**PODER JUDICIÁRIO**
**JUSTIÇA DO TRABALHO**
**TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO**

NATACHA MORAES DE OLIVEIRA
23/10/2026 19:41
MAURICIO ANTONIOLI SCHMITZ
23/10/2026 19:50
CARLOS COSTA JORDÃO
23/10/2026 20:01
GEOVANE DUTRA DE SOUZA
23/10/2026 21:00
ALBERTO DANIEL MULLER
23/10/2026 21:41
CAROLINE ROCHA MOLINA
24/10/2026 12:35

versão janeiro/2026

# CONTRATAÇÃO DE TIC

# ESTUDO TÉCNICO PRELIMINAR

## 1. SOLUÇÃO DE TIC A SER CONTRATADA

**Solução integrada de Detecção e Resposta Estendidas a ataques cibernéticos (XDR) e Detecção e Resposta a Ameaças de Identidade (ITDR), incluindo serviços de treinamento, implantação, operação, monitoramento e sustentação, pelo período de 36 meses.**

## 2. DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

➢ A justificativa deve conter os fatos e fundamentos que especifiquem a necessidade de uso/utilização do bem/serviço, bem como os benefícios a serem alcançados, considerando o problema a ser resolvido, sob a perspectiva do interesse público.

A descrição da necessidade da contratação consta no Documento de Oficialização da Demanda.

## 3. ALINHAMENTO COM O PLANEJAMENTO ESTRATÉGICO DO TRIBUNAL

O alinhamento com o planejamento estratégico consta no Documento de Oficialização da Demanda.

## 4. PREVISÃO NO PLANO DE CONTRATAÇÕES ANUAL

A demanda está prevista no Plano de Contratações de TIC?

(x ) Sim: ID da Demanda nº SGTI-18/2026 e 67/2026 ( ) Não

A demanda está prevista no Plano de Contratações Anual – PCA?

(x ) Sim: ID da Demanda n° SGTI-18/2026 e 67/2026 [1] ( ) Não

## 5. CONTRATAÇÕES CORRELATAS OU INTERDEPENDENTES

[1] De acordo com o Artigo 13 da Portaria GP.TRT4 nº 1.633/2025, as demandas encaminhadas para contratação podem ter uma variação de até 20% em relação ao valor estimado no Plano de Contratações Anual (PCA). Variações negativas acima deste limite devem ser justificadas, enquanto variações positivas acima desse limite precisam de justificativa detalhada e prévio encaminhamento ao Subcomitê de Contratações para deliberação, conforme os procedimentos previstos na Seção V do Capítulo II da mencionada Portaria (alterações realizadas por meio do formulário contido no Anexo Único da Portaria, que deverá ser enviado à Secretaria de Administração).

**PODER JUDICIÁRIO**
**JUSTIÇA DO TRABALHO**
**TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO**

- ➢ Contratação correlata: aquela cujo objeto seja similar ou correspondente ao da contratação pretendida.
- ➢ Contratação interdependente: aquela que, por guardar relação direta na execução do objeto, deve ser contratada juntamente para a plena satisfação da necessidade da demanda ou que poderá afetar ou ser afetada pela execução da contratação pretendida.

Contratação correlata: PROAD 134/2024 - contratação de serviços de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos.

## 6. REQUISITOS DA CONTRATAÇÃO

- ➢ Relacionar e justificar os requisitos mínimos e essenciais para o atendimento da demanda.
- ➢ Justificar detalhadamente a necessidade dos requisitos que limitem a concorrência no certame.

| TIPOS | REQUISITOS | JUSTIFICATIVA |
|---|---|---|
| Negócio | Assegurar a proteção dos ativos tecnológicos, redes, nuvem e identidades de usuários do Tribunal, mediante monitoramento contínuo do ambiente tecnológico, identificação tempestiva de ameaças e vulnerabilidades, investigação e resposta aos incidentes de segurança cibernética | A dependência institucional dos serviços digitais torna necessária a identificação tempestiva de incidentes e a contenção de ameaças que afetem a disponibilidade, integridade, confidencialidade e autenticidade. Nesse contexto, a crescente complexidade das ameaças cibernéticas e a necessidade de proteger os ativos computacionais, as identidades digitais e as informações institucionais exigem mecanismos capazes de identificar comportamentos anômalos, correlacionar eventos de segurança e detectar ataques em componentes críticos do ambiente tecnológico. |
| Capacitação | Prover treinamento contemplando a administração e operação da solução contratada | Realização de treinamento, de forma a prover à equipe técnica do TRT condições adequadas para gerir e operar a solução de acordo com as melhores práticas. |
| Legais e Normativos | Lei n° 14.133/2021 | Lei que institui normas para licitações e contratos da Administração Pública. |
| | Resolução 468 de 15 de julho de 2022 do CNJ | Dispõe sobre as diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação pelos |

**PODER JUDICIÁRIO**
**JUSTIÇA DO TRABALHO**
**TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO**

| | | |
|---|---|---|
| | | órgãos submetidos ao controle administrativo e financeiro do Conselho Nacional de Justiça. |
| | Resolução 310 de 24 de setembro de 2021 do CSJT | Aprova o Guia de Contratações Sustentáveis para inclusão de critérios de sustentabilidade nas contratações de bens e serviços no âmbito da Justiça do Trabalho de primeiro e segundo graus. |
| | 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 a aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional. |
| | Portaria nº 2.714, de 15 de junho de 2022 do TRT4 | Regulamenta o procedimento de apuração de infrações e aplicação de penalidades administrativas no âmbito das licitações e contratações realizadas pelo Tribunal Regional do Trabalho da 4ª Região com base na Lei nº 14.133, de 1º de abril de 2021. |
| | Portaria GP.TRT4 Nº 1.737, de 31 de março de 2023 | Regulamenta, no âmbito do Tribunal Regional do Trabalho da 4ª Região, as licitações e contratações promovidas com fundamento na Lei nº 14.133/2021. |
| | Portaria GP.TRT4 nº 5042 de 2022 | Transforma o Comitê Gestor de TIC em Subcomitê de TIC do TRT4. |
| | Ato CSJT.GP.SG.SETIC N.o 53, DE 19 DE MAIO DE 2026 | Institui o conjunto de Soluções Essenciais de Tecnologia da Informação e Comunicação (TIC) na Justiça do Trabalho de primeiro e segundo graus. |

**PODER JUDICIÁRIO**
**JUSTIÇA DO TRABALHO**
**TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO**

| | | |
|---|---|---|
| Garantia e Manutenção | Garantir subscrições, atualização, correção de falhas, suporte técnico e serviços especializados pelo período contratado, com níveis de serviço mensuráveis. | Considerando a natureza da solução, que envolve subscrições de software e serviços especializados de segurança cibernética, torna-se indispensável a previsão de garantia e suporte integrais durante o período contratual, de modo a assegurar a contínua atualização da solução, o adequado funcionamento dos componentes contratados e o atendimento de eventuais falhas que possam comprometer a efetividade da solução.<br><br>A prestação contínua dos serviços de monitoramento, detecção, investigação e resposta a ataques cibernéticos é essencial para permitir a identificação tempestiva de ameaças e a adoção de medidas de contenção e resposta a incidentes de segurança, reduzindo os riscos de comprometimento dos ativos e das informações institucionais do Tribunal.<br><br>O estabelecimento de requisitos de suporte e níveis de serviço busca assegurar a continuidade operacional da solução, a qualidade dos serviços prestados e o cumprimento das obrigações da contratada durante toda a vigência contratual. |
| Temporais | A solução deverá estar implantada e iniciar sua operação no TRT4 até o dia 07/02/2027, em razão do encerramento da vigência do atual contrato nº 101/2024. Contudo, outros Tribunais possuem contratos vencendo antes dessa data, o que requer urgência na contratação. | Assegurar a continuidade dos serviços para este TRT da 4ª Região, bem como para os demais Tribunais participantes do certame. |
| Segurança da Informação /Transparência, acesso e de proteção aos dados | Atendimento às normas de Segurança deste Tribunal | Visando proteger as informações e dados institucionais, os serviços deverão ser executados em conformidade com as normas da |

**PODER JUDICIÁRIO**
**JUSTIÇA DO TRABALHO**
**TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO**

| | | |
|---|---|---|
| | | Política da Segurança da Informação e Comunicações deste Tribunal |
| Arquitetura Tecnológica (Especificações Técnicas - observar requisitos de qualidade, rendimento, compatibilidade, durabilidade e segurança) | Possuir integração operacional efetiva entre detecção e resposta em ativos (XDR), proteção de identidades (ITDR), correlação de eventos, inteligência de ameaças e fluxos de resposta, com tratamento unificado do contexto do incidente. | Ataques atuais frequentemente têm início no dispositivo e prosseguem por credenciais válidas; inversamente, o comprometimento de identidade pode preceder movimentação lateral e execução maliciosa em endpoints. Ferramentas que enxergam apenas uma dessas dimensões produzem investigações fragmentadas, duplicidade de alertas e atrasos entre a identificação de uma identidade comprometida e a contenção dos dispositivos afetados. A integração deve permitir associação verificável entre usuário, sessão, credencial, dispositivo, processo e evento; correlação temporal e contextual; priorização por criticidade; rastreabilidade da cadeia de ataque; e ações coordenadas, como isolamento de ativo e contenção de identidade, observadas autorizações do órgão. Não basta a mera troca de alertas por API: é necessário demonstrar a preservação do contexto, a latência compatível com os SLAs e a execução ponta a ponta de cenários relevantes. Uma arquitetura unificada elimina as dependências de conectores de terceiros, incompatibilidades de modelos de dados, versões e responsabilidades de suporte, além de facilitar orquestração e evolução integrada em um tempo de resposta mais curto capaz de responder a ameaças automatizadas por Inteligência Artificial. |
| | Demonstrar, por cenários de teste verificáveis, a correlação entre endpoint e identidade, a contenção cruzada, a segregação por órgão e a consulta de telemetria retida. | As funções decisivas para a eficácia do objeto precisam existir de forma operacional, e não somente como alegações comerciais. A verificação objetiva afasta plataformas que apenas agregam módulos sem integração real, com critérios técnicos isonômicos previamente definidos. Uma telemetria de tamanho adequado permite melhor |

**PODER JUDICIÁRIO**
**JUSTIÇA DO TRABALHO**
**TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO**

| | | |
|---|---|---|
| | | investigação de eventos, sendo o valor atual, de 7 dias, considerado pouco para as necessidades atuais. |
| | Permitir executar ações de contenção em endpoints e identidades a partir de uma mesma investigação, mantendo registro verificável de cada medida. | O comprometimento simultâneo de dispositivos e credenciais exige neutralizar os dois vetores para impedir reinfecção ou movimentação lateral. A resposta coordenada é um diferenciador objetivo de soluções verdadeiramente integradas, tornando um XDR essencial. |
| | Armazenamento da totalidade da telemetria ingerida — endpoint, rede, nuvem e identidade — em camada de armazenamento quente (hot storage), com disponibilidade imediata para consulta e correlação por meio da linguagem de busca nativa da plataforma, sem necessidade de reidratação, restauração ou processamento prévio, por período mínimo de 30 (trinta) dias | Investigações frequentemente dependem de reconstrução retrospectiva de eventos anteriores à descoberta do ataque. A disponibilidade imediata de um histórico contínuo de 30 dias permite correlacionar sinais dispersos, estabelecer cronologias e agir com rapidez, sem os atrasos de restauração de arquivos.<br>O armazenamento da telemetria em *hot storage* é essencial para investigação e mitigação tempestiva de incidentes, que ocorrem de forma muito rápida. Um período de 30 dias costuma ser um padrão mínimo de mercado. |
| | A solução deve implementar a coleta e análise de diferentes fontes de eventos. A coleta deve ser realizada para logs, dados de telemetria e/ou de rede, devendo ser possível coletar e analisar eventos das seguintes soluções presentes atualmente de forma predominante no ambiente do contratante | A solução deve prover funcionalidades de SIEM (Security Information and Event Management) nativas a fim de poder correlacionar outros tipos de eventos para melhor capacitação do ambiente. Também é necessária para atendimento às recomendações da ENSEC-PJ e a outros normativos de segurança da informação, trazendo maior assertividade no monitoramento de eventos maliciosos. Um SIEM se mantém como parte essencial para poder correlacionar eventos de fontes diferentes das suportadas pelo fabricante, a fim de que, em uma console única, prover inteligência e visibilidade. |
| | Possuir capacidade de Gerenciamento de Superfície | Ambientes de Tecnologia da Informação da Administração Pública passam por constantes transformações |

PROAD n. 6891/2026 DOC 13. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.MJPL.TKJV: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

**PODER JUDICIÁRIO**
**JUSTIÇA DO TRABALHO**
**TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO**

| | | |
|---|---|---|
| | de Ataque e Exposição de Ameaças (ASM) | (migração para nuvem, publicação de novos serviços digitais ao cidadão, sistemas legados e trabalho remoto/híbrido), criando pontos cegos operacionais (Shadow IT). Soluções de XDR que monitoram apenas ativos previamente cadastrados ou com agentes instalados deixam o Órgão vulnerável a vetores de entrada externos desconhecidos. O ASM provê visibilidade automatizada sob a perspectiva do atacante (outside-in), identificando domínios não catalogados, portas expostas indevidamente, certificados digitais expirados e serviços desatualizados antes que sejam explorados por terceiros. |
| | Utilizar NGAV (Antivírus de Próxima Geração) /EDR (Detecção e Resposta de Endpoint) com análise comportamental e aprendizado de máquina, capaz de detectar ameaças desconhecidas e execução sem arquivo. | Soluções de próxima geração, por meio de sua arquitetura baseada em aprendizagem de máquina, modelos preditivos de proteção e análise comportamental, são capazes de fornecer uma postura proativa mais efetiva da solução para a proteção dos *endpoints* contra ameaças avançadas conhecidas e desconhecidas, largamente utilizadas para realização de ataques maliciosos nos dias atuais. Quando toda esta capacidade é adicionada ao agente único da solução instalado nos *endpoints*, a detecção e resposta aos agentes maliciosos tornam-se mais eficazes e independentes de recursos internos para análise e identificação de riscos potenciais.<br><br>A identificação apenas por indicadores previamente catalogados não é capaz de acompanhar as variantes inéditas e técnicas que utilizam processos legítimos. A análise da sequência de comportamento de processos, memória e acesso a recursos oferece capacidade de prevenção antecipada e resposta a ataques sem assinatura previamente conhecida.<br><br>A defesa não pode depender |

**PODER JUDICIÁRIO**
**JUSTIÇA DO TRABALHO**
**TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO**

| | | |
|---|---|---|
| | | exclusivamente de assinaturas conhecidas, uma vez que as ameaças vêm sendo disseminadas de forma cada vez mais rápida e abrangente, exigindo soluções de detecção com capacidade de identificação de ameaças em tempo real. A automação que o ransomware impôs, e que agora é intensificada com a inteligência artificial, torna obsoleto o uso de hash, assinaturas e vacinas de arquivos, tendo em vista que ataques e programas maliciosos são customizados e dinâmicos, usando menos recursos. |
| | O agente de proteção instalado no endpoint não deverá depender do download, da atualização ou da aplicação recorrente e periódica de arquivos de vacinas, definições de vírus ou hashes estáticos para a execução da proteção preventiva em tempo real. | Principal característica das soluções de próxima geração NGAV, o agente único e independente de vacina ou assinatura reduz significativamente o consumo de recursos computacionais (memória e processamento) e de comunicação de dados envolvidos na proteção dos equipamentos, potencializando o seu uso para a finalidade a que se destinam.<br>Além disso, as soluções independentes de assinaturas e vacinas racionalizam drasticamente o esforço e os recursos envolvidos na gestão da solução, uma vez que a demanda de atualizações é apenas eventual.<br>Novas ameaças extrapolam a capacidade de heurísticas tradicionais e de vacinas, de forma que, para a proteção de novas ameaças, ou ameaças desconhecidas, fazem-se necessários mecanismos que independem de atualização de forma estrita. |
| | Assegurar continuidade da proteção nos endpoints em períodos de indisponibilidade de conectividade com a nuvem, com sincronização posterior da telemetria pertinente. | O ambiente inclui unidades descentralizadas, sujeitas a instabilidade de rede. A proteção local resiliente impede que falhas de comunicação se convertam imediatamente em ausência de defesa. |

**PODER JUDICIÁRIO**
**JUSTIÇA DO TRABALHO**
**TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO**

| | | |
|---|---|---|
| | Monitorar fontes externas, inclusive Deep/Dark Web, para identificar credenciais comprometidas, vazamentos e referências relevantes aos órgãos participantes. | O vazamento de credenciais pode preceder tentativas de acesso não autorizado e ataques de identidade. O monitoramento externo permite antecipar o bloqueio ou a redefinição de credenciais, aprimora a inteligência de ameaças e reduz riscos de acesso indevido e exposição institucional. |
| | Deve ser capaz de realizar avaliação da exposição da marca e vazamentos de informações na Deep/Dark Web, até um total de 20 marcas, submarcas ou nomenclaturas | A atuação institucional do TRT ocorre sob diferentes nomes, siglas e serviços, como PJe, PROAD e unidades de formação. A cobertura dessas denominações amplia a identificação de fraudes, menções e vazamentos vinculados à instituição que não apareçam sob seu nome formal, até como exigência do TCU quanto ao monitoramento de fraudes usando nomes institucionais. |
| | Proteger identidades em Active Directory local e Entra ID, identificar vulnerabilidades de credenciais, abuso de privilégios, ataques de autenticação e movimentação lateral, com análise contextual dos protocolos e das sessões. | O uso de credenciais legítimas por invasores pode contornar controles tradicionais de proteção dos dispositivos. A visibilidade sobre Kerberos, NTLM, alterações em diretórios, privilégios e padrões anômalos de acesso permite distinguir comportamento legítimo de uso indevido, detectar técnicas como password spraying, pass-the-hash e DCSync e conter a progressão de ataques. Enquanto um antivírus protege o dispositivo, um ITDR vai monitorar e agir contra uso de credenciais aparentemente legítimas, porém cujo comportamento denota um agente malicioso por trás. |
| | Registrar a trilha de auditoria de alertas, decisões automatizadas, acessos administrativos e ações de contenção, com exportação de evidências. | A auditabilidade permite a reconstrução do incidente, avaliação dos SLAs, responsabilização e preservação de evidências úteis à apuração administrativa e técnica. |

**PODER JUDICIÁRIO**
**JUSTIÇA DO TRABALHO**
**TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO**

| | | |
|---|---|---|
| | Disponibilizar recursos de IA integrados à solução para interpretar alertas, produzir hipóteses de investigação, enriquecer contextos e executar ou encaminhar fluxos de triagem e resposta, com supervisão e rastreabilidade. | O volume e a velocidade dos alertas exigem redução do esforço repetitivo e agilidade investigativa. Agentes de IA capazes de contextualizar sinais, sugerir causas e orientar ações diminuem o tempo de análise e ampliam a produtividade da operação 24x7. O registro das decisões e a supervisão de ações críticas preservam controle e auditabilidade. |
| Metodologia de trabalho e implantação da solução (Modelo de Prestação do Objeto) | Contratação e implementação independente para cada Tribunal participante do certame. | Prover instâncias, espaços lógicos ou controles equivalentes que assegurem autonomia administrativa, segregação de dados, políticas e incidentes por contratante, sem impor centralização operacional.<br>O registro de preços congrega órgãos autônomos com infraestruturas, calendários de contratação e políticas próprias. A gestão independente minimiza exposição cruzada e preserva competências decisórias. |
| | Disponibilizar os componentes centrais da solução na modalidade SaaS, com os sensores, coletores ou conectores necessários aos ambientes protegidos. | O modelo SaaS fornece atualização contínua, escalabilidade e acesso centralizado à análise de ameaças, reduzindo a necessidade de sustentação local da plataforma e favorecendo a operação distribuída entre órgãos participantes. |
| Capacitação e experiência profissional da equipe | Dispor de equipe técnica comprovadamente qualificada e certificada para implantação, operação e resposta a incidentes. | Uma solução altamente automatizada ainda exige profissionais capazes de interpretar evidências, calibrar regras, conduzir investigações e agir com segurança em ambientes institucionais complexos. Formação e experiência comprováveis reduzem erros de configuração, atrasos de contenção e indisponibilidades causadas por respostas inadequadas, assegurando o real aproveitamento da solução para a finalidade que está sendo contratada.<br>As certificações e qualificações profissionais constituem meios de comprovação da capacitação técnica da equipe responsável pela execução dos serviços, cuja natureza |

PROAD n. 6891/2026 DOC 13. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.MJPL.TKJV: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

**PODER JUDICIÁRIO**
**JUSTIÇA DO TRABALHO**
**TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO**

| | | |
|---|---|---|
| | | especializada exige conhecimentos específicos em segurança cibernética. A qualificação dos profissionais é indispensável para assegurar a adequada operação e sustentação da solução, bem como a efetividade das atividades de detecção, investigação e resposta a ataques cibernéticos, contribuindo para o cumprimento dos níveis de serviço estabelecidos e para a segurança do ambiente tecnológico do Tribunal. |
| | Comprovar experiência anterior compatível com o fornecimento, implantação e sustentação da solução em escala relevante. | A complexidade de ambientes distribuídos, a gestão simultânea de alertas críticos e a sustentação ininterrupta exigem capacidade operacional demonstrada. Atestados proporcionais ao porte e às características essenciais do objeto reduzem o risco de inadimplemento, sem exigir identidade absoluta com a contratação futura.<br>Nesse contexto, a comprovação da capacidade técnica é indispensável para reduzir os riscos associados à implantação e à operação da solução, assegurando que a empresa possui experiência para executar os serviços de forma adequada e atender às necessidades do Tribunal. |

PROAD n. 6891/2026 DOC 13. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.MJPL.TKJV: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

**PODER JUDICIÁRIO**
**JUSTIÇA DO TRABALHO**
**TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO**

| | | |
|---|---|---|
| | Comprovação de conformidade do fabricante da solução ofertada com padrões internacionais de segurança em ambiente de nuvem mediante a apresentação de Relatório SOC 2 Type II. | A exigência de apresentação de Relatório SOC 2 Type II justifica-se pela necessidade de comprovar que o fabricante da solução adota controles de segurança da informação e procedimentos de controle interno adequados à prestação de serviços em ambiente de nuvem. O relatório permite avaliar a implementação e a efetividade desses controles ao longo de um período, especialmente aqueles relacionados à segurança, à disponibilidade, à confidencialidade e à proteção dos dados tratados pela solução. Considerando que a contratação envolve o monitoramento contínuo de eventos e ameaças cibernéticas, bem como o tratamento de informações relevantes para a segurança institucional do Tribunal, a exigência contribui para reduzir riscos associados à hospedagem, ao processamento e ao armazenamento de dados em infraestrutura de terceiros, reforçando a confiabilidade e a segurança da solução contratada. |
| Demais requisitos | Deve ser vedada a subcontratação | A vedação à subcontratação visa assegurar a responsabilidade direta da contratada pela execução da solução integrada XDR e ITDR, cuja operação exige coordenação entre monitoramento, detecção, investigação e resposta a ameaças cibernéticas. A execução fragmentada por terceiros pode gerar dificuldades de integração, atrasos na resposta a incidentes e indefinição de responsabilidades.<br>Ressalva-se a atuação da fabricante nas atividades inerentes ao fornecimento, à operação, à manutenção, à atualização e ao suporte especializado de sua plataforma, permanecendo a contratada integralmente responsável pelo cumprimento das obrigações contratuais e dos níveis de serviço estabelecidos. |

**PODER JUDICIÁRIO**
**JUSTIÇA DO TRABALHO**
**TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO**

| | | |
|---|---|---|
| | Deve ser vedada a participação de empresas reunidas em consórcio | A vedação à participação de empresas reunidas em consórcio justifica-se pela necessidade de assegurar a execução integrada e coordenada do objeto, que compreende, além do fornecimento das subscrições de software, os serviços de implantação, treinamento, suporte técnico e monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos em regime ininterrupto.<br><br>A eficácia dos serviços gerenciados depende diretamente do conhecimento aprofundado da solução fornecida, de sua arquitetura, configurações, políticas de segurança e mecanismos de detecção e resposta. A eventual divisão dessas atividades entre empresas consorciadas poderia introduzir dificuldades de coordenação operacional, conflitos na identificação das causas de falhas, indefinições quanto às providências corretivas e atrasos no tratamento de incidentes críticos, especialmente nas situações que demandam atuação simultânea sobre diferentes componentes da solução.<br><br>Por sua vez, a execução integral do objeto sob responsabilidade de uma única empresa contratada favorece a padronização dos procedimentos, a continuidade operacional, a agilidade na resolução de problemas e a responsabilização direta pelo cumprimento dos níveis de serviço estabelecidos, evitando a transferência de responsabilidades entre diferentes executores.<br><br>Considerando que o objeto pode ser fornecido e operado por empresas especializadas do mercado de segurança cibernética, inclusive mediante atuação como parceiras autorizadas do fabricante, sem |

**PODER JUDICIÁRIO**
**JUSTIÇA DO TRABALHO**
**TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO**

| | | |
|---|---|---|
| | | necessidade de constituição de consórcio, **a vedação busca preservar a unidade de gestão e a eficiência operacional da contratação, sem exigir que a contratada seja a própria fabricante da solução**.<br><br>Dessa forma, justifica-se a vedação à participação de consórcios, nos termos do art. 15 da Lei nº 14.133/2021, visando assegurar a adequada coordenação dos serviços, a continuidade da proteção cibernética e a efetiva responsabilização da contratada pela execução integral do objeto. |

## 7. DESCRIÇÃO DE POSSÍVEIS IMPACTOS AMBIENTAIS E RESPECTIVAS MEDIDAS MITIGADORAS

- ➢ Analisar o Guia de Contratações Sustentáveis do TRT4.
- ➢ Exemplo de medidas mitigadoras: requisitos de baixo consumo de recursos naturais, logística reversa, reciclagem e destinação final dos resíduos gerados em decorrência da contratação, etc.

| IMPACTO AMBIENTAL/CRITÉRIO | MEDIDAS MITIGADORAS |
|---|---|
| <u>Equipamentos:</u><br>( ) Distribuição e racionalização do uso<br>( ) Custo total de propriedade<br>( ) Ciclo de vida do produto<br>( ) Composição<br>( ) Descarte e resíduos<br>( ) Embalagens<br>( ) Emissões<br>( ) Consumo elétrico | |
| <u>Suprimentos e consumíveis:</u><br>( ) Embalagens<br>( ) Durabilidade<br>( ) Logística reversa | |
| <u>Softwares:</u><br>( ) Transformação digital<br>( ) Acessibilidade | - Toda a documentação de software e base de conhecimento deverá estar disponível na internet, de forma a evitar impacto sobre recursos naturais decorrentes de produção de material de impressão, de pacotes e de desfazimento futuro. |

**PODER JUDICIÁRIO**
**JUSTIÇA DO TRABALHO**
**TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO**

| | |
|---|---|
| (x ) Outros | - A realização de treinamentos de forma remota racionaliza o consumo de recursos orçamentários do Tribunal e evita o deslocamento dos servidores, contribuindo para a sustentabilidade nesses dois aspectos |

**A contratação está alinhada com o Plano de Logística Sustentável?**
( x ) Sim
( ) Não
( ) Não se aplica

## 8. LEVANTAMENTO DE MERCADO
## CONSULTAS E ESTUDOS REALIZADOS

| AÇÃO | DOCUMENTAÇÃO GERADA |
|---|---|
| Consulta ao fornecedor NTT | E-mails e orçamentos |
| Consulta ao fornecedor Dropreal | E-mails e orçamentos |
| Consulta ao fornecedor Betta | E-mails e orçamentos |
| Consulta ao Painel de Preços ou Portal Nacional de Contratações Públicas (PNCP) | Foi realizada consulta ao PNCP, no qual foram encontradas as contratações descritas a seguir. |
| Consulta à contratação do STF | Contrato 17/2024 |
| Consulta à contratação do SEFAZ DF | Contrato 051/2026 |
| Consulta à contratação da FUNASA | ARP 03/2026 |
| Consulta ao Catálogo de Soluções de TIC com Condições Padronizadas | Objeto não consta no Catálogo de Soluções de TIC com Condições Padronizadas. |

## 9. LEVANTAMENTO DE MERCADO
## ANÁLISE DAS ALTERNATIVAS POSSÍVEIS E ESTIMATIVA DO VALOR DA CONTRATAÇÃO

| | |
|---|---|
| **Descrição da Solução 1** | **Contratação de Solução integrada de Detecção e Resposta Estendidas a ataques cibernéticos (XDR) e Detecção e Resposta a Ameaças de Identidade (ITDR), incluindo serviços de treinamento, implantação, operação, monitoramento e sustentação, pelo período de 36 meses.** |
| **Atendimento aos Requisitos** | A solução atende a todos os requisitos da contratação especificados neste documento?<br><br>( x ) Sim ( ) Não atende ao requisito |

**PODER JUDICIÁRIO**
**JUSTIÇA DO TRABALHO**
**TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO**

**Estimativa do valor da contratação**
(a eventual falta de estimativa de valor da solução deve ser justificada)

Valor estimado:

➢ Cálculo do Custo Total de Propriedade da Solução, considerando os custos inerentes ao ciclo de vida dos bens e serviços da solução, incluindo custos diretos e indiretos, a exemplo dos valores de aquisição dos ativos, insumos, garantia, manutenção, entre outros.

VALORES ESTIMADOS PARA O TRT4:

| Item | Descrição | CATMAT/ CATSERV | Classificação da Despesa | Unidade | Quantidade de compra inicial | Quantidade total do registro | Vlor unitário estimado | Total | Metodologia de cálculo |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos (XDR) pelo período de 36 meses | 27502 | 33904006 - Locação de software | Ativo monitorado | 0 | 6.500 | 648,59 | 4.215.835,00 | Média dos 2 menores valores |
| 2 | Subscrição do Módulo de Detecção e Resposta a Ameaças de Identidade (ITDR) pelo período de 36 meses | 27502 | 33904006 - Locação de software | Usuários ativos | 0 | 4.500 | 128,07 | 576.315,00 | Média dos 2 menores valores |
| 3 | Módulo de solução Agêntica para resposta, orquestração e triagem de eventos e incidentes | 26972 | 33904000 Serviços de TIC - PJ | Tokens | 0 | 72.000 | 11,49 | 827.280,00 | Média dos 2 menores valores |
| 4 | Ingestão de logs externos - Franquia de Gigabyte por dia por 36 meses | 26972 | 33904000 Serviços de TIC - PJ | Franquia de Gigabyte por dia | 0 | 1.000 | 930,49 | 930.490,00 | Menor valor |
| 5 | Serviço de treinamento na solução proposta | 3840 | 33904020 Treinamento/capacitação em TIC | Serviço único, por turma de treinamento | 0 | 1 | 29.444,46 | 29.444,46 | Média dos 3 menores valores |
| 6 | Serviço de implantação da solução proposta | 26972 | 33904000 Serviços de TIC - PJ | Serviço único por contratante | 0 | 1 | 43.450,00 | 43.450,00 | Média dos 2 menores valores |
| 7 | Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos | 25992 | 33904007 Manutenção corretiva/adaptativa e sustenção softwares | Serviço fixo para 2000 ativos monitorados por mês | 0 | 1 | 6.982,68 | 251.376,48 | Média, excluindo o menor e maior valor |
| 8 | | | | Serviço para 1000 ativos adicionais monitorados por mês | 0 | 5 | 4.081,87 | 734.736,60 | Média |
| | | | | | | | VALOR TOTAL ESTIMADO COMPRA INICIAL | 0,00 | |
| | | | | | | | VALOR TOTAL ESTIMADO REGISTRO | 7.608.927,54 | |

Memória de cálculo:

➢ Informar preços unitários referenciais, memórias de cálculo e documentos que lhe dão suporte.

Conforme metodologia de cálculo constante na tabela acima.

**Justificativa da escolha do tipo de solução a contratar**

Solução escolhida:

( x ) **Sim - Justificativa <u>técnica</u> e <u>econômica</u> da solução escolhida:**

➢ Explicar por quais motivos a solução é a que melhor atende à necessidade do Tribunal, mediante avaliação de custo-benefício, observados os princípios da padronização, eficácia, eficiência, efetividade e economicidade.

A solução integrada reúne XDR, ITDR, inteligência de ameaças, correlação de logs, automação de resposta e serviço gerenciado 24x7 em um ciclo operacional único. Sua superioridade decorre da necessidade de reconhecer e interromper cadeias de ataque que atravessam dispositivos, credenciais, diretórios e serviços de nuvem, preservando contexto, sequência temporal, evidências e

**PODER JUDICIÁRIO**
**JUSTIÇA DO TRABALHO**
**TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO**

| | |
|---|---|
| | comandos de resposta.<br><br>Em uma intrusão com furto de credencial em endpoint e posterior uso indevido de privilégios, a operação integrada permite vincular o processo de origem, a identidade envolvida e as sessões subsequentes, priorizar o incidente e executar o isolamento do equipamento e contenção de acesso, sem conciliar manualmente alertas e registros desconexos. A associação nativa de telemetria e incidentes reduz retrabalho investigativo, inconsistências de severidade e risco de respostas parciais.<br><br>A arquitetura integrada por um mesmo fabricante assegura a plena compatibilidade funcional e evolutiva entre os módulos; elimina a dependência de conectores de terceiros, alterações independentes de APIs e versões, erros na tradução de campos e dificuldades de orquestração; favorece cadeia unificada de desenvolvimento, testes, correção de defeitos e suporte especializado. A responsabilidade por incidentes de integração, integridade dos dados e ações de resposta fica claramente atribuída à contratada, com respaldo técnico do fabricante, eliminando conflitos quanto à origem de falhas que envolvam múltiplos componentes. Em segurança cibernética, a continuidade e a precisão da operação têm especial relevância porque atrasos e zonas cegas podem permitir a propagação do atacante antes da identificação de qual componente falhou.<br><br>A integração de todos os componentes da solução em um console único de gerenciamento proporciona uma visão centralizada e abrangente dos eventos e incidentes de segurança, permitindo correlacionar informações provenientes dos diferentes módulos, reconstruir a cadeia de execução dos ataques e assegurar a rastreabilidade das ações de investigação e resposta. Essa abordagem elimina a necessidade de alternância entre ferramentas e interfaces distintas, reduz a fragmentação das informações e agiliza a identificação, análise e contenção das ameaças. Além de proporcionar maior eficiência operacional, o gerenciamento unificado favorece a atuação coordenada dos mecanismos de proteção de ativos e identidades, reduzindo o tempo de resposta e o risco de falhas decorrentes da utilização de ferramentas isoladas. Pelo fato de os componentes estarem |

PROAD n. 6891/2026 DOC 13. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.MJPL.TKJV:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

**PODER JUDICIÁRIO**
**JUSTIÇA DO TRABALHO**
**TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO**

| | |
|---|---|
| | integrados e serem de um mesmo fabricante, o tempo de implantação é reduzido, o custo de entendimento e integração entre diferentes funcionalidades é nulo e a capacidade de informações mais assertivas é aumentada, pois integrar diferentes fabricantes pode ocasionar perda de informação ou impossibilidade de correlação.<br><br>A solução integrada também engloba requisitos que aprimoram o objeto de 2024: proteção de identidades híbridas (AD e Entra ID), contexto cruzado XDR/ITDR, ingestão e correlação de logs externos, armazenamento pesquisável imediato de telemetria, monitoramento de superfície de ataque, inteligência sobre credenciais expostas e triagem ou resposta assistida por IA. A contratação compartilhada padroniza capacidades e condições de suporte, enquanto cada Tribunal mantém ambiente e gestão próprios e escolhe o momento de adesão à ata de acordo com o encerramento de seus contratos.<br><br>Sob o aspecto econômico, o custo deve ser avaliado pelo ciclo de vida completo, e não apenas pelo somatório das subscrições: implantação, construção e manutenção de integrações, atendimento a incidentes, treinamento, esforço interno, atualizações, continuidade e riscos de indisponibilidade. A pesquisa de preços realizada para contratação do ITDR de forma isolada permite concluir que seu custo seria cerca de 50% superior ao módulo na composição integrada. Esse indicador reforça a potencial economicidade.<br><br>O resultado esperado é um ambiente com menos pontos de falhas operacionais, maior agilidade e custo total administrável.<br><br>Portanto, a arquitetura de fabricante único justifica-se com base em efeitos concretos: integração nativa de todos os componentes da solução, dados e respostas por ela produzidos, evolução sincronizada de versões, independência de conectores e responsabilização coerente pelo funcionamento ponta a ponta.<br><br>( ) Não - Justificativa: |

**PODER JUDICIÁRIO**
**JUSTIÇA DO TRABALHO**
**TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO**

| **Descrição da Solução 2** | **Prorrogação do contrato atual de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos** |
|---|---|
| **Atendimento aos Requisitos** | A solução atende a todos os requisitos da contratação especificados neste documento?<br><br>( ) Sim ( x ) Não atende a pelo menos os requisitos de negócio, de integração operacional, de telemetria, de antivírus de próxima geração - |
| **Estimativa do valor da contratação** (a eventual falta de estimativa de valor da solução deve ser justificada) | Valor estimado:.<br>➢ Cálculo do Custo Total de Propriedade da Solução, considerando os custos inerentes ao ciclo de vida dos bens e serviços da solução, incluindo custos diretos e indiretos, a exemplo dos valores de aquisição dos ativos, insumos, garantia, manutenção, entre outros.<br><br>R$ 4.498.684,04 para 36 meses<br><br>Memória de cálculo:<br>➢ Informar preços unitários referenciais, memórias de cálculo e documentos que lhe dão suporte.<br><br>Subscrições: R$ 1.162.672,40 anual por 3 anos = R$ 3.488.017,20<br>Serviço gerenciado: R$ 28.074,08 mensal por 3 anos = R$ 1.010.666,88 |
| **Justificativa da escolha do tipo de solução a contratar** | Solução escolhida:<br><br>( ) **Sim - Justificativa técnica e econômica da solução escolhida:**<br>➢ Explicar por quais motivos a solução é a que melhor atende à necessidade do Tribunal, mediante avaliação de custo-benefício, observados os princípios da padronização, eficácia, eficiência, efetividade e economicidade.<br><br>(x ) Não - Justificativa:<br><br>A continuidade do contrato atual apresenta apenas benefícios de curto prazo, limitados ao aproveitamento da experiência da equipe e ao menor esforço imediato de migração e manutenção temporária da cobertura existente.<br><br>Todavia, não atende, por si só, à necessidade institucional formalizada no Documento de Oficialização da Demanda para ampliar a proteção de ativos para uma arquitetura de detecção e |

**PODER JUDICIÁRIO**
**JUSTIÇA DO TRABALHO**
**TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO**

| | |
|---|---|
| | resposta que inclua também identidades digitais e ações coordenadas entre os dois domínios.<br><br>O Pregão Eletrônico nº 030/2024, conduzido pelo TRT da Segunda Região e que deu origem ao contrato atual, contemplou a contratação nacional de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos, com subscrições por faixa de ativos, monitoramento de rede, implantação, treinamento e serviços especializados. Sem exigir que a plataforma pertencesse a um mesmo fabricante, a solução contratada à época foi selecionada para atender aos requisitos que representavam as necessidades técnicas e o conjunto de especificações definidas no contexto de 2024.<br><br>Com efeito, a falta de integração nativa entre os componentes da solução atual é fonte de retrabalho e de eventual conflito de responsabilidade, o que se agrava pela execução do objeto por meio de um consórcio que, embora tenha sido permitido naquela contratação, constitui um ponto de dificuldade a ser mitigado na nova contratação.<br><br>O novo objeto, entretanto, estabelece patamar de abrangência e integração distinto. Acrescenta proteção especializada de identidades em Active Directory e nuvem (ITDR), correlação do uso de credenciais com eventos de endpoint, resposta coordenada sobre contas e equipamentos, monitoramento de exposição externa, inteligência sobre vazamento de credenciais, ingestão adicional de logs, consulta imediata a histórico de telemetria e automação assistida por IA. A prorrogação simples inviabiliza a obtenção de todo esse conjunto de novas funcionalidades, integrações e responsabilidades e não resolve a necessidade de assegurar interoperabilidade e cobertura contratual sobre componentes não previstos no objeto original.<br><br>Mesmo que parte dos acréscimos fosse obtida por aquisições complementares, surgiriam custos adicionais, necessidades de novas integrações e delimitação de responsabilidades que aproximariam essa hipótese da alternativa de contratação fragmentada. |

**PODER JUDICIÁRIO**
**JUSTIÇA DO TRABALHO**
**TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO**

| | |
|---|---|
| | Cumpre referir que este Tribunal chegou a dar início ao planejamento da contratação de uma solução de ITDR de forma isolada, com o objetivo de complementar a solução XDR atual. Porém, numa análise mais aprofundada do cenário, optou-se pela unificação dos objetos, devido à necessidade lógica da integração dessas soluções, o que não seria possível assegurar por meio de uma contratação isolada.<br><br>Pelas motivações acima expostas, a prorrogação do contrato atual mostra-se inviável para o atendimento das necessidades institucionais. |
| **Descrição da Solução 3** | **Contratação de solução XDR e ITDR separadamente** |
| **Atendimento aos Requisitos** | A solução atende a todos os requisitos da contratação especificados neste documento?<br><br>( ) Sim ( x ) Não atende a pelo menos os requisitos de integração operacional e de console única |
| **Estimativa do valor da contratação** (a eventual falta de estimativa de valor da solução deve ser justificada) | Valor estimado:.<br>➢ Cálculo do Custo Total de Propriedade da Solução, considerando os custos inerentes ao ciclo de vida dos bens e serviços da solução, incluindo custos diretos e indiretos, a exemplo dos valores de aquisição dos ativos, insumos, garantia, manutenção, entre outros.<br><br>Valor total estimado somente para a solução ITDR: R$ 2.623.247,50 |

| Nº Item | Descrição | Quant. | Unidade | Fonte 1 Valor Unitário | Fonte 2 Valor Unitário | Fonte 3 Valor Unitário | Fonte 4 Valor Unitário | Fonte 5 Valor Unitário | Metodologia de Cálculo | Valor Unit. Estimado | Valor Total Estimado |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Subscrição de uso de solução de proteção de identidades para 36 meses | 4500 | Contas de usuários ativas | 438,18 | 795,66 | 783,68 | 517,66 | 3.565,50 | média 2 menores valores | 477,92 | 2.150.637,00 |
| 2 | Serviço de implantação de solução de proteção de identidades | 1 | serviço | 55.430,00 | 84.006,98 | 20.900,00 | 185.000,00 | 38.852,00 | média 3 menores valores | 38.394,00 | 38.394,00 |
| 3 | Serviço gerenciado da solução de proteção de identidades | 36 | mês | 34.038,10 | 11.455,50 | 2.500,00 | 40.000,00 | 4.496,00 | mediana | 11.455,50 | 412.398,00 |
| 4 | Treinamento | 1 | turma | 180.900,00 | 7.637,00 | - | 40.000,00 | 36.000,00 | média 2 menores valores | 21.818,50 | 21.818,50 |
| VALOR TOTAL ESTIMADO PARA REGISTRO DE PREÇOS | | | | 3.433.511,60 | 4.084.511,98 | | 3.994.464,00 | 16.281.458,00 | | | 2.623.247,50 |
| | | | | | | | | | | DATA DO ORÇAMENTO ESTIMADO | 29/05/2026 |

**PODER JUDICIÁRIO**
**JUSTIÇA DO TRABALHO**
**TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO**

| | |
|---|---|
| | Memória de cálculo:<br>➢ Informar preços unitários referenciais, memórias de cálculo e documentos que lhe dão suporte.<br>Conforme metodologia de cálculo constante na tabela acima, incluindo pesquisa com fornecedores e contratos de órgãos públicos. |
| **Justificativa da escolha do tipo de solução a contratar** | Solução escolhida:<br><br>( ) **Sim - Justificativa técnica e econômica da solução escolhida:**<br>➢ Explicar por quais motivos a solução é a que melhor atende à necessidade do Tribunal, mediante avaliação de custo-benefício, observados os princípios da padronização, eficácia, eficiência, efetividade e economicidade.<br><br>( x ) Não - Justificativa:<br><br>A contratação separada de XDR e ITDR, com produtos de diferentes fabricantes e responsabilidades contratuais apartadas, poderia ampliar possibilidades de combinação de escolhas pontuais por especialidade. Contudo, na necessidade presente, introduz dependências de integração justamente nos processos em que a rapidez, integridade do contexto e previsibilidade de resposta são mais críticas.<br><br>A junção por conectores, APIs ou exportação de alertas não garante equivalência à correlação operacional de telemetria e identidade. Produtos distintos podem utilizar esquemas de dados, níveis de severidade, identificadores de usuário, carimbos temporais, políticas de retenção e modelos de incidente diferentes. Perdas ou atrasos de eventos, normalização incompleta e correlação parcial dificultam reconstruir a sequência entre execução em endpoint, autenticação, privilégio e movimento lateral. Também podem existir limites de API, filas, autenticação entre produtos, indisponibilidades de conectores e mudanças unilaterais de versão que afetem funções anteriormente operacionais. Essas dependências elevam a carga de testes, manutenção e resposta a falhas durante os 36 meses.<br><br>A separação também pode comprometer a eficácia da contenção: um alerta de identidade não necessariamente aciona isolamento do dispositivo, assim como a detecção em endpoint pode não |

PROAD n. 6891/2026 DOC 13. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.MJPL.TKJV:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

| | |
|---|---|
| | produzir bloqueio tempestivo da identidade em outro produto. Ações cruzadas exigem orquestrações adicionais, mapeamento de permissões, tratamento de erros, consistência de estado e validação de comandos; uma integração meramente visual ou de intercâmbio de alertas não atende ao resultado pretendido. Em caso de incidente crítico, a equipe gerenciada dependeria de diferentes consoles e equipes de suporte para identificar a causa da falha, recuperar conectores e executar as remediações, criando risco de transferência de responsabilidades entre fabricantes ou contratadas.<br><br>Além disso, a contratação de soluções apartadas acrescenta o ônus de demonstrar, implantar e manter, sob condições contratualmente verificáveis, o mesmo resultado ponta a ponta de uma arquitetura integrada, com disponibilidade, latência, trilhas de evidência, atualização de versões e responsabilidade de suporte preservadas. Quando os módulos são adquiridos em contratos separados, a fiscalização também precisa coordenar SLAs, incidentes, correções e mudanças entre múltiplos responsáveis, aumentando os riscos de atrasos e disputas sobre causalidade e penalidades.<br><br>Quanto ao custo total, devem ser somadas subscrições, conectores, desenvolvimento e testes de integrações, operação especializada de plataformas distintas, manutenção de compatibilidade, atendimento entre fornecedores e transição futura. O ETP registra cotações do ITDR isolado aproximadamente 50% superiores ao preço associado à solução integrada, resultado favorável à contratação conjunta, desde que as evidências comerciais e a equivalência dos escopos sejam documentadas.<br><br>Assim, embora a alternativa separada seja tecnicamente viável, ela se mostra menos vantajosa para o objeto e o modelo 24x7 pretendidos, em razão de maior risco de descontinuidade da correlação, complexidade de sustentação e fragmentação de responsabilidade, sem benefício econômico demonstrado que compense essas desvantagens. |

**PODER JUDICIÁRIO**
**JUSTIÇA DO TRABALHO**
**TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO**

## 10. ANÁLISE DOS REQUISITOS ADICIONAIS

| Requisito | Solução | Sim | Não | Não se aplica |
|---|---|---|---|---|
| A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública? | Solução 1 | X | | |
| | Solução 2 | X | | |
| | Solução 3 | X | | |
| A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software) | Solução 1 | | X | |
| | Solução 2 | | X | |
| | Solução 3 | | X | |
| A Solução é composta por software livre ou software público? (quando se tratar de software) | Solução 1 | | X | |
| | Solução 2 | | X | |
| | Solução 3 | | X | |
| A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG? | Solução 1 | | | X |
| | Solução 2 | | | X |
| | Solução 3 | | | X |
| A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital) | Solução 1 | | | X |
| | Solução 2 | | | X |
| | Solução 3 | | | X |
| A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos) | Solução 1 | | | X |
| | Solução 2 | | | X |
| | Solução 3 | | | X |

## 11. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

- ➢ Explicitar a solução que melhor atenderá à necessidade do Tribunal.
- ➢ Relacionar as exigências relacionadas à manutenção e à assistência técnica.
- ➢ Justificar, se for o caso, a vigência contratual inicial por prazo superior a 12 (doze) meses.

A solução compreende a contratação integrada de subscrições de software para Detecção e Resposta Estendidas (XDR) e Detecção e Resposta a Ameaças de Identidade (ITDR), incluindo recursos de automação e orquestração de respostas, ingestão de logs externos e serviços de implantação, treinamento, suporte e monitoramento gerenciado de segurança cibernética em regime 24x7x365.

**PODER JUDICIÁRIO**
**JUSTIÇA DO TRABALHO**
**TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO**

A solução deverá proporcionar visibilidade unificada do ambiente tecnológico do TRT, permitindo a correlação de eventos, a investigação de incidentes e a execução coordenada de ações de contenção e resposta a ameaças.

A contratada deverá assegurar garantia e suporte integrais durante toda a vigência contratual, abrangendo todos os componentes da solução, correção de falhas, atualizações e suporte técnico corretivo, proativo e consultivo, com atendimento 24x7x365, sem limitação de chamados ou custos adicionais.

A vigência inicial de 36 meses justifica-se pela natureza continuada dos serviços e pela necessidade de assegurar estabilidade operacional, continuidade da proteção e aproveitamento dos investimentos realizados na implantação e integração da solução, evitando os custos e riscos decorrentes de substituições frequentes de tecnologias críticas de segurança.

## 12. ESTIMATIVA DAS QUANTIDADES

- Justificar as quantidades da contratação, informando as memórias de cálculo e os documentos que lhes dão suporte, que considerem interdependências com outras contratações, de modo a possibilitar economia de escala;
- Exemplos de memórias de cálculos: consumos registrados em exercícios anteriores, número de usuários, dimensões, etc.

| Item | Descrição | Unidade | Qtd compra inicial | Qtd total do registro TRT4 | Justificativa / Memória de Cálculo |
|---|---|---|---|---|---|
| 1 | Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos (XDR) pelo período de 36 meses | Ativo monitorado | 0 | 6.500 | O quantitativo foi definido com base no inventário atual dos equipamentos a serem protegidos pela solução, totalizando 6.211 ativos, com uma margem aproximada de 4,7% para acomodar eventuais ampliações do ambiente tecnológico durante a vigência da contratação. |
| 2 | Subscrição do Módulo de Detecção e Resposta a Ameaças de Identidade (ITDR) pelo período de 36 meses | Usuários ativos | 0 | 4.500 | O quantitativo de referência corresponde a 4.250 identidades ativas atualmente existentes no Tribunal, abrangendo os usuários institucionais que deverão ser protegidos pela solução, inclusive em suas interações com os serviços de diretório Active Directory e os ambientes de identidade em nuvem. Considerando a necessidade de cobertura das identidades existentes e |

PROAD n. 6891/2026 DOC 13. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.MJPL.TKJV: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

**PODER JUDICIÁRIO**
**JUSTIÇA DO TRABALHO**
**TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO**

| | | | | | |
|---|---|---|---|---|---|
| | | | | | de eventuais ampliações durante a vigência contratual, foi considerado o quantitativo de 4.500 identidades. |
| 3 | Módulo de solução Agêntica para resposta, orquestração e triagem de eventos e incidentes | Tokens | 0 | 72.000 | A estimativa considerou o consumo de recursos de inteligência artificial destinados à automatização de atividades de triagem, investigação, correlação de informações e resposta a eventos e incidentes de segurança.<br>Como referência inicial de dimensionamento, foram consideradas faixas de consumo associadas à quantidade de ativos protegidos, nas quais ambientes com 5.000 a 9.999 ativos correspondem a uma previsão de 875 tokens.<br>Considerando que o consumo desses recursos poderá variar conforme a quantidade, a complexidade e a severidade dos eventos investigados, bem como aumentar significativamente durante incidentes de segurança, adotou-se um quantitativo estimado de 2.000 tokens/mês, de modo a proporcionar reserva de capacidade para situações de maior demanda operacional. |
| 4 | Ingestão de logs externos | Franquia de Gigabyte por dia | 0 | 1000 | O quantitativo estimado considera a necessidade de incorporar à solução os registros de eventos gerados por componentes da infraestrutura de rede e segurança do Tribunal. Foi prevista capacidade de ingestão de até 1000 GB por dia, considerando o conjunto das fontes externas a serem integradas e a necessidade de acomodar variações no volume de eventos gerados. |
| 5 | Serviço de treinamento na solução proposta | Serviço único, por turma de treinamento | 0 | 1 | Prevê-se a realização de uma turma de treinamento, com capacidade para até 10 participantes, destinada à capacitação da equipe técnica do TRT4 nas funcionalidades de administração, operação, investigação e resposta a incidentes da solução contratada. |
| 6 | Serviço de implantação da solução proposta | Serviço único por contratante | 0 | 1 | O quantitativo corresponde à necessidade de uma implantação inicial da solução no Tribunal, independentemente da quantidade de ativos e identidades abrangidos. |

PROAD n. 6891/2026 DOC 13. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.MJPL.TKJV: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

**PODER JUDICIÁRIO**
**JUSTIÇA DO TRABALHO**
**TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO**

| | | | | | |
|---|---|---|---|---|---|
| 7 | Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos | Serviço fixo para 2000 ativos monitorados por mês | 0 | 1 | O dimensionamento considera o quantitativo máximo de 6.500 ativos previstos para proteção pelo XDR.<br>O item 7 corresponde à faixa inicial de atendimento, para 2.000 ativos monitorados. E o item 8 prevê unidades adicionais de atendimento, cada uma correspondente a até 1.000 ativos.<br>Foi estimada a contratação de uma unidade do item 7, acrescida de cinco unidades do item 8, proporcionando capacidade de atendimento de até 7.000 ativos, suficiente para abranger os 6.500 ativos previstos no item 1. |
| 8 | | Serviço para 1000 ativos adicionais monitorados por mês | 0 | 5 | |

A quantidade por órgão consta no anexo do ETP.

## 13. JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DA CONTRATAÇÃO

- ➢ O parcelamento do objeto deverá ser adotado sempre que a sua divisão seja tecnicamente viável e economicamente vantajosa e não represente perda de economia de escala.
- ➢ O não parcelamento do objeto deverá ser devidamente justificado com a demonstração das razões técnicas, administrativas e econômicas que o inviabilizem.
- ➢ Devem ser considerados:
  - a responsabilidade técnica;
  - o custo para a Administração de vários contratos frente às vantagens da redução de custos, com divisão do objeto em itens;
  - o dever de buscar a ampliação da competição e de evitar a concentração de mercado.

Considerando que o objeto compreende uma solução integrada de segurança cibernética, composta por subscrições de software de um único fabricante e serviços especializados de implantação, treinamento, suporte e monitoramento, detecção, investigação e resposta a incidentes, **justifica-se o não parcelamento pela elevada interdependência técnica e operacional entre seus componentes**.

A efetividade dos serviços gerenciados depende diretamente da configuração, integração e operação dos módulos da solução, exigindo atuação coordenada e responsabilidade integral sobre os processos de detecção e resposta. O parcelamento entre diferentes fornecedores introduziria riscos adicionais de descontinuidade operacional, dificuldades na identificação e resolução de falhas, conflitos de responsabilidades e atrasos no tratamento de incidentes críticos, com potenciais prejuízos ao cumprimento dos níveis de serviço contratados.

Sob o aspecto econômico e administrativo, a contratação conjunta favorece ganhos de escala, racionaliza os custos de gestão e fiscalização contratual e evita despesas

PROAD n. 6891/2026 DOC 13. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.MJPL.TKJV:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

**PODER JUDICIÁRIO**
**JUSTIÇA DO TRABALHO**
**TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO**

adicionais decorrentes da coordenação de múltiplos fornecedores. Embora o parcelamento possa ampliar a participação de empresas especializadas em segmentos específicos, seus potenciais benefícios não justificam, neste caso, os riscos operacionais e os custos adicionais associados à fragmentação da execução.

**Dessa forma, conclui-se que a contratação em lote único representa a alternativa tecnicamente mais adequada e economicamente mais vantajosa**, assegurando a integração operacional, a continuidade dos serviços e a responsabilização direta da contratada pela execução integral do objeto.

**Há justificativa para a NÃO participação ou criação de cota para ME/EPP?**

(x) Não se aplica, pois não é um bem de natureza divisível; trata-se de solução com interdependência técnica.

( ) Não

( ) Sim – Justificativa:

-

## 14. DEMONSTRATIVO DOS RESULTADOS PRETENDIDOS

➢ Em termos de economicidade e de melhor aproveitamento dos recursos humanos, materiais ou financeiros disponíveis.

| Tipo | Detalhamento |
|---|---|
| ( ) Ganho de produtividade | |
| ( x ) Redução de esforço | A utilização de console única de gerenciamento, com visão integrada dos eventos e incidentes, reduzirá o esforço necessário para consultar diferentes ferramentas, correlacionar informações e realizar análises manuais. O serviço especializado de monitoramento e resposta também contribuirá para reduzir a sobrecarga da equipe técnica do Tribunal nas atividades operacionais de segurança cibernética. |
| ( ) Redução de custo | |
| ( ) Redução de uso de recursos | |
| ( x ) Melhoria de controle | A solução permitirá centralizar a visualização e o acompanhamento dos eventos, alertas e incidentes de segurança cibernética, incluindo aqueles relacionados a ativos computacionais e identidades digitais. A disponibilidade de registros, informações de investigação e acompanhamento das ações de resposta contribuirá para melhorar a rastreabilidade, a supervisão e a gestão dos incidentes. |

**PODER JUDICIÁRIO**
**JUSTIÇA DO TRABALHO**
**TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO**

| | |
|---|---|
| ( x ) Redução de riscos | A contratação proporcionará acesso a recursos tecnológicos integrados e a serviço especializado de monitoramento, investigação e resposta a ataques cibernéticos, fortalecendo a capacidade do Tribunal de prevenir, identificar, analisar e tratar incidentes de segurança, bem como de preservar a continuidade dos serviços institucionais. |
| ( x ) Cumprimento de determinação legal e/ou administrativa | A contratação contribuirá para o aprimoramento dos controles de segurança da informação e de proteção dos dados tratados pelo Tribunal, apoiando o atendimento às obrigações aplicáveis de proteção de dados pessoais e às diretrizes institucionais de segurança cibernética do Poder Judiciário. |
| ( ) Melhoria/adequação nas instalações físicas | |
| ( ) Outro | |

## 15. CARACTERIZAÇÃO DE SERVIÇOS OU FORNECIMENTOS CONTÍNUOS

➢ Serviços contratados e compras realizadas pela Administração Pública para a manutenção de atividades administrativas decorrentes de necessidades permanentes ou prolongadas.

( ) Não se aplica
( x ) Sim – Justificativa:

Os serviços objeto da contratação possuem natureza contínua, uma vez que se destinam ao atendimento de necessidades permanentes de segurança cibernética do Tribunal e são essenciais à proteção do ambiente computacional, das informações institucionais e à continuidade das atividades administrativas e judiciárias.

A contratação abrange subscrições de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos (XDR), módulo de detecção e resposta a ameaças de identidade (ITDR), recursos de automação e orquestração, ingestão de logs e serviços de monitoramento e resposta a incidentes. Esses recursos atuam de forma integrada para identificar ameaças relacionadas aos ativos computacionais e às identidades digitais, permitindo a análise dos eventos e a adoção tempestiva de medidas de resposta.

Dessa forma, diante do caráter permanente da necessidade de segurança cibernética, da importância do monitoramento ininterrupto, dos impactos decorrentes de eventual interrupção e da necessidade de manutenção integrada da solução e dos serviços especializados, caracteriza-se o objeto como contratação de natureza contínua.

PROAD n. 6891/2026 DOC 13. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.MJPL.TKJV:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

**PODER JUDICIÁRIO**
**JUSTIÇA DO TRABALHO**
**TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO**

| 16. PROVIDÊNCIAS A SEREM ADOTADAS PELA ADMINISTRAÇÃO PREVIAMENTE À FORMALIZAÇÃO DA CONTRATAÇÃO (NECESSIDADE DE ADEQUAÇÃO DO AMBIENTE) | |
|---|---|
| **Tipo** | **Detalhamento** |
| ( ) Necessidade de capacitação de gestores e fiscais da contratação | Não se aplica |
| ( ) Instalação elétrica | Não se aplica |
| ( ) Instalação lógica | Não se aplica |
| ( ) Alteração de layout (espaço físico / mobiliário) | Não se aplica |
| ( ) Infraestrutura tecnológica | Não se aplica |
| ( ) Logística de implantação | Não se aplica |
| ( ) Outra | Não se aplica |
| ( ) Não se aplica | Não se aplica |

| 17. RECURSOS NECESSÁRIOS À CONTINUIDADE DO OBJETO CONTRATADO (PROVIDOS PELO TRIBUNAL) | | | |
|---|---|---|---|
| **Descrição** | **Material / Humano** | **Próprio / A ser contratado** | **Área Responsável** |
| Equipe de Gestão e Fiscalização | Humano | Próprio | SGTI |
| Equipe técnica que administrará a solução | Humano | Próprio | Coordenadoria de Segurança da Informação e Proteção de Dados |
| Computadores Desktops e servidores | Material | Próprio | SGTI |

| 18. TRANSIÇÃO E ENCERRAMENTO CONTRATUAL | | |
|---|---|---|
| **Ações Necessárias no Encerramento Contratual** | **Responsável** | **Prazo** |
| ( ) Entrega de versões finais dos produtos | | |
| ( ) Transferência final de conhecimentos | | |
| ( ) Entrega de documentação | | |
| ( ) Devolução de recursos materiais | | |
| ( ) Revogação de perfis de acesso | | |

**PODER JUDICIÁRIO**
**JUSTIÇA DO TRABALHO**
**TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO**

| | | |
|---|---|---|
| ( ) Eliminação de caixas postais | | |
| ( x ) Realizar a exportação em lote de todos os logs, dados de telemetria, eventos e dados de rede que ainda estejam armazenados na solução e abrangidos pelo período de retenção contratado, formato aberto, como xml, csv ou texto puro, podendo ser abertos e lidos em editores de texto sem a necessidade de softwares proprietários ou plugins. | Contratada | 30 dias antes do encerramento do contrato |

## 19. ESTRATÉGIA DE CONTINUIDADE EM EVENTUAL INTERRUPÇÃO CONTRATUAL

**Em caso de interrupção contratual, descreva como serão afetados os serviços prestados pelo Tribunal:**
A interrupção dos serviços poderá comprometer a capacidade do TRT-4 de monitorar continuamente seu ambiente computacional, detectar atividades suspeitas, investigar incidentes e executar ações tempestivas de contenção e resposta a ataques cibernéticos.
A descontinuidade dessas atividades poderá aumentar o risco de comprometimento de sistemas, informações processuais e dados institucionais, bem como de indisponibilidade de recursos tecnológicos essenciais ao funcionamento do Tribunal. Como consequência, poderão ocorrer prejuízos ao regular andamento dos processos judiciais, à realização de atos processuais e ao acesso aos sistemas por magistrados, servidores, advogados e jurisdicionados, afetando a continuidade e a eficiência da prestação jurisdicional.

**Ações de contingência e seus respectivos responsáveis:**
Em caso de interrupção contratual, em primeiro lugar deverão ser avaliados os impactos da descontinuidade, priorizados os ativos e serviços críticos e adotadas as medidas de proteção e monitoramento disponíveis no ambiente do Tribunal, utilizando os recursos e ferramentas institucionais existentes. Deverá, ainda, reforçar o acompanhamento dos registros e alertas de segurança disponíveis, realizar o tratamento prioritário de incidentes identificados e adotar medidas de contenção compatíveis com os riscos verificados.
Responsável: CSIPD/SGTI

Paralelamente deverão ser avaliadas as medidas necessárias ao restabelecimento dos serviços, incluindo a realização de nova contratação ou contratação emergencial.
Responsável: SGTI

## 20. ESTRATÉGIA DE INDEPENDÊNCIA DA ADMINISTRAÇÃO

| | |
|---|---|
| ( x ) Transferência de Conhecimento | (Este campo deverá descrever a forma de transferência de conhecimento. Ex: acompanhamento das atividades de instalação e implantação, manuais, treinamentos fornecidos pela contratada, etc.)<br>A transferência de conhecimento se dará por meio do acompanhamento das atividades de instalação e implantação; e na realização do treinamento. |

**PODER JUDICIÁRIO**
**JUSTIÇA DO TRABALHO**
**TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO**

| | |
|---|---|
| ( ) Direitos de Propriedade Intelectual e Direitos Autorais (Lei nº 9.610/1998) | Não se aplica |

## 21. SEGURANÇA DA INFORMAÇÃO E CONTROLE DE ACESSO

( x ) Durante a prestação do objeto, a Contratada deverá observar as Políticas de Controle de Acesso definidas pelo Tribunal.

( x ) A contratada deverá firmar Termo de Compromisso com a Segurança da Informação.

## 22. POSICIONAMENTO CONCLUSIVO SOBRE A ADEQUAÇÃO DA CONTRATAÇÃO

| | | |
|---|---|---|
| Com base nos estudos preliminares, a contratação demonstra-se adequada para o atendimento da demanda? | ( x ) Sim<br>( ) Não | Justificativa:<br>A contratação pretendida atende aos requisitos necessários para atendimento da demanda do Tribunal, conforme justificado no item "ANÁLISE DAS ALTERNATIVAS POSSÍVEIS" deste documento. |

## Equipe de Planejamento da Contratação

| | |
|---|---|
| *Documento assinado digitalmente*<br>CARLOS COSTA JORDÃO<br>Integrante Demandante | *Documento assinado digitalmente*<br>MAURÍCIO ANTONIOLI SCHMITZ<br>Integrante Técnico |
| *Documento assinado digitalmente*<br>GEOVANE DUTRA DE SOUZA<br>Integrante Administrativo da Secretaria de Administração | *Documento assinado digitalmente*<br>ALBERTO DANIEL MÜLLER<br>Integrante Administrativo da Secretaria-Geral de Tecnologia e Inovação / Requisitante |

## Subcomitê de TIC

*Documento assinado digitalmente*
NATACHA MORAES DE OLIVEIRA
Coordenadora do Subcomitê de Tecnologia da Informação e Comunicações

**PODER JUDICIÁRIO**
**JUSTIÇA DO TRABALHO**
**TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO**

# ANEXO DO ETP
# QUANTIDADES ESTIMADAS POR ÓRGÃO

| Item | Descrição | Unidade | Quantidade total para registro | | | | | | | | | | | | | | | | | TOTAL |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | TRT1 | TRT3 | TRT4 | TRT5 | TRT6 | TRT7 | TRT9 | TRT10 | TRT11 | TRT14 | TRT15 | TRT16 | TRT18 | TRT19 | TRT20 | TRT21 | TRT22 | TST | |
| 1 | Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos (XDR) pelo período de 36 meses | Ativo monitorado | 7.000 | 6.500 | 6.500 | 6.500 | 4.000 | 2.500 | 6.000 | 2.000 | 2.000 | 1.600 | 8.000 | 1.500 | 2.700 | 1.500 | 1.500 | 2.000 | 1.000 | 6.000 | 68.800 |
| 2 | Subscrição do Módulo de Detecção e Resposta a Ameaças de Identidade (ITDR) pelo período de 36 meses | Usuários ativos | 6.000 | 9.450 | 4.500 | 5.000 | 2.500 | 2.400 | 5.000 | 1.500 | 1.220 | 1.300 | 7.000 | 1.100 | 2.700 | 1.300 | 1.300 | 2.000 | 900 | 5.000 | 60.170 |
| 3 | Módulo de solução Agêntica para resposta, orquestração e triagem de eventos e incidentes | Tokens | 72.000 | 72.000 | 72.000 | 72.000 | 36.000 | 36.000 | 72.000 | 36.000 | 40.000 | 36.000 | 86.000 | 36.000 | 25.200 | 13.500 | 30.000 | 25.200 | 14.400 | 60.000 | 834.300 |
| 4 | Ingestão de logs externos - Franquia de Gigabyte por dia por 36 meses | Franquia de Gigabyte por dia | 1.000 | 1.000 | 1.000 | 1.000 | 150 | 500 | 1.000 | 1.000 | 400 | 400 | 1.000 | 400 | 450 | 25 | 100 | 150 | 15 | 1.000 | 10.590 |
| 5 | Serviço de treinamento na solução proposta | Serviço único, por turma de treinamento | 2 | 2 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | 1 | 1 | 1 | 1 | 1 | 1 | 3 | 23 |
| 6 | Serviço de implantação da solução proposta | Serviço único por contratante | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 18 |
| 7 | Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos | Serviço fixo para 2000 ativos monitorados por mês | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 18 |
| 8 | | Serviço para 1000 ativos adicionais monitorados por mês | 5 | 5 | 5 | 5 | 2 | 1 | 4 | 1 | 0 | 0 | 6 | 0 | 1 | 0 | 0 | 0 | 0 | 4 | 39 |

PROAD n. 6891/2026 DOC 13. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.MJPL.TKJV: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml