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

CARLOS COSTA JORDÃO
23/10/2026 18:26

CAROLINE ROCHA MOLINA
23/10/2026 19:44

versão janeiro/2026

CONTRATAÇÃO DE TIC

DOCUMENTO DE OFICIALIZAÇÃO DA DEMANDA

1. SOLUÇÃO DE TIC A SER CONTRATADA[1]

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. IDENTIFICAÇÃO DA UNIDADE DEMANDANTE

Unidade/Setor:	Coordenadoria de Segurança da Informação e Proteção de Dados/ SGTI
Responsável:	Carlos Costa Jordão
Integrante Demandante indicado:	Carlos Costa Jordão

3. JUSTIFICATIVA DA NECESSIDADE DA CONTRATAÇÃO[2]

A digitalização das atividades do Poder Judiciário, consolidada no processo judicial eletrônico e nas iniciativas do Programa Justiça 4.0, tornou os recursos de Tecnologia da Informação e Comunicação (TIC) essenciais à prestação jurisdicional. Nesse cenário, a disponibilidade, a integridade e a confidencialidade dos sistemas e das informações constituem requisitos fundamentais para a continuidade dos serviços judiciários e administrativos.

Paralelamente, as ameaças cibernéticas evoluíram significativamente em sofisticação, velocidade e capacidade de comprometimento dos ambientes tecnológicos, cenário agravado pela crescente utilização da inteligência artificial na execução e no aperfeiçoamento dos ataques. Além da exploração de vulnerabilidades em equipamentos e sistemas, destacam-se ameaças relacionadas ao comprometimento de credenciais, ao uso indevido de identidades legítimas, ao abuso

[1] Este campo deve conter a descrição de forma resumida do objeto a ser contratado.

[2] A justificativa deve conter os fatos e fundamentos que especifiquem a necessidade da contratação, bem como os benefícios a serem alcançados, considerando o problema a ser resolvido, sob a perspectiva do interesse público.

de privilégios de acesso e à exploração de mecanismos de autenticação, inclusive em serviços e aplicações em nuvem.

No âmbito do Poder Judiciário brasileiro, incidentes de segurança registrados nos últimos anos, inclusive em Tribunais do Trabalho, demonstram que essas ameaças representam riscos concretos à continuidade dos serviços, à proteção de dados e à confiabilidade dos sistemas judiciais.

Diante desse cenário, torna-se necessário fortalecer os mecanismos de segurança cibernética por meio de uma abordagem integrada, capaz de proporcionar visibilidade abrangente dos ambientes tecnológicos, identificar comportamentos suspeitos, correlacionar eventos de diferentes origens e executar ações tempestivas de contenção e resposta a incidentes.

Para essa finalidade, propõe-se a contratação de uma solução integrada de **Detecção e Resposta Estendidas (XDR — Extended Detection and Response)** e **Detecção e Resposta a Ameaças de Identidade (ITDR — Identity Threat Detection and Response)**, acompanhada dos serviços especializados necessários à sua implantação, operação, monitoramento e sustentação.

A tecnologia XDR proporciona capacidades de proteção, detecção, investigação e resposta a ameaças em diferentes componentes do ambiente tecnológico, incluindo estações de trabalho, servidores e outras fontes de informação integradas à solução. Mediante a correlação de eventos, a aplicação de inteligência sobre ameaças e a automação de ações de segurança, permite identificar ataques complexos e reduzir o tempo necessário à sua contenção.

Complementarmente, a tecnologia ITDR amplia essas capacidades para as infraestruturas de identidade, especialmente os serviços de diretório Active Directory e os ambientes de identidade em nuvem. Sua finalidade é identificar comportamentos anômalos e tentativas de comprometimento de identidades, como utilização indevida de credenciais, abuso de privilégios, movimentação lateral e exploração de mecanismos de autenticação e autorização.

A integração das capacidades de XDR e ITDR constitui requisito fundamental da solução pretendida, permitindo correlacionar eventos de segurança dos dispositivos e demais componentes tecnológicos com as atividades relacionadas às identidades que acessam esses recursos. Essa integração favorece a identificação de ataques que exploram simultaneamente equipamentos, credenciais e privilégios de acesso, além de viabilizar respostas coordenadas sobre os componentes envolvidos,

reduzindo lacunas de visibilidade, complexidade operacional e tempo de contenção das ameaças.

A iniciativa encontra respaldo na **Resolução CNJ nº 396/2021**, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ). Em seu art. 11, a norma estabelece diretrizes para elevar o nível de segurança das infraestruturas críticas, contemplando, entre outras medidas, a utilização de tecnologias capazes de consolidar registros de auditoria provenientes de diferentes fontes, automatizar ações de segurança e fornecer inteligência para análise de eventos e ameaças cibernéticas.

De forma complementar, a **Portaria CNJ nº 162/2021** aprovou protocolos e manuais de referência para implementação da ENSEC-PJ, incluindo o Manual de Referência de Proteção de Infraestruturas Críticas. Esse documento recomenda práticas como a centralização de registros de auditoria, a utilização de ferramentas de correlação e análise de eventos, a identificação de comportamentos anômalos e o aperfeiçoamento contínuo dos mecanismos de monitoramento, diretrizes diretamente relacionadas às capacidades pretendidas com a contratação.

No âmbito da Justiça do Trabalho, a necessidade da contratação é reforçada pelo **Ato CSJT.GP.SG.SETIC nº 53, de 19 de maio de 2026**, que institui o conjunto de Soluções Essenciais de Tecnologia da Informação e Comunicação (TIC) da Justiça do Trabalho de primeiro e segundo graus. Em seu Anexo Único, o Ato classifica expressamente como de **prioridade ALTA** as soluções de proteção de endpoints (item 18), contemplando funcionalidades de detecção e resposta a incidentes (EDR/XDR), bem como as soluções de gestão de identidades e acessos (item 20) e de gestão de eventos de segurança (item 21). Essas capacidades estão diretamente relacionadas ao objeto da presente contratação, evidenciando seu alinhamento às prioridades institucionais estabelecidas pelo CSJT para o fortalecimento da segurança cibernética, a prevenção de incidentes e a continuidade dos serviços judiciais e administrativos.

A iniciativa também se alinha à **Resolução CNJ nº 370/2021**, que instituiu a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD) para o período de 2021 a 2026, contemplando, entre seus objetivos estratégicos, o aprimoramento da segurança da informação e da gestão de dados, da infraestrutura tecnológica e das aquisições e contratações de TIC.

A solução pretendida também observa as boas práticas estabelecidas pela **ABNT NBR ISO/IEC 27002:2022**, especialmente os controles relacionados à inteligência de ameaças (5.7), gestão de identidades (5.16), informações de

autenticação (5.17), direitos de acesso (5.18), avaliação de eventos de segurança (5.25), resposta a incidentes (5.26), coleta de evidências (5.28), proteção de registros (5.33), registros de eventos (8.15) e monitoramento de atividades (8.16).

Considerando que os serviços tecnológicos que sustentam a atividade jurisdicional permanecem sujeitos a ameaças cibernéticas ininterruptamente, a disponibilidade de mecanismos automatizados de detecção e resposta deve ser acompanhada de capacidade especializada de monitoramento e atuação contínua.

Nesse sentido, a contratação deverá contemplar **serviços gerenciados de segurança cibernética, com monitoramento, análise e resposta a incidentes em regime de 24 horas por dia, sete dias por semana, para todos os órgãos participantes**, de modo a assegurar o acompanhamento contínuo dos eventos e o tratamento tempestivo das ameaças, inclusive fora do horário regular de expediente do TRT.

Além de proporcionar cobertura operacional ininterrupta, esses serviços permitirão incorporar conhecimento especializado e boas práticas de segurança, assegurando maior aproveitamento das funcionalidades da solução e contribuindo para o aprimoramento contínuo dos mecanismos de detecção e resposta. Também permitirão que as equipes internas de TIC concentrem seus esforços nas demais atividades estratégicas e operacionais sob sua responsabilidade.

A contratação deverá ser realizada por meio do **Sistema de Registro de Preços, sob gerenciamento do Tribunal Regional do Trabalho da 4ª Região, com participação de outros órgãos da Justiça do Trabalho**, adotando-se o modelo de contratação compartilhada que busca proporcionar ganhos de escala, economicidade, padronização de requisitos técnicos, racionalização dos procedimentos administrativos e melhores condições de contratação, mediante a consolidação das demandas dos órgãos participantes em um único procedimento licitatório.

Embora a contratação seja compartilhada, cada órgão manterá seu ambiente de segurança e sua gestão operacional independentes, preservando sua autonomia administrativa, as particularidades de sua infraestrutura tecnológica e o controle sobre seus próprios eventos, incidentes e políticas de segurança.

A utilização do Sistema de Registro de Preços permitirá, ainda, que **cada órgão participante formalize sua contratação no momento mais adequado às suas necessidades**, considerando os contratos e soluções de segurança atualmente existentes, seus respectivos prazos de vigência, as condições de transição tecnológica e a disponibilidade orçamentária. Dessa forma, a adoção da nova solução poderá

ocorrer de maneira planejada e individualizada, sem exigir a substituição simultânea das ferramentas em todos os órgãos participantes.

Diante do exposto, **justifica-se a contratação compartilhada de solução integrada de XDR e ITDR, acompanhada de serviços gerenciados de segurança cibernética em regime ininterrupto**, como medida necessária ao aprimoramento das capacidades de prevenção, detecção, investigação e resposta a ameaças, à redução dos riscos de comprometimento dos ambientes tecnológicos e à preservação da continuidade, confiabilidade e segurança dos serviços prestados pela Justiça do Trabalho à sociedade.

4. QUANTIDADE A SER CONTRATADA E JUSTIFICATIVA[3]

Os quantitativos estimados para o TRT4 foram definidos considerando o parque tecnológico atualmente existente, o número de identidades digitais a serem protegidas, a necessidade de integração de fontes adicionais de eventos de segurança e os serviços necessários à implantação, operação e sustentação da solução.

Para os itens de subscrição, foram consideradas as necessidades atuais do Tribunal e margens destinadas a acomodar eventuais ampliações durante a vigência contratual de 36 meses, observadas as características e unidades de licenciamento de cada componente.

Os quantitativos apresentados referem-se exclusivamente às necessidades do TRT4, não contemplando as demandas dos demais órgãos participantes do Registro de Preços, que serão consolidadas separadamente para composição dos quantitativos totais da licitação.

Item 1 — Subscrição de solução de Detecção e Resposta Estendidas (XDR), pelo período de 36 meses

Quantidade: 6.500 ativos

O quantitativo foi definido com base no inventário atual dos equipamentos a serem protegidos pela solução, compreendendo:

- Estações de trabalho e notebooks: 5.521;

[3] Estimativas das quantidades para a contratação, acompanhadas das memórias de cálculo e dos documentos que lhes dão suporte, que considerem interdependências com outras contratações, de modo a possibilitar economia de escala.

- Servidores Linux: 517;
- Servidores Windows: 173.

O parque totaliza **6.211 ativos**, sendo previstas 6.500 licenças, o que representa uma margem aproximada de 4,7% para acomodar eventuais ampliações do ambiente tecnológico durante a vigência da contratação.

Item 2 — Subscrição de solução de Detecção e Resposta a Ameaças de Identidade (ITDR), pelo período de 36 meses

Quantidade: 4.500 identidades

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 de eventuais ampliações durante a vigência contratual, o quantitativo a registrar deverá ser igual ou superior ao universo atual de **4.500 identidades**.

Item 3 — Módulo de IA Agêntica para triagem, orquestração e resposta a eventos e incidentes de segurança

Quantidade: 2.000 tokens/mês

A estimativa considera 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.

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.

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.

A unidade de consumo e os critérios de dimensionamento deverão ser uniformizados no Termo de Referência, de forma a permitir a comparação objetiva das propostas dos diferentes fornecedores.

PROAD n. 6891/2026 DOC 2. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.GKDM.LTLP:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

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

Item 4 — Capacidade de ingestão de registros de eventos (logs) de fontes externas

Quantidade: 1.000 GB/dia

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, especialmente o firewall central Check Point e os equipamentos de segurança associados à infraestrutura da rede de longa distância SD-WAN, distribuída nas unidades judiciárias e administrativas do Rio Grande do Sul.

A ingestão desses registros permitirá ampliar a capacidade de correlação entre eventos de rede, equipamentos e identidades, proporcionando maior visibilidade sobre atividades suspeitas e possíveis incidentes de segurança.

Foi prevista capacidade de ingestão de até **1.000 GB por dia**, considerando o conjunto das fontes externas a serem integradas e a necessidade de acomodar variações no volume de eventos gerados.

Item 5 — Serviço de treinamento na solução contratada

Quantidade: 1 turma

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.

O quantitativo é suficiente para atender à equipe diretamente responsável pela gestão e acompanhamento da solução no Tribunal.

Item 6 — Serviço de implantação da solução

Quantidade: 1 serviço

Prevê-se um serviço de implantação para o ambiente tecnológico do TRT4, contemplando as atividades necessárias à instalação ou disponibilização, configuração, integração e entrada em operação dos componentes contratados.

O quantitativo corresponde à necessidade de uma implantação inicial da solução no Tribunal, independentemente da quantidade de ativos e identidades abrangidos.

Itens 7 e 8 — Serviços gerenciados de monitoramento, detecção, investigação e resposta a incidentes de segurança

PROAD n. 6891/2026 DOC 2. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.GKDM.LTLP:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

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

Quantidades: 1 unidade do item 7 e 5 unidades do item 8

O dimensionamento considera o quantitativo máximo de 6.500 ativos previstos para proteção pelo XDR, com prestação dos serviços gerenciados em regime ininterrupto, 24 horas por dia, sete dias por semana.

O item 7 corresponde à faixa inicial de atendimento, destinada aos órgãos com até 2.000 ativos monitorados. Para os órgãos que ultrapassarem esse limite, o item 8 prevê unidades adicionais de atendimento, cada uma correspondente a até 1.000 ativos.

No caso do TRT4, a contratação de uma unidade do item 7, acrescida de cinco unidades do item 8, proporcionará capacidade de atendimento de até 7.000 ativos, suficiente para abranger os 6.500 ativos previstos no item 1.

O dimensionamento decorre das faixas de prestação dos serviços gerenciados, que são contratadas em unidades inteiras, de acordo com o porte do ambiente tecnológico de cada órgão participante.

5. PREVISÃO DA DATA EM QUE DEVE SER ENTREGUE O BEM OU INICIADA A PRESTAÇÃO DOS SERVIÇOS

Data 07/02/2027 Motivo: A solução deverá estar implantada e iniciar sua operação em 07/02/2027, em razão do encerramento da vigência do atual contrato nº 101/2024

( ) Não se aplica

6. ALINHAMENTO COM O PLANO DE CONTRATAÇÕES

A demanda está prevista no Plano de Contratações de TIC?

(x) Sim: ID SGTI-18/2026 e 67/2026 ( ) Não

7. INDICAÇÃO DA FONTE DE RECURSOS

( ) Programa de Apreciação de Causas da Justiça do Trabalho

( ) Manutenção do Sistema Nacional de TI

(x) Segurança da Informação nas Unidades do Poder Judiciário - SIUPJ

( ) Outra:

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

8. ALINHAMENTO ESTRATÉGICO[4]

A contratação está alinhada a algum objetivo do Plano Estratégico Institucional do Tribunal?

( ) Sim – Qual?

- **( )** Fortalecer a comunicação e as parcerias institucionais
- **( )** Promover o trabalho decente e a sustentabilidade
- **( )** Garantir a duração razoável do processo
- **( )** Promover a integridade e a transparência em relação aos atos de gestão praticados
- **( )** Assegurar o tratamento adequado dos conflitos trabalhistas
- **( )** Garantir a efetividade do tratamento das demandas repetitivas
- **( )** Fortalecer a governança e a gestão estratégica
- **( )** Aperfeiçoar a gestão orçamentária e financeira
- **( )** Incrementar modelo de gestão de pessoas em âmbito nacional
- **(x)** Aprimorar a governança de TIC e a proteção de dados

(X) Não

A contratação está alinhada a algum objetivo da Estratégia Nacional de TIC do Poder Judiciário?

(X) Sim – Qual?

- **( )** Aumentar a Satisfação dos Usuários do Sistema Judiciário;
- **( )** Promover a Transformação Digital;
- **( )** Reconhecer e Desenvolver as Competências dos Colaboradores;
- **( )** Buscar a Inovação de Forma Colaborativa;
- **( )** Aperfeiçoar a Governança e a Gestão;
- **( )** Aprimorar as Aquisições e Contratações;
- **(X)** Aprimorar a Segurança da Informação e a Gestão de Dados;
- **( )** Promover Serviços de Infraestrutura e Soluções Corporativas.

( ) Não

RESPONSÁVEL DA ÁREA DEMANDANTE

Documento assinado digitalmente
CARLOS COSTA JORDÃO
Coordenador de Segurança da Informação e Proteção de Dados

[4] A consulta detalhada aos objetivos estratégicos pode ser realizada no Plano Estratégico Institucional 2021-2026, disponível no site do Tribunal (Planejamento Estratégico).