pela Portaria SGD/MGI no 1.070/2023, os requisitos no que tange a interoperabilidade da solução com padrões definidos no âmbito do SISF, estão aderentes no que for aplicável e encontra-se implantada em diversos órgãos da Administração Pública.

4.13.3. Diante dessas diretrizes, foi elaborado um quadro de análise comparativa de soluções, considerando aspectos técnicos, operacionais e estratégicos relevantes para a contratação. O levantamento incluiu a avaliação de diferentes modelos de prestação dos serviços especializados de segurança cibernética, analisando a adequação às necessidades institucionais, a eficiência na alocação de recursos e a conformidade com as melhores práticas do setor.

4.13.4. O quadro comparativo apresenta as principais características das soluções disponíveis no mercado, destacando vantagens, limitações e alinhamento com os requisitos normativos e estratégicos do Tribunal. Essa análise permitiu a identificação da alternativa mais vantajosa para a administração pública, garantindo a escolha de uma solução que atenda aos objetivos institucionais com segurança, eficiência e economicidade.

Requisitos	Solução 1 (Postos de Trabalho)	Solução 2 (Métrica UST)	Solução 3 (Pagamento Fixo / Níveis Mínimos de Serviço - NMS)
Aderência Legal/Normativa	Não Atende (Vedado). Modelo vedado pela Resolução CNJ nº 468/2022 (Art. 8º, IX) para postos puros, por focar em mão de obra e não em resultados.	Atende com Ressalvas (Não Recomendado). Modelo não recomendado pelo TCU (Acórdãos 2.037/2019 e 1508/2020) para serviços contínuos de suporte à infraestrutura.	Atende Plenamente. Alinhado às recomendações legais (ex: Portaria SGD/MGI 1.070/2022), pois foca em resultados, indicadores de qualidade e eficiência.
Negociais	Foco na disponibilidade da mão de obra. Baixa previsibilidade de entregas reais, com risco de ociosidade remunerada.	Foco no cumprimento de tarefas pontuais do catálogo. Risco de o faturamento ser maior quanto maior for a instabilidade do ambiente ("paradoxo lucro-incompetência").	Foco na entrega de valor e resiliência do ambiente. Alta previsibilidade orçamentária por meio de parcelas fixas mensais.
Tecnológicos	Gestão técnica centralizada no Órgão, que define "como" e "quem" executa. Risco de obsolescência técnica por falta de incentivo à inovação da contratada.	Orientada a microatividades. Dificulta a implementação de arquiteturas modernas (como Zero Trust e CSMA) que exigem visão holística em vez de tarefas isoladas.	Estimula a automação e o uso de melhores práticas (ITIL/COBIT/CIS Controls) para garantir os níveis de serviço com maior eficiência técnica.
Vinculação do Pagamento	Disponibilidade. Pagamento pela disponibilidade do profissional (hora/homem), sem garantia intrínseca de entrega ou volume de serviços.	Atividade (OS). Pagamento por tarefa/atividade executada (UST), conforme catálogo de serviços e complexidade definida.	Resultado (Valor Fixo). Pagamento de valor fixo mensal, condicionado estritamente ao atingimento dos Níveis Mínimos de Serviço (NMS) definidos.
Gestão e Fiscalização (Contratante)	Alta Carga (Gestão). Contratante gerencia diretamente os profissionais e suas entregas. Risco de desvio de função.	Alta Carga (Fiscalização). Exige elevada maturidade do Contratante para definir catálogo, complexidade e auditar cada OS faturada. Alta complexidade no acompanhamento da execução.	Gestão Simplificada. Foco na aferição de indicadores (NMS) e aplicação de glosas. A Contratada gerencia o quantitativo de pessoal para atingir o resultado.
Principais Riscos Identificados	Risco de pagamento por ociosidade ou por atividades estranhas ao objeto. Risco legal elevado (vedação CNJ).	Risco de distorção entre esforço e valor (gastos excessivos) ou sub-remuneração que prejudica a qualidade.	Risco de pagamento por ociosidade caso a demanda real seja muito inferior à planejada (pagamento fixo).
Resultado da Análise	Inviável	Inviável	Víável e Recomendado

Tabela 27 - Análise Comparativa das Soluções / Alternativas de mercado

4.14. JUSTIFICATIVA DA SOLUÇÃO DE TI ESCOLHIDA

4.14.1. Atualmente, o **TRE-PA** utiliza, majoritariamente, os serviços da empresa CTIS Tecnologia S/A através do Contrato 28/2020 para suporte à infraestrutura, cuja métrica de remuneração é a Unidade de Serviço Técnico (UST), modelo baseado em catálogo de tarefas e esforço estimado. Complementarmente, a Coordenadoria de Gestão da Segurança Cibernética (CGSI) dispõe de 3 (três) profissionais analistas alocados via contrato de postos de trabalho (CTO 121/2022).

4.14.2. Conforme mencionado, a métrica UST exige a definição de variáveis de complexidade, prioridade e esforço baseado em séries históricas para quantificar o valor de cada tarefa. No modelo atual, a menor unidade possível equivale a uma hora de trabalho na atividade de menor complexidade, buscando correlacionar o custo ao esforço técnico despendido na execução das atividades de infraestrutura.

4.14.3. Embora a UST permita o controle de serviços pré-estabelecidos, a experiência prática demonstrou ser uma métrica de difícil gestão para serviços de execução permanente e continuada. A necessidade de revisões constantes no catálogo, das Ordens de Serviço de Abertura e Fechamento, e a falta de padronização expõem a **Justiça Eleitoral do Pará** a riscos de imprecisão no cálculo dos serviços efetivamente entregues, dificultando o foco no resultado final.

4.14.4. Auditorias do Tribunal de Contas da União (TCU), realizadas entre 2019 e 2020 em 55 contratações federais, apontaram deficiências críticas no uso da UST. O trabalho constatou falhas na estimativa de preços, dimensionamento injustificado de quantitativos e, principalmente, a desconexão entre o pagamento e a efetiva entrega de resultados, prejudicando a fiscalização contratual eficiente.

4.14.5. Diante desses achados, o TCU entende que a métrica UST não deve ser adotada sem a devida padronização e justificativa técnica de seus pesos e parâmetros. A ausência de memória de cálculo para os referenciais utilizados em diversos contratos da Administração Pública Federal motivou recomendações para a busca de modelos de contratação mais transparentes e eficazes.

4.14.6. Nesse cenário, a padronização dos serviços de TI fundamenta-se em modelos de boas práticas como o ITIL (Information Technology Infrastructure Library). Tais frameworks orientam a otimização de processos e a entrega de valor, sendo essenciais para estruturar contratações que priorizem a disponibilidade e a qualidade dos serviços de TIC em detrimento do simples esforço braçal.

4.14.7. Em decorrência dos **Acórdãos nº 2.037/2019 e nº 1.508/2020 – TCU – Plenário**, consolidou-se o entendimento de que a métrica UST é inadequada para a remuneração de serviços de suporte contínuo de TI. O Tribunal recomenda que os órgãos observem premissas que vinculem o pagamento à qualidade e ao cumprimento de metas mensuráveis de desempenho.

4.14.8. Considerando que diversos órgãos do SISP e do Poder Judiciário estão migrando seus modelos contratuais, as orientações sintetizadas pelos acórdãos citados servem de guia para a tomada de decisão desta EPC. O objetivo é adotar um modelo que minimize riscos jurídicos e maximize a **proteção de dados** institucional.

4.14.9. Foram avaliadas as alternativas de "(1) Posto de Serviço com pagamento mensal fixo baseado em resultados" e "(2) Unidade de Serviço Técnico (UST)". Para as necessidades do **TRE-PA**, definiu-se que o objeto principal seguirá o modelo de pagamento fixo mensal vinculado a níveis mínimos de serviço, com definição de perfis profissionais mínimos para fins de planejamento, dimensionamento e execução.

4.14.10. Destarte, optou-se pelo modelo disciplinado pela **Portaria SGD/MGI nº 1.070/2023**, com remuneração baseada em Valor Fixo Mensal condicionado a Níveis Mínimos de Serviço (NMS). Este modelo assegura que o pagamento seja vinculado à qualidade e disponibilidade do ambiente de TIC, com glosas aplicadas em caso de descumprimento dos resultados esperados ou obrigações não entregues.

4.14.11. Fundamental destacar que os perfis profissionais escolhidos para esta contratação foram rigorosamente **padronizados conforme o Catálogo de Funções da Portaria SGD/MGI nº 1.070/2023**, especificamente para o segmento de **Segurança da Informação e Defesa Cibernética**. Esta padronização técnica garante que os profissionais possuam as competências essenciais exigidas pelo órgão central do SISP, assegurando que a execução dos serviços esteja alinhada aos padrões nacionais de maturidade em segurança.

4.14.12. A escolha justifica-se pela alta especialização exigida, demandando profissionais com sólidos conhecimentos em frameworks como **CIS Controls, MITRE ATT&CK e NIST**. A natureza crítica da Justiça Eleitoral do Pará requer disponibilidade operacional contínua e pronta resposta a incidentes, com atuação de profissionais que atendam aos perfis mínimos exigidos e com presença presencial sempre que tecnicamente necessária.

4.14.13. A adoção do modelo da Portaria 1.070/2023 mostra-se a mais vantajosa para a Administração por atender à demanda crescente de segurança cibernética com maior previsibilidade orçamentária. O modelo supera a defasagem da UST, eliminando a demanda reprimida de ações essenciais e permitindo uma gestão contratual focada na resiliência do ambiente tecnológico.

4.14.14. Nestes termos, o objeto desta licitação consolidará a **Contratação de Serviços Gerenciados de Segurança da Informação**, abrangendo Administração, Operação, Gestão de Vulnerabilidades, Resposta a Incidentes e Monitoramento Cibernético. Tais serviços são pilares vitais para a **proteção de dados** e a continuidade operacional do **TRE-PA**.

Quadro-Resumo: Comparação entre a Solução de TIC escolhida e a solução atual (CTO 28/2020)			
Dimensão de Análise	Cenário Atual (Modelo UST)	Solução Escolhida (pagamento fixo mensal, vinculado a NMS)	Justificativa da Mudança
Métrica de Remuneração	Unidade de Serviço Técnico (UST).	Valor Fixo Mensal	A UST é considerada inadequada pelo TCU para serviços contínuos.
Foco da Entrega	Esforço por tarefa e catálogo de atividades.	Resultados, Qualidade e Disponibilidade (NMS).	Focar na "Segurança Garantida" em vez da "Tarefa Executada".
Base Normativa	Contrato 28/2020 e modelos tradicionais.	Portaria SGD/MGI nº 1.070/2023 e Lei 14.133/2021.	Alinhamento com as novas diretrizes de padronização do SISP e Judiciário.

Perfis Profissionais	Arelados a ordens de serviço pontuais.	Perfis Padronizados em Segurança e Defesa Cibernética.	Garantia de competências técnicas específicas (NIST, MITRE ATT&CK).
Gestão e Fiscalização	Complexa (exige conferência de inúmeras OS).	Avaliação simplificada (baseada em indicadores de desempenho).	Redução da carga burocrática e maior controle e transparência no faturamento.
Riscos Mitigados	Imprecisão de faturamento e demanda reprimida.	Falta de prontidão e vulnerabilidades cibernéticas.	Proteção da integridade do processo eleitoral e conformidade com a LGPD.

Tabela 28 - Quadro comparativo entre as soluções: escolhida e solução atual.

4.15. Justificativa econômica da escolha da solução

4.15.1. A solução selecionada é a única que apresenta total aderência ao modelo de contratação padronizado pela Portaria SGD/MGI no 1.070/2023, sendo, portanto, a alternativa de menor risco e maior previsibilidade orçamentária para a Administração.

4.15.2. A economicidade é comprovada pela utilização do Mapa de Valores de Referência (Anexo II da Portaria SGD/MGI no 1.070/2023, atualizado pela Portaria SGD/MGI nº 6.055, de 26 de agosto de 2025). O enquadramento dos perfis profissionais necessários — analistas de segurança e defesa cibernética — nos limites validados pelo órgão central do SISP assegura que os preços contratados estarão em estrita conformidade com a média de mercado, evitando sobrepreço e garantindo a seleção da proposta mais vantajosa sob o critério de melhor preço global.

4.15.3. Ademais, a substituição da métrica UST pelo Valor Fixo Mensal elimina a "demanda reprimida" gerada pela limitação de créditos de unidades de serviço, permitindo que a contratada execute melhorias contínuas na postura de segurança do TRE-PA sem oscilações drásticas nos custos mensais, otimizando o emprego dos recursos públicos.

4.16. Benefícios a serem alcançados com a contratação

4.16.1. Além do necessário aprimoramento do atual modelo de operação infraestrutura e sustentação das atividades de defesa cibernética, o TRE-PA também pretende atingir os seguintes resultados, dentre outros:

- a) **Melhoria na qualidade dos serviços:** Através da definição de padrões de qualidade e indicadores mensuráveis, será possível elevar o nível de excelência na entrega dos serviços contratados.
- b) **Aumento da produtividade:** Ao adequar o quadro de profissionais de acordo com as demandas específicas, haverá uma maior eficiência na execução das tarefas, resultando em um aumento da produtividade.
- c) **Maior flexibilidade na alocação de recursos:** Esse modelo permite a adequação do número de profissionais conforme a necessidade do projeto ou em momentos de maior demanda, garantindo que a equipe seja dimensionada de acordo com a urgência e criticidade das atividades.
- d) **Especialização contínua:** A contratação de profissionais dedicados possibilita o acesso constante a especialistas em segurança cibernética, que podem aprimorar suas habilidades de forma contínua, acompanhando as inovações tecnológicas e novas ameaças.
- e) **Redução de riscos operacionais:** A equipe dedicada se concentrará na detecção e resposta a incidentes cibernéticos, ajudando a mitigar riscos e reduzir o tempo de inatividade dos sistemas, o que é fundamental para garantir a continuidade das operações.
- f) **Transferência de conhecimento e boas práticas:** Profissionais terceirizados podem trazer experiência de outros projetos e organizações, contribuindo para a melhoria dos processos internos e disseminação de boas práticas de segurança cibernética.
- g) **Aumento da agilidade na resposta a incidentes:** Com equipes dedicadas, a capacidade de resposta a incidentes de segurança é significativamente melhorada, o que minimiza os danos causados por ataques e acelera a recuperação dos sistemas afetados.
- h) **Acompanhamento de conformidade regulatória:** Uma equipe especializada em segurança cibernética estará atualizada sobre as exigências legais e normativas, assegurando que a organização esteja em conformidade com leis como a LGPD e regulamentos específicos de segurança da informação.
- i) **Monitoramento proativo e contínuo:** As equipes podem realizar um monitoramento contínuo das redes e sistemas, permitindo a identificação precoce de vulnerabilidades e a implementação de medidas preventivas antes que ocorram incidentes graves.

4.16.2. Diante do exposto, principalmente ante a complexidade, relevância e criticidade do tema cibersegurança para a Tribunal Regional Eleitoral do Pará e para a Justiça Eleitoral, justificamos a necessidade de contratação de empresa especializada no fornecimento de serviços especializados em segurança da informação, visando complementar a quantidade de servidores dedicados de forma exclusiva às atividades de defesa cibernética, em compliance com as recomendações do Tribunal Superior Eleitoral e as diretrizes e parâmetros previstos na Estratégia Nacional de Cibersegurança da Justiça Eleitoral (2021 a 2024 TSE e TRES).

4.17. Quadro de Gerenciamento de Riscos - Migração de Modelo Contratual

4.17.1. A migração de um modelo de remuneração baseado em Unidade de Serviço Técnico (UST) para o modelo de Valor Fixo Mensal vinculado a Níveis Mínimos de Serviço (NMS) constitui um marco crítico na governança de TI do TRE-PA. Embora o novo modelo proporcione maior previsibilidade e foco em resultados, a mudança de paradigma exige um monitoramento rigoroso dos riscos operacionais e jurídicos.

4.17.2. O Quadro de Gerenciamento de Riscos apresentado a seguir foi estruturado para endereçar três pilares fundamentais:

- **Continuidade Operacional:** Dado que o objeto envolve a segurança da informação e proteção de dados, qualquer lacuna na transição entre empresas ou modelos pode resultar em janelas de vulnerabilidade. O risco de perda de conhecimento tático sobre o ambiente do TRE-PA é mitigado por um Plano de Transição que impõe a coexistência técnica (shadowing) e a transferência de ativos de conhecimento.
- **Qualificação e Padronização:** A adoção de perfis profissionais estritamente alinhados à Portaria SGD/MGI nº 1.070/2023 visa eliminar o risco de alocação de mão de obra desqualificada. A fundamentação do risco foca em garantir que analistas de defesa cibernética possuam o domínio dos frameworks exigidos (NIST, CIS, MITRE), assegurando a resiliência institucional.

Identificação do Risco	Impacto	Probabilidade	Medidas de Mitigação (Tratamento)
1. Perda de conhecimento técnico na transição	Alto	Média	Estabelecer um Plano de Transição e Desmobilização detalhado no TR, exigindo que a nova contratada realize o shadowing (acompanhamento) da equipe atual por um período mínimo de 15 a 30 dias.
2. Subdimensionamento da equipe frente ao novo modelo de NMS	Muito Alto	Baixa	Utilizar o Catálogo de Serviços da CGSI v1.3 para validar a volumetria histórica e garantir que os perfis padronizados pela Portaria 1.070/2023 possuam quantitativo suficiente para as metas de SLA/NMS.
3. Dificuldade na mensuração de resultados (NMS vs. Tarefas)	Médio	Alta	Realizar treinamento da equipe de fiscalização do TRE-PA no novo modelo de gestão por resultados e definir indicadores (NMS) claros, objetivos e automatizáveis via ferramenta de gestão de serviços (GLPI) e Monitoramento de Infraestrutura (Zabbix).
4. Resistência cultural da fiscalização ao abandonar a UST	Baixo	Média	Promover reuniões de alinhamento com a CGSI para demonstrar que o foco na "disponibilidade e resiliência" reduz a carga burocrática de conferir centenas de ordens de serviço (OS) de baixa complexidade.
5. Não conformidade dos perfis com a Portaria 1.070/2023	Alto	Baixa	Exigir no Termo de Referência a comprovação de certificações e competências específicas listadas no Catálogo de Funções da SGD para os segmentos de Segurança e Defesa Cibernética.

Tabela 29 - Mapa de riscos identificados da transição contratual.

4.17.3. A metodologia aplicada seguiu as diretrizes da IN 94/2022 e da Lei nº 14.133/2021, classificando os riscos por impacto e probabilidade para definir ações preventivas e de contingência. Com este mapeamento, a EPC assegura que a contratação não apenas atenda aos requisitos técnicos, mas que possua os mecanismos de salvaguarda necessários para enfrentar picos de demanda e crises cibernéticas sem prejuízo ao erário ou à segurança das eleições.

4.18. Análise quanto as condições semelhantes às do setor privado

4.18.1. Conforme a análise realizada, foi certificado que a **contratação de serviços especializados de segurança cibernética, com pagamento mensal fixo baseado em medição de resultados**, observarão condições semelhantes às do setor privado. Essa certificação é baseada em uma avaliação criteriosa das práticas e condições usuais de contratação dos serviços similares no mercado privado, de forma a garantir a transparência, competitividade e eficiência na contratação.

4.18.2. Ao conduzir o processo de contratação, foram adotadas medidas para assegurar que os critérios de seleção, o procedimento de licitação e os termos contratuais estejam em conformidade com as práticas comerciais estabelecidas no setor privado. Dessa forma, busca-se garantir que o processo de contratação seja justo, competitivo e proporcione resultados eficientes para a organização.

4.18.3. Além disso, foram realizadas pesquisas de mercado e consultas a fornecedores especializados, a fim de identificar as melhores práticas e condições usuais de contratação. Foram considerados aspectos como qualidade, preço, prazos de entrega, capacidade técnica e capacidade de fornecimento dos serviços relacionados.

4.18.4. Portanto, com base nessas análises e certificações, podemos afirmar que contratação de serviços especializados de segurança cibernética, seguirão condições semelhantes às do setor privado, buscando assim garantir uma contratação eficiente e de acordo com os padrões comerciais estabelecidas.

4.18.5. Além disso, adotaremos critérios claros e transparentes na seleção das empresas, buscando aquelas que apresentem as melhores propostas, levando em conta não apenas o preço, mas também a qualidade dos serviços oferecidos.

4.18.6. Para tanto, enfatizamos que nosso objetivo é assegurar uma contratação justa, eficiente e economicamente viável para nossa instituição, alinhada com as melhores práticas do setor privado.

5. ANÁLISE COMPARATIVA DE CUSTOS

Fundamentação: análise comparativa de custos, que **deverá considerar apenas as soluções técnica e funcionalmente viáveis**, incluindo (i) cálculo dos custos totais de propriedade por meio da obtenção dos custos inerentes ao ciclo de vida dos bens e serviços de cada solução e (ii) memória de cálculo que referencie os preços e os custos utilizados na análise, com vistas a permitir a verificação da origem dos dados (inciso V do § 1º do art. 18 da Lei 14.133/2021 e Art. 11, inciso III da IN 94/2022).

5.1. Registro de soluções consideradas inviáveis

Conforme demonstrado na seção **"4.13. Análise Comparativa das Soluções"**, as soluções abaixo foram consideradas técnica ou normativamente inviáveis para a contratação dos serviços de **segurança da informação e proteção de dados** e, portanto, dispensam um cálculo detalhado de Custo Total de Propriedade (TCO):

- **Solução 1 – Postos de Trabalho:** A inviabilidade desta solução reside na sua vedação normativa explícita para esta modalidade de contratação. A Lei 14.133/2021 prioriza a contratação por resultado, desempenho ou nível de serviço prestado, e desestimula/veda a simples alocação de mão de obra por “posto de trabalho”, salvo hipóteses muito específicas de dedicação exclusiva em serviços contínuos devidamente motivados. Portanto, este modelo foca na alocação de mão de obra e não em resultados, apresentando alto risco de pagamento por ociosidade e desalinhamento com os objetivos da contratação.
- **Solução 2 – Por Métrica de Unidade de Serviços Técnicos (UST):** Esta alternativa foi descartada por não ser recomendada pelo Tribunal de Contas da União (TCU) para serviços contínuos de suporte à infraestrutura (conforme Acórdãos 2.037/2019 e 1508/2020). O modelo exige maturidade de gestão elevada, apresenta risco de distorção de custos e dificulta a fiscalização focada em resultados (NMS).

Dada a inviabilidade normativa e o alto risco operacional associado, a análise de custos prosseguirá focando exclusivamente na única solução viável identificada: a Solução 3 (Valor fixo mensal vinculado ao atendimento de Níveis Mínimos de Serviço).

Dessa forma, com base no § 1º do art. 11 da IN 94/2022 da SGD/ME, as soluções identificadas e consideradas inviáveis deverão ser registradas no Estudo Técnico Preliminar da Contratação (breve descrição e justificativa), dispensando-se a realização dos respectivos cálculos de custo total de propriedade. Para fins de registro formal, segue a tabela resumo:

Soluções	Justificativa
Solução 1 – Postos de trabalho	Conforme item 4.13 - Análise Comparativa das Soluções (Tabela 24).
Solução 2 – UST	Conforme item 4.13 - Análise Comparativa das Soluções (Tabela 24).

Tabela 30 - Soluções consideradas inviáveis

Para efeitos de comparação de custos a equipe técnica considerou apenas a solução técnica e funcionalmente viável, serviços continuados de suporte e operação de segurança da informação e defesa cibernética por **pagamento fixo mensal vinculado ao atendimento de Níveis Mínimos de Serviço (NMS)** (Portaria SGD/MGI nº 1.070/2023), em atendimento do disposto no inciso III do art. 11 da Instrução Normativa SGD/ME nº 94/2022.

5.2. Cálculo dos Custos Totais de Propriedade (Total Cost Ownership - TCO) da solução viável

5.2.1. A análise baseou-se nos valores de referência da Portaria SGD/MGI nº 1.070/2023, nas contratações realizadas no âmbito da Administração Pública com objeto similar, bem como em pesquisa em sites especializados de salários dos perfis profissionais necessários para a prestação dos serviços.

5.2.2. Os valores constantes do Anexo II, da Portaria SGD/MGI nº 1.070/2023, atualizados pela [Portaria SGD/MGI nº 6.055, de 26 de agosto de 2025](#), cumprem o disposto da Instrução Normativa Seges/ME nº 65, de 2021, para fins de pesquisa de preços das contratações que utilizarem os perfis e insumos do referido Anexo, em que foram complementados com perfis de mercado não englobados pela respectiva norma e alguns definidos por similaridade.

5.2.3. Com base na memória de cálculo detalhada dos Custos Totais de Propriedade (TCO), o custo previsto dos serviços para o período inicial de vigência de 36 (trinta e seis) meses, é constante da tabela abaixo:

DESCRIÇÃO DA SOLUÇÃO	ANO 1	ANO 2	ANO 3	TOTAL
SOLUÇÃO VIÁVEL - ALTERNATIVA 3	R\$ 2.622.991,44	R\$ 2.622.991,44	R\$ 2.622.991,44	R\$ 7.868.974,32

Tabela 31 - Custos Totais de Propriedade (TCO), Solução Viável 1, com base nos valores da Tabela 36.

5.2.4. A metodologia e a memória de cálculo detalhada dos Custos Totais de Propriedade (TCO) encontram-se integralmente descritas no item 8 deste ETP.

6. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO A SER CONTRATADA (descrição/especificação da solução escolhida)

Fundamentação: A descrição da solução como um todo deverá indicar a solução escolhida e conter, de forma detalhada, motivada e justificada, o quantitativo de bens e serviços necessários para a sua composição, considerado todo o ciclo de vida do objeto, inclusive das exigências relacionadas à manutenção e à assistência técnica, quando for o caso (inciso VII do § 1º do art. 18 da Lei 14.133/2021).

A solução escolhida foi a de "Valor Fixo Mensal Vinculado ao Atendimento de Níveis Mínimos de Serviço (NMS)"

6.1. A solução adotada é a Alternativa 3 – Valor Fixo Mensal Vinculado ao Atendimento de Níveis Mínimos de Serviço (NMS), com base na Portaria SGD/MGI no 1.070/2023, e demais condições estabelecidas neste Estudo Técnico e seus Apêndices, para atender as necessidades do TRE-PA, por meio de processo de

licitação na modalidade de pregão, na forma eletrônica, em Grupo Único. O modelo proposto é orientado a resultados, no qual a prestação dos serviços de resposta a incidentes de segurança da informação e a operação da infraestrutura do Tribunal, Data Center e nuvem, serão avaliadas quanto à qualidade e à disponibilidade. Tal avaliação fundamenta-se nos Níveis Mínimos de Serviços Exigidos (NMSE), prevendo-se a aplicação de glosas específicas em caso de descumprimento dos resultados esperados ou de obrigações contratuais. Dessa forma, o pagamento mensal fixo permanece estritamente vinculado ao atendimento integral dos níveis de serviço previamente estabelecidos.

6.2. Em razão do regime de execução e do elevado nível de serviço exigido no objeto da contratação, o presente modelo configura-se como prestação continuada de serviços especializados, com pagamento fixo mensal vinculado a níveis mínimos de serviço, executada por perfis profissionais que atendam aos perfis mínimos definidos para a solução, sem caracterização de cessão de equipe residente ou contratação por postos de trabalho. Essa disponibilidade operacional é indispensável.

6.3. A adoção de pagamento fixo mensal associado ao atendimento de Níveis Mínimos de Serviço (NMS) é mensurada a partir da estimativa de Categorias de Serviço e seus respectivos Perfis de Trabalho, por meio de Mapa Salarial de referência, utilização de Fator-K único, e apoiada por Planilhas de Composição de Custos e Formação de Preços, para a estimativa do valor mensal dos serviços.

6.4. Da Conduta e do Sigilo das Informações

6.4.1. A CONTRATADA estará compelida a obedecer à Política de Segurança da Informação da Justiça Eleitoral (Resolução TSE Nº 23.644/2021), à Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709/2018), assim como às Normas Complementares de Segurança da Informação instituídas no âmbito do TRE-PA. A CONTRATADA compromete-se a não divulgar, sem autorização prévia e expressa do CONTRATANTE, as informações restritas, confidenciais ou classificadas como pessoais de propriedade ou sob a custódia do Órgão. Para tanto, a empresa deverá assinar o **Termo de Compromisso de Sigilo** e entregar juntamente com a documentação exigida (em até 5 dias úteis a contar da assinatura do contrato) e, seus empregados, o **Termo de Ciência do Compromisso de Sigilo** e o **Termo de Responsabilidade** devidamente assinados.

6.4.2. As informações a serem tratadas de forma sigilosa, restrita e confidencialmente são aquelas que, por sua natureza, não podem ser de conhecimento de terceiros não autorizados, incluindo, mas não se limitando a:

- Programas de computador, seus códigos-fonte e códigos-objeto, bem como suas listagens e documentações;
- Informações relacionadas a programas de computador, rotinas, scripts e fluxogramas existentes ou em fase de desenvolvimento;
- Documentos relativos à lista de usuários da Secretaria de Tecnologia da Informação (STI) e seus respectivos dados, armazenados sob qualquer forma;
- Metodologias, processos e ferramentas de serviços, desenvolvidos ou utilizados pela STI;
- Parte ou totalidade dos modelos de dados que subsidiem os sistemas de informações da STI;
- Relatórios de análise de vulnerabilidades, resultados de testes de intrusão (pentests) e planos de correção;
- Configurações de segurança de ativos de TIC, como firewalls, Servidores, sistemas operacionais e demais soluções de segurança;
- Registros de eventos (logs), dados de inteligência sobre ameaças e informações detalhadas sobre incidentes de segurança da informação;
- Qualquer dado pessoal ou dado pessoal sensível, nos termos da LGPD, que seja acessado, processado ou armazenado em decorrência da execução dos serviços;
- Planos de Continuidade de Negócio, Planos de Resposta a Incidentes e toda a documentação estratégica de segurança da informação do CONTRATANTE.

6.4.3. Em caso de dúvida acerca da confidencialidade ou da classificação de determinada informação, a CONTRATADA e seus profissionais deverão tratá-la com o mais alto grau de sigilo, abstendo-se de divulgá-la até que venham a ser expressamente autorizados, por escrito, pelo fiscal do contrato ou pelo Secretário da STI.

6.4.4. Em hipótese alguma se interpretará o silêncio do Contratante ou da fiscalização do contrato como liberação de qualquer dos compromissos de sigilo e confidencialidade ora assumidos.

6.4.5. A CONTRATADA obriga-se expressamente a:

- Preservar a integridade, a disponibilidade e a confidencialidade das informações a que tiver acesso;
- Cumprir a política de segurança e as normativas correlatas, sob pena de incorrer nas sanções disciplinares e legais cabíveis;
- Utilizar os sistemas de informação e os recursos a eles relacionados estritamente para os fins previstos no objeto da contratação;
- Manter o caráter pessoal, intransferível e sigiloso das senhas de acesso aos recursos e sistemas da STI;
- Não compartilhar, sob qualquer forma, informações confidenciais com outros que não tenham a devida autorização de acesso;
- Responder por todo e qualquer acesso aos recursos de informática e dados da STI, bem como pelos efeitos desses acessos efetivados através de suas credenciais;
- Utilizar o acesso privilegiado concedido para inspecionar, copiar ou analisar dados e configurações estritamente para os fins previstos no objeto contratual, sendo vedada qualquer outra utilização, em especial para benefício próprio ou de terceiros;
- Devolver e/ou destruir de forma segura, mediante comprovação e ao término da prestação dos serviços, todos os materiais, registros e documentos de qualquer natureza que tenham sido usados, criados ou que tenham estado sob seu controle e que contenham informações sigilosas relacionadas à STI;
- Notificar imediatamente ao fiscal do contrato qualquer violação de segurança, incidente ou vazamento de dados, real ou suspeito, que tenha sido causado por seus empregados ou que tenha ocorrido sob sua responsabilidade, colaborando ativamente na investigação e mitigação dos danos; e
- Cumprir as disposições instituídas pela Resolução TRE/PA nº 5.699/2021 (Política Geral de Privacidade e Proteção de Dados Pessoais - PGPPD, no âmbito do TRE-PA).

6.5. Composição da Solução

6.5.1. Os serviços especializados de segurança cibernética serão fornecidos em regime de pagamento mensal fixo, condicionado ao cumprimento das metas estabelecidas nos Níveis Mínimos de Serviço (NMS), conforme estipulado na Portaria SGD/MGI nº 1.070/2023. O não cumprimento dos NMS resultará em reduções ou descontos proporcionais ao desempenho insuficiente.

6.5.2. Para a execução dos serviços, será adotado um modelo de trabalho baseado no conceito de delegação de responsabilidade. Nesse modelo, o Contratante assume a gestão e fiscalização do contrato, incluindo a validação da conformidade dos serviços prestados com os padrões de qualidade estabelecidos. Para alinhar a execução à norma vigente, os serviços serão acionados formalmente por meio de Ordens de Serviço (OS), nas quais estarão previstas as quantidades e os perfis profissionais mínimos que fundamentam o modelo de pagamento fixo mensal. A Contratada será responsável pela execução dos serviços e pela gestão de sua equipe, garantindo que todos os profissionais estejam devidamente capacitados para desempenhar suas funções com eficiência.

6.5.3. Os serviços deverão ser realizados de acordo com as melhores práticas de mercado, seguindo as diretrizes da biblioteca Information Technology Infrastructure Library (ITIL®), do framework de governança COBIT® 5 e dos padrões internacionais de segurança da informação e cibernética, incluindo ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27035 (Gestão de Incidentes de Segurança da Informação), ISO/IEC 27005 (Gestão de Riscos), ISO/IEC 20.000 (Gestão de Serviços de TI), NIST Cybersecurity Framework (CSF), NIST Special Publications 800-53 e 800-61, CIS Controls v8 e MITRE ATT&CK.

6.5.4. A Contratada deverá demonstrar competência técnica comprovada para atender integralmente às demandas, garantindo a proteção proativa dos ativos digitais e a mitigação de riscos cibernéticos. A equipe de segurança cibernética proposta no ETP foi dimensionada e ajustada conforme a complexidade, criticidade e volumetria dos serviços a serem executados, considerando a infraestrutura de TIC envolvida, a necessidade de resposta ágil a incidentes, o monitoramento contínuo e a adoção de estratégias de defesa em profundidade, alinhadas às melhores práticas e regulamentações vigentes.

6.6. Necessidade de Equipes Especializadas em Segurança Cibernética

6.6.1. O objeto da presente contratação visa assegurar a prestação de serviços continuados de suporte e operação de segurança da informação e defesa cibernética para o Tribunal Regional Eleitoral do Pará (TRE-PA). A natureza crítica das atividades finalísticas da **Justiça Eleitoral do Pará**, que lidam com dados sensíveis do cadastro eleitoral e a garantia do processo democrático, exige uma estrutura de serviços de **segurança da informação** robusta, madura e proativa.

6.6.2. A complexidade crescente das ameaças cibernéticas e a rigorosa necessidade de conformidade legal, notadamente a Lei Geral de Proteção de Dados (LGPD), impõem que a estratégia de defesa não seja meramente reativa, mas preditiva, inteligente e organizada em múltiplos níveis de atuação.

6.7. Descrição dos perfis profissionais

A solução deverá ser composta pelos serviços descritos de acordo com os perfis mínimos selecionados descritos na tabela abaixo:

ITEM	DESCRIÇÃO	ID	CBO DE REFERÊNCIA	PERFIL	CÓDIGO	QTDE
1 – Serviços técnicos especializados de atendimento ao usuário de TIC	Gerente de suporte técnico de tecnologia da informação	1.1	1425-25	Gerente de infraestrutura de tecnologia da informação	GERSUP	1
	Segurança Cibernética, gerenciamento, Análise de Vulnerabilidades e Atuação Preventiva, Preditiva e Corretiva	1.2	2123-20	Administrador em segurança da informação - Sênior	ASEG-03	3
		1.3	2123-21	Administrador em segurança da informação - Pleno	ASEG-02	2
		1.4	2123-22	Administrador em segurança da informação - Júnior	ASEG-01	3
	TOTAL					9

Tabela 32 - Perfis profissionais e descrição resumida

6.7.1. Os colaboradores responsáveis pela operação e análise de segurança da informação devem possuir os conhecimentos técnicos (formação, certificações, experiência e habilidades) detalhados no ANEXO IX - Equipe Técnica e Qualificação Profissional para a Execução dos Serviços, devendo estar aptos a realizar as atribuições ali descritas.

6.7.2. Para fins de execução contratual, a CONTRATADA deverá encaminhar a relação dos profissionais que executarão os serviços de segurança da informação e proteção de dados na Justiça Eleitoral do Pará no prazo máximo de 10 (dez) dias úteis a partir da assinatura do contrato. A relação deve ser acompanhada do curriculum vitae de cada profissional, documentos pessoais, cópia da carteira de trabalho, exames admissionais, além dos demais comprovantes de experiência, formação e cursos exigidos, com exceção das certificações cujo prazo de apresentação é distinto.

6.7.3. A comprovação das certificações exigidas deverá ser efetuada em até 90 (noventa) dias do início da vigência do contrato, podendo esse prazo ser prorrogado, motivadamente e a critério do CONTRATANTE, uma única vez por igual período.

6.7.4. O quantitativo de perfis profissionais mínimos foi dimensionado com base na análise da complexidade do ambiente tecnológico da Justiça Eleitoral do Pará, do volume de ativos de TIC a serem monitorados, da necessidade de análise contínua de eventos de segurança e dos requisitos de conformidade legal e normativa (vide Seção do ETP 3. ESTIMATIVA DA DEMANDA).

6.8. Métricas de Prestação dos Serviços

6.8.1. O modelo de trabalho proposto é focado em resultados, onde os serviços mensais de suporte e operação de segurança da informação e defesa cibernética serão avaliados quanto à qualidade e à efetividade na mitigação de riscos e na resposta a incidentes, com base nos Níveis Mínimos de Serviço Exigidos (NMSE), em conformidade ao item 12 do Anexo A da Portaria SGD/MGI nº 1.070/2023, prevendo glosas específicas por não cumprimento dos resultados esperados ou de obrigações contratuais.

6.8.2. Os Níveis Mínimos de Serviço (NMS) estabelecem critérios objetivos para mensurar o desempenho da Contratada, garantindo que os serviços atinjam os padrões de qualidade esperados pelo Contratante. Os NMS são projetados para:

- a) Assegurar que a prestação dos serviços atinja o nível de satisfação esperado pelo Contratante;
- b) Promover a melhoria contínua dos serviços fornecidos;
- c) Monitorar e controlar a execução dos serviços pela Contratada;
- d) Avaliar o desempenho da Contratada de forma justa e objetiva.

6.8.3. Este modelo visa assegurar que o foco permaneça na eficiência e na eficácia dos serviços especializados de segurança cibernética prestados. O **item "4.11. Diferentes métricas de prestação do serviço e de pagamento (alínea j)"**, detalha quais indicadores podem ser utilizados na referida contratação para mensuração da qualidade dos serviços.

6.8.4. Estruturação e Consequência dos Níveis Mínimos de Serviço

6.8.4.1. O modelo de medição do contrato adotará a seguinte metodologia:

- O modelo de medição adotado observará exclusivamente critérios de resultado, em estrita observância ao art. 9º da Resolução CNJ nº 468/2022 e ao art. 2º da Portaria SGD/MGI nº 1.070/2023. O pagamento mensal estará condicionado à comprovação objetiva do atingimento dos Níveis Mínimos de Serviço (NMS), definidos com base nos indicadores da seção 8. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO. A disponibilização dos perfis profissionais mínimos constitui meio necessário à execução dos serviços, não se configurando, em nenhuma hipótese, como critério autônomo de medição, consumo garantido ou remuneração;
- Remuneração mensal fixa (Item 01): prestação de serviços especializados de forma rotineira e contínua, cuja remuneração mensal estará exclusivamente condicionada ao atingimento dos Níveis Mínimos de Serviço (NMS) definidos neste Termo de Referência, voltados à mitigação de riscos de segurança da informação e à efetividade da operação de defesa cibernética. A disponibilização de perfis profissionais mínimos constitui meio necessário à execução dos serviços, não se configurando, em nenhuma hipótese, como critério autônomo de medição, consumo garantido ou remuneração.

6.8.4.2. Os NMS foram definidos considerando níveis de severidade e impacto dos eventos de segurança da informação, com aplicação de glosas automáticas, proporcionais e cumulativas em caso de descumprimento, conforme quadro exemplo a seguir:

Indicador	Faixas de ajuste no pagamento e Sanções
EFICÁCIA EM MANUTENÇÃO PERIÓDICA DA INFRAESTRUTURA (PCMP)	PCMP ≥ 95%: Pagamento integral (100%). 90% ≤ PCMP < 95%: Glosa de 2,5% sobre o valor da fatura mensal. 85% ≤ PCMP < 90%: Glosa de 3% sobre o valor da fatura mensal. PCMP < 85%: Glosa de 5% sobre o valor da fatura mensal.

EFICÁCIA NO TRATAMENTO DE VULNERABILIDADES CRÍTICAS E ALTAS (ITV)	ITV = 100%: Pagamento integral (100%). 95% ≤ ITV < 100%: Glosa de 2% sobre o valor da fatura mensal. 90% ≤ ITV < 95%: Glosa de 4% sobre o valor da fatura mensal. ITV < 90%: Glosa de 5% sobre o valor da fatura mensal e abertura de processo administrativo.
---	---

Tabela 33 - Estruturação e Consequência dos Níveis Mínimos de Serviço

6.8.4.3. O não atingimento dos NMS implicará redução do valor mensal devido, vedado pagamento integral sem a comprovação dos resultados.

6.9. Do Fluxo de Atendimento

6.9.1. A execução dos serviços será fundamentada nas melhores práticas da biblioteca ITIL® v4 e no framework COBIT® 5, focando na entrega de valor e na garantia da continuidade operacional. O atendimento especializado será direcionado exclusivamente para atuação no formato de Nível 3 - N3 (Infraestrutura e Segurança, Execução e Operação, Nível Especializado), abrangendo as áreas de Infraestrutura de Segurança, Gestão de Serviços Corporativos e Monitoramento de Ativos de TIC.

6.9.2. Todo o fluxo de execução dos serviços será baseada no padrão ITIL, gerenciado por meio da plataforma de ITSM do Tribunal, compreendendo, pelo menos, as melhores práticas:

- a) Gerenciamento de Disponibilidade e Capacidade;
- b) Gerenciamento de Mudanças;
- c) Gerenciamento de Requisição;
- d) Gerenciamento de Incidentes;
- e) Gerenciamento de Operações de TI;
- f) Gerenciamento de Conhecimento;
- g) Gerenciamento de Problemas;
- h) Gerenciamento de Liberação e Implantação;
- i) Gerenciamento de Riscos;
- j) Gerenciamento de Continuidade de Serviço;
- k) Gerenciamento de Configuração e Ativos de Serviços;
- l) Gerenciamento de Catálogo de Serviços;
- m) Gerenciamento de Nível de Serviço.

6.9.3. O processo de gestão de serviços e controles de defesa cibernética compreende, no mínimo, as seguintes atividades executadas de forma integrada:

- a) Gerenciamento e Resposta a Incidentes (CSIRT): Identificação, registro e tratamento de eventos que afetem a segurança da informação, visando a contenção imediata e a redução do tempo médio de resposta (MTTR). Inclui o suporte especializado de Nível 3 (N3) para a resolução de incidentes complexos e o apoio às equipes de 1º e 2º Nível mediante a criação de roteiros e scripts de remediação.
- b) Gestão e Operação da Infraestrutura de Segurança e TIC: Instalação, configuração, customização, manutenção e supervisão de ativos de TIC e Segurança (hardware e software), sejam on-premise ou em nuvem. Planejamento, gerenciamento e execução de mudanças na infraestrutura, mantendo o controle de configuração. Administração de soluções de virtualização e gerenciamento de capacidade dos recursos computacionais.
- c) Monitoramento, Observabilidade e Inteligência (ITIM/ITOM): Operação contínua (regime 8x5 ou conforme definido em NMS) de soluções de SIEM, EDR e NDR, para detecção de anomalias e defesa ativa. Uso de ferramentas de monitoramento de infraestrutura (ITIM) e operações (ITOM) para promover informações gerenciais que auxiliem a tomada de decisão. Inclui a análise proativa do ambiente tecnológico para antecipar falhas e identificar ameaças antes que impactem a continuidade dos serviços da Justiça Eleitoral do Pará.
- d) Gerenciamento de Vulnerabilidades e Ciclo de Vida de Ativos: Realização de varreduras proativas e gestão do ciclo de vida de correções (patches e hardening). Envolve a manutenção de baselines de configuração segura e o gerenciamento de componentes, processos e serviços de TIC para mitigar riscos de exposição.
- e) Proteção de Dados, Privacidade e Identidade (LGPD & Zero Trust): Operação de ferramentas de DLP (Data Loss Prevention), suporte à classificação de dados e gestão de acessos privilegiados (PAM). Inclui a administração do ambiente de mensageria, colaboração e identidade (usuários), garantindo a conformidade com a Lei Geral de Proteção de Dados. Gestão de Identidade e Acesso (IDP/IAM) e implementação de controles baseados em Zero Trust Architecture (ZTA) e Segurança de Identidade.
- f) Sustentação DEVOPS / DEVSECOPS: Suporte e administração de arquiteturas modernas, auxiliando as equipes de desenvolvimento na criação e manutenção de "esteiras" de CI/CD automatizadas. Foco na integração da segurança desde a concepção do software (Security by Design) e automação de componentes.
- g) Governança, Políticas e Conscientização: Apoio na elaboração, manutenção e revisão da Política de Segurança da Informação (PSI) e dos Planos de Continuidade de Negócios (PCN) e Contingência. Proposição de ações para conformidade com normas do Governo Federal e padrões de mercado. Apoio técnico em campanhas de conscientização e divulgação de boas práticas para usuários.
- h) IA e Automação de Defesa (AI Security): Operação de plataformas de segurança baseadas em Inteligência Artificial para antecipação de ameaças e automação de políticas de segurança.
- i) Cumprimento de Requisições e Rotinas Operacionais: Execução de tarefas descritas no Catálogo de Serviços da CGSI, assegurando a conformidade com as políticas internas. Inclui a execução rigorosa de rotinas de backup, restauração de dados (restore) e a realização periódica de testes de integridade das cópias de segurança.

6.9.4. Durante a execução do contrato, a CONTRATADA deverá implementar a automação nos processos de Operação de Infraestrutura de TIC. Este processo deverá ser continuamente aprimorado para aumentar a eficiência operacional, bem como para reduzir o tempo de resposta e melhorar a satisfação do usuário.

6.10. Dos Processos de Trabalho - CIS Controls

6.10.1. Todos os serviços executados no escopo desta contratação possuem relação direta com as práticas e os controles preconizados pelo framework CIS Critical Security Controls (CIS Controls), visando a melhoria contínua da maturidade em segurança cibernética da Justiça Eleitoral do Pará.

6.10.2. O escopo dos serviços da presente contratação envolve a implementação, operação e melhoria contínua dos controles de segurança, com priorização baseada nos Grupos de Implementação (IG1, IG2, IG3) definidos pelo framework CIS Controls, de forma a fortalecer a postura de defesa cibernética do Tribunal contra as ameaças mais prevalentes.

6.10.3. A supervisão, pela contratada, da postura de segurança deve rever, analisar e propor recomendações para a melhoria contínua na implementação dos controles. O objetivo é alinhar as defesas às necessidades de proteção do negócio, reduzir a superfície de ataque e manter a operação dos serviços de segurança da informação em conformidade com os níveis de risco aceitáveis.

6.10.4. Nesse sentido, são objeto de implementação, operação e/ou melhoria contínua os processos associados aos seguintes Controles CIS:

- CIS Control 1: Inventário e Controle de Ativos Corporativos;
- CIS Control 2: Inventário e Controle de Ativos de Software;
- CIS Control 3: Proteção de Dados;
- CIS Control 7: Gerenciamento Contínuo de Vulnerabilidades;
- CIS Control 8: Gerenciamento de Logs de Auditoria;
- CIS Control 10: Defesas Contra Malware;
- CIS Control 11: Recuperação de Dados;
- CIS Control 13: Monitoramento e Defesa da Rede;
- CIS Control 17: Gerenciamento de Resposta a Incidentes.

6.10.5. As melhorias na implementação dos controles serão submetidas a auditorias e à verificação dos resultados obtidos, mensurando a eficácia e a abrangência de sua aplicação em relação à efetiva mitigação de riscos para o ambiente da Justiça Eleitoral do Pará.

6.10.6. Ao longo da execução do contrato, espera-se uma melhoria gradual e contínua na postura de segurança, fruto das otimizações propostas e implementadas, contribuindo para o aumento da maturidade em segurança cibernética. Para essa finalidade, é fundamental o monitoramento de indicadores de eficácia dos controles, a análise de métricas de segurança e a coleta de dados para identificar oportunidades de aprimoramento em todos os processos de defesa.

6.10.7. A título de exemplo, detalham-se a seguir os ciclos de vida de alguns processos essenciais associados a Controles CIS específicos:

1) Processo de Gerenciamento de Resposta a Incidentes (CIS Control 17):

- Preparação: Prover as ferramentas, processos e treinamentos necessários para responder a incidentes de forma eficaz.
- Detecção e Análise: Identificar e validar incidentes de segurança, determinando seu escopo e impacto.
- Contenção, Erradicação e Recuperação: Conter o incidente para limitar o dano, erradicar a causa raiz e restaurar os sistemas ao estado normal de operação de forma segura.
- Atividades Pós-Incidente: Documentar o incidente, analisar as lições aprendidas e implementar melhorias para prevenir a recorrência.
- Objetivo: Este processo visa não apenas conter e remediar os impactos de um ataque, mas também aprender com o evento para fortalecer as defesas, sendo fundamental para a resiliência cibernética da Justiça Eleitoral do Pará.

2) Processo de Proteção de Dados (CIS Control 3):

- Identificação e Classificação: Realizar o mapeamento dos repositórios de dados para identificar onde residem informações críticas, classificando-as quanto ao nível de sensibilidade (público, interno, confidencial, etc.).
- Gerenciamento de Controles de Acesso: Garantir que o acesso aos dados seja concedido com base no princípio do menor privilégio, utilizando listas de controle de acesso e revisões periódicas de permissões.
- Implementação de Prevenção à Perda de Dados (DLP): Operar e ajustar ferramentas que monitoram e bloqueiam a exfiltração não autorizada de dados sensíveis por meio de canais como e-mail, USB e nuvem.
- Retenção e Descarte Seguro: Apoiar na aplicação das políticas de retenção de dados e executar procedimentos para o descarte seguro (eliminação permanente) de informações que já cumpriram seu ciclo de vida legal ou operacional.
- Objetivo: Este processo visa garantir a confidencialidade, integridade e disponibilidade dos dados da Justiça Eleitoral do Pará, em especial os dados pessoais e sensíveis, assegurando a conformidade com a Lei Geral de Proteção de Dados (LGPD) e outras normativas aplicáveis.

3) Processo de Recuperação de Dados (CIS Control 11):

- Definição e Aplicação de Políticas de Backup: Executar rotinas de cópia de segurança conforme as políticas estabelecidas, que definem a frequência, o escopo e o tipo de backup para cada ativo de informação.
- Execução e Monitoramento Contínuo: Operar a solução de backup, monitorando a execução das rotinas para garantir que sejam concluídas com sucesso e sem erros.
- Testes Periódicos de Restauração: Realizar, de forma planejada e documentada, testes de restauração dos backups em ambiente controlado para validar a integridade e a viabilidade da recuperação dos dados.
- Execução de Procedimentos de Restauração: Em caso de incidente de perda de dados, executar os procedimentos de restauração para recuperar as informações no menor tempo possível, de acordo com os objetivos de tempo de recuperação (RTO) definidos.
- Objetivo: Este processo é fundamental para garantir a resiliência operacional e a continuidade dos serviços da Justiça Eleitoral do Pará diante de eventos adversos, como falhas de hardware, erros humanos ou ataques cibernéticos (ex: ransomware), assegurando que os dados possam ser restaurados de forma íntegra e tempestiva.

6.10.8. Da Matriz de Compatibilidade: Riscos, Necessidades Tecnológicas e Controles CIS

6.10.8.1. A estratégia de defesa cibernética desta contratação fundamenta-se na correlação direta entre os riscos identificados, as ferramentas tecnológicas operadas e os controles de segurança estabelecidos. Esta abordagem garante que cada processo de trabalho executado pela CONTRATADA contribua efetivamente para a mitigação de ameaças reais à **Justiça Eleitoral do Pará**, utilizando o framework **CIS Controls v8** como métrica de maturidade e conformidade técnica. A tabela abaixo detalha essa integração, estabelecendo a fundamentação para a priorização das medidas operacionais e a aferição da eficácia dos controles:

Risco Mapeado	Descrição do Risco	Necessidades Tecnológicas (Controles)	Estratégia de Tratamento no Contrato	Alinhamento CIS Controls
R1	Ataque de Ransomware	e) Proteção Ransomware; g) Backup; l) EDR/XDR.	Detecção por IA e garantia de continuidade através da restauração rápida.	CIS 10 (Malware) e CIS 11 (Recuperação)
R2	Vazamento de dados pessoais	c) Gestão de Vulnerabilidades; h) Criptografia; m) Logs.	Varreduras proativas e proteção da confidencialidade em trânsito/repouso.	CIS 3 (Proteção de Dados) e CIS 7 (Vulnerabilidades)
R3	Indisponibilidade de sistemas	a) SIEM; b) NDR; k) SOAR.	Monitoramento perimetral e interno para bloqueio imediato de ameaças.	CIS 13 (Defesa de Rede) e CIS 1 (Ativos de Hardware)
R4	Atraso na contenção	k) SOAR; j) Capacitação contínua.	Redução do MTTR (Time to Respond) através de orquestração automatizada.	CIS 17 (Resposta a Incidentes)
R5	Comprometimento de Credenciais	d) Soluções PAM; m) Logs e Auditoria.	Rastreabilidade total de usuários privilegiados e blindagem de contas críticas.	CIS 8 (Logs) e CIS 6 (Controle de Acessos)
R6	Falha de Segurança em Nuvem	f) Segurança em nuvem; i) Ambiente de testes.	Padronização de políticas de segurança em arquitetura de malha (Cloud/Local).	CIS 2 (Ativos de Software) e CIS 13 (Defesa de Rede)

Tabela 34 - Mapeamento de Riscos, Controles e Estratégias de Tratamento.

6.11. Da Gestão das Operações de Segurança e Plataforma ITSM

6.11.1. A gestão e a operação dos serviços deverão seguir as melhores práticas internacionais, utilizando os princípios de gestão de serviços de tecnologia (ITSM) da **biblioteca ITIL e/ou da norma ISO 20000** como base para a organização, registro e mensuração das demandas na plataforma de gestão.

6.11.2. Todos os serviços serão solicitados ou gerados por meio de registros formais na plataforma de gestão de requisições e incidentes do CONTRATANTE. Tais registros podem ser originados de alertas automáticos de ferramentas de segurança, soluções de orquestração (p.ex. N8N), incidentes reportados por usuários (via Central de Serviços de TIC), requisições de serviço de segurança ou tarefas proativas planejadas (ex: análise de vulnerabilidades, threat hunting).

6.11.3. Independente do canal de comunicação utilizado, todos os incidentes devem ser convergidos, mantidos, atualizados e registrados na plataforma única de gestão de serviços provida pelo CONTRATANTE, de forma a garantir que todas as informações estejam sempre consolidadas, atualizadas e fiéis.

6.11.4. O CONTRATANTE deverá disponibilizar o acesso à plataforma de gestão, assim como documentações, bases de conhecimento, sistemas de monitoramento, sistemáticas e processos complementares, necessários à operação, à produção de informações, à base de conhecimentos e aos relatórios de segurança da informação.

6.11.5. Ao longo da execução contratual, o CONTRATANTE estruturará na sua plataforma de gestão o catálogo de serviços, os fluxos de trabalho, base de conhecimento e fluxos do processo de mudança. Caberá à CONTRATADA, como parte de suas atribuições, propor ativamente ajustes e melhorias contínuas nesses processos para otimizar a eficácia dos serviços de segurança.

6.11.6. Os colaboradores da CONTRATADA receberão treinamento para operar a plataforma de gestão fornecida pelo CONTRATANTE.

6.11.7. A CONTRATANTE disponibilizará, para a execução das atividades, infraestrutura física adequada nas dependências da Justiça Eleitoral do Pará. Esta infraestrutura compreende mobiliário ergonômico, estações de trabalho de alto desempenho, conectividade à rede corporativa e acesso às ferramentas de software, monitoramento (dashboard) e equipamentos de teste necessários à plena prestação dos serviços de segurança da informação e proteção de dados.

6.11.8. A CONTRATANTE disponibilizará os sistemas de ITSM e as plataformas de monitoramento e segurança necessários à execução dos serviços. Caberá à CONTRATADA a responsabilidade técnica por prover e integrar, nestes sistemas, todas as informações e configurações operacionais, incluindo a manutenção de um painel de controle (dashboard) que exiba em tempo real os alertas, incidentes em curso, status de ativos críticos e as filas de tarefas da equipe, garantindo o gerenciamento completo e a transparência total dos registros para a fiscalização.

6.11.9. A plataforma de gestão, dentre outras fontes de informação, será utilizada para a extração de insumos para o Relatório Mensal de Atividades e Desempenho, necessário para o acompanhamento dos serviços.

6.11.10. Do Gerenciamento dos Registros na Plataforma

i) Os registros de requisição de serviços e incidentes poderão ser abertos pelos usuários do Tribunal a qualquer dia e horário, tanto em dias úteis como em finais de semana e feriados, e devem ser atendidos de acordo com os Níveis Mínimos de Serviço.

ii) Após o registro na plataforma classificação e priorização da Central de Serviços de TI, a equipe N3 da CONTRATADA realizará a triagem, classificação (conforme matriz de risco e criticidade) e priorização do(s) evento(s) de segurança. A Central de Serviços de TIC do Tribunal atuará como um dos canais para o registro de incidentes reportados por usuários, encaminhando-os para a(s) fila(s) de atendimento das unidades de serviços corporativos e defesa cibernética.

iii) Ao concluir o tratamento de um registro, o profissional da CONTRATADA documentará na plataforma todas as análises, ações e a solução adotada, referenciando os itens do catálogo de serviço e alterando o status do registro para "Solucionado" ou "Encerrado".

6.11.11. Da Governança sobre Encerramento, Reabertura e Cancelamento de Registros

i) A qualidade do serviço será aferida pela equipe de fiscalização, com base nos Níveis Mínimos de Serviços. Nenhum registro poderá ser encerrado pela CONTRATADA sem a anuência expressa do fiscal do contrato ou de servidor a quem ele delegar.

ii) Caso um registro seja indevidamente encerrado, poderá ser reaberto pela equipe de fiscalização do Tribunal no prazo de até 30 (trinta) dias corridos, voltando a contar o prazo do Nível Mínimo de Serviço a partir da data e hora da abertura original, inclusive para efeitos de aplicação de glosas e sanções.

iii) Um registro somente poderá ser cancelado com a autorização expressa do fiscal do contrato, que deverá analisar a situação para possível readequação de prazos e outras providências que se fizerem necessárias.

iv) A homologação mensal dos registros solucionados consistirá na verificação de conformidade das atividades executadas com as evidências apresentadas e com as soluções consignadas no Catálogo de Serviços, sendo a base para a apuração dos níveis de serviço alcançados e eventual aplicação de glosas.

6.11.12. Do Prazo para Refazimento dos Serviços

i) Os serviços prestados em cada chamado solucionado poderão ser refeitos no prazo de até 48 horas, após o fechamento, sem que haja prejuízo ao nível de serviço exigido;

ii) Nesse período, o usuário poderá classificar o status do chamado para não solucionado e os serviços nele descritos serão refeitos com total transparência e, ao mesmo, sem ônus para o CONTRATANTE;

iii) Após o refazimento dos serviços, caso haja necessidade, o serviço poderá ser refeito novamente, no prazo de 48 horas, sem que haja prejuízo ao nível de serviço exigido;

iv) É importante destacar que, durante o período de refazimento dos serviços, serão aplicados os mesmos níveis de serviços exigidos; e

v) Os serviços executados que apresentem problemas ou incorreções por imperícia na execução, mesmo após o período de 48 horas aqui tratado, poderão ensejar a correção ou nova execução, a pedido da fiscalização do contrato, dentro da vigência do contrato.

6.11.13. Da Prioridade de Atendimento

i) Os chamados de suporte técnico constituem a solicitação formal de serviços à CONTRATADA e devem ser processados exclusivamente via sistema de ITSM provido pela CONTRATANTE, observando-se rigorosamente os critérios, prazos e parâmetros estabelecidos neste Termo de Referência;

ii) Os chamados serão classificados pela CONTRATANTE quanto à categoria (incidente ou requisição) e criticidade (baixa, média, alta ou crítica), conforme as definições contidas no Catálogo de Serviços;

iii) Chamados classificados como de alta prioridade ou críticos terão precedência imediata na fila de atendimento. Nestes casos, admite-se a suspensão temporária da contagem do prazo de atendimento de chamados de menor prioridade já iniciados, desde que comprovada a indisponibilidade momentânea de pessoal técnico especializado e mediante justificativa formal no sistema;

iv) Os demais chamados deverão ser atendidos estritamente dentro dos prazos de resposta e solução estabelecidos. O descumprimento injustificado desses prazos sujeitará a CONTRATADA à aplicação de glosas proporcionais na fatura mensal, sem prejuízo das sanções administrativas previstas em contrato;

v) Todos os eventos relacionados ao atendimento, desde a triagem até o encerramento com o aceite do usuário/fiscal, deverão ser registrados de forma detalhada pela CONTRATADA, garantindo a transparência necessária para a medição dos indicadores de desempenho.

6.12. Dos Materiais e do Ambiente de Trabalho

6.12.1. O TRE-PA disponibilizará nas dependências do Anexo 1 - Sede TRE-PA, os computadores (desktops ou notebooks), licenças de softwares, mesas, cadeiras, infraestrutura de rede e quaisquer materiais complementares para que a equipe técnica da CONTRATADA possa realizar suas atribuições. Deste modo, todos os profissionais que compõem a equipe de segurança da informação da CONTRATADA deverão atuar alocados exclusivamente nas dependências do CONTRATANTE.

6.12.2. A seu critério, a CONTRATADA poderá propor a utilização de softwares e sistemas próprios (incluindo ferramentas de código aberto), desde que sejam devidamente legalizados e previamente submetidos à análise para homologação e autorização expressa da equipe técnica do TRE-PA. A CONTRATADA deverá garantir a permanente disponibilização e o acesso do CONTRATANTE às informações geradas por tais ferramentas, que deverão passar por uma avaliação de segurança antes de sua implantação no ambiente do Tribunal.

6.13. Do Catálogo de Serviços

6.13.1. O modelo de prestação de serviços baseia-se na operação continuada, fundamentada em processos definidos e previamente documentados. As demandas serão detalhadas em Catálogo de Serviços, o qual especifica as atividades a serem executadas pela CONTRATADA. Esta deverá observar estritamente os processos, padrões e procedimentos descritos na Base de Conhecimento do CONTRATANTE, incluindo os *Playbooks* de resposta a incidentes e os *Runbooks* operacionais.

6.13.2. A adoção de catálogos de serviços para descrição dos serviços prestados pela área de TIC, tem por objetivo informar a lista de serviços de TIC atualmente suportados, disponível às partes interessadas, cujos resultados esperados e níveis mínimos de qualidade exigidos são fundamentais para assegurar a estabilidade e previsibilidade do processo de gerenciamento dos serviços de TIC.

6.13.3. Os serviços e soluções aplicadas aos chamados categorizados serão descritos no documento Catálogo de Serviços da CGSI. Para garantir que este catálogo reflita as melhores práticas de defesa cibernética e esteja alinhado aos desafios contemporâneos da **segurança da informação e proteção de dados**, os serviços, tarefas e atividades nele descritos foram modelados e estruturados com base no framework de Controles do Center for Internet Security (CIS) v.8. Esta abordagem assegura que a prestação de serviços pela futura contratada esteja alinhada a um padrão robusto, priorizado e reconhecido pelos órgãos de controle, focado na mitigação efetiva dos riscos cibernéticos que afetam organizações como a **Justiça Eleitoral do Pará**.

6.13.4. A utilização de catálogo de serviços de TIC não se confunde com a mensuração dos serviços para fins de pagamento, mas trata-se de uma prática constante da ABNT NBR ISO/IEC 20.000-1:2020. Deste modo, é uma boa prática possuir um Catálogo de Serviços com todas as atividades documenta, correspondendo aos serviços efetivamente prestados e executados pela CONTRATADA. Os serviços constantes no Catálogo de Serviços geralmente são organizados com a seguinte classificação:

a) **Catálogo de Serviços Negocial:** Contém os serviços de TIC atualmente em operação e disponíveis para os clientes ou sendo preparados para serem entregues aos clientes; e

b) **Catálogo de Serviços Técnico:** Contém todas as requisições de serviço disponíveis para os clientes e usuários de serviços de TI.

6.13.5. Neste sentido, o Catálogo de Serviços (anexo ao Termo de Referência) constitui o Catálogo de Serviços Negocial da Coordenadoria de Gestão da Segurança da Informação e Infraestrutura de Data Center do TRE-PA, seguindo o modelo da Portaria 1.070/2023. Para a operacionalização da solução de serviços técnicos especializados em **segurança da informação e proteção de dados**, objeto desta contratação, o Termo de Referência (TR) deverá fazer menção direta e utilizar como base o Catálogo de Serviços Negocial da CGSI/STI. Este documento, portanto, funcionará como a fonte de dados centralizada que detalha o escopo de todas as tarefas e atividades técnicas a serem executadas. O referido catálogo descreve formalmente os serviços que a CGSI/STI oferece aos seus usuários, consolidando as informações essenciais sobre como acessá-los, o suporte técnico disponível, os pré-requisitos necessários e os Acordos de Nível de Serviço (SLAs) associados a cada entrega.

6.13.6. O sistema de gerenciamento dos chamados – ITSM, será alimentado pelo Catálogo de Serviços Técnico do TRE-PA, composto pelas tarefas que detalham as atividades e complexidades relacionadas a cada requisição de serviço, muitas das quais representam a operacionalização das salvaguardas definidas nos Controles CIS v.8. O Catálogo de Serviços Técnico é um arquivo vivo e deve ser compreendido como a lista básica e não exaustiva de serviços, atividades, instruções de trabalho processos, categorizadas de acordo com o escopo de atuação da área da CGSI/STI, que serão atendidas nesta contratação pelos perfis profissionais contratados e deverá ser alimentado e atualizado em conjunto com a CONTRATADA durante toda a vigência da contratação. Este catálogo técnico detalha também os prazos acordados, podendo ser alterado, corrigido, ampliado, suprimido ou acrescido de novos serviços durante a execução contratual, mantendo-se o escopo da presente contratação.

6.13.7. Por razões de segurança da informação, o Catálogo de Serviços Técnicos, as bases de conhecimento e os documentos técnicos complementares — que detalham a execução específica das tarefas — serão disponibilizados às empresas interessadas exclusivamente durante a Vistoria Técnica. O acesso a tais documentos fica condicionado à assinatura prévia de um Termo de Confidencialidade (NDA). Esta medida visa proteger dados sensíveis sobre a infraestrutura, estratégias de defesa e fluxos operacionais do Tribunal, impedindo que o detalhamento técnico seja utilizado por agentes maliciosos para a identificação de vulnerabilidades ou tentativas de intrusão mediante engenharia reversa nos sistemas do TRE-PA.

6.13.8. O detalhamento técnico exaustivo de todas as atividades a serem executadas encontra-se consolidado no Catálogo de Serviços, nas Bases de Conhecimento e nos demais documentos técnicos complementares. Este acervo documental constitui a referência obrigatória para a prestação dos serviços e permanecerá disponível para consulta e atualização pela CONTRATADA durante toda a vigência contratual. A observância integral desses instrumentos visa assegurar a padronização operacional, a rastreabilidade das ações de segurança cibernética e o alinhamento contínuo com as diretrizes estratégicas do Tribunal.

6.14. Conformidade com o Art. 9º da IN SEGES 05/2017

A solução foi modelada para assegurar que a prestação dos serviços de segurança da informação e proteção de dados não resulte na transferência de atividades estratégicas ou de poder decisório à contratada. O planejamento desta contratação foi estruturado em estrita observância ao Art. 9º da IN SEGES nº 05/2017, garantindo que o objeto se limite a atividades de apoio técnico e operacional, conforme detalhado a seguir:

1) Preservação do Poder Decisório e Planejamento (Incisos I e II): A execução dos serviços, abrangendo as atividades do N3, possui natureza estritamente técnica, operacional e consultiva. Todas as atividades de planejamento estratégico, coordenação e a palavra final sobre as políticas de segurança permanecem sob a égide dos servidores da Coordenadoria de Gestão da Segurança da Informação (CGSI). A contratada fornecerá subsídios e execução de rotinas, contudo, o controle de processos, o conhecimento crítico e a governança das tecnologias de proteção são retidos pelo Tribunal, mitigando qualquer risco ao controle institucional.

2) Natureza Auxiliar e Vedação à Substituição de Funções (Inciso IV e Parágrafo Único): Os serviços caracterizam-se como atividades acessórias e instrumentais de suporte à infraestrutura e resposta a incidentes. Tais atividades não se confundem com as atribuições inerentes às categorias funcionais do quadro de pessoal do TRE-PA. Conforme preceitua o parágrafo único do referido artigo, a responsabilidade pela prática de atos administrativos e a gestão de riscos permanecem exclusivamente com os servidores públicos, sendo vedada qualquer transferência de responsabilidade decisória à contratada.

7. PROVIDÊNCIAS PRÉVIAS AO CONTRATO

Fundamentação: providências a serem adotadas pela Administração previamente à celebração do contrato (inciso X do § 1º do art. 18 da Lei 14.133/2021 e Art. 9º, inciso XI da IN 58/2022).

7.1. A Equipe de Planejamento da Contratação apresenta a seguir as necessidades de recursos materiais e humanos do TRE-PA, no que se refere à implantação, uso e à manutenção da Solução de TIC, para que o contrato possa ser devidamente executado e a solução de TIC atinja seus objetivos:

TIPO DE NECESSIDADE	UNIDADE RESPONSÁVEL	DESCRIÇÃO
Infraestrutura tecnológica	N/A	Para o referido projeto, entende-se por infraestrutura tecnológica necessária o fornecimento de computadores, monitores, laptops e respectivos componentes acessórios, disponibilizados pelo TRE-PA, para uso da(s) equipe(s) a serem contratadas durante a vigência da contratação, objetivando a execução dos serviços que tratam o objeto. Nesse projeto, não há pendências relacionadas a este aspecto. Todo o ambiente do TRE-PA está apto para a execução contratual.
Mudança ou Configuração	SDC/CGSI	Configuração de credenciais de acesso, grupos de email-s, credenciais privilegiadas aos sistemas mantidos pela CGSI/STI, será efetuado pela equipe de Defesa Cibernética.
Infraestrutura elétrica	N/A	Nesse projeto, não há pendências relacionadas a este aspecto. Todo o ambiente está apto para a execução contratual.
Obtenção de licenças	N/A	Nesse projeto, não há pendências relacionadas a este aspecto. Todo o ambiente está apto para a execução contratual.
Logística de implantação	N/A	Nesse projeto, não há pendências relacionadas a este aspecto. Todo o ambiente está apto para a execução contratual.

Espaço físico	N/A	Nesse projeto, não há pendências relacionadas a este aspecto. Todo o ambiente está apto para a execução contratual. O espaço físico da STI é adequado para a recepção das equipes e realização das atividades pertinentes ao Contrato.
Mobiliário	N/A	Nesse projeto, não há pendências relacionadas a este aspecto. Todo o ambiente está apto para a execução contratual. O mobiliário disponível na STI é adequado para a recepção das equipes e realização das atividades pertinentes ao Contrato.
Impacto ambiental	N/A	Nesse projeto, não há pendências relacionadas a este aspecto. Todo o ambiente está apto para a execução contratual.
Capacitação fiscalização / gestão contratual	A gestão e fiscalização do contrato serão realizadas por equipe técnica capacitada, com responsabilidade específica pela aferição mensal dos NMS, validação das evidências apresentadas e aplicação de glosas, garantindo aderência à Lei nº 14.133/2021 e à Portaria SGD/MGI nº 6.680/2024.	Nesse projeto, não há pendências relacionadas a este aspecto. Todo o ambiente está apto para a execução contratual. A CGSI/STI possui bases de conhecimento em texto, vídeo e outros documentos técnicos, relacionada aos processos de trabalho e à infraestrutura de defesa cibernética que poderá ser consultada pela(s) equipe(s) relacionada(s) ao Contrato.
Recursos Humanos	Fiscal técnico	Gerenciar e acompanhar as demandas técnicas, prazos e nível de serviço.
	Gestor do contrato	Atestar as faturas e realizar a fiscalização e gestão do contrato

Tabela 35 - Providências prévias ao Contrato.

8. ESTIMATIVA DO CUSTO TOTAL DA CONTRATAÇÃO

8.1. Memória de Cálculo das Soluções Viáveis

8.1.1. Considerando a escolha da **Solução 3 - Remuneração por Valor Fixo Mensal vinculado ao atendimento de Níveis Mínimos de Serviço (NMS), suportada por Perfis Profissionais Mínimos de referência**, faz-se necessário efetuar a pesquisa de salário de referência para os perfis a serem exigidos, para assim obter a composição de custos e estimativa de preços dos serviços a serem contratados, conforme os itens a seguir.

8.2. Dos Valores Salariais

8.2.1. Durante a pesquisa local foi encontrada a fonte de pesquisa salarial instituída pela Secretaria de Governo Digital (SGD) do Ministério de Gestão e Inovação dos Serviços Públicos (MGI), disponível no site referente ao [Modelo de Contratação de Serviços de Operação de Infraestrutura e de Atendimento a Usuários de TIC](#). O Modelo compõe-se dos seguinte elementos:

- **Modelo de Contratação de Serviços de Operação de Infraestrutura e de Atendimento a Usuários de TIC:** Os serviços descritos neste documento abrangem a operação de infraestrutura, bem como o atendimento a usuários de TIC, entendendo-se por operação de infraestrutura de TIC a prestação de serviços técnicos que estão relacionados à segurança da informação, intercomunicação e rede de comunicação de voz e dados, banco de dados, servidores de rede, sistemas operacionais, sistemas de backup, recursos de armazenamento de dados, monitoramento e gerenciamento operacional.
- **Modelo de planilha simplificada para estimativa dos serviços por parte dos órgãos e entidades do SISP:** Trata-se de planilha auxiliar que deverá ser utilizada pelos órgão e entidades contratantes para realizar a estimativa de preços dos serviços a serem contratados.
- **Modelo de planilha de custos e formação de preços:** Trata-se de planilha a ser preenchida pelas licitantes para explicitação dos custos relacionados à prestação do serviços, nos moldes do Anexo VII-D da [Instrução Normativa SEGES/MP nº 5, de 26 de maio de 2017](#).

8.2.2 O Modelo de Contratação possui os seguintes documentos de referência relacionados:

- [Portaria SGD/MGI nº 6.055, de 26 de agosto de 2025](#) - Altera a [Portaria SGD/MGI nº 1.070, de 1º de junho de 2023](#), que estabelece modelo de contratação de serviços de operação de infraestrutura e atendimento a usuários de Tecnologia da Informação e Comunicação, no âmbito dos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.
- [Nota Metodológica do Modelo \(2025\)](#) - demonstração dos procedimentos e métodos adotados na realização de pesquisa de preços para obtenção de mapa de pesquisa salarial e do fator-k limite a serem adotados na estimativa do valor mensal de contratos que utilizam o Modelo de Contratação de Serviços de Operação de Infraestrutura e de Atendimento a Usuários de TIC instituído pela Secretaria de Governo Digital.
- [Mapa de Pesquisa Salarial \(2025\)](#) - Planilha auxiliar da Nota Metodológica - mapa de pesquisa salarial.
- [Memória de cálculo da composição do Fator k \(2025\)](#) - Planilha auxiliar da Nota Metodológica - Fator k.
- [Portaria SGD/MGI nº 6.680, de 04 de outubro de 2024](#) - Altera a [Portaria SGD/MGI nº 1.070, de 1º de junho de 2023](#), que estabelece modelo de contratação de serviços de operação de infraestrutura e atendimento a usuários de Tecnologia da Informação e Comunicação, no âmbito dos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

8.2.3. O Mapa de Pesquisa Salarial (2025), planilha auxiliar da Nota Metodológica vinculada à Portaria SGD/MGI nº 1.070/2023, constitui referência oficial de custos salariais para os perfis profissionais previstos no novo modelo de contratação de serviços de TIC. Este documento foi utilizado para a estimativa do valor da contratação, **servindo como base para a Planilha Simplificada para estimativa do valor mensal do serviço**. Trata-se, portanto, de pesquisa de preços estruturada, utilizada oficialmente para estimar o valor mensal dos contratos que seguem o Modelo de Contratação de Serviços de Operação de Infraestrutura e de Atendimento a Usuários de TIC.

8.2.3. Devido sua robustez, metodologia e recente atualização (agosto/2025), o **mapa de pesquisa salarial** da Secretaria de Governo Digital foi adotado como **fonte primária de estimativa salarial para a presente contratação**. Deste modo, o **mapa de pesquisa salarial da SGD/MGI será utilizado para a definição do preço de referência da licitação**, estabelecendo o patamar mínimo de presunção relativa de inexecuibilidade e na definição de parâmetros a serem utilizados na aplicação na modalidade de remuneração escolhida, qual seja, remuneração por Valor Fixo Mensal vinculado ao atendimento de Níveis Mínimos de Serviço (NMS).

8.2.4. Logo, os valores salariais para os perfis profissionais mínimos exigidos na contratação, derivam estritamente do referido Mapa de Pesquisa Salarial da Secretaria de Governo Digital (SGD), atualizado pela [Portaria SGD/MGI nº 6.055, de 26 de agosto de 2025](#). A adoção direta destes valores afasta a necessidade de realização de procedimentos específicos de pesquisa de preços (conforme IN SEGES/ME nº 65/2021) e garante que a estimativa do órgão reflita a real média praticada no mercado de TIC, assegurando a atratividade da licitação e a contratação de profissionais qualificados.

8.3. Obtenção do Valor de Referência da Licitação

8.3.1. Para estimar o custo da contratação foi utilizado a metodologia recomendada pela Portaria SGD/MGI nº 1.070/2023 (atualizada pelas Portarias nº 6.680/2024 e nº 6.055/2025), com a obtenção do salário de referência para cada perfil, multiplicado pelo **Fator k 2,28, conforme memória de cálculo descrita na planilha simplificada a seguir**, elaborada em conformidade com Anexo A do Modelo de Contratação, que constitui o Anexo I da Portaria.

ANEXO IV - PLANILHA SIMPLIFICADA PARA ESTIMATIVA DO VALOR MENSAL DO SERVIÇO (Valores de referência - Portaria SGD/MGI Nº 6.055)					
ITEM 1	Serviços continuados de suporte e operação de segurança da informação e defesa cibernética (Valores de referência - Portaria SGD/MGI nº 1.070, de 1º de Junho de 2023, atualizada pela Portaria SGD/MGI nº 6.680, de 04 de outubro de 2024)			ITEM	Fator-K
				(item 1.1):	1,98
				(item 1.2):	1,95
				(item 1.3):	1,99
				(item 1.4):	2,05
				Média do Fator K dos perfis	1,99
				Fator K (majorado em 0,29)	2,28
Perfil	Salário de referência	Quantidade	Custo unitário mensal do Perfil	Custo total mensal por Perfil	
	(A)	(B)	(C = A x Fator K)	(D = C x B)	
1.1	Gerente de suporte técnico de tecnologia da informação	R\$ 10.365,31	1	R\$ 23.632,91	R\$ 23.632,91
1.2	Administrador em segurança da informação - Sênior	R\$ 15.056,97	3	R\$ 34.329,89	R\$ 102.989,67
1.3	Administrador em segurança da informação - Pleno	R\$ 9.716,67	2	R\$ 22.154,01	R\$ 44.308,02
1.4	Administrador em segurança da informação - Júnior	R\$ 6.966,67	3	R\$ 15.884,01	R\$ 47.652,02
Quantitativo Total Equipe:			9	Valor fixo mensal:	R\$ 218.582,62
				(F)	
Custo Total do ITEM 1 (12 meses)					R\$ 2.622.991,44
Custo Total do ITEM 1 (36 meses)					R\$ 7.868.974,32

Tabela 36 - Planilha simplificada, estimativa dos custos da contratação para 12 meses.

8.3.2. A Portaria 1.070/2023 admite que o órgão adote um valor de Fator-K diferente da tabela da SGD, desde que isso seja justificado com a apresentação da respectiva memória de cálculo. Contudo, a Portaria impõe uma trava absoluta, determinando que o Fator-K (tanto na estimativa quanto na análise crítica das propostas das licitantes) não pode ser superior a 3.

8.3.3. Deste modo, para a estimativa do valor K, a equipe de planejamento utilizou a majoração em 0,29 da "Média do Fator K dos Perfis", que **fundamenta-se na necessidade internalização dos custos de deslocamentos técnicos e regime de prontidão (plantões eleitorais, atuação eventual e programada) ao valor fixo mensal, cuja previsão de uso estarão diluídos no cronograma financeiro ao longo do período contratual**. Esta medida observa a vedação de reembolso direto prevista no art. 5º, inciso V, da IN SGD/ME nº 94/2022, possibilitando margem para a condição de exequibilidade indispensável para contratação. Deste modo, o valor para 12 meses com fator k = 1,99 (média do Fator k dos perfis), é de **R\$ 2.289.365,33**. A diferença entre o Custo Total da contratação com Fator k majorado em 0,29 (fator k de 2,28) é de **R\$ 333.626,10**. A estimativa de custos com eventual deslocamento e atendimento e regime de plantão pode ser obtida pela licitante com base na série histórica do item 3.9.5 Histórico de diárias, passagens e Acionamentos Excepcionais Fora do Horário Regular" deste ETP.

8.3.4. A tabela detalha a composição financeira para os 9 perfis profissionais exigidos, contendo as seguintes colunas de cálculo para evidenciar o valor de referência final para 36 (trinta e seis) meses:

- Salário de Referência (A).
- Média do Fator K dos perfis (1,98).
- Fator K' (majorado em 0,29) = 2,28
- Custo Unitário Mensal do Perfil (C = B1 * Fator K').
- Custo Total Mensal do Perfil (D = C * Quantidade de profissionais)
- Valor fixo mensal = Σ Custo total mensal por Perfil
- Custo Total do ITEM 1 (12 meses) = 12 x Valor fixo mensal
- Custo Total do ITEM 1 (36 meses) = 3 x Custo Total do ITEM 1 (12 meses)

8.3.5. O valor fixo vinculado ao atendimento de Níveis Mínimos de Serviço, estimado para 36 meses é de **R\$ 7.868.974,32** (sete milhões oitocentos e sessenta e oito mil novecentos e setenta e quatro reais e trinta e dois centavos).

8.3.6. A planilha simplificada, utilizada anteriormente pela equipe de planejamento, não se confunde com a **Planilha de Custos e Formação de Preços** que deve ser entregue pelas empresas licitantes. No Anexo B do Modelo de Contratação (o qual integra o Anexo I da Portaria SGD/MGI nº 1.070/2023), constam orientações sobre a Planilha de Custos e Formação de Preços, a ser recebida durante a fase de seleção do fornecedor. A proposta ofertada pelo Licitante deve englobar todas as despesas diretas e indiretas necessárias à prestação do serviço, não havendo reembolso extra ou pagamento sob demanda para custos operacionais ou de deslocamento.

8.3.7. Para demonstrar a composição exata do seu preço, é obrigatório utilizar o Anexo VII - Modelo de Planilha de Preços e Formação de Custos constante do Termo de Referência. É por meio deste documento que a empresa deverá discriminar detalhadamente as Bonificações e Despesas Indiretas (BDI), os Encargos Sociais e todos os demais custos relacionados, com os respectivos valores devidamente adequados ao valor final da proposta vencedora

9. POSSÍVEIS IMPACTOS AMBIENTAIS E RESPECTIVAS MEDIDAS MITIGADORAS

Fundamentação: descrição de possíveis impactos ambientais e respectivas medidas mitigadoras, incluídos requisitos de baixo consumo de energia e de outros recursos, bem como logística reversa para desfazimento e reciclagem de bens e refugos, quando aplicável (inciso XII do § 1º do art. 18 da Lei 14.133/2021).

9.1. Nesta contratação não há qualquer tipo de impactos ambientais, ou eventuais processos relacionados a resíduos resultantes da contratação, tais como embalagens, logística reversa, dentre outros, uma vez que o objeto trata da contratação de serviços continuados de suporte e operação de segurança da informação, com remuneração baseada em Valor Fixo Mensal, condicionado ao cumprimento rigoroso de Níveis Mínimos de Serviço (NMS).

10. ESTRATÉGIA DA CONTRATAÇÃO DO OBJETO

- (X) Pregão Eletrônico Tradicional
- () Pregão Eletrônico - SRP

- () Adesão a Ata de Registro de Preços*
- () IRP (Intenção de Registro de Preços)
- () Contratação Direta - Inexigibilidade de Licitação (Art. 74 e incisos da Lei 14.133/2021)
- () Contratação Direta - Dispensa de Licitação (Art. 75 e incisos da Lei 14.133/2021)

10.1. Parcelamento do Objeto e Adjudicação

Conforme os §§ 2º e 3º do art. 40 da Lei 14.133/2021, o parcelamento do objeto é a regra e deve ser adotado sempre que se comprovar tecnicamente viável e economicamente vantajoso.

No presente caso, a contratação visa a prestação de serviços continuados de suporte e operação de segurança da informação, com remuneração baseada em **Valor Fixo Mensal**, condicionado ao cumprimento rigoroso de **Níveis Mínimos de Serviço (NMS)**. A execução será suportada por uma estrutura de **Perfis Profissionais Mínimos** definidos para garantir a continuidade operacional, sendo tecnicamente inviável e desvantajoso o parcelamento do objeto, visto que a fragmentação da equipe de defesa cibernética (*Blue Team*) comprometeria a visão integrada de riscos e a eficácia da resposta a incidentes.

O serviços que compõe o fornecimento funcionam de maneira única e integrada, sendo tecnicamente inviável e desvantajoso o parcelamento do serviço previsto na contratação. A contratação do serviço de forma separada criaria os seguintes riscos:

- Risco de descontinuidade operacional: a divisão de responsabilidades entre fornecedores distintos comprometeria a continuidade do monitoramento, da gestão de incidentes e da resposta a alertas, ampliando janelas de vulnerabilidade.
- Risco de lacunas na responsabilização técnica: em caso de incidente cibernético, haveria dificuldade de identificar o responsável e acionar o prestador adequado, atrasando a contenção e a recuperação do ambiente.
- Risco de quebra da visão integrada de segurança: a atuação segmentada impediria o tratamento unificado de políticas, controles e mecanismos de defesa, reduzindo a eficiência do gerenciamento de riscos e da postura de segurança institucional.

Deste modo, entende-se que a segurança cibernética exige uma visão integrada; fragmentar a responsabilidade entre múltiplos fornecedores criaria "lacunas de responsabilidade" e riscos de descontinuidade operacional, o que justifica a exceção à regra do parcelamento prevista no art. 40, § 3º da Lei 14.133/2021.

Nestes termos, o parcelamento da solução não é tecnicamente viável nem economicamente vantajoso, devendo a contratação ocorrer de forma global para o item único do objeto, que envolve várias categorias de serviços afins e perfis profissionais relacionados, de modo a garantir a integridade e a eficiência do suporte operacional em segurança da informação e proteção de dados.

10.2. Modelo de Adjudicação, Consórcio e Subcontratação

10.2.1. A adjudicação do objeto ocorrerá por **item único**, com critério de julgamento de **menor preço por item único**, em razão da indivisibilidade técnica do serviço. Caso houvesse adjudicação fragmentada, surgiriam riscos como:

- **Risco de descoordenação operacional**, com múltiplos fornecedores atuando sobre componentes interdependentes de segurança.
- **Risco de falhas de integração**, prejudicando a continuidade do monitoramento e a gestão unificada dos incidentes.
- **Risco de sobreposição ou lacunas de responsabilidades**, impactando diretamente o tempo de resposta em situações críticas.

10.2.2. Não será permitida a participação de empresas em consórcio. A adoção de consórcio implicaria riscos como:

- **Risco de diluição da responsabilização técnica**, dificultando a identificação do responsável em incidentes de segurança.
- **Risco de inconsistência na comprovação da qualificação técnica**, uma vez que a capacidade operacional poderia ser fragmentada entre empresas sem domínio integral da solução.
- **Risco de divergência contratual interna**, interferindo na governança e nas rotinas de atendimento.

10.2.3. Não será permitida a subcontratação do objeto. A autorização dessa prática acarretaria:

- **Risco de perda de controle sobre a execução**, comprometendo a conformidade com os protocolos e níveis de serviço contratados.
- **Risco de exposição a terceiros não avaliados tecnicamente**, aumentando a superfície de ataque e fragilizando a segurança institucional.
- **Risco de quebra da cadeia de confiança**, essencial para serviços críticos de segurança da informação, especialmente aqueles operados no modelo de Pagamento Fixo Mensal vinculado a Níveis de Serviço (NMS).

10.3. Modalidade e Tipo de Licitação

Nos termos do art. 29 da Lei 14.133/2021, é obrigatória a utilização da modalidade Pregão, em sua forma eletrônica, para a contratação de bens e serviços comuns. O serviço de suporte e operação de segurança da informação e defesa cibernética, embora especializado, é considerado comum, pois seus padrões de desempenho e qualidade podem ser objetivamente definidos no edital, com base em especificações usuais de mercado (níveis de serviço, prazos, cobertura, etc.). O critério de julgamento será o de menor preço.

10.4. Análise de Atas de Registro de Preços e Intenções de Registro de Preços (IRP)

Foi realizada consulta ao Portal Nacional de Contratações Públicas (PNCP) na data de 27/03/2026, e não foram encontradas Atas de Registro de Preços ou Intenções de Registro de Preços vigentes cujo objeto fosse compatível com a necessidade específica do TRE-PA.

Dada a especificidade do objeto, que se vincula a serviços de TIC, conclui-se pela inviabilidade de participação ou adesão a instrumentos de outros órgãos, sendo necessário o prosseguimento com licitação própria.

11. AVALIAÇÃO QUANTO À NECESSIDADE DE CLASSIFICAÇÃO DO ETP, NOS TERMOS DA LEI Nº 12.527/2011 (OBRIGATÓRIO)

11.1. Considerando não se tratar de licitação cujas informações nele constantes sejam sensíveis e imprescindíveis à segurança da sociedade e do Estado, não há necessidade de se atribuir qualquer tipo de classificação ao presente documento, nos termos dispostos na Lei nº 12.527/2011.

12. DECLARAÇÃO DA VIABILIDADE DA CONTRATAÇÃO

Fundamentação: A Declaração de viabilidade da contratação está disposta no inciso V do artigo 11 da IN 94/2022, e nela estabelece que haverá "a justificativa da solução escolhida, que deverá abranger a identificação dos benefícios a serem alcançados em termos de eficácia, eficiência, efetividade e economicidade."

Esta equipe de planejamento declara viável a presente contratação com base neste Estudo Técnico Preliminar, consoante o inciso V do art. 11 da IN 94, de 23 de dezembro de 2022, - SGD-ME.

Assinam eletronicamente este ETP, o integrante técnico, integrante demandante e o integrante administrativo, conforme equipe de planejamento designada nos autos, além da autoridade máxima da área de TIC.



Documento assinado eletronicamente por **CLEBER SOUSA FANJAS, Coordenador**, em 20/04/2026, às 09:42, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **ANTONIO EDIVALDO DE OLIVEIRA GASPAS, Coordenador**, em 20/04/2026, às 09:49, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site https://sei.tre-pa.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2995216** e o código CRC **901B9512**.

0009441-28.2024.6.14.8000

2995216v2