KARINA DURIGON
24/11/2026 15:12

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

PREGÃO ELETRÔNICO Nº: 27/2026
COMPRAS.GOV.BR Nº 316/2026

PROCESSO ADMINISTRATIVO Nº: 6891/2026

UASG: 080014

OBJETO: Registro de preço para aquisição de solução integrada de detecção e resposta estendidas a ataques cibernéticos (XDR) e detecção e resposta a ameaças de identidade (ITDR)

VALOR TOTAL ESTIMADO DA CONTRATAÇÃO:
R$ 74.913.935,98, para todos os participantes (órgão gerenciador e órgãos participantes), para o período de 36 meses.

DATA DA SESSÃO PÚBLICA:
Dia 10/12/2026 às 11h (horário de Brasília)

CRITÉRIO DE JULGAMENTO:
Menor preço por grupo

MODO DE DISPUTA:
Aberto e Fechado

TRATAMENTO FAVORECIDO ME/EPP/EQUIPARADAS: NÃO

MARGEM DE PREFERÊNCIA PARA ALGUM ITEM: NÃO

PROGRAMA NACIONAL DE PREVENÇÃO À CORRUPÇÃO PARTICIPANTE

A adesão do TRT da 4ª Região ao
Programa Nacional de Prevenção à Corrupção
reforça o compromisso institucional com a transparência, a ética e a integridade.

Acesse aqui o Guia de Conduta de Ética e Integridade para Licitantes, Fornecedores e Contratados

Sumário

1. DO OBJETO 3
2. DA PARTICIPAÇÃO NA LICITAÇÃO 7
3. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO 9
4. DO PREENCHIMENTO DA PROPOSTA 11
5. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES 12
6. DA FASE DE JULGAMENTO 15
7. DA FASE DE HABILITAÇÃO 17
8. DOS RECURSOS 22
9. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES 23
10. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO 26
11. DO REGISTRO DE PREÇOS 27
12. DA CONTRATAÇÃO 29
13. DO PAGAMENTO 30
14. DA GARANTIA CONTRATUAL 32
15. DA PROTEÇÃO DE DADOS 32
16. DA GESTÃO E FISCALIZAÇÃO DO CONTRATO 32
17. DAS DISPOSIÇÕES GERAIS 32

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO
Coordenadoria de Licitações e Contratos
PROAD 6891/2026
UASG 080014

Torna-se público que o **TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO** (TRT da 4ª Região), por meio da Coordenadoria de Licitações Contratos, sediado na Av. Praia de Belas nº 1.100, em Porto Alegre/RS, inscrito no CNPJ sob o nº 02.520.619/0001-52, realizará licitação, na modalidade **PREGÃO**, na forma **ELETRÔNICA**, pelo sistema de **REGISTRO DE PREÇOS**, nos termos da Lei nº 14.133/2021, e demais legislação aplicável e, ainda, de acordo com as condições estabelecidas neste Edital.

1. DO OBJETO

1.1. O objeto da presente licitação é o Registro de Preço para 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, sob o regime de empreitada por preço unitário, conforme condições e exigências estabelecidas no Anexo I - Termo de Referência, e seus anexos, nos quantitativos que seguem:

Grupo	Item	Descrição	Unidade	Quantidade total a registrar	Preço Unitário máximo admitido (R$)	Preço Total máximo admitido (R$)
1	1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos (XDR).	Ativo monitorado	**61.500**	648,59	39.888.285,00
	2	Subscrição do Módulo de Detecção e Resposta a Ameaças de Identidade (ITDR).	Usuários ativos	**54.850**	128,07	7.024.639,50
	3	Módulo de solução Agêntica para resposta, orquestração e triagem de eventos e incidentes	Tokens	**748.300**	11,49	8.597.967,00
	4	Ingestão de logs externos	Franquia de Gigabyte por dia	**9.590**	930,49	8.923.399,10
	5	Serviço de treinamento na solução proposta	Serviço único, por turma de treinamento	**21**	29.444,46	618.333,66

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

	6	Serviço de implantação da solução proposta	Serviço único por contratante	**17**	43.450,00	738.650,00
	7	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Serviço fixo para 2000 ativos monitorados por mês	**612***	6.982,68	4.273.400,16
	8	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Serviço para 1000 ativos adicionais monitorados por mês	**1.188***	4.081,87	4.849.261,56
PREÇO GLOBAL DO GRUPO 1 MÁXIMO ADMITIDO PARA 36 MESES (R$)						**74.913.935,98**

* ***A quantidade dos itens 7 e 8 decorrem da multiplicação da quantidade para registro de preços de cada Regional participante por 36 meses previsto para a contratação.***

1.2. A Ata de Registro de Preços decorrente desta licitação terá como órgão gerenciador o Tribunal Regional do Trabalho da 4ª Região e como órgãos participantes os Tribunais elencados a seguir, cujos quantitativos, por órgão, estão discriminados no subitem 1.5 do Termo de Referência:

1.2.1. Tribunal Regional do Trabalho da 1ª Região - TRT1 (UASG: 080009)
1.2.2. Tribunal Regional do Trabalho da 3ª Região - TRT3 (UASG: 080008)
1.2.3. Tribunal Regional do Trabalho da 5ª Região - TRT5 (UASG: 080007)
1.2.4. Tribunal Regional do Trabalho da 6ª Região - TRT6 (UASG: 080006)
1.2.5. Tribunal Regional do Trabalho da 7ª Região - TRT7 (UASG: 080004)
1.2.6. Tribunal Regional do Trabalho da 9ª Região - TRT9 (UASG: 080012)
1.2.7. Tribunal Regional do Trabalho da 10ª Região - TRT10 (UASG: 080016)
1.2.8. Tribunal Regional do Trabalho da 11ª Região - TRT11 (UASG: 080002)
1.2.9. Tribunal Regional do Trabalho da 14ª Região - TRT14 (UASG: 080015)
1.2.10. Tribunal Regional do Trabalho da 16ª Região - TRT16 (UASG 080018)
1.2.11. Tribunal Regional do Trabalho da 18ª Região - TRT18 (UASG 080020)
1.2.12. Tribunal Regional do Trabalho da 19ª Região - TRT19 (UASG 080022)
1.2.13. Tribunal Regional do Trabalho da 20ª Região - TRT20 (UASG 080023)
1.2.14. Tribunal Regional do Trabalho da 21ª Região - TRT21 (UASG 080021)
1.2.15. Tribunal Regional do Trabalho da 22ª Região - TRT22 (UASG 080024)
1.2.16. Tribunal Superior do Trabalho - TST (UASG:080001).

1.3. Conforme demonstrado no quadro constante no subitem 1.1, supra, o valor total estimado do registro de preços para 36 meses envolvendo todos os participantes (órgão gerenciador e órgãos participantes) é de R$ 74.913.935,98 (setenta e quatro milhões, novecentos e treze mil, novecentos e trinta e cinco reais e noventa e oito centavos). O valor total estimado para o TRT da 4ª Região é de R$ 7.608.927,54 (sete milhões, seiscentos e oito mil, novecentos e vinte e sete reais e cinquenta e quatro centavos).

1.4. As especificações técnicas constam no Anexo I do Termo de Referência.

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

1.5. A disponibilização das subscrições e serviços **(itens 1, 2, 3 e 4**), e a execução completa da Implantação da Solução (**item 6**) devem ocorrer em até **60 dias** a contar da assinatura do contrato.

1.5.1. A vigência das subscrições dos itens 1 e 2 será de **36 meses**, contados a partir da data de emissão do Termo de Recebimento Definitivo do objeto, após a conclusão da implantação e a entrada da solução em produção, em pleno funcionamento, de acordo com as especificações do fabricante da solução e em conformidade com os requisitos da contratação.

1.5.1.1. As subscrições poderão ser disponibilizadas de forma anual, hipótese em que cada disponibilização deverá assegurar o período de vigência correspondente, observadas as condições estabelecidas na contratação.

1.5.1.2. Durante a etapa de implantação, é facultado à contratada o uso de licenças temporárias (trial), visando não onerá-la antes da efetiva entrada em produção, evitando o cômputo precoce do prazo de vigência das subscrições, desde que tais licenças não apresentem limitações ao uso inicial da solução.

1.5.1.3. Eventuais atrasos na implantação motivados pelo Contratante não postergarão o início da vigência das subscrições já adquiridas e disponibilizadas, desde que estas estejam efetivamente disponíveis para uso, conforme as condições estabelecidas na contratação.

1.5.1.4. As subscrições e os serviços correspondentes aos itens 2, 3, 4, 7 e 8, quando contratados conjuntamente com o item 1 na primeira contratação, observarão o mesmo marco temporal de referência e a mesma data de encerramento estabelecida para a vigência inicial do item 1 (36 meses), respeitadas as condições específicas de execução de cada item.

1.5.1.5. Na hipótese de contratação posterior dos itens 1, 2, 3, 4, 7 e 8, a vigência das respectivas subscrições ou dos serviços ficará limitada ao período remanescente da vigência inicial do item 1, de modo que suas datas de encerramento coincidam com a data de encerramento estabelecida para a primeira contratação do item principal.

1.5.1.6. Nas contratações posteriores previstas no subitem anterior, os quantitativos, os períodos de fornecimento e os valores correspondentes deverão ser ajustados proporcionalmente ao período efetivo de utilização ou prestação dos serviços, considerando os preços unitários contratados e as respectivas unidades de fornecimento, vedada a remuneração por períodos não contratados.

1.5.1.6.1. Na hipótese prevista no subitem anterior, o valor dos itens será calculado proporcionalmente ao período efetivo de sua vigência, com base no preço unitário contratado.

1.5.2. O serviço gerenciado (**itens 7 e 8**) terá início imediatamente após o recebimento definitivo do objeto e possuirá vigência de 36 meses.

1.5.3. O serviço de Treinamento (item 5), caracterizado como serviço contratado por escopo, deverá ser integralmente executado e concluído no prazo máximo de 180 (cento e oitenta)

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

dias, contados da assinatura do primeiro contrato referente ao item 1, observadas as condições estabelecidas no Termo de Referência.

1.5.4. Os serviços de Treinamento (item 5) e Implantação da Solução (item 6) serão executados uma única vez, no âmbito da primeira contratação do item 1, não sendo objeto de novas contratações decorrentes da mesma Ata de Registro de Preços.

1.6. O primeiro contrato decorrente da Ata de Registro de Preços, que deverá contemplar obrigatoriamente o item 1, terá sua vigência iniciada na data de sua assinatura, abrangendo a etapa de implantação da solução e o período inicial de 36 (trinta e seis) meses de disponibilização das subscrições e prestação dos serviços, contado da emissão do Termo de Recebimento Definitivo, podendo ser prorrogado nos termos dos arts. 106 e 107 da Lei nº 14.133/2021, observadas as condições legais e contratuais aplicáveis.

1.6.1. A primeira contratação do item 1 estabelecerá o marco temporal de referência para a vigência das demais contratações decorrentes da Ata de Registro de Preços, de modo que os itens 2, 3, 4, 7 e 8, quando contratados conjuntamente ou em momento posterior, deverão observar a mesma data de encerramento da vigência inicial estabelecida para o item 1 na cláusula 1.6.

1.6.1.1. Os contratos referentes aos itens 1, 2, 3, 4, 7 e 8, celebrados em momento posterior à primeira contratação do item 1, terão sua vigência iniciada na data de sua assinatura, encerrando-se, obrigatoriamente, na mesma data estabelecida para o término da vigência inicial do item 1, independentemente da data de sua formalização.

1.6.1.2. A contratação dos itens 2, 3, 4, 5, 6, 7 e 8 fica condicionada à contratação do item 1, em razão da interdependência técnica e operacional dos componentes e serviços que integram a solução, observadas as condições específicas de contratação e execução previstas neste instrumento.

1.6.2. 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.

1.7. As demais condições e especificações constam no Termo de Referência mencionado no subitem 1.1.

1.8. Havendo divergência entre as especificações do objeto constantes no sistema Portal de Compras do Governo Federal e as que constam neste Edital, prevalecem as especificações do Edital.

1.9. Na hipótese de haver divergência entre os termos do presente Edital e os termos do Anexo I do Edital - Termo de Referência, prevalece o disposto no presente Edital.

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

2. DA PARTICIPAÇÃO NA LICITAÇÃO

2.1. Poderão participar deste Pregão os interessados que estiverem previamente credenciados no Sistema de Cadastramento Unificado de Fornecedores - SICAF e no Sistema de Compras do Governo Federal (www.gov.br/compras), por meio de Certificado Digital conferido pela Infraestrutura de Chaves Públicas Brasileira – ICP – Brasil.

2.1.1. Os interessados deverão atender às condições exigidas no cadastramento no Sicaf até o terceiro dia útil anterior à data prevista para recebimento das propostas.

2.1.2. Em caso de dúvidas relativas ao sistema “Portal de Compras do Governo Federal”, as interessadas devem entrar em contato com as Centrais de Atendimento “Portal de Compras do Governo Federal” ou “SIASG” pelo telefone 0800-9789001.

2.2. O licitante se responsabiliza exclusiva e formalmente pelas transações efetuadas em seu nome, assume como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou do órgão ou entidade promotora da licitação por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

2.3. É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais nos Sistemas relacionados no item anterior e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

2.4. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação.

2.5. Não poderão disputar esta licitação:

2.5.1. aquele que não atenda às condições deste Edital e seu(s) anexo(s);

2.5.2. autor do anteprojeto, do projeto básico ou do projeto executivo, pessoa física ou jurídica, quando a licitação versar sobre serviços ou fornecimento de bens a ele relacionados;

2.5.3. empresa, isoladamente ou em consórcio, responsável pela elaboração do projeto básico ou do projeto executivo, ou empresa da qual o autor do projeto seja dirigente, gerente, controlador, acionista ou detentor de mais de 5% (cinco por cento) do capital com direito a voto, responsável técnico ou subcontratado, quando a licitação versar sobre serviços ou fornecimento de bens a ela necessários;

2.5.4. pessoa física ou jurídica que se encontre, ao tempo da licitação, impossibilitada de participar da licitação em decorrência de sanção que lhe foi imposta;

2.5.5. servidores que tenham participado do planejamento da contratação ou que desempenhem função na área de licitações e contratos do TRT4;

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

2.5.6. servidores ocupantes de cargos ou funções de direção, chefia ou assessoramento vinculados à Secretaria de Administração, à Diretoria-Geral, à Assessoria Jurídica da Presidência, à Secretaria-Geral da Presidência e às demais unidades envolvidas no procedimento licitatório;

2.5.7. o Presidente do Tribunal ou o desembargador que estiver no exercício da Presidência do TRT4;

2.5.8. o Diretor da Escola Judicial do TRT4 ou o desembargador que estiver no exercício do cargo, em relação às contratações da referida unidade;

2.5.9. cônjuge, companheiro ou parente, em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, dos agentes públicos referidos nos itens 2.5.5, 2.5.6, 2.5.7 e 2.5.8.

2.5.10. pessoas jurídicas que tenham em seus quadros societários as pessoas referidas nos itens 2.5.5, 2.5.6, 2.5.7, 2.5.8 e 2.5.9.

2.5.11. aquele que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com as pessoas referidas nos itens 2.5.5, 2.5.6, 2.5.7, 2.5.8 e 2.5.9;

2.5.12. empresas que não atuem no ramo de atividade pertinente ao objeto do presente pregão;

2.5.13. empresas controladoras, controladas ou coligadas, nos termos da Lei nº 6.404/1976, concorrendo entre si;

2.5.14. pessoa física ou jurídica que, nos 5 (cinco) anos anteriores à divulgação do edital, tenha sido condenada judicialmente, com trânsito em julgado, por exploração de trabalho infantil, por submissão de trabalhadores a condições análogas às de escravo ou por contratação de adolescentes nos casos vedados pela legislação trabalhista;

2.5.15. Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição;

2.5.16. Não poderá participar, direta ou indiretamente, da licitação ou da execução do contrato agente público do TRT da 4ª Região, devendo ser observadas as situações que possam configurar conflito de interesses no exercício ou após o exercício do cargo ou emprego, nos termos da legislação que disciplina a matéria, conforme § 1º do art. 9º da Lei n.º 14.133/2021.

2.5.17. pessoas jurídicas reunidas em **consórcio**.

2.6. A vedação descrita nos itens 2.5.5, 2.5.6, 2.5.7, 2.5.8, 2.5.9, 2.5.10 e 2.5.11 se estende às contratações cujo procedimento licitatório tenha sido deflagrado quando os magistrados e servidores geradores de incompatibilidade estavam no exercício dos respectivos cargos e funções, assim como às licitações iniciadas até 6 (seis) meses após a desincompatibilização (conforme §3º do art. 2º da Resolução CNJ nº 7/2005 e § 1º do art. 7º do Código de Conduta e Valores Éticos do TRT4 - Portaria GP.TRT4 Nº 4.573/2023).

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

2.7. O impedimento de que trata o item 2.5.4 será também aplicado ao licitante que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do licitante.

2.8. A critério da Administração e exclusivamente a seu serviço, o autor dos projetos e a empresa a que se referem os itens 2.5.2 e 2.5.3 poderão participar no apoio das atividades de planejamento da contratação, de execução da licitação ou de gestão do contrato, desde que sob supervisão exclusiva de agentes públicos do órgão ou entidade.

2.9. Equiparam-se aos autores do projeto as empresas integrantes do mesmo grupo econômico.

2.10. O disposto nos itens 2.5.2 e 2.5.3 não impede a licitação ou a contratação de serviço que inclua como encargo do contratado a elaboração do projeto básico e do projeto executivo, nas contratações integradas, e do projeto executivo, nos demais regimes de execução.

2.11. A vedação de que trata o item 2.5.9 estende-se a terceiro que auxilie a condução da contratação na qualidade de integrante de equipe de apoio, profissional especializado ou funcionário ou representante de empresa que preste assessoria técnica.

3. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

3.1. Na presente licitação, a fase de habilitação sucederá as fases de apresentação de propostas e lances e de julgamento.

3.2. Os licitantes encaminharão, exclusivamente por meio do sistema eletrônico, a proposta com o **preço de cada item**, até a data e o horário estabelecidos para abertura da sessão pública (**dia 10/12/2026 às 11h**).

3.3. No cadastramento da proposta inicial, o licitante declarará, em campo próprio do sistema, que:

3.3.1. está ciente e concorda com as condições contidas no edital e seus anexos, bem como de que a proposta apresentada compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de sua entrega em definitivo e que cumpre plenamente os requisitos de habilitação definidos no instrumento convocatório;

3.3.2. não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7°, XXXIII, da Constituição;

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

3.3.3. não possui, em sua cadeia produtiva, empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;

3.3.4. cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

3.3.5. cumpre a reserva de cargos prevista em lei para aprendiz, bem como as reservas de cargos previstas em outras normas específicas, quando cabíveis.

3.4. O licitante organizado em cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 16 da Lei nº 14.133/2021.

3.5. A falsidade da declaração de que trata os itens 3.3 ou 3.4 sujeitará o licitante às sanções previstas na Lei nº 14.133/2021 e neste Edital.

3.6. Os licitantes poderão retirar ou substituir a proposta até a abertura da sessão pública.

3.7. Não haverá ordem de classificação na etapa de apresentação da proposta e dos documentos de habilitação pelo licitante, o que ocorrerá somente após os procedimentos de abertura da sessão pública e da fase de envio de lances.

3.8. Serão disponibilizados para acesso público os documentos que compõem a proposta dos licitantes convocados para apresentação de propostas, após a fase de envio de lances.

3.9. Desde que disponibilizada a funcionalidade no sistema, o licitante poderá parametrizar o seu valor final mínimo quando do cadastramento da proposta e obedecerá às seguintes regras:

3.9.1. a aplicação do intervalo mínimo de diferença de valores ou de percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta; e

3.9.2. os lances serão de envio automático pelo sistema, respeitado o valor final mínimo estabelecido e o intervalo de que trata o subitem acima.

3.10. O valor final mínimo parametrizado no sistema poderá ser alterado pelo fornecedor durante a fase de disputa, sendo vedado valor superior ao lance já registrado pelo fornecedor no sistema.

3.11. O valor final mínimo parametrizado na forma do item 3.10 possuirá caráter sigiloso para os demais fornecedores e para o órgão ou entidade promotora da licitação, podendo ser disponibilizado estrita e permanentemente aos órgãos de controle externo e interno.

3.12. Caberá ao licitante interessado em participar da licitação acompanhar as operações no sistema eletrônico durante o processo licitatório e se responsabilizar pelo ônus decorrente da perda de negócios diante da inobservância de mensagens emitidas pela Administração ou de sua desconexão.

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

3.13. O licitante deverá comunicar imediatamente ao provedor do sistema qualquer acontecimento que possa comprometer o sigilo ou a segurança, para imediato bloqueio de acesso.

4. DO PREENCHIMENTO DA PROPOSTA

4.1. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos:

4.1.1. **valor do item;**

4.1.2. **Fabricante (Item 1);**

4.1.3. Descrição do objeto, contendo as informações similares à especificação do Termo de Referência*;*

4.2. Todas as especificações do objeto contidas na proposta vinculam o licitante.

4.3. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na execução do objeto.

4.4. Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.

4.5. Se o regime tributário da empresa implicar o recolhimento de tributos em percentuais variáveis, a cotação adequada será a que corresponde à média dos efetivos recolhimentos da empresa nos últimos doze meses.

4.6. Independentemente do percentual de tributo inserido na planilha, no pagamento serão retidos na fonte os percentuais estabelecidos na legislação vigente.

4.7. A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o que dispõe o Termo de Referência, assumindo o proponente o compromisso de executar o objeto licitado nos seus termos, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.

4.8. O prazo de validade da proposta não será inferior a 60 (sessenta) dias**,** a contar da data de sua apresentação.

4.9. Os licitantes devem respeitar os preços máximos estabelecidos nas normas de regência de contratações públicas federais, quando participarem de licitações públicas;

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

4.10. O descumprimento das regras supramencionadas pela Administração por parte dos contratados pode ensejar a responsabilização pelo Tribunal de Contas da União e, após o devido processo legal, gerar as seguintes consequências: assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do art. 71, inciso IX, da Constituição; ou condenação dos agentes públicos responsáveis e da empresa contratada ao pagamento dos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

4.11. O licitante deve informar os preços de cada item, em moeda corrente nacional (Real), obrigatoriamente com duas casas decimais (centavos de Real), incluindo eventuais descontos ou acréscimos, inclusive os decorrentes de insumos, impostos, taxas e demais encargos inerentes à prestação do objeto.

4.11.1. Na hipótese de o lance vencedor apresentar valor com número superior de casas decimais, serão consideradas apenas os centavos de reais, desconsiderando-se as demais casas após a vírgula.

5. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES

5.1. A abertura da presente licitação dar-se-á automaticamente em sessão pública, por meio de sistema eletrônico, na data, horário e local indicados neste Edital.

5.2. Os licitantes poderão retirar ou substituir a proposta ou os documentos de habilitação, quando for o caso, anteriormente inseridos no sistema, até a abertura da sessão pública.

5.2.1. Será desclassificada a proposta que identifique o licitante.

5.2.2. A desclassificação será sempre fundamentada e registrada no sistema, com acompanhamento em tempo real por todos os participantes.

5.2.3. A não desclassificação da proposta não impede o seu julgamento definitivo em sentido contrário, levado a efeito na fase de aceitação.

5.3. O sistema ordenará automaticamente as propostas classificadas, sendo que somente estas participarão da fase de lances.

5.4. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os licitantes.

5.5. Iniciada a etapa competitiva, os licitantes deverão encaminhar lances exclusivamente por meio de sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

5.6. O lance deverá ser ofertado pelo valor da cada item.

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

5.7. Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no Edital.

5.8. O licitante somente poderá oferecer lance de valor inferior ao último por ele ofertado e registrado pelo sistema.

5.9. O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta, deverá ser de ***0,1% (um décimo por cento)***.

5.10. O licitante poderá, uma única vez, excluir seu último lance ofertado, no intervalo de quinze segundos após o registro no sistema, na hipótese de lance inconsistente ou inexequível.

5.11. Para o envio de lances no pregão eletrônico será adotado o modo de disputa **"aberto e fechado**", em que os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.

5.11.1. A etapa de lances da sessão pública terá duração inicial de quinze minutos. Após esse prazo, o sistema encaminhará aviso de fechamento iminente dos lances, após o que transcorrerá o período de tempo de até dez minutos, aleatoriamente determinado, findo o qual será automaticamente encerrada a recepção de lances.

5.11.2. Encerrado o prazo previsto no subitem anterior, o sistema abrirá oportunidade para que o autor da oferta de valor mais baixo e os das ofertas com preços até 10% (dez por cento) superiores àquela possam ofertar um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

5.11.3. No procedimento de que trata o subitem supra, o licitante poderá optar por manter o seu último lance da etapa aberta, ou por ofertar melhor lance.

5.11.4. Não havendo pelo menos três ofertas nas condições definidas neste item, poderão os autores dos melhores lances subsequentes, na ordem de classificação, até o máximo de três, oferecer um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

5.11.5. Após o término dos prazos estabelecidos nos itens anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores.

5.12. Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.

5.13. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.

5.14. No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

5.15. Quando a desconexão do sistema eletrônico para o pregoeiro persistir por tempo superior a dez minutos, a sessão pública será suspensa e reiniciada somente após decorridas vinte e quatro horas da comunicação do fato pelo Pregoeiro aos participantes, no sítio eletrônico utilizado para divulgação. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta.

5.16. Só poderá haver empate entre propostas iguais (não seguidas de lances), ou entre lances finais da fase fechada do modo de disputa aberto e fechado.

5.16.1. Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 60 da Lei nº 14.133/2021, nesta ordem:

5.16.1.1. disputa final, hipótese em que os licitantes empatados poderão apresentar nova proposta em ato contínuo à classificação;

5.16.1.2. avaliação do desempenho contratual prévio dos licitantes, para a qual deverão preferencialmente ser utilizados registros cadastrais para efeito de atesto de cumprimento de obrigações previstos nesta Lei;

5.16.1.3. desenvolvimento pelo licitante de ações de equidade entre homens e mulheres no ambiente de trabalho, conforme regulamento;

5.16.1.4. desenvolvimento pelo licitante de programa de integridade, conforme orientações dos órgãos de controle.

5.16.2. Persistindo o empate, será assegurada preferência, sucessivamente, aos bens e serviços produzidos ou prestados por:

5.16.2.1. empresas brasileiras;

5.16.2.2. empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País, devendo apresentar a devida comprovação desta condição junto com os documentos de habilitação.

5.16.2.3. empresas que comprovem a prática de mitigação, nos termos da Lei nº 12.187/2009.

5.17. Encerrada a etapa de envio de lances da sessão pública, o pregoeiro poderá negociar condições mais vantajosas, após definido o resultado do julgamento.

5.17.1. A negociação poderá ser feita com os demais licitantes, segundo a ordem de classificação inicialmente estabelecida, quando o primeiro colocado, mesmo após a negociação, for desclassificado em razão de sua proposta permanecer acima do preço máximo definido pela Administração.

5.17.2. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

5.17.3. O resultado da negociação será divulgado a todos os licitantes e anexado aos autos do processo licitatório

5.17.4. O pregoeiro solicitará ao licitante mais bem classificado que, no prazo de **2 (duas) horas**, envie a proposta adequada ao último lance ofertado após a negociação realizada, **conforme Anexo IV - Modelo de Proposta**, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

5.17.5. É facultado ao pregoeiro prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante, antes de findo o prazo.

5.18. Após a negociação do preço, o Pregoeiro iniciará a fase de aceitação e julgamento da proposta.

6. DA FASE DE JULGAMENTO

6.1. A classificação das propostas será apurada pelo critério de **menor preço por grupo.**

6.2. Encerrada a etapa de negociação, o pregoeiro verificará se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei nº 14.133/2021, legislação correlata e no item 2.5 do edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

a) SICAF;

b) Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/ceis);

c) Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/cnep); e

d) Cadastro de Empregadores que tenham submetido trabalhadores a condições análogas à de escravo (Lista Suja do Trabalho Escravo), mantido pelo Ministério do Trabalho e Emprego.
(https://www.gov.br/trabalho-e-emprego/pt-br/assuntos/inspecao-do-trabalho/areas-de-atuacao/combate-ao-trabalho-escravo-e-analogo-ao-de-escravo).

6.3. Fica a licitante ciente de que, na fase de verificação da regularidade da licitante (habilitação), será efetuado consulta ao **CADIN (Cadastro Informativo de créditos não quitados do setor público federal)** e, constatando irregularidade, será notificada para que solucione as pendências, sob pena de, após a adjudicação do objeto e a homologação do certame, ser impedida de celebrar a contratação ou emitir a Nota de Empenho. Nova consulta será efetuada após a homologação do certame e, persistindo as

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

pendências, será novamente notificada, sendo-lhe concedido o prazo de **10 (dez) dias úteis** para comprovar a regularização da situação.

6.3.1. Será realizada, ainda, consulta ao CADIN em eventuais aditivos contratuais e, caso verificadas pendências naquele Cadastro, será a contratada notificada para que comprove a regularização, no prazo de **10 dias úteis**, prorrogáveis a critério da Administração, sob pena de não celebração do respectivo aditivo.

6.4. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força da vedação de que trata o artigo 12 da Lei n° 8.429/1992.

6.5. Caso conste na Consulta de Situação do licitante a existência de Ocorrências Impeditivas Indiretas, o Pregoeiro diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas. (art. 29, *caput*, da IN SEGES/ME nº 3/2018)

6.5.1. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros. (art. 29, §1º, da IN SEGES/ME nº 3/2018).

6.5.2. O licitante será convocado para manifestação previamente a uma eventual desclassificação. (art. 29, §2º, da IN SEGES/ME nº 3/2018).

6.5.3. Constatada a existência de sanção, o licitante será reputado inabilitado, por falta de condição de participação.

6.6. Caso atendidas as condições de participação, será iniciado o procedimento de habilitação.

6.7. Verificadas as condições de participação, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos, observado o disposto no artigo 29 a 35 da IN SEGES/ME nº 73/2022.

6.8. Será desclassificada a proposta vencedora que:

6.8.1. contiver vícios insanáveis;

6.8.2. não obedecer às especificações técnicas contidas no Termo de Referência;

6.8.3. apresentar preços inexequíveis ou permanecerem acima do preço máximo definido para a contratação;

6.8.4. não tiverem sua exequibilidade demonstrada, quando exigido pela Administração;

6.8.5. apresentar desconformidade com quaisquer outras exigências deste Edital ou seus anexos, desde que insanável.

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

6.9. No caso de bens e serviços em geral, é indício de inexequibilidade das propostas valores inferiores a 50% (cinquenta por cento) do valor orçado pela Administração.

6.9.1. A inexequibilidade, na hipótese de que trata o **caput**, só será considerada após diligência do pregoeiro, que comprove:

6.9.1.1. que o custo do licitante ultrapassa o valor da proposta; e

6.9.1.2. inexistirem custos de oportunidade capazes de justificar o vulto da oferta.

6.10. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, para que a empresa comprove a exequibilidade da proposta.

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

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

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

6.12. O pregoeiro poderá solicitar amostra do objeto do licitante classificado em primeiro lugar, sob pena de não aceitação da proposta.

6.13. Se a amostra apresentada pelo primeiro classificado não for aceita, o pregoeiro analisará a aceitabilidade da proposta ou lance ofertado pelo segundo classificado. Seguir-se-á com a verificação da(s) amostra(s) e, assim, sucessivamente, até a verificação de uma que atenda às especificações constantes no Termo de Referência.

7. DA FASE DE HABILITAÇÃO

7.1. Os documentos necessários e suficientes para demonstrar a capacidade do licitante de realizar o objeto da licitação, para fins de habilitação, nos termos dos arts. 62 a 70 da Lei nº 14.133/2021, são os que seguem:

a) **Habilitação Jurídica**, conforme o caso:

a.1) registro comercial, no caso de empresa individual;

a.2) ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, em se tratando de sociedades comerciais e, no caso de sociedades por ações, acompanhado de documentos de eleição de seus administradores;

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

a.3) inscrição do ato constitutivo, no caso de sociedades civis, acompanhada de prova de diretoria em exercício;

a.4) decreto de autorização, devidamente arquivado, em se tratando de empresa ou sociedade estrangeira em funcionamento no País.

b) **Regularidade Fiscal, Social e Trabalhista**:

b.1) prova de regularidade com a Fazenda Federal, consistindo na apresentação de certidão conjunta relativa a tributos federais, à Dívida Ativa da União e a Contribuições Sociais (INSS), expedida pela Receita Federal do Brasil;

b.2) prova de regularidade com a Fazenda Estadual do domicílio ou sede da licitante, ou outra equivalente, na forma da lei, a qual deverá incluir todos os tributos estaduais;

b.3) prova de regularidade com a Fazenda Municipal do domicílio ou sede da licitante;

b.4) prova de regularidade relativa ao FGTS - Fundo de Garantia por Tempo de Serviço;

b.5) prova de regularidade com as obrigações trabalhistas, mediante a apresentação da Certidão Negativa de Débitos Trabalhistas (CNDT), expedida no portal do TST.

c) **Qualificação Técnica**:

c.1) **Qualificação técnica-profissional:**

c.1.1) A licitante deverá indicar os profissionais das equipes técnicas com apresentação da seguinte documentação:

I) Pelo menos 3 (três) profissionais da equipe técnica, **responsáveis pela implantação e sustentação da solução**, deverão ter certificação oficial do fabricante da solução proposta de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos (itens 1 a 4 da contratação). Não serão aceitos certificados de participação em cursos ou workshops.

II) Os profissionais da equipe técnica, **responsáveis pela detecção, notificação e investigação de ataques cibernéticos**, deverão possuir certificação em segurança ofensiva, detendo, individualmente ou em conjunto, pelo menos 3 (três) das seguintes certificações, contabilizando no máximo 2 (dois) certificados por profissional:

- ***a)*** CompTIA PenTest+;
- ***b)*** EC-Council Licensed Penetration Tester (LPT);
- ***c)*** IACRB Certified Expert Penetration Tester (CEPT);
- ***d)*** GIAC Exploit Researcher and Advanced Penetration Tester (GXPN);
- ***e)*** GIAC Reverse Engineering Malware (GREM);
- ***f)*** Offensive Security Certified Professional (OSCP);
- ***g)*** Ethical Hacking Post Exploitation (EHPX);
- ***h)*** Offensive Security Experienced Penetration Tester (OSEP);
- ***i)*** Offensive Security Web Expert (OSWE);
- ***j)*** Certified Red Team Expert (CRTE);
- ***k)*** Offensive Security Certified Expert (OSCE) ou OSCE³;
- ***l)*** Certified Ethical Hacker (CEH).

III) Os profissionais da equipe técnica, **responsáveis pela resposta a ataques cibernéticos, deverão ter certificação em segurança defensiva**, detendo, individualmente ou em conjunto, pelo menos 3 (três) das seguintes certificações, contabilizando no máximo 2 (dois) certificados por profissional:

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

a) Certified Information Security Manager (CISM);
b) GIAC Experienced Cybersecurity Specialist (GX-CS);
c) GIAC Reverse Engineering Malware (GREM);
d) Ethical Hacking Post Exploitation (EHPX);
e) CompTIA Security+;
f) CompTIA Advanced Security Practitioner;
g) EC-Council Security Analyst (ECSA) ou CPENT (Certified Penetration Testing Professional);
h) Certified Information Systems Security Professional (CISSP);
i) CompTIA CYSA+ - Cybersecurity Analyst.

c.1.1.1) *É de responsabilidade da contratada dimensionar a quantidade de profissionais para a adequada prestação dos serviços previstos e delimitados por esta especificação, principalmente no que se refere aos acordos de níveis de serviço e metas estabelecidas.*

c.1.1.2) *Os profissionais cuja documentação for apresentada pela licitante deverão ser alocados na execução dos serviços.*

c.1.1.3) *Excepcionalmente, a contratada poderá substituir o profissional para a execução dos serviços, desde que comprovadas as condições de qualificação exigidas, condicionadas à prévia avaliação dos requisitos de qualificação e aceite por parte do contratante.*

c.1.1.4) ***Até a data do início dos serviços****, a contratada deverá comprovar que os profissionais que prestarão os serviços integram o quadro de pessoal permanente da contratada. A comprovação deverá ser feita mediante apresentação de:*

c.1.1.4.1) *Documento que comprove vínculo de emprego, ou*

c.1.1.4.2) *Documento que comprove ser o profissional sócio da empresa, ou*

c.1.1.4.3) *Contrato civil de prestação de serviços.*

c.2) **Qualificação técnica-operacional:**

c.2.1) Atestado(s) de capacidade técnica, fornecido por pessoa jurídica de direito público ou privado, no qual esteja expressa a aptidão do interessado no fornecimento, implantação e prestação de serviço gerenciado de solução de Monitoramento, Detecção, Notificação, Investigação e Resposta a Ataques Cibernéticos, para uma **quantidade mínima de 40% do total de licenças previsto no item 1**, devendo pelo menos **10%** serem do mesmo fabricante da solução que a empresa ofertar na presente contratação.

c.2.1.1) A organização emitente do atestado de capacidade técnica deverá ser usuária do objeto fornecido, não sendo aceitos atestados emitidos por quaisquer intermediários.

c.2.1.2) **Alternativamente ao atestado** de capacidade técnica, será aceita declaração emitida pelo fabricante da solução, atestando que a licitante possui capacidade técnica e operacional para fornecer e prestar os serviços de implantação e o serviço gerenciado previstos no objeto, ou documento que comprove que a licitante é parceira autorizada do fabricante para serviços gerenciados de monitoramento e resposta a incidentes.

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

c.2.2) 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.

d) **Qualificação Econômico-Financeira**

d.1) **certidão negativa de feitos sobre falência** expedida pelo Distribuidor da sede do licitante.

d.2) **balanço patrimonial (BP) e demonstração do resultado do exercício (DRE)**, do último exercício social, que permitam comprovar*:*

I - que os índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC) são superiores a 1 (um), a serem calculados pelas seguintes fórmulas:

$$LG = \frac{AC + RLP}{PC + PNC} \qquad SG = \frac{AT}{PC + PNC} \qquad LC = \frac{AC}{PC}$$ onde:

AC = Ativo Circulante

RLP = Realizável a Longo Prazo

PC = Passivo Circulante

PNC = Passivo não circulante

AT = Ativo Total

ou

II - Patrimônio Líquido de, no mínimo, R$ 2.497.131,19 (dois milhões, quatrocentos e noventa e sete mil, cento e trinta e um reais e dezenove centavos), correspondente a 10% (dez por cento) do valor total **anual estimado** da contratação**.**

7.1.1. A documentação exigida para fins de habilitação jurídica, fiscal, social e trabalhista e econômico-financeira, poderá ser substituída pelo registro cadastral no SICAF.

7.2. Os documentos exigidos para fins de habilitação poderão ser apresentados em original, por cópia.

7.3. Os documentos exigidos para fins de habilitação poderão ser substituídos por registro cadastral emitido por órgão ou entidade pública, desde que o registro tenha sido feito em obediência ao disposto na Lei nº 14.133/2021.

7.4. Será verificado se o licitante apresentou declaração de que atende aos requisitos de habilitação, e o declarante responderá pela veracidade das informações prestadas, na forma da lei (art. 63, I, da Lei nº 14.133/2021).

7.5. Será verificado se o licitante apresentou no sistema, sob pena de inabilitação, a declaração de que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

7.6. O licitante deverá apresentar, sob pena de desclassificação, declaração de que suas propostas econômicas compreendem a integralidade dos custos para atendimento dos direitos trabalhistas

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas.

7.7. A habilitação será verificada por meio do Sicaf, nos documentos por ele abrangidos.

7.7.1. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital ou quando a lei expressamente o exigir. (art. 4º, §1º, e art. 6º, §4º, da IN SEGES/ME nº 3/2018).

7.8. É de responsabilidade do licitante conferir a exatidão dos seus dados cadastrais no Sicaf e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados. (art. 7º, *caput*, da IN SEGES/ME nº 3/2018).

7.8.1. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação. (art. 7º, parágrafo único, da IN SEGES/ME nº 3/2018).

7.9. A verificação pelo pregoeiro, em sítios eletrônicos oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova, para fins de habilitação.

7.9.1. Os documentos exigidos para habilitação que não estejam contemplados no Sicaf serão enviados por meio do sistema, em formato digital, no prazo de 2 (duas) horas, prorrogável por igual período, contado da solicitação do pregoeiro.

7.10. A verificação no Sicaf ou a exigência dos documentos nele não contidos somente será feita em relação ao licitante vencedor.

7.10.1. Os documentos relativos à regularidade fiscal somente serão exigidos, em qualquer caso, em momento posterior ao julgamento das propostas, e apenas do licitante mais bem classificado.

7.11. Após a entrega dos documentos para habilitação, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência, para (art. 64 da Lei nº 14.133/2021, e art. 39, §4º, da IN SEGES/ME nº 73/2022):

7.11.1. complementação de informações acerca dos documentos já apresentados pelos licitantes e desde que necessária para apurar fatos existentes à época da abertura do certame; e

7.11.2. atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas;

7.12. Na análise dos documentos de habilitação, o pregoeiro poderá sanar erros ou falhas, que não alterem a substância dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível a todos, atribuindo-lhes eficácia para fins de habilitação e classificação.

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

7.13. Na hipótese de o licitante não atender às exigências para habilitação, o pregoeiro de contratação examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao presente edital.

7.14. Somente serão disponibilizados para acesso público os documentos de habilitação do licitante cuja proposta atenda ao edital de licitação, após concluídos os procedimentos de que trata o subitem anterior.

8. DOS RECURSOS

8.1. A interposição de recurso referente ao julgamento das propostas, à habilitação ou inabilitação de licitantes, à anulação ou revogação da licitação, observará o disposto no art. 165 da Lei nº 14.133/2021.

8.2. O prazo recursal é de 3 (três) dias úteis, contados da data de intimação ou de lavratura da ata.

8.3. Quando o recurso apresentado impugnar o julgamento das propostas ou o ato de habilitação ou inabilitação do licitante:

8.3.1. a intenção de recorrer deverá ser manifestada imediatamente, sob pena de preclusão, no prazo máximo de 10 minutos;

8.3.2. o prazo para apresentação das razões recursais será iniciado na data de intimação ou de lavratura da ata de habilitação ou inabilitação;

8.4. Os recursos deverão ser encaminhados em campo próprio do sistema.

8.5. O recurso será dirigido à autoridade que tiver editado o ato ou proferido a decisão recorrida, a qual poderá reconsiderar sua decisão no prazo de 3 (três) dias úteis, ou, nesse mesmo prazo, encaminhar recurso para a autoridade superior, a qual deverá proferir sua decisão no prazo de 10 (dez) dias úteis, contado do recebimento dos autos.

8.6. Os recursos interpostos fora do prazo não serão conhecidos.

8.7. O prazo para apresentação de contrarrazões ao recurso pelos demais licitantes será de 3 (três) dias úteis, contados da data da intimação pessoal ou da divulgação da interposição do recurso, assegurada a vista imediata dos elementos indispensáveis à defesa de seus interesses.

8.8. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

8.9. O acolhimento do recurso invalida tão somente os atos insuscetíveis de aproveitamento.

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

9. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

9.1. Comete infração administrativa, nos termos da lei, o licitante que:

9.1.1. deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pelo pregoeiro durante o curso do processo licitatório;

9.1.2. salvo em decorrência de fato superveniente devidamente justificado, não mantiver a proposta em especial quando:

9.1.2.1. não enviar a proposta adequada ao último lance ofertado ou após a negociação;

9.1.2.2. recusar-se a enviar o detalhamento da proposta quando exigível;

9.1.2.3. pedir para ser desclassificado quando encerrada a etapa competitiva; ou

9.1.2.4. deixar de apresentar amostra;

9.1.2.5. apresentar proposta ou amostra em desacordo com as especificações do edital;

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

9.1.3.1. recusar-se, sem justificativa, a assinar o contrato ou a ata de registro de preços, ou a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração;

9.1.4. apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação

9.1.5. fraudar a licitação

9.1.6. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza, em especial quando:

9.1.6.1. agir em conluio ou em desconformidade com a lei;

9.1.6.2. induzir deliberadamente a erro no julgamento;

9.1.6.3. apresentar amostra falsificada ou deteriorada;

9.1.7. praticar atos ilícitos com vistas a frustrar os objetivos da licitação

9.1.8. praticar ato lesivo previsto no art. 5º da Lei n.º 12.846/2013.

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

9.2. Com fulcro na Lei nº 14.133/2021, a Administração poderá, garantida a defesa escrita, aplicar aos licitantes e/ou adjudicatários as seguintes sanções, sem prejuízo da responsabilidade civil e criminal que couber:

9.2.1. advertência;

9.2.2. multa;

9.2.3. impedimento de licitar e contratar com a União e

9.2.4. declaração de inidoneidade para licitar ou contratar com a Administração Pública direta e indireta de todos os entes federativos, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação perante a própria autoridade que aplicou a penalidade.

9.3. Na aplicação das sanções serão considerados:

9.3.1. a natureza e a gravidade da infração cometida.

9.3.2. as peculiaridades do caso concreto

9.3.3. as circunstâncias agravantes ou atenuantes

9.3.4. os danos que dela provierem para a Administração Pública

9.3.5. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

9.3.6. Para as infrações previstas nos itens 9.1.1, 9.1.2, 9.1.4, 9.1.5, 9.1.6, 9.1.7 e 9.1.8 a multa será de 2% (dois por cento) do valor total do lance, limitada a R$ 1.000,00 (um mil reais) por ocorrência.

9.3.7. Na hipótese de atraso na disponibilização das subscrições e serviços (itens 1, 2, 3, 4, 7 e 8) e na execução da implantação da solução (item 6), a contratada estará sujeita a multa diária de 0,5% (cinco décimos por cento) sobre o valor da obrigação objeto do atraso, limitada a 10% (dez por cento) do respectivo valor.

9.3.8. Na hipótese de atraso na solução dos chamados de suporte técnico, a contratada estará sujeita a multa nos percentuais descritos a seguir, sobre o valor mensal dos itens 7 e 8, limitada a 10% (dez por cento) do respectivo valor:

a) Severidade A0 (crítica): 1% (um por cento) por hora de atraso
b) Severidade A1 (alta): 0,5% (cinco décimos por cento) por hora de atraso
c) Severidade A2 (média): 0,5% (cinco décimos por cento) por día útil de atraso
d) Severidade A3 (baixa): 0,2% (dois décimos por cento) por dia útil de atraso
e) Severidade A4 (pesquisa): 0,1% (um décimo por cento) por día útil de atraso

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

9.3.9. Na hipótese de atraso na realização do treinamento (item 5), a contratada estará sujeita a multa diária de 0,5% (cinco décimos por cento) sobre o valor do item em atraso, limitada a 10% (dez por cento) do respectivo valor.

9.3.10. Na hipótese de inexecução total ou parcial do objeto, a contratada estará sujeita à aplicação de multa compensatória de 10% (dez por cento) sobre o valor da parcela não executada do contrato.

9.3.11. Na hipótese de descumprimento total da obrigação dos itens 1, 2 e 4, além da multa prevista no subitem 9.3.10 e da possibilidade de aplicação da sanção administrativa de impedimento de licitar e contratar com a União prevista no subitem 9.2.3, ficará a contratada obrigada a restituir ao contratante o valor total da contratação dos respectivos itens. Em caso de execução parcial do objeto, o valor a ser devolvido corresponderá ao montante da(s) parcela(s) não executada(s).

9.4. As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar poderão ser aplicadas, cumulativamente ou não, à penalidade de multa.

9.5. Na aplicação da sanção de multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

9.6. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos itens 9.1.1, 9.1.2 e 9.1.3, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo a qual pertencer o órgão ou entidade, pelo prazo máximo de 3 (três) anos.

9.7. Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos itens 9.1.4, 9.1.5, 9.1.6, 9.1.7 e 9.1.8, bem como pelas infrações administrativas previstas nos itens 9.1.1, 9.1.2 e 9.1.3 que justifiquem a imposição de penalidade mais grave que a sanção de impedimento de licitar e contratar, cuja duração observará o prazo previsto no art. 156, §5º, da Lei nº 14.133/2021.

9.8. A recusa injustificada do adjudicatário em assinar o contrato ou a ata de registro de preços, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração, descrita no item 9.1.3, caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades e à imediata perda da garantia de proposta em favor do órgão ou entidade promotora da licitação, nos termos do art. 45, §4º, da IN SEGES/ME nº 73/2022.

9.9. A apuração de responsabilidade relacionada às sanções de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar demandará a instauração de processo de responsabilização a ser conduzido por comissão composta por 2 (dois) ou mais servidores estáveis, designados pela Portaria GP.TRT4 nº 3.822/2022, que avaliará fatos e circunstâncias conhecidos e intimará o licitante ou o adjudicatário para, no prazo de 15 (quinze) dias úteis, contado da data de sua intimação, apresentar defesa escrita e especificar as provas que pretenda produzir.

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

9.10. Caberá recurso no prazo de 15 (quinze) dias úteis da aplicação das sanções de advertência, multa e impedimento de licitar e contratar, contado da data da intimação, o qual será dirigido à autoridade que tiver proferido a decisão recorrida, que, se não a reconsiderar no prazo de 5 (cinco) dias úteis, encaminhará o recurso com sua motivação à autoridade superior, que deverá proferir sua decisão no prazo máximo de 20 (vinte) dias úteis, contado do recebimento dos autos.

9.11. Caberá a apresentação de pedido de reconsideração da aplicação da sanção de declaração de inidoneidade para licitar ou contratar no prazo de 15 (quinze) dias úteis, contado da data da intimação, e decidido no prazo máximo de 20 (vinte) dias úteis, contado do seu recebimento.

9.12. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

9.13. A aplicação das sanções previstas neste edital não exclui, em hipótese alguma, a obrigação de reparação integral dos danos causados.

9.14. A apuração dos descumprimentos e a eventual cominação de sanções administrativas observarão o disposto na Portaria GP.TRT4 nº 2.714/2022.

9.15. A defesa escrita e os recursos administrativos deverão ser encaminhados exclusivamente por meio eletrônico para o endereço dg@trt4.jus.br.

10. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

10.1. Qualquer pessoa é parte legítima para impugnar este Edital por irregularidade na aplicação da Lei nº 14.133/2021, ou para solicitar esclarecimento sobre os seus termos, devendo protocolar o pedido até 3 (três) dias úteis antes da data da abertura do certame.

10.2. A resposta à impugnação ou ao pedido de esclarecimento será divulgado em sítio eletrônico oficial no prazo de até 3 (três) dias úteis, limitado ao último dia útil anterior à data da abertura do certame.

10.3. A impugnação e o pedido de esclarecimento deverão ser realizados por forma eletrônica, pelo e-mail ***pregao@trt4.jus.br*** até às 23h59min do último dia do prazo.

10.4. As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.

10.4.1. A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo pregoeiro/agente de contratação/comissão de contratação, nos autos do processo de licitação.

10.5. Acolhida a impugnação, será definida e publicada nova data para a realização do certame.

10.6. As impugnações e pedidos de esclarecimentos apresentados, bem como as respectivas respostas, serão divulgados no *site* deste Tribunal, no link

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

https://www.trt4.jus.br/portais/trt4/licitacoes-compras-e-contratos, ficando as interessadas em participar do certame obrigadas a acessá-lo para obtenção das informações prestadas.

11. DO REGISTRO DE PREÇOS

11.1. Os preços registrados não obrigam o Tribunal Regional do Trabalho da 4ª Região a firmar a(s) contratação(ões) que deles poderão advir, sendo facultada a realização de licitação específica para a aquisição pretendida, assegurando-se ao(s) beneficiário(s) do registro o fornecimento em igualdade de condições.

11.2. O prazo de vigência do presente Registro de Preços será de 1 ano, prorrogável por igual período, nos termos do art. 84 da Lei n° 14.133/2021.

11.2.1. A prorrogação da vigência da ata fica condicionada à anuência da detentora dos preços registrados.

11.2.2. A prorrogação do prazo de vigência da ata de registro de preços implicará, nos termos do inciso II do § 3º do art. 96 da Portaria TRT4 nº 1.737/2023:

11.2.2.1. A renovação, tão-somente, dos quantitativos remanescentes do primeiro ano de vigência (saldos dos itens).

11.3. A ata de registro de preços não poderá ser utilizada por órgãos ou entidades não participantes, considerando o critério de julgamento adotado, pelo menor preço global, a fim de afastar a possibilidade de prejuízo ao erário, em consonância com o entendimento proferido pelo Acórdão nº 1.347/2018 do Plenário do TCU.

11.4. Após a declaração do(s) vencedor(es), antes de encerrar a sessão, o Pregoeiro fará a convocação para que os participantes manifestem o interesse de aderir ao CADASTRO DE RESERVA.

11.4.1. A manifestação de interesse em aderir ao cadastro de reserva deverá ser realizada no prazo de até 24 horas após o lançamento da homologação do certame no sistema compras.gov.br.

11.4.2. Os interessados em aderir ao cadastro dos licitantes deverão informar se aceitam fornecer os bens, as obras ou os serviços com preços iguais aos do adjudicatário, observada a classificação na licitação, ou se manterão os preços da sua proposta original.

11.4.3. A(s) licitante(s) que quiserem aderir ao cadastro de reserva deverão encaminhar, no prazo estabelecido no item 11.4.1, o formulário constante do Anexo III do Edital, para o e-mail pregao@trt4.jus.br.

11.5. Após a homologação da presente licitação, será lavrada Ata de Registro de Preços (**Anexo II** do Edital), visando a eventuais contratações futuras, na qual será(ão) registrado(s) o(s) preço(s) da(s) empresa(s) declarada(s) vencedora(s) no(s) respectivo(s) item(ns).

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

11.6. A Ata de Registro de Preços deverá ser assinada por 1 (um) representante que venha a responder por sua representada, devendo esse se identificar mediante encaminhamento, via e-mail, de cópia de sua Carteira de Identidade ou outro documento equivalente, sendo indispensável, ainda, a apresentação dos seguintes documentos, em cópia autenticada ou publicação oficial, os quais farão parte do processo licitatório:

a) ato constitutivo, estatuto ou contrato social em vigor, em se tratando de sociedades comerciais, e, no caso de sociedade por ações, acompanhado do documento de eleição de seus administradores, quando a licitante for representada por pessoa que estatutariamente tenha poder para tal, comprovando esta capacidade jurídica;

b) procuração particular ou carta de credenciamento, estabelecendo poderes para representar a licitante, expressamente quanto à formulação de propostas e a praticar todos os demais atos inerentes ao Pregão, acompanhada de 1 (um) dos documentos citados na alínea anterior, conforme o caso, para fins de confirmação dos poderes para subscrevê-la, ou ainda, cópia autenticada de traslado de procuração por instrumento público, na hipótese de representação por meio de preposto;

11.7. Decairá do direito ao registro do(s) preço(s) a licitante que, regularmente convocada, não assinar a Ata de Registro de Preços no prazo estipulado, hipótese em que se caracterizará a inexecução total do objeto, sujeitando-se a(s) empresa(s) declarada(s) vencedora(s) às sanções administrativas previstas no presente Edital.

11.8. Ocorrendo a hipótese descrita no item anterior, este Tribunal reserva-se o direito de convocar as licitantes remanescentes.

11.9. Os preços registrados poderão ser reajustados em caso de prorrogação da Ata de Registro de Preços, mediante solicitação do fornecedor, com base no índice de Custo da Tecnologia da Informação (ICTI), estabelecido no guia da Resolução CNJ nº 468/2022, com data base vinculada à elaboração do orçamento estimado (**22/10/2026**), aplicando-se sua variação a partir da referida data.

11.9.1. O reajustamento será calculado mediante a aplicação da variação acumulada do índice de reajuste sobre os preços praticados à época de sua concessão.

11.9.2. Caso a variação acumulada no período seja positiva, o reajuste será concedido mediante requerimento do fornecedor à fiscalização e o valor resultante da aplicação do índice poderá ser objeto de negociação entre as partes.

11.9.3. Caso a variação acumulada no período seja negativa, o valor registrado será diminuído, automaticamente, com base na aplicação do índice.

11.9.4. A prorrogação da vigência da Ata de Registro de Preços sem prévio requerimento do reajuste implicará na preclusão do direito do fornecedor.

11.10. A alteração dos preços registrados e o cancelamento do registro de preços observarão o disposto nos artigos 25 a 29 do Decreto nº 11.462/2023.

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

11.11. Considerando o critério de julgamento adotado, pelo menor preço global, a fim de afastar a possibilidade de prejuízo ao erário, em consonância com o entendimento proferido pelo Acórdão nº 1.347/2018 do Plenário do TCU, a contratação somente será realizada nos seguintes casos:

a) para aquisição da totalidade dos itens, respeitadas as proporções de quantitativos definidos no certame;

b) para aquisição de itens isolados, desde que o preço registrado represente o melhor lance válido obtido na disputa do respectivo item.

c) para aquisição de itens complementares ao item 1 (solução principal), em razão da interdependência técnica e operacional entre os componentes, desde que previamente contratado o item 1 e demonstrada a manutenção da vantajosidade econômica global, mediante análise cumulativa das contratações realizadas e daquela pretendida,

c.1) para fins da hipótese prevista na alínea “c”, deverá ser avaliada, previamente a cada contratação, a totalidade dos quantitativos e valores já contratados, acrescidos daqueles relativos à contratação pretendida, verificando a manutenção das proporções entre os quantitativos dos itens estabelecidas no certame e a preservação da vantajosidade econômica da proposta global adjudicada..

11.11.1. Caberá à unidade requisitante e a cada TRT participante da ARP analisar a vantajosidade da proposta vencedora em caso de prorrogação da vigência e/ou acréscimo quantitativo de itens cujo valor não represente o melhor lance válido obtido na disputa.

11.11.2. Para contratação de item específico constante em grupo de itens de ata de registro de preços, sempre que o intervalo entre a demanda e a pesquisa de preços anterior ultrapassar 180 (cento e oitenta) dias, é necessário que a unidade requisitante realize prévia pesquisa de mercado e demonstre a vantajosidade econômica.

12. DA CONTRATAÇÃO

12.1. A contratação do objeto será efetivada mediante assinatura do instrumento de contrato, cuja minuta encontra-se anexa, após a homologação da presente licitação.

12.1.1. Fica estabelecido o prazo de 5 dias úteis, contados a partir da comunicação deste Tribunal, para a licitante assinar o contrato decorrente desta licitação, o qual, na forma do art. 95 da Lei nº 14.133/2021, constitui, neste procedimento, documento hábil à formalização da contratação do objeto.

12.2. Como condição para contratação, prorrogações e acréscimos contratuais, a licitante vencedora deste certame deverá apresentar as certidões de regularidade fiscal, social e trabalhista. Na hipótese de as provas de regularidade não se encontrarem disponíveis nas respectivas homepages, a licitante deverá providenciar sua emissão no prazo máximo de 10 dias úteis contados da intimação deste Tribunal.

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

12.3. Decairá do direito à contratação a licitante que, regularmente convocada, não assinar o contrato no prazo estipulado no subitem anterior, ou ainda, não apresentar as certidões de regularidade fiscal, social e trabalhista, ficando caracterizado o descumprimento total da obrigação assumida, sujeitando-se às sanções previstas neste Edital.

12.4. Ocorrendo a hipótese descrita no item anterior, este Tribunal reserva-se o direito de convocar outra licitante para firmar a contratação, observada a ordem de classificação.

12.4.1. A licitante eventualmente convocada, na hipótese do disposto no *caput* deste item, caso aceite a convocação, ficará sujeita às mesmas obrigações e penalidades.

13. DO PAGAMENTO

13.1. O pagamento será realizado mediante crédito em conta corrente bancária até o décimo dia útil após a entrega do documento fiscal correspondente ao objeto, devidamente atestado pela fiscalização, conforme critérios de medição e pagamento constantes do quadro abaixo, sendo efetuada a retenção na fonte dos tributos e contribuições elencados na legislação em vigor, tais como IR, CSLL, COFINS e PIS/PASEP e, se for o caso, ISS:

Item	Descrição	Forma de Recebimento	Prazo	Forma de pagamento
1	Entrega das subscrições de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Termo de Recebimento Definitivo	60 dias da assinatura do contrato	Pagamento anual após o recebimento definitivo do objeto
2	Entrega das subscrições de Módulo de Detecção e Resposta a Ameaças de Identidade (ITDR)	Termo de Recebimento Definitivo	60 dias da assinatura do contrato	Pagamento anual após o recebimento definitivo do objeto
3	Módulo de solução Agêntica para resposta, orquestração e triagem de eventos e incidentes	Ateste na nota fiscal	mensal	Pagamento mensal
4	Disponibilização da ingestão de logs externos	Termo de Recebimento Definitivo	60 dias da assinatura do contrato	Pagamento anual após o recebimento definitivo do objeto
5	Realização do Treinamento	Ateste na nota fiscal	180 dias da assinatura do contrato	Pagamento único após a realização do treinamento
6	Conclusão do serviço de implantação	Termo de Recebimento Definitivo	60 dias da assinatura do contrato	Pagamento único após o recebimento definitivo do objeto
7 e 8	Prestação do serviço mensal de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Ateste na nota fiscal	mensal	Pagamento mensal após a realização do serviço

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

13.1.1. A presente contratação permite a antecipação de pagamento (itens 1, 2 e 4) que ocorrerá com prazo não superior a 30 dias contados do prazo estabelecido para o início do fornecimento/prestação do serviço.

13.1.2. Os itens 1, 2 e 4 serão pagos em 3 (três) parcelas anuais, de igual valor, condicionadas à disponibilização anual das respectivas licenças e observados os seguintes marcos de pagamento: a primeira parcela será paga após a emissão do respectivo Termo de Recebimento Definitivo; a segunda, em até 12 (doze) meses após o pagamento da primeira; e a terceira, em até 12 (doze) meses após o pagamento da segunda. A segunda e a terceira parcelas são reajustáveis pelo ICTI (Índice de Custo de Tecnologia da Informação).

13.1.3. O item 3 será pago mensalmente com base em um dos seguintes critérios:

13.1.3.1. Quantidade de tokens consumidos no período de apuração, de acordo com os registros de consumo da solução, devendo a CONTRATADA apresentar a memória de cálculo juntamente com o relatório mensal de medição.

13.1.3.2. Quantidade de tokens previamente estimados pela fiscalização do contrato para consumo no período de apuração.

13.1.4. O pagamento dos itens 7 e 8 será realizado mensalmente, após a execução dos serviços e entrega ao contratante, pela contratada, dos resultados dos indicadores apurados.

13.2. O documento fiscal deverá ser obrigatoriamente registrado no Portal do SIGEO - JT para ateste, liquidação e pagamento.

13.2.1. A contratada deverá efetuar o cadastro no Portal do SIGEO - JT para apresentação dos documentos fiscais (notas fiscais) com vistas à liquidação e pagamento. Por meio do link https://portal.sigeo.jt.jus.br/portal-externo, a contratada terá acesso ao SIGEO - JT e, pelo link https://sigeo.jt.jus.br/ajuda, a um guia detalhado das funcionalidades do sistema.

13.3. A contratada fica obrigada a emitir Nota Fiscal Eletrônica (NF-e) para fornecimento do material objeto da presente licitação, nos termos do Protocolo ICMS nº 42/2009 e inciso VIII do art. 26-A do Livro II do Regulamento do ICMS do Estado do Rio Grande do Sul.

13.4. Na hipótese de a proposta ser apresentada pela matriz e o faturamento *for realizado por CNPJ de filial, ou vice-versa,* tal condição deverá constar expressamente da proposta, na qual deverão ser informados os respectivos números de CNPJ, bem como a licitante deverá encaminhar, para fins de habilitação, as provas de regularidade fiscal pertinente a ambos os números.

13.5. A forma de pagamento referida no subitem 13.1 deste item é cláusula indisponível à licitante, sendo que qualquer outra forma de pagamento porventura disposta na proposta será desconsiderada.

13.6. Para todos os fins, considera-se como data do pagamento, o dia da emissão da ordem bancária.

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

13.7. No caso de os documentos de habilitação fiscal, social e trabalhista estiverem vencidos quando da apresentação do documento fiscal, a licitante deverá providenciar a regularização.

13.8. Na eventualidade de atraso no pagamento entre a data do vencimento e a data do efetivo pagamento, serão devidos por este TRT:

a) juros de mora de 0,5% a.m. (cinco décimos por cento ao mês) ou 6% a.a. (seis por cento ao ano), por dia de atraso na efetivação do pagamento;

b) multa moratória no percentual de 1% (um por cento) do valor da fatura em atraso; e

c) atualização financeira pelo IGP-DI.

13.9. Não serão devidas quaisquer taxas de atualização financeira, juros ou multa moratória nas hipóteses em que houver a concorrência da contratada para o atraso no pagamento.

14. DA GARANTIA CONTRATUAL

14.1. As regras para garantia contratual estão previstas na Minuta do Contrato.

15. DA PROTEÇÃO DE DADOS

15.1. As regras para proteção de dados estão previstas na Minuta do Contrato.

16. DA GESTÃO E FISCALIZAÇÃO DO CONTRATO

16.1. As regras para gestão e fiscalização do contrato estão previstas no Termo de Referência e Minuta do Contrato.

17. DAS DISPOSIÇÕES GERAIS

17.1. Será divulgada ata da sessão pública no sistema eletrônico.

17.2. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário, pelo pregoeiro.

17.3. Todas as referências de tempo no Edital, no aviso e durante a sessão pública observarão o horário de Brasília - DF.

17.4. É vedada a subcontratação do objeto contratual, não sendo considerada subcontratação a atuação do fabricante da solução nas atividades inerentes ao fornecimento, operação, manutenção, atualização e suporte técnico especializada da plataforma, permanecendo a contratada integralmente responsável pelo cumprimento das obrigações contratuais.

17.5. A homologação do resultado desta licitação não implicará direito à contratação.

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

17.6. As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.

17.7. Os licitantes assumem todos os custos de preparação e apresentação de suas propostas e a Administração não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

17.8. Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente no TRT da 4ª Região.

17.9. A contratada, o preposto e os empregados, vinculados à presente contratação, deverão conhecer e observar a Resolução Administrativa TRT4 nº 11/2025, que regulamenta o tratamento das notícias de assédio moral, assédio sexual e discriminação no âmbito da Justiça do Trabalho da 4ª Região, de acordo com a Política de Prevenção e Combate ao Assédio Moral na Justiça do Trabalho de 1º e 2º graus e com a Política de Prevenção e Enfrentamento do Assédio Moral, do Assédio Sexual e da Discriminação.

17.10. Os procedimentos de assinatura de documentos do processo serão feitos via Portal PROAD (Processo Administrativo deste TRT), mediante cadastramento prévio do representante legal da licitante junto ao TRT da 4ª Região.

17.10.1. É de exclusiva responsabilidade do usuário o sigilo e o uso das senhas, não cabendo ao TRT da 4ª Região a responsabilidade por eventuais danos decorrentes de uso indevido das senhas, ainda que por terceiros.

17.11. Todas as despesas decorrentes da presente licitação correrão por conta de recursos específicos consignados para este Tribunal no Orçamento Geral da União para o(s) exercício(s) de 2026 e 2029, Programa de Trabalho: 214192 - Segurança da Informação nas Unidades do Poder Judiciário, Classificação: 33904006 - locação de software, 33904019 - computação de nuvem - software como serviço (SAAS) e 33904011 - suporte de infraestrutura de TIC e Programa de Trabalho: [214193] - Capacitação de Servidores de TI, Classificação: 33904020 - treinamento/capacitação em TIC, os quais serão discriminados nas respectivas notas de empenho.

17.12. Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital.

17.13. O Edital e seus anexos estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas (PNCP) e endereço eletrônico https://www.trt4.jus.br/portais/trt4/licitacoes-compras-e-contratos.

17.14. Integram este Edital, para todos os fins e efeitos, os seguintes anexos:

17.14.1. ANEXO I DO EDITAL- Termo de Referência

17.14.1.1. Anexo I do Termo de Referência - Especificações Técnicas da Solução

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

17.14.1.2. Anexo II do Termo de Referência - Termo de Compromisso com a Segurança da Informação

17.14.1.3. Anexo III do Termo de Referência - Formulário de Pesquisa de Preço

17.14.1.4. Anexo IV do Termo de Referência - Estudo Técnico Preliminar

17.14.2. ANEXO II DO EDITAL - Minuta de Ata de Registro de Preços

17.14.3. ANEXO III DO EDITAL - Formulário para Manifestação de Interesse no Cadastro de Reserva de Ata de Registro de Preços

17.14.4. ANEXO IV DO EDITAL - Modelo de Proposta

17.14.5. ANEXO V DO EDITAL - Minuta de Contrato

17.14.5.1. Anexo I da Minuta de Contrato - Especificações Técnicas da Solução

17.14.5.2. Anexo II da Minuta de Contrato - Termo de Compromisso com a Segurança da Informação

Porto Alegre/RS, 24 de novembro de 2026.

Documento assinado digitalmente

KARINA DURIGON

Coordenadora de Licitações e Contratos

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

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

TERMO DE REFERÊNCIA

1 DEFINIÇÃO DO OBJETO

1.1. 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, conforme condições, quantidades e exigências estabelecidas neste instrumento.

1.2. Detalhamento dos bens e serviços que compõem a solução:

Item	Descrição	Unidade	Quantidade compra inicial	Quantidade total do registro
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos (XDR) pelo período de 36 meses	Ativo monitorado	0	61.500
2	Subscrição do Módulo de Detecção e Resposta a Ameaças de Identidade (ITDR) pelo período de 36 meses	Usuários ativos	0	54.850
3	Módulo de solução Agêntica para resposta, orquestração e triagem de eventos e incidentes	Tokens	0	748.300
4	Ingestão de logs externos	Franquia de Gigabyte por dia	0	9.590
5	Serviço de treinamento na solução proposta	Serviço único, por turma de treinamento	0	21
6	Serviço de implantação da solução proposta	Serviço único por contratante	0	17
7	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Serviço fixo para 2000 ativos monitorados por mês	0	17
8		Serviço para 1000 ativos adicionais monitorados por mês	0	33

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

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

1.3. Os itens do objeto devem ser agrupados em grupo[1]?

(x) Sim - Justificativa para o não parcelamento do objeto:

A contratação em lote único justifica-se pela interdependência técnica dos componentes da solução de segurança cibernética, que exige perfeita integração tecnológica entre os módulos, compartilhamento de informações e funcionamento coordenado dos recursos de monitoramento, detecção, investigação e resposta a incidentes.

( ) Não

1.4. A Ata de Registro de Preços resultante da presente licitação terá como órgão gerenciador o Tribunal Regional do Trabalho da 4ª Região (UASG 080014) e os seguintes órgãos participantes:

1.4.1 Tribunal Regional do Trabalho da 1ª Região – TRT1 (UASG: 080009)
1.4.2 Tribunal Regional do Trabalho da 3ª Região – TRT3 (UASG: 080008)
1.4.3 Tribunal Regional do Trabalho da 5ª Região – TRT5 (UASG: 080007)
1.4.4 Tribunal Regional do Trabalho da 6ª Região – TRT6 (UASG: 080006)
1.4.5 Tribunal Regional do Trabalho da 7ª Região – TRT7 (UASG: 080004)
1.4.6 Tribunal Regional do Trabalho da 9ª Região – TRT9 (UASG: 080012)
1.4.7 Tribunal Regional do Trabalho da 10ª Região – TRT10 (UASG: 080016)
1.4.8 Tribunal Regional do Trabalho da 11ª Região – TRT11 (UASG: 080002)
1.4.9 Tribunal Regional do Trabalho da 14ª Região – TRT14 (UASG: 080015)
1.4.10 Tribunal Regional do Trabalho da 16ª Região - TRT16 (UASG 080018)
1.4.11 Tribunal Regional do Trabalho da 18ª Região - TRT18 (UASG 080020)
1.4.12 Tribunal Regional do Trabalho da 19ª Região - TRT19 (UASG 080022)
1.4.13 Tribunal Regional do Trabalho da 20ª Região - TRT20 (UASG 080023)
1.4.14 Tribunal Regional do Trabalho da 21ª Região - TRT21 (UASG 080021)
1.4.15 Tribunal Regional do Trabalho da 22ª Região - TRT22 (UASG 080024)
1.4.16 Tribunal Superior do Trabalho - TST (UASG:080001).

---

[1] 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.

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

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

1.5. Quantidades por órgão participante:

		Quantidade total para registro																
Item	**Descrição**	**TRT1**	**TRT3**	**TRT4**	**TRT5**	**TRT6**	**TRT7**	**TRT9**	**TRT10**	**TRT11**	**TRT14**	**TRT16**	**TRT18**	**TRT19**	**TRT20**	**TRT21**	**TRT22**	**TST**
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos (XDR)	7.000	6.500	6.500	6.500	4.000	2.500	6.000	2.700	2.000	1.600	1.500	2.700	1.500	1.500	2.000	1.000	6.000
2	Subscrição do Módulo de Detecção e Resposta a Ameaças de Identidade (ITDR)	6.000	9.450	4.500	5.000	2.500	2.400	5.000	3.200	1.200	1.300	1.100	2.700	1.300	1.300	2.000	900	5.000
3	Módulo de solução Agêntica para resposta, orquestração e triagem de eventos e incidentes	72.000	72.000	72.000	72.000	36.000	36.000	72.000	36.000	40.000	36.000	36.000	25.200	13.500	30.000	25.200	14.400	60.000
4	Ingestão de logs externos - Franquia de Gigabyte por dia por 36 meses	1.000	1.000	1.000	1.000	150	500	1.000	1.000	400	400	400	450	25	100	150	15	1.000
5	Serviço de treinamento na solução proposta	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	3
6	Serviço de implantação da solução proposta	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
7	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
8		5	5	5	5	2	1	4	1	0	0	0	1	0	0	0	0	4

2 PREVISÃO NO PLANO DE CONTRATAÇÕES DE TIC

2.1. A demanda está prevista no Plano de Contratações de TIC de 2026 e no Plano de Contratações Anual do Tribunal (PCA), conforme ID SGTI-18/2026 e 67/2026.

3 FUNDAMENTAÇÃO DA CONTRATAÇÃO

3.1. A fundamentação da presente contratação faz parte dos estudos técnicos preliminares constantes nos seguintes documentos:

3.1.1 Documento de Oficialização da Demanda;

3.1.2 Estudos Técnicos Preliminares;

3.1.3 Mapa de Riscos.

4 DESCRIÇÃO DA SOLUÇÃO COMO UM TODO[2]

4.1. 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.

4.2. 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.

4.3. 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.

4.4. 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.

---

2 A descrição da solução como um todo deverá considerar o ciclo de vida do objeto, na sua totalidade, inclusive a especificação da garantia, quando couber, e as exigências relacionadas à manutenção e à assistência técnica, quando for o caso, de modo a permitir a avaliação da viabilidade técnica e econômica da contratação.

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

5 ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO

5.1. Especificações técnicas

5.1.1 As especificações técnicas constam no Anexo I.

CRITÉRIOS DE SUSTENTABILIDADE

5.2. A contratação possui critérios de sustentabilidade e/ou observou as práticas sustentáveis do Guia de Contratações?

( ) Não

(x) Sim - Discrimine a seguir:

5.2.1 A solução a ser contratada promove a transformação digital ou racionalização de serviços atualmente realizados por meio de análise humana, especificamente através de recursos de inteligência artificial para a correlação de eventos e geração de relatórios.

5.2.2 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;

5.2.3 Assinatura digital é um ato de transformação digital, portanto, sustentável;

5.2.4 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.

6 MODELO DE EXECUÇÃO DO OBJETO

6.1. Prazos e Condições:

6.1.1 A vigência do contrato terá início com sua assinatura e encerra-se no prazo de **36 meses** contados da data de início da prestação dos serviços (data do recebimento definitivo do objeto), podendo ser prorrogado, na forma dos artigos 106 e 107 da Lei nº 14.133/2021.

6.1.1.1 Na hipótese de serem celebrados contratos posteriores para qualquer item ou serviço diverso do Item 1, a vigência desses contratos se findará no mesmo dia de encerramento do contrato do Item 1.

6.1.2 No prazo máximo de **10 dias**, contados da assinatura do contrato, deverá ser realizada a reunião inicial de gestão do contrato.

6.1.2.1 Deverão estar presentes na reunião o preposto e um integrante da equipe técnica da contratada.

6.1.2.2 A pauta da reunião deverá abordar o planejamento detalhado da implantação da solução contratada, além das condições contratuais.

6.1.3 A disponibilização das subscrições e serviços (itens 1, 2, 3 e 4), e a execução completa da Implantação da Solução (item 6) devem ocorrer em até **60 dias** a contar da assinatura do contrato.

6.1.4 A vigência das subscrições dos itens 1 e 2 será de **36 meses**, contados a partir da data de emissão do Termo de Recebimento Definitivo do objeto, após a conclusão da implantação e a entrada da solução em produção, em pleno funcionamento, de acordo com as especificações do fabricante da solução e em conformidade com os requisitos da contratação.

6.1.4.1 As subscrições poderão ser disponibilizadas de forma anual, hipótese em que cada disponibilização deverá assegurar o período de vigência correspondente, observadas as condições estabelecidas na contratação.

6.1.4.2 Durante a etapa de implantação, é facultado à contratada o uso de licenças temporárias (trial), visando não onerá-la antes da efetiva entrada em produção, evitando o cômputo precoce do prazo de vigência das subscrições, desde que tais licenças não apresentem limitações ao uso inicial da solução.

6.1.4.3 Eventuais atrasos na implantação motivados pelo Contratante não postergarão o início da vigência das subscrições já adquiridas e disponibilizadas, desde que estas estejam efetivamente disponíveis para uso, conforme as condições estabelecidas na contratação.

6.1.4.4 Caso a contratação das subscrições referentes ao Item 2 ocorra em data posterior à contratação do Item 1, a vigência das subscrições do Item 2 deverá ser ajustada de modo que sua data de encerramento coincida com a data de encerramento das subscrições do Item 1.

6.1.4.4.1 Na hipótese prevista no subitem anterior, o valor das subscrições do Item 2 será calculado proporcionalmente ao período efetivo de sua vigência, com base no preço unitário contratado.

6.1.5 O serviço gerenciado (itens 7 e 8) terá início imediatamente após o recebimento definitivo do objeto e possuirá vigência de 36 meses.

6.1.6 O treinamento (item 5) deverá ser concluído no prazo máximo de 180 dias a contar da assinatura do contrato.

6.2. Garantia

6.2.1 A solução como um todo, englobando software, módulos, coletores, sensores, integrações e serviços associados, deverá contar com garantia e suporte integrais prestados pela CONTRATADA com respaldo do fabricante (Garantia Compreensiva), durante todo o período de vigência contratual.

6.2.2 A garantia deve cobrir a correção de quaisquer bugs, falhas de funcionamento, erros de código, atualizações de assinaturas, atualizações de versão (major e minor releases), patches e hotfixes, sem nenhum custo adicional para o CONTRATANTE.

6.2.3 A assistência técnica em garantia deve assegurar o fornecimento de acesso irrestrito (24 horas por dia, 7 dias da semana) do CONTRATANTE à área de suporte do fabricante, especialmente ao endereço eletrônico (web site) e a toda a documentação técnica pertinente (guias de instalação e configuração atualizados, FAQ's, bases de conhecimento e bases de soluções, com pesquisa efetuada através de ferramentas de busca).

6.3. Serviço de Suporte Técnico

6.3.1 O suporte técnico inclui todos os serviços técnicos necessários para assegurar o pleno funcionamento da solução conforme as especificações do objeto, sem qualquer custo adicional para o CONTRATANTE.

6.3.2 Os serviços de suporte deverão ser corretivos, proativos e consultivos, envolvendo atividades como: auxílio na configuração de políticas e administração da solução; garantia do fornecimento e da instalação de novas versões, patches e hotfixes (tanto de componentes on premises quanto em nuvem); análise de dúvidas sobre melhores práticas de configuração, entre outros.

6.3.3 A abertura de chamados pelo CONTRATANTE deve poder ser efetuada:

6.3.3.1 Pela plataforma web, em sistema de atendimento da CONTRATADA;

6.3.3.2 Pelo envio de mensagem de correio eletrônico;

6.3.3.3 Por meio do módulo de gestão de incidentes de segurança da solução ofertada;

6.3.3.4 Por telefone.

6.3.4 O atendimento aos chamados deve estar disponível em regime 24x7x365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco

dias ao ano).

6.3.5 Não poderá haver qualquer restrição de quantidade de abertura de chamados no suporte técnico.

6.3.6 Todas as comunicações e documentação relacionada aos atendimento de chamados deverão ser realizadas ou disponibilizadas em Português.

6.3.7 Para a aferição e a avaliação dos níveis de serviço, a CONTRATADA deverá apresentar mensalmente à fiscalização do contrato um relatório gerencial de serviços, até o quinto dia útil do mês subsequente ao da prestação do serviço. O relatório deverá conter, entre outras informações, a medição dos indicadores/metas de níveis de serviço, recomendações técnicas, e demais informações relevantes para a gestão contratual.

6.3.8 Os prazos de solução dos chamados deverão atender aos seguintes critérios:

Severidade	Classificação	Prazo de Solução
A0 - Crítica	Chamados referentes a situações de emergência ou problema crítico, caracterizados pela existência de ambiente paralisado.	2 horas a contar da abertura do chamado
A1 - Alta	Chamados associados a situações de alto impacto, incluindo os casos de degradação severa de desempenho.	6 horas a contar da abertura do chamado
A2 - Média	Chamados referentes a situações de baixo impacto ou para aqueles problemas que se apresentem de forma intermitente.	2 dias úteis a contar da abertura do chamado
A3 - Baixa	Chamados com objetivo de sanar dúvidas quanto ao uso ou à implementação do produto, dúvidas, problemas na utilização, esclarecimentos da documentação, sugestões, Impacto mínimo para os usuários.	5 dias úteis a contar do próximo dia útil da abertura do chamado
A4 - Pesquisa	Chamados com objetivo de melhorar a ferramenta, implantar novas funcionalidades ou configurações que demandem tempo e planejamento	10 dias úteis a contar do próximo dia útil da abertura do chamado

6.4. Serviço de suporte a incidentes

6.4.1 O serviço de operação e gestão da solução deverá classificar os incidentes de segurança conforme a seguir:

Prioridade	Descrição do impacto	Peso
P0 - Crítico	Alertas de invasão de ativos classificados como críticos; Comprometimento em massa de dados sensíveis; Comprometimento de credenciais administrativas; Movimentação lateral no ambiente;	**4**
P1 - Alto	Degradação de ativos classificados como críticos; Comprometimento parcial de dados sensíveis; Comprometimento de credenciais não administrativas;	**3**
P2 - Médio	Comprometimento ou degradação de ativos classificados como não críticos; Comprometimento de dados não sensíveis;	**2**
P3 - Baixo	Comprometimento ou degradação de ativos classificados como de baixa relevância. Representa uma oportunidade de melhoria no ambiente.	**1**

* ‘Dado pessoal sensível’ terá o significado da LGPD. A criticidade da informação observará adicionalmente a política de segurança da informação do CONTRATANTE.

6.4.2 Os seguintes Indicadores de Nível de Serviço de incidentes de segurança serão considerados:

Prioridade	Tempo máximo de percepção do incidente de segurança (MTTD)	Tempo máximo de resposta ao incidente de segurança	Tempo máximo de contenção (MTTR)
P0 - Crítico	15 min	35 min	90 min
P1 - Alto	30 min	90 min	150 min
P2 - Médio	2 horas	6 horas	10 horas
P3 - Baixo	4 horas	12 horas	24 horas

6.4.2.1 Tempo máximo de percepção do incidente de segurança: é o limite contratual (SLA) que estabelece o tempo máximo aceitável para que a plataforma ou serviço correlacione a telemetria e identifique uma atividade maliciosa, medindo o intervalo entre a primeira evidência técnica do ataque no ambiente e a geração do alerta qualificado para os analistas. Essa métrica atua como o teto para o tempo de detecção (MTTD), visando minimizar a

permanência velada do atacante na rede (dwell time) e servindo como parâmetro objetivo de conformidade e aplicação de penalidades ao fornecedor.

6.4.2.2 Tempo máximo de resposta ao incidente de segurança: é o limite contratual de tempo (SLA) exigido para que, a partir do momento em que uma ameaça é detectada e qualificada, sejam executadas as medidas operacionais e automatizadas de contenção e mitigação interrompendo ativamente a progressão do ataque e minimizando o impacto no ambiente antes que a remediação definitiva seja concluída.

6.4.2.3 Tempo Máximo de Contenção: é o limite temporal estabelecido para que a equipe de analistas investigue, realize a triagem e confirme a veracidade de um alerta gerado pela plataforma, medindo o intervalo entre a emissão do alerta e a sua classificação definitiva como um incidente real (verdadeiro positivo) ou um alarme falso (falso positivo).

6.4.2.4 Todos os tempos serão contados a partir do início do incidente de segurança. O tempo de início é medido a partir do momento em que houver registros das atividades maliciosas ou a partir do momento que houver impacto resultante da atividade maliciosa - o que ocorrer primeiro.

6.4.2.4.1 Os tempos serão aferidos com base nos registros de data e hora do sistema de gestão de incidentes, relacionados aos registros da plataforma, disponibilizados para auditoria.

6.4.2.5 Quando o atendimento de um incidente depender de providência a cargo do CONTRATANTE, a contagem do tempo para cumprimento do SLA será suspensa durante o período de efetiva dependência dessa providência, sendo retomada a partir de seu atendimento pelo CONTRATANTE.

6.4.2.5.1 A suspensão da contagem somente será admitida quando houver dependência objetiva de providência do CONTRATANTE, devidamente registrada pela CONTRATADA, com indicação da ação requerida, da data e hora do acionamento, das evidências correspondentes e da data e hora do atendimento da solicitação pelo CONTRATANTE. Não será admitida a suspensão retroativa da contagem.

6.4.2.5.2 Quando o período de suspensão ultrapassar o dobro do tempo máximo previsto para validação e houver mais de um acionamento do CONTRATANTE para a mesma finalidade, a justificativa para a duração da suspensão deverá ser formalmente

registrada e submetida à validação do CONTRATANTE. A suspensão somente será considerada válida se comprovada a efetiva necessidade do tempo utilizado para as validações, não sendo admitida sua utilização indevida para afastar ou reduzir a responsabilidade da CONTRATADA pelo cumprimento dos níveis de serviço estabelecidos.

6.4.2.5.3 Não serão incluídos na contagem de totais os incidentes abertos e fechados de forma automática. Em caso de um incidente fechado de forma automática se mostrar como verdadeiro-positivo, este será tratado como se houvesse descumprimento de SLA.

6.4.2.6 O descumprimento de qualquer um dos tempos descritos nos Indicadores de Nível de Serviço será considerado como incidente de segurança não atendido no prazo.

6.4.2.7 O descumprimento dos níveis descritos implicará em glosa a ser aplicada sobre a parcela total mensal dos itens 7 e 8, conforme tabela a seguir:

6.4.2.7.1 Periodicidade de medição: Mensal

6.4.2.7.2 Fórmula: somatória ponderada dos incidentes que descumpriram o SLA dividida pela somatória ponderada de todos os chamados.

6.4.2.7.3 ICSLA = (QTin / Tin) * 100

6.4.2.7.4 ICSLA = Índice de Conformidade de SLA

6.4.2.7.5 QTin = Quantidade de incidentes de segurança atendidos nos prazos: $\Sigma_{\text{Incidentes com SLA cumprido}}$(P0 * peso P0 + P1 * peso P1 + P2 * peso P2 + P3 * peso P3)

6.4.2.7.6 Tin = Total de incidentes de segurança registrado: $\Sigma_{\text{incidentes}}$(P0 * peso P0 + P1 * peso P1 + P2*peso P2 + P3 * peso P3)

6.4.2.7.7 Apuração e Glosa:

Faixa	Níveis Alcançados	Glosa
1	ICSLA => 95%	Sem glosa
2	90% <= ICSLA < 95%	5%
3	85% <= ICSLA < 90%	10%
4	ICSLA < 85%	20%

6.4.2.8 Todo incidente do tipo P0 e P1 (crítico e alto) deverá ser comunicado por telefone, além do registro no sistema de tíquetes;

6.4.2.9 Para P0/P1, a CONTRATADA apresentará relatório com linha do tempo, vetor, MITRE ATT&CK quando aplicável, ativos afetados, evidências, causa-raiz/hipóteses, contenção, remediação, impacto, lições, recomendações, responsáveis e prazos.

6.4.2.10 A classificação A0–A4 aplica-se exclusivamente ao suporte técnico. P0–P3 aplica-se aos incidentes de segurança. Em sobreposição, prevalecerá a classificação de incidente de segurança.

6.5. Índice de disponibilidade

6.5.1 A disponibilidade mensal da solução será apurada com base nos registros da própria plataforma e, quando disponível, em mecanismo independente de monitoramento. A perda de coleta de dados, de telemetria ou de cobertura dos ativos monitorados deverá ser aferida por indicadores próprios.

6.5.2 O índice mensal de disponibilidade da solução deverá ser igual ou superior a 99,8%.

6.5.3 Caso o índice mensal de disponibilidade seja inferior a **99,8%**, será aplicada glosa no percentual correspondente a 10 vezes a diferença entre a disponibilidade medida no mês e a disponibilidade mínima contratada, sobre o valor mensal dos itens 7 e 8.

6.6. Deveres e Responsabilidades do Tribunal:

6.6.1 Proporcionar as facilidades indispensáveis à boa execução dos serviços.

6.6.2 Relatar, por escrito, com a devida comprovação, as eventuais irregularidades na prestação de serviços;

6.6.3 Sustar a execução de quaisquer trabalhos por estarem em desacordo com o especificado ou por qualquer outro motivo que caracterize a necessidade de tal medida;

6.6.4 Efetuar os pagamentos devidos.

6.7. Deveres e Responsabilidades da Contratada:

6.7.1 Indicar um preposto para o contrato, sendo este o interlocutor da contratada junto ao Tribunal para os assuntos relativos ao cumprimento das cláusulas contratuais e para participar de reuniões de acompanhamento, sempre que solicitado pelo CONTRATANTE.

6.7.2 Responsabilizar-se técnica e administrativamente pelo objeto contratado,

não sendo aceita, sob qualquer pretexto, a transferência de responsabilidade a outras entidades, sejam fabricantes, técnicos ou quaisquer outros.

6.7.3 Responder integralmente por perdas e danos que vier a causar ao CONTRATANTE ou a terceiros em razão de ação ou omissão, dolosa ou culposa, sua ou dos seus prepostos, independentemente de outras combinações contratuais ou legais a que estiver sujeita.

6.7.4 Fornecer a seus empregados todos os instrumentos necessários à execução dos serviços.

6.7.5 Informar a relação dos empregados que prestarão serviços nas dependências deste Regional.

6.7.6 Responder pelas despesas relativas a encargos trabalhistas, de seguro de acidentes, impostos, contribuições previdenciárias e quaisquer outras que forem devidas e referentes aos serviços executados por seus empregados, uma vez que estes não têm nenhum vínculo empregatício com o Tribunal.

6.7.7 Responder por valores adicionais ao valor do contrato, tais como custos de deslocamento, alimentação, transporte, alojamento, trabalho em sábados, domingos, feriados ou em horário noturno, bem como qualquer outro valor adicional.

6.7.8 Garantir o mais rigoroso sigilo sobre quaisquer dados, informações, documentos e especificações a que venham a ter acesso em razão dos serviços prestados, não podendo, sob qualquer pretexto, revelá-los, divulgá-los ou reproduzi-los, conforme o Termo de Compromisso com a Segurança da Informação (Anexo II).

6.7.9 Manter, durante toda a vigência do contrato, as condições de habilitação exigidas na contratação.

6.7.10 Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual.

6.7.11 Propiciar todos os meios necessários à fiscalização do contrato pela contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, sempre que considerar a medida necessária.

6.7.12 Quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de Tecnologia da Informação e Comunicação (TIC).

6.8. Subcontratação:

6.8.1 É vedada a subcontratação do objeto contratual, não sendo considerada subcontratação a atuação do fabricante da solução nas atividades inerentes ao fornecimento, operação, manutenção, atualização e suporte técnico especializada da plataforma, permanecendo a contratada integralmente responsável pelo cumprimento das obrigações contratuais.

6.9. Consórcio:

6.9.1 Não será admitida a participação de empresas reunidas em consórcio, nos termos do art. 15 da Lei nº 14.133/2021, visando assegurar a execução integrada e coordenada do objeto e evitar a fragmentação das responsabilidades entre o fornecimento das subscrições de software e os serviços de implantação, treinamento, suporte, monitoramento, detecção, investigação e resposta a incidentes.

7 MODELO DE GESTÃO DO CONTRATO

7.1. Indicação da Equipe de Gestão e Fiscalização do Contrato:

Integrante	Titular	Substituto	Unidade
Gestor:	Carlos Costa Jordão	Charles Ferreira Falcao	Coordenadoria de Segurança da Informação e Proteção de Dados
Fiscal Técnico:	Maurício Antonioli Schmitz	Carlos Augusto Nantes de Castilho Rivilino	Coordenadoria de Segurança da Informação e Proteção de Dados
Fiscal Demandante:	Rodrigo Zarth	Mateus Both	Coordenadoria de Segurança da Informação e Proteção de Dados
Fiscal Administrativo:	Alberto Daniel Müller	Ricardo Krause Kurylenko	Coordenadoria de Gestão e Apoio à Governança de TIC

7.2. Procedimentos de Gestão e Fiscalização do Contrato:

7.2.1 O gestor do contrato ficará responsável por:

7.2.1.1 Organizar a reunião inicial;

7.2.1.2 Encaminhar alterações contratuais;

7.2.1.3 Controlar prazos e indicadores contratuais;

7.2.1.4 Atestar notas fiscais;

7.2.1.5 Tratar eventuais irregularidades constatadas na execução contratual;

7.2.1.6 Realizar o recebimento definitivo, emitindo o respectivo termo;

7.2.1.7 Verificar as obrigações previstas no encerramento do contrato.

7.2.2 O Fiscal Administrativo do contrato ficará responsável por:

7.2.2.1 Participar da reunião inicial;

7.2.2.2 Conferir cumprimento de prazos contratuais;

7.2.2.3 Conferir o atendimento dos níveis de serviços contratados;

7.2.2.4 Conferir documentação exigida no contrato;

7.2.2.5 Verificar a conformidade do faturamento do objeto contratado;

7.2.2.6 Informar ao gestor do contrato qualquer irregularidade na execução do objeto ou descumprimento dos níveis de serviços contratados;

7.2.3 O fiscal demandante do contrato ficará responsável por:

7.2.3.1 Participar da reunião inicial;

7.2.3.2 Acompanhar a execução do objeto de acordo com o contrato;

7.2.3.3 Monitorar cumprimento de prazos contratuais;

7.2.3.4 Encaminhar demandas para a contratada por meio de ordens de serviço e/ou chamados;

7.2.3.5 Aferir as entregas da execução em relação ao objeto contratado;

7.2.3.6 Atestar se os requisitos de negócio da contratação foram atendidos;

7.2.3.7 Informar ao gestor do contrato qualquer irregularidade na execução do objeto ou descumprimento dos níveis de serviços contratados.

7.2.4 O fiscal técnico do contrato ficará responsável por:

7.2.4.1 Participar da reunião inicial;

7.2.4.2 Acompanhar a execução do objeto de acordo com o contrato;

7.2.4.3 Monitorar cumprimento de prazos contratuais;

7.2.4.4 Encaminhar demandas para a contratada por meio de ordens de serviço e/ou chamados;

7.2.4.5 Aferir as entregas da execução em relação ao objeto contratado;

7.2.4.6 Atestar se os requisitos técnicos da contratação foram atendidos;

7.2.4.7 Assinar o ateste de fiscalização do contrato, quando cabível;

7.2.4.8 Informar ao gestor do contrato qualquer irregularidade na execução do objeto ou descumprimento dos níveis de serviços contratados.

7.3. Mecanismos Formais de Comunicação

7.3.1 Será realizada uma reunião inicial do contrato com a participação da contratada, do gestor e fiscais do contrato.

7.3.2 O mecanismo formal de comunicação utilizado no contrato será o e-mail, conforme detalhamento a seguir:

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

Assunto	E-mail
Envio de notas fiscais	Deve ser feito através do sistema SIGEO-JT
Informações sobre faturamento	sgti.contratos@trt4.jus.br
Informações técnicas	setic.csipd@trt4.jus.br

8 CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

8.1. O objeto será recebido da seguinte forma:

8.1.1.1 Provisoriamente, com verificação posterior da conformidade do objeto com os requisitos da contratação e;

8.1.1.2 Definitivamente, após a verificação do atendimento dos requisitos da contratação.

8.2. Detalhamento dos Critérios de Medição e Pagamento

Item	Descrição	Forma de Recebimento	Prazo	Forma de pagamento
1	Entrega das subscrições de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Termo de Recebimento Definitivo	60 dias da assinatura do contrato	Pagamento anual após o recebimento definitivo do objeto
2	Entrega das subscrições de Módulo de Detecção e Resposta a Ameaças de Identidade (ITDR)	Termo de Recebimento Definitivo	60 dias da assinatura do contrato	Pagamento anual após o recebimento definitivo do objeto
3	Módulo de solução Agêntica para resposta, orquestração e triagem de eventos e incidentes	Ateste na nota fiscal	mensal	Pagamento mensal
4	Disponibilização da ingestão de logs externos	Termo de Recebimento Definitivo	60 dias da assinatura do contrato	Pagamento anual após o recebimento definitivo do objeto
5	Realização do Treinamento	Ateste na nota fiscal	180 dias da assinatura do contrato	Pagamento único após a realização do treinamento
6	Conclusão do serviço de implantação	Termo de Recebimento Definitivo	60 dias da assinatura do contrato	Pagamento único após o recebimento definitivo do objeto
7 e 8	Prestação do serviço mensal de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Ateste na nota fiscal	mensal	Pagamento mensal após a realização do serviço

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

8.3. Os itens 1, 2 e 4 serão pagos em 3 (três) parcelas anuais, de igual valor, condicionadas à disponibilização anual das respectivas licenças e observados os seguintes marcos de pagamento: a primeira parcela será paga após a emissão do respectivo Termo de Recebimento Definitivo; a segunda, em até 12 (doze) meses após o pagamento da primeira; e a terceira, em até 12 (doze) meses após o pagamento da segunda. A segunda e a terceira parcelas são reajustáveis pelo ICTI (Índice de Custo de Tecnologia da Informação).

8.4. O item 3 será pago mensalmente com base em um dos seguintes critérios:

8.4.1 Quantidade de tokens consumidos no período de apuração, de acordo com os registros de consumo da solução, devendo a CONTRATADA apresentar a memória de cálculo juntamente com o relatório mensal de medição.

8.4.2 Quantidade de tokens previamente estimados pela fiscalização do contrato para consumo no período de apuração.

8.5. O pagamento dos itens 7 e 8 será realizado mensalmente, após a execução dos serviços e entrega ao CONTRATANTE, pela CONTRATADA, dos resultados dos indicadores apurados.

8.6. A contratada deverá efetuar cadastro no Portal do SIGEO - JT para apresentação dos Documentos Fiscais (Notas Fiscais) com vistas à liquidação e pagamento das faturas.

8.6.1 Por meio do link https://sigeo.jt.jus.br/ajuda, a contratada terá acesso ao link do SIGEO – JT e a um guia detalhado das funcionalidades do sistema.

9 REAJUSTE CONTRATUAL

9.1. O reajuste contratual, quando cabível, será aplicado de acordo com o Índice de Custo da Tecnologia da Informação (ICTI), estabelecido no guia da Resolução 468 do CNJ.

10 ESTIMATIVA DO VALOR DA CONTRATAÇÃO

10.1. O valor total estimado para a contratação é de R$ 74.913.935,98

10.1.1 O valor total estimado para o Tribunal Regional do Trabalho da 4ª Região é de R$ 7.608.927,54

10.2. O detalhamento da pesquisa de preços realizada consta no Anexo III do Termo de Referência.

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

11 ADEQUAÇÃO ORÇAMENTÁRIA

( ) 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:

12 FORMA DE SELEÇÃO DO FORNECEDOR

Forma de Seleção
(x) Pregão Eletrônico
( ) Concorrência
( ) Dispensa de Licitação
( ) Outra:

Hipóteses para utilização do Sistema de Registro de Preços:
( ) Necessidade de contratações permanentes ou frequentes devido às características do objeto.
( ) É conveniente a aquisição de bens com previsão de entregas parceladas ou contratação de serviços remunerados por unidade de medida, por quantidade de horas de serviço ou em regime de tarefa.
(x) É conveniente para atendimento a mais de um órgão ou entidade.
( ) Não é possível definir previamente o quantitativo a ser demandado pela administração, devido à natureza do objeto.
Execução de obras e serviços de engenharia: ( ) Existência de projeto padronizado, sem complexidade técnica e operacional; ( ) Necessidade permanente ou frequente de obra ou serviço a ser contratado.
( ) Não será utilizado Sistema de Registro de Preços.
Deverá ser prevista no Edital a renovação dos quantitativos no caso de prorrogação da Ata de Registro de Preços? ( ) Sim (x) Não

Critério de Julgamento

( ) Menor preço por item
( ) Menor preço por grupo de itens
(x) Menor preço global
( ) Maior desconto
( ) Outro:

13 CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

13.1. Os critérios de habilitação jurídica, fiscal, social, trabalhista e econômico-financeira serão previstos no edital.

13.2. Os critérios de habilitação técnica a serem atendidos pelo fornecedor serão:

13.2.1 Qualificação técnico-profissional:

13.2.1.1 A licitante deverá indicar os profissionais das equipes técnicas com apresentação da seguinte documentação:

13.2.1.1.1 Pelo menos 3 (três) profissionais da equipe técnica **responsáveis pela implantação e sustentação da solução** deverão ter certificação oficial do fabricante da solução proposta de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos (itens 1 a 4 da contratação). Não serão aceitos certificados de participação em cursos ou workshops.

13.2.1.1.2 Os profissionais da equipe técnica **responsáveis pela detecção, notificação e investigação de ataques cibernéticos** deverão possuir certificação em segurança ofensiva, detendo, individualmente ou em conjunto, pelo menos 3 (três) das seguintes certificações, contabilizando no máximo 2 (dois) certificados por profissional:

13.2.1.1.2.1 CompTIA PenTest+;

13.2.1.1.2.2 EC-Council Licensed Penetration Tester (LPT);

13.2.1.1.2.3 IACRB Certified Expert Penetration Tester (CEPT);

13.2.1.1.2.4 GIAC Exploit Researcher and Advanced Penetration Tester (GXPN);

13.2.1.1.2.5 GIAC Reverse Engineering Malware (GREM);

13.2.1.1.2.6 Offensive Security Certified Professional (OSCP);

13.2.1.1.2.7 Ethical Hacking Post Exploitation (EHPX);

13.2.1.1.2.8 Offensive Security Experienced Penetration Tester (OSEP);

13.2.1.1.2.9 Offensive Security Web Expert (OSWE);

13.2.1.1.2.10 Certified Red Team Expert (CRTE);

13.2.1.1.2.11 Offensive Security Certified Expert (OSCE) ou OSCE³;

13.2.1.1.2.12 Certified Ethical Hacker (CEH).

13.2.1.1.3 Os profissionais da equipe técnica **responsáveis pela resposta a ataques cibernéticos**, deverão ter certificação em segurança defensiva, detendo, individualmente ou em conjunto, pelo menos 3 (três) das seguintes certificações, contabilizando no máximo 2 (dois) certificados por profissional:

13.2.1.1.3.1 Certified Information Security Manager (CISM);

13.2.1.1.3.2 GIAC Experienced Cybersecurity Specialist (GX-CS);

13.2.1.1.3.3 GIAC Reverse Engineering Malware (GREM);

13.2.1.1.3.4 Ethical Hacking Post Exploitation (EHPX);

13.2.1.1.3.5 CompTIA Security+;

13.2.1.1.3.6 CompTIA Advanced Security Practitioner;

13.2.1.1.3.7 EC-Council Security Analyst (ECSA) ou CPENT (Certified Penetration Testing Professional);

13.2.1.1.3.8 Certified Information Systems Security Professional (CISSP);

13.2.1.1.3.9 CompTIA CYSA+ - Cybersecurity Analyst.

13.2.1.2 É de responsabilidade da CONTRATADA dimensionar a quantidade de profissionais para a adequada prestação dos serviços previstos e delimitados por esta especificação, principalmente no que se refere aos acordos de níveis de serviço e metas estabelecidas.

13.2.1.3 Os profissionais cuja documentação for apresentada pela licitante deverão ser alocados na execução dos serviços.

13.2.1.4 Excepcionalmente, a contratada poderá substituir o profissional para a execução dos serviços, desde que comprovadas as condições de qualificação exigidas, condicionadas à prévia avaliação dos requisitos de qualificação e aceite por parte do CONTRATANTE.

13.2.1.5 A CONTRATADA deverá promover, no prazo máximo de 3 (três) meses, a atualização das certificações de seus profissionais caso haja atualização de versão ou migração para uma nova solução de TI devido à modernização do ambiente tecnológico do CONTRATANTE. Este prazo se iniciará a partir da comunicação formal do CONTRATANTE.

13.2.1.6 Até a data do início dos serviços, a contratada deverá comprovar que os profissionais que prestarão os serviços integram o quadro de pessoal permanente da contratada. A comprovação deverá ser feita mediante apresentação de:

13.2.1.6.1 Documento que comprove vínculo de emprego, ou

13.2.1.6.2 Documento que comprove ser o profissional sócio da empresa, ou

13.2.1.6.3 Contrato civil de prestação de serviços.

13.2.2 Qualificação técnico-operacional

13.2.2.1 A empresa a ser contratada deverá possuir experiência compatível com a complexidade da solução pretendida, mediante apresentação da documentação que segue:

13.2.2.1.1 Atestado(s) de capacidade técnica, fornecido por pessoa jurídica de direito público ou privado, no qual esteja expressa a aptidão do interessado no fornecimento, implantação e prestação de serviço gerenciado de solução de Monitoramento, Detecção, Notificação, Investigação e Resposta a Ataques Cibernéticos, para uma quantidade mínima de 40% do total de licenças previsto no item 1, devendo pelo menos 10% serem do mesmo fabricante da solução que a empresa ofertar na presente contratação.

13.2.2.1.1.1 A organização emitente do atestado de capacidade técnica deverá ser usuária do objeto fornecido, não sendo aceitos atestados emitidos por quaisquer intermediários.

13.2.2.1.1.2 Alternativamente ao atestado de capacidade técnica, será aceita declaração emitida pelo fabricante da solução, atestando que a licitante possui capacidade técnica e operacional para fornecer e prestar os serviços de implantação e o serviço gerenciado previstos no objeto, ou documento que comprove que a licitante é parceira autorizada do fabricante para serviços gerenciados de monitoramento e resposta a incidentes.

13.2.2.1.2 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.

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

14 SANÇÕES APLICÁVEIS

14.1. As sanções relativas a advertências, inexecução total ou parcial, impedimento de licitar e contratar e, se for o caso, declaração de inidoneidade serão previstas no edital;

14.2. Na hipótese de atraso na disponibilização das subscrições e serviços (itens 1, 2, 3, 4, 7 e 8) e na execução da implantação da solução (item 6), a contratada estará sujeita a multa diária de 0,5% (cinco décimos por cento) sobre o valor da obrigação objeto do atraso, limitada a 10% (dez por cento) do respectivo valor.

14.3. Na hipótese de atraso na solução dos chamados de suporte técnico, a contratada estará sujeita a multa nos percentuais descritos a seguir, sobre o valor mensal dos itens 7 e 8, limitada a 10% (dez por cento) do respectivo valor:

14.3.1 Severidade A0 (crítica): 1% (um por cento) por hora de atraso;

14.3.2 Severidade A1 (alta): 0,5% (cinco décimos) por hora de atraso;

14.3.3 Severidade A2 (média): 0,5% (cinco décimos) por dia útil de atraso;

14.3.4 Severidade A3 (baixa): 0,2% (dois décimos) por dia útil de atraso;

14.3.5 Severidade A4 (pesquisa): 0,1% (um décimo) por dia útil de atraso;

14.4. Na hipótese de atraso na realização do treinamento (item 5), a contratada estará sujeita a multa diária de 0,5% (cinco décimos por cento) sobre o valor do item em atraso, limitada a 10% (dez por cento) do respectivo valor.

APROVAÇÃO DO TERMO DE REFERÊNCIA	
Equipe de Planejamento da Contratação	
Documento assinado digitalmente CARLOS COSTA JORDÃO Integrante Demandante	*Documento assinado digitalmente* MAURÍCIO ANTONIOLI SCHMITZ Integrante Técnico
Documento assinado digitalmente GEOVANE DUTRA DE SOUZA Integrante Administrativo da Secretaria de Administração	*Documento assinado digitalmente* ALBERTO DANIEL MÜLLER Integrante Administrativo da Secretaria-Geral de Tecnologia e Inovação / Requisitante
Autoridade máxima da área de TIC / Subcomitê de TIC	
Documento assinado digitalmente NATACHA MORAES DE OLIVEIRA Coordenadora do Subcomitê de Tecnologia da Informação e Comunicações Secretária-Geral de Tecnologia e Inovação	

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

Anexo I

ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO

1. Definições para fins desta especificação:

1.1. Define-se “Ativo monitorado” como sendo uma estação de trabalho, notebook, dispositivo móvel, servidor, container, firewall, ativo de rede ou qualquer equipamento similar ao listado que possua endereço IP próprio e distinto e que deverá ser monitorado pela solução proposta. Poderá ser físico ou virtual e poderá estar hospedado em ambiente local (on-premise) ou em nuvem.

1.1.1. Relativo a container, deverá ser contabilizado como “Ativo monitorado” o host que hospeda o(s) container(s), para efeito de subscrição.

1.1.2. As licenças para *container* estarão limitadas a 4% de todos os ativos contratados.

1.2. Caso o ativo possua mais de um endereço IP, será contabilizado um único “Ativo monitorado” para efeito de subscrição.

1.3. Para os dados do ambiente do CONTRATANTE que serão coletados pela solução proposta, adotam-se as seguintes definições:

1.3.1. “Dados de logs”, “logs de evento” ou simplesmente “log”: informações produzidas sobre eventos ocorridos nos sistemas operacionais, aplicações, servidores, endpoints, ativos de rede ou outros componentes do ambiente computacional.

1.3.2. “Dados de telemetria”: informações produzidas pelos agentes a serem instalados nos ativos monitorados (quando a solução fizer uso de agentes).

1.3.3. “Dados de rede”: informações sobre o tráfego de rede.

1.4. Tokens: Unidades de consumo de Inteligência Artificial, utilizados em agentes inteligentes para automação de tarefas.

1.5. Usuários ativos: usuários que fazem uso dos recursos do Active Directory, pertencentes a uma organização ou restritos a uma ou mais OUs (Unidades Organizacionais) dentro da subárvore do Active Directory.

1.6. Define-se “Área de Armazenamento” como sendo a área disponibilizada por meio da solução contratada para armazenamento dos logs em ambiente SaaS, coletados pela solução.

1.7. Será utilizada a métrica de GB/dia (gigabytes por dia) para a ingestão de logs no SIEM da solução contratada, sendo que:

1.7.1. O volume de logs ingeridos no SIEM a partir dos demais módulos da solução do fabricante ofertadas na proposta não deverão ser contabilizados;

1.7.2. Serão contabilizados a ingestão de apenas fontes externas vindas de outros fabricantes, cuja cobrança será baseado no consumo

médio de GB/dia;

1.7.3. Caberá à CONTRATADA estimar e controlar o volume de logs de fontes externas ingeridos na solução, se desejar fazer uso deste recurso;

1.7.4. A ingestão de logs externos no volume de até 10 GB/dia será considerado isento de cobrança;

1.7.5. Considera-se o arredondamento bancário para as frações de GB/dia aferidas.

1.8. Os itens 2, 3 e 4 estão vinculados à contratação do item 1 e não podem ser contratados separadamente.

2. ITENS 1 a 4 – Requisitos mínimos da solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos

2.1. A solução contratada visa o monitoramento contínuo e ininterrupto dos ativos computacionais do CONTRATANTE (supramencionados como “Ativos monitorados”) por meio das etapas de, mas não se limitando à, coleta, processamento e correlação de logs de eventos, dados de telemetria e/ou de rede de tais ativos, com o objetivo de, após análise contextualizada das etapas mencionadas, identificar eventos suspeitos ou incomuns, direcionados ao CONTRATANTE e permitir ações de proteção de forma automatizada ou manual.

2.2. A solução deve possuir as características mínimas constantes nesta especificação, devendo ser constituída de softwares, licenças, subscrições e garantias, de tal forma que haja a total compatibilidade entre seus componentes.

2.3. A CONTRATADA deve prover, ao ambiente, soluções de segurança cibernética que permitam a visibilidade de logs, dados de telemetria, tráfego de rede e de informações correlatas, capazes de identificar eventos suspeitos ou incomuns que possam comprometer os serviços tecnológicos do CONTRATANTE, por meio da coleta, processamento e correlação dos logs de eventos, dados de telemetria e/ou de rede dos ativos monitorados e do tráfego de rede.

2.4. Para a prestação desse serviço, deve ser utilizada uma solução de Monitoramento, Detecção, Notificação, Investigação e Resposta a Ataques Cibernéticos, com capacidades de Coleta e Correlacionamento de Logs e Mecanismos de Detecção de Comportamento Anômalo de Usuários e Aplicações (UEBA – User and Entity Behavior Analytics). Neste caso, entende-se por “Aplicações” como sendo os softwares instalados nos ativos monitorados.

2.5. A solução permitirá monitorar em regime 24x7 (vinte e quatro horas por dia, sete dias por semana) eventos de segurança cibernética, identificando incidentes relativos a ataques, violações de conformidade e comportamento suspeito nas aplicações, rede e ativos computacionais do CONTRATANTE, compreendendo:

2.5.1. Analisar, classificar, categorizar, correlacionar e notificar os eventos e incidentes classificados como ameaças à segurança cibernética, ou que sejam

considerados relevantes de acordo com diretrizes estabelecidas pelo CONTRATANTE;

2.5.2. Registrar e comunicar os incidentes de segurança cibernética para o CONTRATANTE, com as respectivas recomendações para tratamento e mitigação das ameaças, conforme especificação técnica contida neste documento;

2.5.3. Elaborar procedimentos padronizados contendo as melhores práticas para tratamento e resposta dos incidentes confirmados, que serão posteriormente executados pelas equipes responsáveis do CONTRATANTE;

2.5.4. Registrar os incidentes no módulo de gestão de incidentes da solução ofertada, cujo acesso deverá estar disponível para o CONTRATANTE.

2.5.4.1. O módulo de gestão de incidentes deverá ser nativo da solução ofertada ou ser implementado por meio de ferramenta de ITSM (IT Service Management), complementar e integrado à solução ofertada. As funcionalidades do módulo ou da ferramenta devem conter os dados dos alertas, incidentes e chamados além de informações sobre SLA para acompanhamento do tratamento dos chamados.

2.5.4.1.1. O módulo ou ferramenta deve ser capaz de, minimamente:

2.5.4.1.1.1. Permitir a criação e acompanhamento de incidentes cibernéticos, de forma manual e automática, com no mínimo as seguintes características:

2.5.4.1.1.1.1. Sumário do incidente, incluindo título, sumário, detalhes, e a fonte geradora do incidente. Também deverá incluir o status do incidente, incluindo data de criação, de modificação, de fechamento, tempo em que o chamado está aberto, número de alertas agregados e, opcionalmente, prioridade e analistas envolvidos;

2.5.4.1.1.1.2. Classificação inicial da ameaça, incluindo categoria, origem (interna/externa), possibilidade de modificação manual da prioridade e justificativa, além de informações específicas para subsidiar o relatório de incidentes e possibilidade de inclusão de documentação adicional através da anexação de arquivos;

2.5.4.1.1.1.3. Possibilidade de manter o histórico de atividades realizadas pelos analistas, tais como criação de registros, atualização de campos, etc;

2.5.4.1.1.1.4. Permitir inserir comentários dos analistas no incidente, de tal forma a possibilitar o registro de todas as atividades de análise;

2.5.4.1.1.1.5. Permitir inserir evidências coletadas de eventual análise forense de host e rede como um complemento da análise do incidente;

2.5.4.1.1.1.6. Permitir registrar ações de remediação que incluam contenção, erradicação, educação de usuários e melhorias no programa do SOC;

2.5.4.1.1.1.7. Permitir registrar os resultados de um Incidente incluindo sua confirmação, categoria de ataque, identificação de técnicas utilizadas, detalhes sobre o alvo dos ataques e eficácia dos controles de detecção, prevenção e investigação.

2.5.4.1.1.2. Permitir o recebimento de alertas de segurança, de forma automática, com no mínimo as seguintes características:

2.5.4.1.1.2.1. Nome do alerta, fonte geradora, prioridade, data de criação, data original do alerta, categoria, ação, tipo, nível de severidade, descrição, serviço afetado, e

detalhes do alerta;

2.5.4.1.1.2.2. Dados de origem e destino: IPs e portas; quando disponível, informações de contexto de negócio de cada dispositivo de origem e destino: domínios, endereços MAC, nomes dos dispositivos, tipos, unidades de negócio, geolocalização, índices de criticidade e conformidade e proprietários;

2.5.4.1.1.2.3. Capacidade de incluir arquivos anexos, de acordo com a necessidade de aprofundamento de detalhes dos alertas.

2.5.4.1.1.3. Gerar relatórios mensais do acordo de nível de serviço (SLA – Service Level Agreement).

2.5.4.1.1.3.1. Os relatórios gerados deverão ser encaminhados para o CONTRATANTE.

2.5.5. O módulo ou ferramenta de ITSM deverá estar licenciado para o CONTRATANTE, devendo ser hospedado em regime SaaS (Software as a Service) pela CONTRATADA, bem como deve estar protegido por autenticação do tipo MFA - Multi-Factor Authentication e acesso criptografado ponto a ponto.

2.6. A solução deve ser fornecida no modelo Software as a Service (SaaS) permitindo a instalação de múltiplos coletores e agentes on-premises e em nuvem, a fim de realizar a implantação distribuída da arquitetura.

2.6.1. Deve ter instância própria para cada CONTRATANTE, isto é, exclusiva e dedicada para cada Tribunal e sem compartilhamento com outros clientes da CONTRATADA.

2.6.2. Todas as licenças e subscrições necessárias para o pleno funcionamento da solução deverão ser fornecidas pela CONTRATADA, conforme as quantidades e faixas discriminadas nesta especificação.

2.6.3. Coletores de logs: o software dos coletores de logs, bem como os respectivos sistemas operacionais, sistemas gerenciadores de banco de dados, entre outros componentes eventualmente necessários para a coleta e centralização de logs de eventos e/ou dados de telemetria deverão ser fornecidos pela CONTRATADA;

2.6.4. O CONTRATANTE disponibilizará, no máximo, os seguintes recursos em ambiente virtual a serem usados pelos coletores de logs (os recursos podem ser distribuídos entre diversas máquinas virtuais - uma para cada coletor, se necessário):

2.6.4.1. 12 vCPUs;

2.6.4.2. 32Gb vRAM;

2.6.4.3. 200GB de espaço em disco.

2.6.5. Caso os recursos em ambiente virtual necessários para o pleno funcionamento da solução extrapolem os recursos disponibilizados pelo CONTRATANTE, a CONTRATADA deve demonstrar, por meio de documento técnico do fabricante e/ou de boas práticas, a necessidade de aumento dos recursos, que serão disponibilizados pelo CONTRATANTE conforme comprovação apresentada. Caso não haja comprovação, a critério do CONTRATANTE, a CONTRATADA deverá providenciar, sem custos adicionais

para o CONTRATANTE, a entrega da infraestrutura (total ou remanescente) e em conformidade com a estrutura computacional do CONTRATANTE.

2.6.6. Agentes: software de baixo consumo de processamento que é instalado nos ativos suportados para centralizar e monitorar os dados de segurança cibernética. O agente oferece visibilidade e detecção de ataques nos endpoints, coletando informações on-line do sistema, incluindo informações básicas de identificação de ativos, processos em execução, logs e outros dados de telemetria e enviando essas informações à solução para análise.

2.6.7. O console de gerência deve ser acessado via web, de forma segura (HTTPS) e deve possuir compatibilidade com, no mínimo, os seguintes navegadores:

2.6.7.1. Google Chrome;

2.6.7.2. Microsoft Edge

2.6.8. O console de gerência deve estar disponível no ambiente do próprio fabricante, que é responsável pelas manutenções, atualizações e disponibilidade da solução.

2.6.8.1. Os ambientes utilizados pela solução, inclusive os do fabricante, devem estar localizados no Brasil ou em país que confira grau de proteção de dados pessoais adequado ao previsto na Lei nº 13.709/2018 (LGPD), assim entendido o país que possua legislação geral de proteção de dados pessoais de conteúdo equivalente à LGPD ou ao Regulamento (UE) 2016/679 (GDPR) e autoridade de controle independente com poderes de fiscalização e sanção.

2.6.8.2. É vedado utilizar dados, logs, telemetria, incidentes, prompts ou resultados para treinamento, ajuste ou desenvolvimento de modelos próprios ou de terceiros, salvo autorização expressa do CONTRATANTE. Subprocessadores deverão ser previamente informados.

2.6.9. O console de gerência deve possuir a capacidade de autenticação multifator (MFA - Multi-Factor Authentication).

2.7. A solução deve ser fornecida dimensionada para a quantidade de ativos a serem monitorados de forma a abranger o escopo completo de ativos do CONTRATANTE, conforme conceito apresentado nesta especificação técnica.

2.8. 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;

2.8.1. As análises realizadas e alertas devem estar disponíveis de forma integral por pelo menos 90 dias.

2.8.2. Retenção de logs de auditoria da plataforma e de artefatos coletados pelos agentes por período mínimo de 180 (cento e oitenta) dias.

2.8.3. Os logs do SIEM deverão ser armazenados por 30 dias para correlação

com os dados de telemetria.

2.8.4. Em caso de encerramento do contrato, substituição da solução ou mediante solicitação do CONTRATANTE durante o processo de transição, a CONTRATADA deverá permitir a exportação em lote de todos os logs, dados de telemetria, eventos e dados de rede do CONTRATANTE que ainda estejam armazenados na solução e abrangidos pelo período de retenção contratado, em 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.

2.8.5. A solução não deve possuir mecanismos que limitem ou onerem o CONTRATANTE com base na quantidade/volume de dados a serem exportados.

2.9. A solução deve possuir capacidade de monitorar e identificar o comportamento de usuários que representar ameaça (UEBA - User and Entity Behavior Analytics), em nível de ativos monitorados ou em nível de logs de eventos, do Microsoft Active Directory e do OpenLDAP, monitorando diferentes vetores de ataque, como:

2.9.1. Movimentação lateral com uso de credenciais locais de máquina;

2.9.2. Ataques de força bruta em contas locais de máquinas;

2.9.3. Usuários locais que tentam apagar arquivos de evento dos registros da máquina.

2.9.4. Adicionalmente, para ambientes com Microsoft Active Directory:

2.9.4.1. Movimentação lateral com uso de credenciais de domínio;

2.9.4.2. Ataques de força bruta em contas de domínio;

2.9.4.3. Usuários de domínio que tentem apagar arquivos de evento dos registros da máquina;

2.10. A solução deve permitir, para ambientes com Microsoft Active Directory, monitorar ações de todos os usuários, permitindo campanhas de caças a ameaças, auditoria e criação de alertas para usuários específicos.

2.11. A solução deve monitorar qualquer tipo de acesso de usuário:

2.11.1. Em máquinas com credenciais locais – monitoramento com uso de agente da própria solução;

2.11.2. Com credenciais do domínio – monitoramento do Microsoft Active Directory;

2.11.3. Ingress Authentication – como VPN, Google Workspace/Google Apps e Office 365;

2.11.3.1. Para autenticações vindas de fora do ambiente – Ingress Authentication – a solução deve identificar e correlacionar a informações da origem do acesso – minimamente data, hora e IP.

2.12. A solução deve suportar IPv4 ou IPv4/IPv6.

2.13. Para detectar incidentes, a solução deverá implementar o recebimento e análise de logs, dados de telemetria e/ou de rede de, no mínimo:

2.13.1. Firewalls;

2.13.2. Web Application Firewalls;

2.13.3. IPS (Intrusion Prevention System) / IDS (Intrusion Detection System);
2.13.4. Web filtering;
2.13.5. Antivírus;
2.13.6. Microsoft Active Directory;
2.13.7. Open LDAP;
2.13.8. IAM (Identity and Access Management) / PAM (Privileged Access Management);
2.13.9. Servidores HTTP (HTTP Servers);
2.13.10. Balanceadores de Carga (Load Balancers);
2.13.11. DNS;
2.13.12. DHCP;
2.13.13. ELK Stack;
2.13.14. Sistemas Operacionais.

2.14. A solução que fizer uso de parsers para análise dos dados recebidos deve permitir a ingestão de fontes de eventos por meio de, no mínimo, o protocolo Syslog.

2.14.1. A solução deve permitir a leitura de logs e arquivos nos formatos CSV, XML, JSON e texto puro, de forma a permitir a inclusão de outras fontes de evento que não tenham conectores nativos.

2.14.2. A solução deve possuir módulo nativo (já incluso) para realização de parsers customizados.

2.14.2.1. A solução deve permitir utilização de expressões regulares (regex) nos parsers.

2.14.2.2. A solução deve prover identificação de eventos com erro de parsing e de eventos sem suporte de coleta.

2.15. A solução deve ter funcionalidade de coleta de eventos de auditoria de bancos de dados por meio de conectores nativos, coleta de logs, dados de telemetria e/ou de rede.

2.16. Para detectar incidentes, a solução também deverá suportar o recebimento e processamento de eventos de tráfego de rede e, opcionalmente, flow de rede.

2.17. 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:

2.17.1. De forma nativa (sem a necessidade de customização de parsers):
2.17.1.1. Checkpoint para proteção de perímetro (Firewall);
2.17.1.2. Fortinet FortiGate para proteção de perímetro (Firewall);
2.17.1.3. Forcepoint para proteção de perímetro (Firewall);
2.17.1.4. Microsoft Active Directory para serviços de diretório.

2.17.2. De forma nativa (sem a necessidade de customização de parsers) ou não:
2.17.2.1. Open LDAP para serviços de diretório;
2.17.2.2. OpenVPN;

2.17.2.3. Citrix;
2.17.2.4. RDP e RDPWeb;
2.17.2.5. Senha Segura para serviços de gerenciamento de acesso privilegiado;
2.17.2.6. Cyberark para serviços de gerenciamento de acesso privilegiado
2.17.2.7. Hashicorp Vault e Hashicorp Boundary para serviços de gerenciamento de acesso privilegiado;
2.17.2.8. Keycloak para gerenciamento de identidade e acesso;
2.17.2.9. midPoint para segurança de identidades (identity security);
2.17.2.10. ForeScout CounterACT (eyeSight e eyeControl) para serviços de NAC (Network Access Control);
2.17.2.11. Loqed;
2.17.2.12. Varonis;
2.17.2.13. IBM Spectrum Protect Plus para proteção de dados;
2.17.2.14. Kaspersky para proteção de endpoint;
2.17.2.15. Blackberry Cylance para proteção de endpoint.
2.17.2.16. Check Point Harmony para proteção de endpoint;
2.17.2.17. Tenable One para gerenciamento de exposição (exposure management platform);
2.17.2.18. Tenable.ep / Nessus para gerenciamento de vulnerabilidades;
2.17.2.19. Tenable.ad para proteção do Active Directory;
2.17.2.20. Trivy para varredura de vulnerabilidades;
2.17.2.21. VMware/vCenter para virtualização de máquinas;
2.17.2.22. VMware/Horizon para virtualização de estações de trabalho;
2.17.2.23. Hyper-V para virtualização de máquinas;
2.17.2.24. Ovirt para virtualização de máquinas;
2.17.2.25. Docker e Kubernetes;
2.17.2.26. Apache HTTP Server;
2.17.2.27. HAProxy;
2.17.2.28. Ingress;
2.17.2.29. Nginx;
2.17.2.30. Switches Cisco MDS;
2.17.2.31. Switches H3C;
2.17.2.32. Switches HP;
2.17.2.33. Switches Huawei;
2.17.2.34. Roteadores Cisco;
2.17.2.35. Roteadores Juniper;
2.17.2.36. Roteadores MikroTik;
2.17.2.37. Access Points Aruba;
2.17.2.38. Access Points Ruckus;
2.17.2.39. Controladoras Virtuais Aruba;
2.17.2.40. Bacula para serviços de backup;
2.17.2.41. Commvault (software de backup);

2.17.2.42. Veeam (software de backup);
2.17.2.43. Storage Huawei;
2.17.2.44. Storage IBM;
2.17.2.45. TSM Server IBM Spectrum Protect para serviços de backup;
2.17.2.46. Dell EMC Data Domain;
2.17.2.47. Dell EMC Isilon.

2.18. A solução deve ser capaz de coletar e processar fontes de eventos oriundas dos seguintes serviços de Cloud:

2.18.1. De forma nativa (sem a necessidade de customização de parsers):
2.18.1.1. AWS CloudTrail, via SQS ou API;
2.18.1.2. Google Cloud Platform, via API;
2.18.1.3. Google Workspace/Google Apps, via API;
2.18.1.4. Microsoft Office 365, via API.

2.19. A solução deve suportar e implementar a coleta e o processamento de fontes de eventos oriundas, no mínimo, dos seguintes sistemas operacionais. Para as soluções que fazem uso de agentes ou outro software externo/nativo do sistema operacional, eles devem ser compatíveis com as versões 32 e 64 bits dos sistemas operacionais (quanto existirem). Caso a solução não faça uso de agentes, os dados devem ser obtidos por meio da coleta do tráfego de rede.

2.19.1. De forma nativa (sem a necessidade de customização de parsers):
2.19.1.1. Windows 10;
2.19.1.2. Windows 11;
2.19.1.3. Windows Server 2016;
2.19.1.4. Windows Server 2019;
2.19.1.5. Windows Server 2022;
2.19.1.6. Windows Server 2025;
2.19.1.7. Red Hat Enterprise Linux / Oracle Enterprise Linux / Rocky Linux 8.4;
2.19.1.8. Red Hat Enterprise Linux / Oracle Enterprise Linux / Rocky Linux 8.5;
2.19.1.9. Red Hat Enterprise Linux / Oracle Enterprise Linux / Rocky Linux 9.0;
2.19.1.10. Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 7;
2.19.1.11. Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 8.0;
2.19.1.12. Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 8.1;
2.19.1.13. Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 8.2;
2.19.1.14. Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 8.3;
2.19.1.15. Amazon Linux;
2.19.1.16. Debian Linux;
2.19.1.17. Ubuntu Linux.

2.20. Para os itens 2.13, 2.17, 2.18 e 2.19, as listas de soluções são do tipo "não exaustivas", devendo ser considerada pela CONTRATADA, por meio de configuração da solução, a possibilidade de inclusão ou alteração de produtos em decorrência da evolução do parque tecnológico do CONTRATANTE.

2.20.1. A inclusão ou alteração de tecnologias pertencentes ao escopo

ordinário será realizada sem custo adicional. Ampliações substanciais dependerão de formalização contratual.

2.21. A solução deve ser capaz de detectar comportamentos caracterizados como maliciosos de acordo com o MITRE ATT&CK Framework levando-se em consideração os dados recebidos dos ativos monitorados e gerados pelo coletor de tráfego de rede.

2.22. A solução deve cobrir detecções nativas de, ao menos, os grupos de atacantes categorizados pelo MITRE ATT&CK.

2.23. A solução deverá informar com qual técnica e tática do MITRE ATT&CK Framework o ataque está relacionado, além de possuir link direto para o site da organização.

2.24. A solução deve possuir de maneira nativa detecções de, no mínimo, os seguintes vetores de ataque:

2.24.1. Requisição a domínio suspeito;

2.24.2. Execução de processos suspeitos;

2.24.3. Requisição de dados de registro do sistema de nome de domínio (DNS);

2.24.4. Comunicação com servidores Command & Control;

2.24.5. Tentativa de desabilitar recursos de Sysmon;

2.24.6. Execução de processos LSASS (Local Security Authority Subsystem Service) com objetivo de detectar dump de memória para acessar possíveis credenciais armazenadas;

2.24.7. Detecção do uso de msrsc.exe - Microsoft Terminal Services Client;

2.24.8. Detecção do uso de comandos estruturados consistentes pela ferramenta Impacket e Impacket-Obfuscation;

2.24.9. Detecção de atividade de linha de comando da execução da função GetSystem, usada pelo Meterpreter ou Cobalt Strike;

2.24.10. Detecção de execução do Mimikatz e variações;

2.24.11. Detecção de processos que utilizam resultados do comando wget via Bash, Perl e Python;

2.24.12. Detecção de tentativas de criação de reverse shells para Command & Control.

2.25. A solução deve possuir a capacidade de identificar e monitorar o comportamento de atacantes baseados em IoC’s (Indicators of Compromise) do próprio fabricante e de terceiros (threat intelligence).

2.26. A solução deve possuir listas de terceiros com informações de IoC’s com, no mínimo, IPs, domínios, URLs e hashes da família SHA e, opcionalmente, MD5.

2.27. A solução deve possuir a capacidade de integração e/ou ingestão de dados de outras ferramentas de threat intelligence, de maneira manual ou por API, importando arquivos com base CSV ou STIX (Structured Threat Information Expression), através de assinatura de feeds de inteligência de ameaças de terceiros, aceitando, no mínimo, os seguintes tipos: IPs, domínios, URLs e hashes da família SHA e, opcionalmente, MD5.

2.28. A solução deve disponibilizar informações a respeito dos principais ataques que estão ocorrendo no mundo, quais plataformas e países são afetados, além de links para obter mais informações.

2.29. A solução deve possui Inteligência de ameaças própria, reconhecida no quadrante mágico "2026 Gartner® Magic Quadrant™ for Cyberthreat Intelligence Technologies" ou permitir o enriquecimento de dados relacionados a endereços IPs, buscando informações adicionais em fontes de OSINT (Open Source Intelligence)

2.30. A solução deve prover relatórios de inteligência de ameaças avançadas mais recentes e indicadores de comprometimento para ajudar na defesa proativa contra ameaças.

2.30.1. A solução deve integrar relatórios de inteligência criados por especialistas em ameaças do fabricante e de terceiros para ajudar na identificação de ameaças.

2.30.2. Após análise dos relatórios de ameaças pela CONTRATADA, deverá ser feita uma investigação dentro do ambiente computacional do CONTRATANTE e registrado um incidente caso sejam identificadas atividades presentes nos relatórios.

2.30.3. Cada relatório deve possuir, no mínimo, informações como: região/país alvo, plataforma alvo e campanhas de ataques relacionadas aos dados do relatório.

2.31. Ter capacidade de Gerenciamento de Superfície de Ataque e Exposição de Ameaças (ASM):

2.31.1. Capacidade de realizar o mapeamento contínuo e sem necessidade de agentes adicionais de todos os ativos da organização expostos à internet pública (endereços IP, domínios, serviços, portas e recursos em nuvem), combinado com a identificação automatizada de ativos internos e não gerenciados (*Shadow IT*) realizada pela telemetria nativa da plataforma;

2.31.2. Funcionalidade de identificação automatizada e sem interrupção de vulnerabilidades conhecidas (CVEs), portas de alto risco expostas e configurações inadequadas de segurança em tempo real, dispensando o agendamento manual ou a execução de varreduras (*scans*) invasivas tradicionais;

2.31.3. Mapeamento e visualização gráfica automatizada das rotas potenciais de exploração, identificando de forma clara como um invasor pode se aproveitar de uma exposição externa ou vulnerabilidade local para realizar movimentação lateral e comprometer sistemas e dados críticos (*crown jewels*);

2.31.4. Cálculo dinâmico do nível de risco das exposições identificadas, correlacionando pontuação CVSS, aplicabilidade técnica no ambiente, criticidade do ativo e dados de inteligência de ameaças

em tempo real (existência de exploits ativos no mundo real) para ordenar as vulnerabilidades que exigem correção imediata;

2.31.5. Integração direta entre o módulo de exposição e os fluxos de automação nativos da própria plataforma (XDR/SOAR), permitindo o disparo de ações imediatas ou guiadas de mitigação (como isolamento de host, bloqueio de portas ou alteração de políticas) diretamente a partir da console central;

2.31.6. Disponibilização de painéis consolidados em tempo real com métricas de postura de segurança, histórico de redução da superfície de ataque, cálculo de tendência de risco e exportação de relatórios executivos para suporte a auditorias e conformidade;

2.32. O serviço deve gerar um relatório mensal que indique como corrigir os problemas que venham a ser encontrados.

2.33. A solução que fizer uso de agentes deve permitir sua instalação de forma “silenciosa” nos ativos a serem monitorados.

2.34. A solução deve possuir as funcionalidades de:

2.34.1. Monitoramento de comportamento (behavior monitor);

2.34.2. Controle de aplicação;

2.34.3. Monitoramento de eventos;

2.34.4. Auditoria de alterações no sistema;

2.34.5. Resposta automatizada a ameaças com a possibilidade de, mas não se limitando a, executar as ações propostas no item 2.61.

2.34.6. Capacidade de fornecer proteção contra malware desconhecido sem exigir uma conexão com o console de gerenciamento ou com a Internet;

2.34.7. Capacidade de proteção contra malware sem a necessidade de assinaturas, utilizando padrões e/ou heurísticas;

2.35. A solução deve monitorar os ativos em tempo real, estando eles dentro ou fora do domínio.

2.36. Os agentes devem poder coexistir com outras soluções de proteção, como antivírus, instaladas nos ativos monitorados sem que gerem conflito nem incompatibilidade entre os softwares.

2.36.1. Serão aceitas apenas soluções de NGAV/EDR cujo motor primário de detecção e prevenção opere por meio de análise comportamental contínua de processos e aprendizado de máquina (Machine Learning), capaz de avaliar tanto o comportamento de execução de arquivos quanto de atividades em memória (*fileless*). A solução deverá ser capaz de detectar e bloquear ameaças mesmo quando não houver assinatura, hash, indicador de comprometimento ou conhecimento prévio específico da ameaça;

2.36.2. Não serão aceitas soluções que possuam apenas mecanismos de detecção baseados em assinaturas, hashes, reputação ou indicadores de comprometimento previamente conhecidos. A existência de módulos baseados em assinaturas será aceita como camada complementar de proteção, desde que

a solução também possua, de forma nativa e habilitada, mecanismos de análise comportamental e Machine Learning para detecção e prevenção de ameaças conhecidas e desconhecidas, mesmo que tais módulos possam ser desabilitados ou parametrizados nas configurações do produto para simular o uso exclusivo do motor comportamental.

2.36.3. 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;

2.36.4. Capacidade de fornecer proteção contra malware desconhecido sem exigir uma conexão com o console de gerenciamento ou com a Internet;

2.37. Os agentes devem executar de maneira que não haja impacto na performance ou disponibilidade dos ativos monitorados.

2.37.1. Durante a implantação será estabelecido *baseline* de CPU, memória, disco e rede; degradação superior aos limites acordados será não conformidade.

2.38. Os agentes e os coletores devem, em caso de desconexão com o console, manter as informações sendo coletadas a fim de serem enviadas quando a conexão for restabelecida.

2.39. Os agentes e coletores devem enviar os dados para o console de maneira:

2.39.1. Segura e criptografada;

2.39.2. Que não haja impacto na performance ou disponibilidade da rede do CONTRATANTE.

2.40. Os agentes e coletores, ao enviarem os dados para o console, não devem degradar o tráfego de saída da rede do CONTRATANTE.

2.41. A solução deve monitorar, no mínimo:

2.41.1. Força bruta no ativo (brute force – asset);

2.41.2. Força bruta em conta local (brute force – local account);

2.41.3. Detecção de evasão - Deleção de log de evento (detection evasion – event log deletion);

2.41.4. Detecção de evasão - Deleção de log de evento local (detection evasion – local event log deletion);

2.41.5. Correspondência de Threat Intel (endpoint threat intelligence match);

2.41.6. Exploração mitigada (exploit mitigated);

2.41.7. Hash sinalizado no ativo (flagged hash on asset) - a solução deve permitir cadastrar um hash qualquer para gerar um alerta quando for acessado no ativo;

2.41.8. Processo sinalizado no ativo (flagged process on asset);

2.41.9. Exploração de elevação de privilégio Kerberos (kerberos privilege elevation exploit);

2.41.10. Movimentação lateral com personificação de administrador local (lateral movement – local administrator impersonation);

2.41.11. Movimentação lateral com credenciais locais (lateral movement – local

credentials);

2.41.12. Tentativa de escalação de privilégio em honey credential local (local honey credential privilege escalation attempt);

2.41.13. Hash malicioso no ativo (malicious hash on asset) - a solução deve gerar um alerta quando um hash já conhecido como malicioso é acessado no ativo;

2.41.14. Criação de nova conta de usuário local (new local user account created);

2.42. A solução deve ser capaz de fornecer uma listagem dos ativos sendo monitorados.

2.43. A solução deve ser capaz de fornecer uma listagem dos ativos que estejam se comunicando no ambiente computacional do CONTRATANTE e que não estejam sendo monitorados.

2.44. A solução deve ser capaz de identificar acessos a URLs maliciosas além das portas padrão 80 e 443.

2.44.1. A solução deverá permitir classificar alertas relacionados a URLs em exceção para redução de falsos-positivos.

2.45. A solução deve correlacionar logs e/ou dados de telemetria/de rede dos ativos monitorados para:

2.45.1. Identificar comportamentos anômalos que aconteçam localmente no ativo monitorado;

2.45.2. Identificar quais eventos devem gerar alertas;

2.45.3. A solução deverá permitir classificar alertas relacionados a usuários e ativos em exceção para redução de falsos-positivos.

2.46. O console de correlacionamento deve estar disponível no ambiente do próprio fabricante, que é responsável pelas manutenções, atualizações e disponibilidade da solução.

2.47. A solução deve fazer uso de inteligência de ameaças do fabricante para analisar e correlacionar os dados recebidos.

2.48. A solução deve detectar ameaças conhecidas usando casos de uso de detecção constantemente atualizados, e desconhecidas por meio de conjuntos de dados aprendidos.

2.49. A solução deve prover funcionalidade de detecção de padrões em eventos coletados:

2.49.1. A solução deve prover detecção de padrões de ataque em todas as suas fases, com base no modelo Cyber Kill Chain, MITRE ou NIST;

2.50. A solução deve permitir a criação de alertas customizados baseados em um comportamento específico ou em um contexto de combinação de eventos.

2.51. Os modelos de detecção deverão possuir níveis de severidade (score) individuais para cada modelo em pelo menos os seguintes níveis:

2.51.1. Crítico;

2.51.2. Alto;

2.51.3. Médio;

2.51.4. Baixo.

2.52. A solução deve consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento.

2.53. A solução deve informar qual o escopo de impacto ou dimensionar o impacto em servidores, estações de trabalho e usuários, indicando a quantidade de componentes afetados no ataque.

2.53.1. Essas informações podem ser disponibilizadas por interação humana após investigação.

2.54. A solução deve permitir a visualização da correlação entre usuários, servidores, processos/comandos, arquivos e demais componentes correlacionados em determinado ataque.

2.55. A solução deve permitir o encerramento remoto de processos ativos executados nas estações de trabalho e servidores sob sua gestão.

2.56. A solução deve ser capaz de isolar uma estação de trabalho, desconectando-a da rede e permitindo se comunicar exclusivamente com a central da solução.

2.56.1. A solução deve ser capaz de restaurar a conectividade da estação de trabalho com a rede.

2.57. A solução deve ser capaz de realizar as ações dos itens 2.55. e 2.56. sem a necessidade de fornecimento de credenciais de usuário administrativo, o que não significa que o agente (caso a solução faça uso) não possa ser instalado com direitos administrativos.

2.58. A solução deve possuir a capacidade de monitorar a integridade de arquivos (FIM – File Integrity Monitoring) nos servidores monitorados.

2.58.1. Nativamente, para os seguintes formatos de arquivos, no mínimo:

2.58.1.1. .bat
2.58.1.2. .cfg
2.58.1.3. .conf
2.58.1.4. .config
2.58.1.5. .dll
2.58.1.6. .exe
2.58.1.7. .ini
2.58.1.8. .sys

2.58.2. A solução deve permitir a inclusão de novos formatos de arquivos diferentes dos nativos.

2.59. O serviço de segurança cibernética de Caça a Ameaças (Threat Hunting) deverá ser prestado diretamente pelo fabricante da solução ou pela CONTRATADA, desde que sua equipe possua certificações oficiais emitidas pelo fabricante. Em ambos os casos, deverão ser observados os níveis mínimos de serviço (SLA) estabelecidos para as atividades de Detecção e Resposta Gerenciadas (MDR) e Threat Hunting, os quais deverão ser validados ou auditados pelo fabricante;

2.60. A solução deve, junto com o monitoramento do tráfego de rede (ou por meio de agentes), implementar regras de detecção de intrusão para correlacionar

e trazer as informações sobre possíveis anomalias e ataques no nível de rede.

2.60.1. A solução deve permitir a criação de regras e/ou fornecer um conjunto de regras pré definidas.

2.60.1.1. No caso da solução possuir regras pré-definidas, deve haver sua atualização periódica cobrindo as informações de novas ameaças.

2.61. A solução deve possuir funcionalidade de automação na resposta de incidentes com playbooks de resposta já funcionais, devendo suportar, no mínimo, a automação das seguintes tarefas:

2.61.1. Envio de e-mails.

2.61.2. Com a utilização de agentes (não deve haver a necessidade de fornecimento de credenciais de usuário administrativo, o que não significa que o agente não possa ser instalado com direitos administrativos) ou outro mecanismo que a solução utilize para a automação:

2.61.2.1. Isolamento de uma máquina – caso seja detectado uma ameaça ou comportamento anômalo em uma máquina, deve ser possível isolá-la da rede;

2.61.2.2. Encerrar um processo malicioso – caso o agente detecte algum processo malicioso na máquina, a solução deve ter a capacidade de finalizar esse processo;

2.61.3. Com integrações para as soluções nativas indicadas no item 2.17.1:

2.61.3.1. Alertas relacionados a usuários do Microsoft Active Directory – se um alerta for gerado associado a uma credencial de domínio, a solução deve desabilitar o usuário para conter a ameaça de maneira rápida;

2.61.3.2. Sugerir e/ou criar regras no firewall – se um alerta for gerado associado a uma consulta DNS a um domínio considerado malicioso, a solução deve possibilitar a criação de regras de bloqueio no firewall ou sugerir qual regra deve ser criada para tal.

2.61.4. A solução deve permitir que cada tarefa nos playbooks de resposta de incidentes possa ser configurada de forma a:

2.61.4.1. Ser totalmente automática;

2.61.4.2. Aguardar uma interação humana para ser realizada.

2.62. Em casos de identificação de uma ameaça, a solução deve ter a capacidade de bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do sistema operacional ou demais aplicações instaladas no ativo.

2.63. A solução deve conter regras pré-definidas para detecção de ransomware e as principais famílias deste tipo de malware.

2.64. A solução deve possuir módulo de investigação e detecção integrados.

2.65. A solução deve apresentar os alertas de ameaças consolidados e correlacionados para melhor investigação e resposta aos incidentes.

2.66. A solução deve permitir configuração de notificações por e-mail (SMTP) e Webhooks (do Google Workspaces, no mínimo) para envio de alertas e notificações.

2.66.1. As notificações podem ser nativas ou, caso necessário, serem

desenvolvidas pela CONTRATADA, sem custo para o CONTRATANTE, para viabilizar sua integração.

2.67. A solução deve permitir que as detecções sejam correlacionadas com dados recebidos dos ativos monitorados.

2.68. A solução deve, através dos dados do alerta, permitir a criação de um incidente e vinculá-lo ao alerta, possibilitando a definição da gravidade do incidente com dados de gravidade da fonte do alerta.

2.69. A solução deve permitir visualizar uma lista de incidentes e suas descrições, solicitar enriquecimentos e executar ações sobre os incidentes.

2.70. A solução deve criar uma linha do tempo (timeline) do ataque detectado, incluindo as evidências sobre cada alerta gerado e informando qual ativo gerou aquela evidência.

2.70.1. A solução deve prover visualização em linha do tempo com informações dos eventos monitorados em cada estação de trabalho.

2.71. A solução deve ser capaz de classificar a relevância dos eventos, minimamente, em “crítico”, “alto”, “médio” e “baixo”.

2.72. A solução deve permitir a alteração do status dos incidentes de acordo com seu tratamento e indicar falsos positivos para a plataforma.

2.73. A solução deve permitir visualizar as atividades suspeitas de forma a sinalizar a causa raiz, seguindo as categorias do MITRE ATT&CK.

2.74. A solução deve permitir investigar os alertas gerados pelos modelos de detecção por meio de análise de impacto e análise de causa raiz.

2.74.1. Deve ser possível ativar ou desativar qualquer modelo de detecção.

2.74.2. A solução deverá possuir todos os módulos de detecção completamente licenciados, sem custo para o CONTRATANTE, independentemente da quantidade de modelos de detecção que venham a ser disponibilizados futuramente.

2.74.3. A solução deve permitir a análise automatizada de causa raiz de qualquer alerta, incluindo os alertas de rede, se os dados do endpoint estiverem disponíveis;

2.74.4. Visualização das cadeias de execução que levam a um alerta;

2.74.5. Visualização da cadeia de execução de eventos não envolvidos com alertas (Caça de ameaça - Threat Hunt);

2.74.6. Visualização de análise da linha do tempo para ver todas as ações e alertas em uma linha do tempo;

2.74.7. Consulta de indicadores de comprometimento (IoCs) e comportamentos de endpoint;

2.74.8. Para investigação em estações ou servidores deverá ser possível o registro minimamente dos seguintes itens:

2.74.8.1. Processo executado, incluindo datas e horários;

2.74.8.2. Atividades realizadas em arquivos;

2.74.8.3. Criação e encerramento de processos;

2.74.8.4. Threads de processo;
2.74.8.5. Protocolos de rede utilizados: solicitações DNS, conexão HTTP, desconexão HTTP;
2.74.8.6. Estatísticas de rede: histórico de conexões realizadas e processos associados;
2.74.8.7. Alterações em valores do registro;
2.74.8.8. Sessões de usuários no sistema operacional.

2.75. A solução deve permitir a criação de listas de exceção de objetos para redução de falsos positivos.

2.76. A solução deve adicionar os logs, dados de telemetria e/ou de rede coletados/correlacionados aos incidentes/alertas detectados.

2.77. A solução deve permitir o registro de incidentes por demanda, sem a necessidade de a própria solução ter gerado um alerta.

2.78. A solução deve possibilitar que, para cada incidente gerado, um analista seja vinculado ao incidente e que ele possa criar anotações sobre como está a evolução da resposta deste incidente;

2.79. A solução deve permitir que incidentes possam ser fechados após atividades serem encerradas, permitir marcação como falsos positivos e, também, que possam ser reabertos.

2.80. A solução deve exibir os eventos de forma a priorizar os alertas mais críticos para que o analista realize a investigação, indicando criticidade e níveis de prioridade.

2.80.1.1. A classificação quanto ao nível de criticidade deve ser baseada nas regras do MITRE.

2.81. A solução deve ter a capacidade de realizar buscas avançadas para localizar dados ou objetos no ambiente para análise avançada de atividades ou detecções.

2.82. A solução deve permitir realizar buscas e filtros de objetos para possibilitar pesquisas e análises avançadas.

2.83. A solução deve possibilitar a interação com cada um dos objetos relacionados ao evento para análise avançada e resposta.

2.83.1.1. Ao clicar em quaisquer dos objetos, a solução deve permitir a realização de buscas específicas pelo objeto ou ainda executar ações como executar investigações mais aprofundadas.

2.84. A solução deve prover diferentes métodos de pesquisa, filtros e uma linguagem de consulta para identificar, categorizar e recuperar os resultados da pesquisa.

2.85. A solução deve permitir a realização de buscas através de strings parciais, exatas, valores nulos, coringas (wildcards) e caracteres especiais.

2.86. A solução deve permitir salvar pesquisas com os critérios de busca e operadores lógicos utilizados para futuras consultas.

2.87. A solução deve permitir a criação de dashboards e relatórios baseados em bibliotecas prontas ou, também, criar do zero.

2.87.1.1. Deve possuir dashboards pré-configurados e permitir sua customização ou mesmo a criação de novos para refletir necessidades específicas do CONTRATANTE.

2.87.1.2. Deve fornecer a possibilidade de criação de relatórios e dashboards para dados de todas as fontes de dados ingeridas (endpoints, rede, e-mail, nuvem, etc.), seja por meio de criação de consultas (queries) ou a partir de cliques com o mouse.

2.87.2. Deve possuir dashboards pré-configurados que permitam a visualização executiva dos principais incidentes e atividades no ambiente com base em usuários, aplicações acessadas e estações de trabalho/servidores.

2.87.3. Deve possuir, ao menos, 15 (quinze) dashboards em sua biblioteca, incluindo dashboards de fácil visualização de:

2.87.3.1. Alertas e incidentes mais frequentes;

2.87.3.2. Nível de risco do ambiente;

2.87.3.3. Relatório dos últimos 30 (trinta) dias da detecção de incidentes;

2.87.3.4. Top 10 (dez) ativos com incidentes;

2.87.3.5. Os ativos que mais sofreram incidentes em um determinado período;

2.87.3.6. Os usuários que mais sofreram incidentes em um determinado período;

2.87.3.7. Ativos e contas descobertas;

2.87.3.8. Ameaças descobertas e classificadas conforme a cadeia de ataque.

2.87.4. Deve permitir configuração de atualização do tempo de cada dashboard.

2.87.5. Deve permitir exportação dos relatórios para os seguintes formatos:

2.87.5.1. Planilha: CSV e/ou Excel;

2.87.5.2. Texto: HTML e/ou PDF.

2.88. A solução deve permitir o gerenciamento de usuários, funções e permissões.

2.89. A solução deve permitir a criação de usuários com permissões distintas, contendo no mínimo, permissão total e permissão para realizar investigações.

2.90. A solução deve permitir uma gestão de usuários, com recursos de permissionamento RBAC, onde usuários podem ser excluídos da console sem prejuízos à auditoria ou a funcionalidades.

2.91. A solução deve registrar todas as atividades efetuadas pelos seus usuários, permitindo auditoria das ações realizadas.

2.91.1. Registros de auditoria de usuários, administradores e componentes integrarão os dados do CONTRATANTE e serão exportáveis ao

encerramento.

2.92. A solução deve disponibilizar APIs, com documentação e sem custo adicional, para integração com outras soluções.

MONITORAMENTO DEEP/DARK WEB (MONITORAMENTO DE MARCA E AMEAÇAS GLOBAIS)

2.93. A CONTRATADA deverá realizar serviços de monitoramento de Deep/Dark Web por meio da solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos ofertada (nativamente ou por meio de solução complementar). Os serviços e a respectiva solução utilizada para a realização do monitoramento de Deep/Dark Web devem atender às seguintes especificações mínimas:

2.93.1. A solução de monitoramento de Deep/Dark Web deve ter como objetivo principal o rastreamento de salas, blogs, fóruns e sites na Deep/Dark Web para identificar informações relativas ao CONTRATANTE e seus colaboradores como: credenciais roubadas e outros vazamentos de informações pessoais identificáveis.

2.93.2. A solução de monitoramento de Deep/Dark Web deve estar licenciada para monitorar até 6 (seis) domínios DNS do CONTRATANTE e uma quantidade de no mínimo 500 (quinhentos) termos por domínio.

2.93.3. O serviço de monitoramento de Deep/Dark Web deve ser prestado no regime 24x7 (vinte e quatro horas por dia, sete dias por semana).

2.93.4. A solução de monitoramento de Deep/Dark Web deve realizar buscas, no mínimo:

2.93.4.1. Na Darknet;

2.93.4.2. Em plataformas de compartilhamento de documentos;

2.93.4.3. Pelas seguintes categorias:

2.93.4.3.1. Por Bucket: Darknet TOR, Whois, Usenet, Leaks, Bot Logs, Wikileaks, Public Leaks, Dumpster, Sci-Hub;

2.93.4.3.2. Por Site Público: .com, .org, .net, .info, .eu.

2.93.4.3.3. Por Geolocalização.

2.93.5. A solução de monitoramento de Deep/Dark Web deve permitir a busca de termos:

2.93.5.1. Domínio DNS;

2.93.5.2. Endereço de e-mail;

2.93.5.3. IP e CIDR;

2.93.5.4. Número de telefone;

2.93.5.5. Número do cartão de crédito;

2.93.5.6. URL.

2.93.6. Deve detectar resultados de itens pesquisa duplicados, apresentando-os de forma consolidada, otimizando a busca por

informações relevantes.

2.93.7. A solução de monitoramento de Deep/Dark Web deve ter a capacidade de buscar dados pelo período mínimo de 1 (um) ano.

2.93.8. A solução de monitoramento de Deep/Dark Web deve ter a capacidade de filtrar e classificar os resultados das buscas:

2.93.8.1. Com base na data ou no tempo de publicação das informações encontradas (antigas e novas);

2.93.8.2. Com base nos domínios, e-mails e URLs encontrados;

2.93.8.3. Com base nos resultados mais relevante, menos relevante, mais recente e mais antigo;

2.93.8.4. Com capacidade de combinar ou excluir termos de pesquisa a fim de encontrar com eficiência informações relevantes no banco de dados.

2.93.9. A solução de monitoramento de Deep/Dark Web deve ter a capacidade de manter históricos de resultados de busca.

2.93.10. A solução de monitoramento de Deep/Dark Web deve contemplar os seguintes itens:

2.93.10.1. Monitoramento de atividades na Deep/Dark Web relacionadas às informações sobre domínios, URLs, IPs, hashes, credenciais, e-mails e informações sensíveis do CONTRATANTE.

2.93.10.2. Amplitude de rastreamento contemplando dados e informações disponibilizadas na Deep/Dark Web como:

2.93.10.2.1. Monitoramento das credenciais de funcionários em listas e bases de dados de credenciais vazadas na Deep/Dark Web, marketplaces, entre outros;

2.93.10.2.2. Monitoramento do Pastebin, incluindo posts deletados e outros sites, buscando por referências sobre a empresa, domínios ou endereços IP;

2.93.10.2.3. Monitoramento de documentos vazados ou roubados da empresa em páginas da Deep/Dark Web e fóruns hackers;

2.93.10.2.4. Monitoramento de referências aos sistemas em páginas da Deep/Dark Web e fóruns hackers, além de Threat Intelligence e listas de IoC’s;

2.93.10.2.5. Busca de informações sobre redes sociais e plataformas de divulgação de vulnerabilidades vazadas na Deep/Dark Web.

2.93.10.3. Deve ser possível encontrar marketplaces, fóruns e agentes de ameaças;

2.93.10.4. 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;

2.93.10.5. Investigação de origens de vazamentos de, no mínimo:

2.93.10.5.1. Grupos de hackers;

2.93.10.5.2. Ameaças em fóruns;

2.93.10.5.3. Salas de chats reservadas;

2.93.10.5.4. Carteira de bitcoins e endereços;

2.93.10.5.5. Registros históricos.

2.93.10.6. As investigações deverão ser realizadas por uma equipe especializada à medida que informações monitoradas forem identificadas na Deep/Dark Web.

2.93.10.7. Geração e notificação de alertas acompanhados da enumeração das ameaças e riscos relacionados e ações de mitigação sugeridas.

2.93.11. A coleta e tratamento serão limitados à finalidade de segurança cibernética, vedada utilização diversa e observados necessidade, segurança, prevenção e responsabilização.

2.94. A solução como um todo, bem como os seus componentes devem contar com garantia e suporte integrais conforme especificado neste documento.

2.95. O serviço de segurança cibernética de Caças Ameaças (Threat Hunting) deverá ser realizado através de análise humana e operar em caráter contínuo, regime 24 horas x 7 dias da semana, em busca de ameaças cibernéticas, anomalias, comportamentos suspeitos e ou maliciosos, análise e revisão da telemetria gerada pelos dispositivos e estratégias avançadas utilizadas por atores maliciosos, sem a dependência de alertas ou detecções. Ou seja, as atividades listadas devem ocorrer independente de alertas e detecções.

REQUISITOS PARA PROTEÇÃO DE IDENTIDADES

2.96. A solução deverá fornecer capacidades de Detecção e Resposta a Ameaças de Identidade (ITDR) integradas à plataforma XDR para ambientes Active Directory (on-premises) e Entra ID (nuvem), sendo capaz de avaliar continuamente vulnerabilidades e riscos em credenciais, detectar ataques em andamento (incluindo técnicas como Password Spray, DCSync, Pass-the-Hash e Skeleton Key), prevenir ou identificar movimentações laterais associadas ao uso indevido de protocolos de administração remota e investigar comportamentos anômalos nos fluxos e acessos de autenticação que envolvam os protocolos Kerberos e NTLM.

2.97. A solução deverá suportar a detecção e monitoramento de identidades não-humanas, incluindo contas de serviço, aplicações, APIs e identidades gerenciadas.

2.98. A ferramenta deverá analisar o comportamento de cada conta de usuário e conta de computador, além de estabelecer o perfil comportamental padrão dos

acessos comuns, com o intuito de alertar ou bloquear condições anormais, utilizando técnicas de User and Entity Behavior Analytics (UEBA), incluindo técnicas de análise comportamental avançada, estatística e/ou aprendizado de máquina.

2.99. A solução deverá possuir capacidade de detecção baseada em anomalia de protocolo, identificando desvios em protocolos de autenticação e comunicação de diretório que não correspondam aos padrões documentados ou ao comportamento legítimo de sistemas operacionais homologados, independentemente da assinatura de um ataque específico.

2.100. A solução deverá identificar caminhos de ataque (attack paths) que permitam a elevação de privilégios ou comprometimento de ativos críticos a partir de identidades com menor privilégio.

2.101. A solução deverá permitir a execução de ações de contenção imediata diretamente a partir do console ou de seus componentes técnicos (sensores/coletores), incluindo, no mínimo, mecanismos de invalidação de credenciais e sessões de autenticação, tanto em ambientes on-premises quanto em nuvem, de forma imediata e centralizada, devendo abranger credenciais Kerberos, tokens de autenticação e sessões ativas.

2.102. A solução deverá analisar configurações inadequadas, detalhar os riscos, o que deve ser feito para remediar, além de listar todas as identidades afetadas, incluindo minimamente:

2.102.1. Contas com SPN vulneráveis;
2.102.2. Utilização de protocolos vulneráveis como NTLMv1;
2.102.3. Contas configuradas para nunca expirar a senha;
2.102.4. Contas configuradas como uma política de senhas fraca;
2.102.5. Contas inativas;
2.102.6. Domain Controllers com o serviço Print Spooler em execução;
2.102.7. Caminhos onde contas regulares podem adotar para se tornarem contas privilegiadas.
2.102.8. Usuários com Account Lockout;
2.102.9. Alterações de senhas;
2.102.10. Alterações em contas;
2.102.11. Usuários desabilitados;
2.102.12. Usuários com senhas há muito tempo sem trocar;
2.102.13. Principais falhas de login;
2.102.14. Contas vulneráveis a Kerberoasting;
2.102.15. Contas vulneráveis a DCSync e Pass the Hash;
2.102.16. Informar se a conta KRBTGT precisa ser alterada para mitigar ataques como Golden Ticket;
2.102.17. Conta oculta identificada (contas que possuem configurações que impedem administradores de encontrá-las em buscas no serviço de diretório);

2.102.18. Identificação de permissões excessivas que possibilitem usuários comuns manipular políticas de acesso e autenticação de contas privilegiadas;
2.102.19. Identificar alterações no objeto AdminSDHolder;
2.102.20. Contas sincronizadas com o Entra ID que possuam privilégios excessivos ou MFA desabilitado.

2.103. A detecção de ameaças deverá ocorrer em tempo real ou próximo de tempo real e permitir que ações sejam tomadas para evitar que futuros ataques aconteçam, incluindo, mas não se limitando a ataques e técnicas, tais como:
2.103.1. Golden Ticket;
2.103.2. Suspicious Protocol Implementation (Pass the Hash);
2.103.3. NTLM Relay;
2.103.4. Suspicious LDAP Search (Kerberos Misconfiguration);
2.103.5. Suspicious LDAP search (Accounts);
2.103.6. DCSync;
2.103.7. Ataque DCSync com conta MSOL;
2.103.8. Ataques de DCShadow (replicação fraudulenta de objetos);
2.103.9. Forged PAC Attack;
2.103.10. Suspicious Kerberos Ticket Reuse;
2.103.11. Password Brute Force;
2.103.12. Credential Scanning;
2.103.13. Bronze Bit exploit;
2.103.14. CredSSP Vulnerability;
2.103.15. Skeleton Key Attack;
2.103.16. Pass-the-Ticket;
2.103.17. Overpass-the-Hash;
2.103.18. Token replay e abuso de tokens de autenticação;
2.103.19. Injeção de SID-History em contas de usuário;
2.103.20. Acesso incomum a um endpoint;
2.103.21. Acesso excessivo a múltiplos endpoints;
2.103.22. Atividade excessiva de acesso a múltiplos endpoints;
2.103.23. Acesso de um IP envolvido com outros incidentes ou qualificado como danoso pelo sistema de inteligência.
2.103.24. Administradores de Domínio com SPN;
2.103.25. Contas com senhas em branco;
2.103.26. Escalação de Privilégio via Grupo;
2.103.27. Atividades recentes vindas de contas dormentes;
2.103.28. Conta de computador - abuso de Serviços Kerberos para Usuário (S4U);

2.104. Para cada ataque identificado, a solução deverá minimamente fornecer as seguintes informações e possibilidades:

2.104.1. Data e hora da detecção;
2.104.2. Descrição do ataque;
2.104.3. Severidade;
2.104.4. Tática e técnica associada ao framework MITRE ATT&CK;
2.104.5. Conta comprometida;
2.104.6. Host de origem, de onde o ataque foi realizado;
2.104.7. Host de destino, quando o ataque está relacionado a uma movimentação lateral;
2.104.8. Recomendações com ações que devem ser realizadas para conter tal ataque;
2.104.8.1. Marcar o ataque como resolvido;
2.104.8.2. Marcar o ataque como falso positivo e não alertar ataques similares.

2.105. A solução deverá permitir a configuração de políticas de acesso para minimamente os seguintes cenários:
2.105.1. Em caso de detecção de um ataque pré-definido (como DCSync ou Pass the Hash), a solução deverá automaticamente adicionar a conta comprometida a uma lista de contenção; e, em seguida, bloquear ou restringir autenticações e sessões desta mesma conta, mediante aprovação manual ou configuração prévia de políticas de automação baseadas em níveis de confiança, com o fim de interromper uma movimentação lateral;
2.105.2. Impedir a autenticação (Logon) de usuários incluídos em lista de contenção;
2.105.3. Alertar ou bloquear quando usuários privilegiados sejam utilizados em horários fora do normal (como fora do horário comercial).

2.106. A solução deverá fornecer capacidades de investigação de contas de usuários e acessos suspeitos, permitindo minimamente a visualização de:
2.106.1. Autenticações realizadas, incluindo sucesso e falha, com capacidade de filtragem por usuário, origem e destino;
2.106.2. Eventos de replicação de domínio, Account Lockout e acesso RPC;
2.106.3. Acessos realizados por contas de serviço e por contas com privilégios específicos (como Domain Admin);
2.106.4. Capacidade de listar em tempo real todas as sessões ativas de um usuário em múltiplos endpoints.

2.107. Deverá ser possível emitir relatórios para as funcionalidades de proteção de identidade minimamente dos seguintes indicadores:
2.107.1. Account Lockouts por endpoint;
2.107.2. Account Lockouts por usuário;
2.107.3. Uso de NTLM por usuário;
2.107.4. Uso de NTLM por endpoint;

2.107.5. Resumo de novos incidentes de segurança relacionados às identidades;
2.107.6. Top 10 incidentes por severidade;
2.107.7. Top 10 usuários com riscos significativos;
2.107.8. Usuários que nunca efetuaram Logon no domínio;
2.107.9. Administradores inativos;
2.107.10. Administradores com privilégios ocultos.

2.108. A solução deverá possuir capacidade de detectar, correlacionar, alertar e responder a ameaças relacionadas a autenticações e identidades em tempo real ou próximo de tempo real, utilizando mecanismos nativos, integrações ou ações automatizadas compatíveis com sua arquitetura.

2.109. A solução deverá permitir ações de contenção e resposta a incidentes relacionados a identidades, de forma automatizada ou manual, utilizando recursos nativos e/ou integração com plataformas de segurança, autenticação ou orquestração

2.110. As ações de bloqueio, restrição ou contenção de autenticação deverão ser executadas diretamente pela solução, não dependendo exclusivamente de integrações externas para sua efetivação.

2.110.1. As ações automatizadas serão classificadas como automáticas, dependentes de aprovação ou proibidas, conforme Matriz de Autonomia definida pelo CONTRATANTE.

2.111. A capacidade de detecção e resposta a ameaças de identidade deverá estar disponível de forma nativa, não dependendo da criação manual de regras ou correlações para identificação de ataques conhecidos.

2.112. A solução não deverá depender exclusivamente da instalação de agentes em endpoints para detecção de ameaças de identidade, devendo ser capaz de analisar autenticações diretamente a partir de controladores de domínio, serviços de diretório ou tráfego de autenticação.

2.113. A solução deverá prover visibilidade e proteção de identidades mesmo em sistemas que não suportam instalação de agentes, incluindo sistemas legados, dispositivos de rede e aplicações, por meio da análise de autenticações e credenciais.

2.114. A solução deverá apresentar encadeamento de eventos (timeline) permitindo a visualização da cadeia de ataque relacionada a uma identidade comprometida.

2.115. A solução deverá correlacionar eventos provenientes de múltiplas fontes, incluindo diretórios, autenticações, endpoints e sistemas integrados, para identificação de ataques complexos.

2.116. A solução deverá permitir o monitoramento e a rastreabilidade de alterações relacionadas a identidades, grupos e permissões no ambiente de diretório, incluindo registro e consulta de eventos associados.

2.117. A solução deverá fornecer evidências e contexto detalhado para cada detecção, permitindo a rastreabilidade e compreensão do motivo do alerta.

2.118. A solução deverá permitir a priorização de incidentes com base em risco agregado, considerando múltiplos fatores, como comportamento, exposição e criticidade da identidade.

2.119. A solução deverá identificar quando um usuário desativado tenta autenticar;

2.120. A solução deverá possuir capacidade de identificar comportamentos anômalos relacionados à autenticação e acesso às identidades, incluindo desvios de comportamento, padrões incomuns de acesso ou eventos suspeitos correlacionados;

2.121. A solução deverá identificar tentativas suspeitas relacionadas à autenticação NTLM, destacando comportamentos anômalos, como coleta de credenciais e volume incomum de autenticações em hosts de destino, permitindo a análise desses eventos em diferentes janelas de tempo, incluindo a última hora;

2.122. A solução deverá identificar quando um host procura se registrar como um novo controlador de domínio e alertar quando houver tráfego de sincronização de dados de um controlador de domínio legítimo;

2.123. A solução deverá identificar quando um usuário tenta se autenticar em um host via NTLM e não o fez nos últimos 30 dias;

2.124. Realizar Análise de Caminhos de Ataque, que é o mapeamento de como um invasor poderia realizar elevação de privilégio ou fazer movimentação lateral;

2.125. A solução deverá identificar comportamento que caracteriza uma quantidade excessiva de logins;

2.126. A solução deverá possuir módulo que seja capaz de identificar Brute Force em usuário e senha;

2.127. A solução deverá identificar contas de usuário que possuem permissões administrativas diretas (ACLs) em objetos do serviço de diretório, sem que estas contas pertençam formalmente a grupos de administradores;

2.128. A solução deverá fornecer uma pontuação de Risco por Usuário, calculado com base no comportamento e nas exposições da identidade, permitindo priorizar a investigação de contas com maior probabilidade de comprometimento;

2.129. A detecção de ameaças não deverá depender exclusivamente da ingestão de logs, devendo a solução ser capaz de identificar atividades maliciosas de forma independente, inclusive em cenários de evasão, como limpeza, manipulação ou ausência de logs. Todas as comunicações entre componentes da solução e os Controladores de Domínio devem priorizar o uso de protocolos seguros (como Kerberos ou LDAPS), evitando a utilização de protocolos legados sempre que tecnicamente possível (como NTLM).

2.130. A solução deverá funcionar em sua plenitude (com todos os recursos), sem depender de reboots nos Domain Controllers.

2.131. A solução deverá possuir capacidade de integração com ferramentas de segurança e infraestrutura, como SIEM, SOAR, EDR/XDR e soluções de gestão de identidade, por meio de APIs ou conectores nativos.

2.132. A solução deve possuir APIs documentadas para integração com ferramentas de orquestração (SOAR), permitindo que ações de contenção sejam disparadas de forma externa;

2.133. A solução deverá possuir mecanismos para identificação de tentativas suspeitas de enumeração, acesso indevido, movimentação lateral ou abuso de credenciais privilegiadas, podendo utilizar recursos nativos de detecção, análise comportamental, correlação ou tecnologias complementares;

MÓDULO DE SOAR AGÊNTICO

2.134. A solução deve dispor de agentes virtuais baseados em Inteligência Artificial integrados à solução capazes de interpretar alertas, formular hipóteses de investigação e tomar decisões de roteamento sem a necessidade de fluxogramas totalmente pré-configurados.

2.134.1. A utilização de IA não transfere à Administração responsabilidade pelas ações da plataforma. A CONTRATADA responderá pela operação, controles e rastreabilidade dos agentes.

2.135. O uso de módulo de SOAR agêntico consumirá *tokens* para execução de suas funções;

2.136. A CONTRATADA deve fornecer exemplos de cenários de uso de agentes inteligentes e seu consumo estimado de tokens;

2.137. Deverá existir alertas graduais (p. ex: 50%, 80%, 90%) de consumo e a possibilidade de bloqueios automáticos no uso da ferramenta a fim de evitar oneração imprevista acima do teto estabelecido pelo CONTRATANTE;

2.138. A quantidade de tokens contratados poderá ser utilizada durante todo o período contratual, sendo que o faturamento será sobre o número de tokens mensais previamente contratados até o limite estabelecido.

2.139. A solução deve operar de forma integrada combinando automações determinísticas (playbooks de regras fixas para execução previsível) e automações agênticas (IA adaptativa baseada em objetivos).

2.139.1. Alterações de playbook decorrentes de mecanismo agêntico deverão ser versionadas e registradas e observar a política de autorização antes de ações de alto impacto.

2.140. Capacidade de criar, implantar e gerenciar múltiplos agentes de IA autônomos e especializados (ex: Agente de Triagem, Agente de Investigação de Nuvem, Agente de Threat Hunting e Agente de Remediação).

2.141. Os agentes virtuais de inteligência artificial devem ser capazes de colaborar entre si, compartilhando contexto, dividindo tarefas complexas e orquestrando o fluxo de trabalho do incidente do início ao fim.

2.142. A solução deve permitir a criação automática de playbooks ou adaptação do fluxo de resposta em tempo real com base no raciocínio da IA, eliminando a dependência de manutenção de regras estáticas.

2.143. A solução deve permitir análise automatizada do alerta no momento de sua geração, atribuindo um índice de confiança (*confidence score*) e determinando se o alerta corresponde a um falso positivo ou uma ameaça real.

2.144. O agente deve ter capacidade de investigar árvores de processos, logs de chamadas de API em nuvem (ex: AWS, Azure, GCP), eventos de rede e telemetria de identidade de forma automatizada para correlacionar o ataque.

2.145. A solução deve permitir a identificação e mapeamento automático das táticas, técnicas e procedimentos (TTPs) utilizados pelo atacante durante a investigação do incidente.

2.146. A solução deve permitir a geração automática de narrativas detalhadas e resumos executivos do incidente em Português (Brasil) ou Inglês, cobrindo causa-raiz, cronologia dos fatos, ativos e identidades impactadas.

2.146.1. Resultados automatizados de causa-raiz serão apresentados como hipótese, acompanhados das evidências, grau de confiança e validação do analista.

2.147. A solução deve prover interface conversacional de suporte ao analista que permite realizar perguntas operacionais e investigativas sobre o ambiente de segurança em linguagem natural em Português ou inglês;

2.148. A solução deve sugerir os próximos passos de mitigação e remediação mais adequados com base no contexto específico da infraestrutura.

2.149. A solução deve permitir mecanismos de governança para limitar o nível de autonomia que cada agente de IA possui sobre a infraestrutura.

2.150. A solução deve permitir a possibilidade de configurar travas operacionais obrigatórias para que ações de contenção/resposta de alto risco (ex: isolar servidor crítico, revogar acesso de usuário VIP) dependam de autorização prévia por um operador humano.

2.151. A solução manterá registro auditável dos eventos, entradas relevantes, regras/políticas, agente, ação, resultado, data/hora e justificativa operacional, sem exigir exposição de raciocínio interno proprietário do modelo.

3. ITEM 5 – Requisitos mínimos de treinamento na solução

3.1. Deve ser realizado treinamento de administração e de operação da solução para até 10 (dez) profissionais da CONTRATANTE, contemplando, ao menos, os seguintes temas: instalação, configuração, operação e utilização da solução contratada.

3.1.1. O treinamento deve contemplar todos os recursos e configurações existentes na solução ofertada.

3.2. O treinamento deverá proporcionar aos participantes condições de:

3.2.1. Compreender a arquitetura da solução;

3.2.2. Identificar e configurar os recursos disponibilizados no produto;
3.2.3. Configurar fontes de eventos;
3.2.4. Instalar e configurar agentes, coletores e outros módulos necessários para o perfeito funcionamento da solução;
3.2.5. Configurar funcionalidade de deception, quando a solução tiver essa capacidade;
3.2.6. Configurar regras;
3.2.7. Configurar alertas;
3.2.8. Configurar playbooks;
3.2.9. Investigar incidentes;
3.2.10. Pesquisar em logs;
3.2.11. Criar dashboards;
3.2.12. Criar relatórios e agendamento de relatórios;
3.2.13. Gerenciar usuários, funções e permissões;
3.2.14. Identificar as possíveis causas de problemas e atuar na sua resolução;
3.2.15. Monitorar o funcionamento da solução (analisar mensagens de log, efetuar acesso remoto, atualizar os componentes que fazem parte da solução, administração e utilização dos recursos disponibilizados);
3.2.16. Conhecer os procedimentos para abertura de chamados técnicos;
3.2.17. Conhecer os procedimentos para obtenção de atualizações de software.

3.3. O treinamento deve ser oficial ou autorizado pelo fabricante da solução, devendo ser realizado na plataforma online do fabricante ou do centro autorizado de treinamento.
3.3.1. O conteúdo do treinamento poderá seguir o padrão de treinamento utilizado pelo fabricante para os módulos ofertados na solução, enquanto demais conteúdos que extrapolem o contexto padronizado do fabricante podem ser complementados pela CONTRATADA através de treinamento próprio.

3.4. O treinamento deve ser ministrado por pessoa certificada na solução.

3.5. A CONTRATADA deverá apresentar, juntamente à documentação técnica, a programação, conteúdo programático e carga horária do curso, a fim de serem ajustados às necessidades do CONTRATANTE.

3.6. É de responsabilidade da CONTRATADA todo material audiovisual, didático e eletrônico para a realização do treinamento.

3.7. O treinamento deve ter duração mínima de 40 horas.

3.8. O treinamento deverá ser ministrado em horário definido pelo CONTRATANTE, em dias úteis.
3.8.1. A critério da CONTRATANTE e havendo disponibilidade da CONTRATADA, o treinamento poderá ser realizado em meio-turno ou turno inteiro.

3.9. O treinamento deverá ser ministrado em língua portuguesa do Brasil.

3.10. O material escrito (PDF, apresentações, imagens etc) deverá ser fornecido, preferencialmente, em Português (Brasil). Em caso de não disponibilidade dessa versão, a mesma deverá ser disponibilizada em Inglês.

3.11. Deve ser realizado na modalidade telepresencial síncrona.

3.12. O prazo para execução do treinamento é de até 180 dias após a assinatura do contrato.

3.13. A CONTRATADA deverá fornecer, ao término, certificado de realização, em português do Brasil, para cada participante, contendo, no mínimo: nome do curso, carga horária, conteúdo programático, nome do instrutor e período de realização.

3.14. A CONTRATANTE poderá solicitar, sem custo adicional, a repetição total ou parcial do treinamento quando forem identificadas, mediante critérios objetivos de avaliação, falhas no cumprimento da carga horária, conteúdo programático, condições de realização ou requisitos mínimos estabelecidos neste Termo de Referência, devendo a CONTRATADA realizar a nova capacitação em prazo acordado entre as partes.

3.15. O treinamento será aceito após comprovação da carga horária, conteúdo, participação e entrega dos materiais.

4. ITEM 6 – Requisitos mínimos de implantação da solução

4.1. A fase de ativação dos serviços deverá ser conduzida e concluída nos primeiros 60 dias corridos contados a partir da assinatura do contrato, quando serão executados o planejamento para implantação das ferramentas e a adequação de processos de gestão de segurança cibernética que nortearão a prestação de serviços do Centro de Operações de Segurança Cibernética (SOC).

4.1.1. A CONTRATADA deve realizar o planejamento, a implantação, configuração e ativação dos serviços e soluções propostas no prazo de até 60 dias corridos, contados a partir da assinatura do contrato, conforme objetivos, escopo, requisitos, premissas e demais condições elencadas nesta especificação.

4.2. As atividades que propiciarão criar, alterar e manter controles de segurança cibernética, além de medir a eficiência e eficácia dos serviços de SOC quanto à sua utilização dentro do negócio, serão adequadas nesta fase de ativação do contrato, conforme parâmetros (baseline) a serem acordados entre as partes.

4.3. Os papéis e responsabilidades das partes nos processos de gestão de segurança cibernética, bem como indicadores necessários para medir e melhorá-los continuamente, serão definidos também com base nos referidos parâmetros (baseline).

4.4. As atividades de implantação e ativação do contrato poderão ocorrer de forma remota e deverão contemplar, no mínimo, as seguintes fases:

4.4.1. Planejamento e Projeto:

4.4.1.1. Reunião de kick-off;

4.4.1.2. Coleta de dados e requisitos complementares;

4.4.1.3. Detalhamento de cronograma;

4.4.1.4. Apresentação de parâmetros (baseline) e adequação de

processos de gestão de segurança cibernética.

4.4.2. Implantação, Configuração e Ativação da solução:

4.4.2.1. Instalação e ativação da solução on-line e console de gerência;

4.4.2.2. Instalação e ativação dos agentes, coletores, console de gerência e demais componentes da solução (pertinentes aos ativos monitorados) no ambiente computacional do CONTRATANTE: servidores, estações de trabalho, firewalls, servidores de diretório e cloud;

4.4.2.3. Instalação e ativação dos coletores de logs;

4.4.2.4. Configuração e o correto funcionamento da coleta, processamento e correlação de logs de eventos em que a solução possua conectores nativos, ou seja, que não necessitem de customização de parsers para tal funcionamento (os conectores nativos devem contemplar a coleta, processamento e correlação de logs para os ambientes que constam nos itens 2.17.1, 2.18.1 e 2.19.1);

4.4.2.5. Testes e homologação.

4.4.3. Definição de Processos e Outras Configurações:

4.4.3.1. Implementação dos processos e recursos propostos;

4.4.3.2. Desenvolvimento de playbooks de resposta a ataques cibernéticos;

4.4.3.3. Configuração e correto funcionamento da coleta, processamento e correlação de logs de eventos em que haja a necessidade de customização de parsers para tal funcionamento (item 2.17.2).

4.4.3.4. Testes e homologação;

4.4.3.5. Desenvolvimento de um plano de continuidade que contemple minimamente a exportação de:

4.4.3.5.1. Base de incidentes em aberto (em tratamento);

4.4.3.5.2. Playbooks implementados.

4.4.4. Treinamento de equipes.

4.4.5. Operação, Sustentação e Melhoria Contínua:

4.4.5.1. Sustentação/On-Going;

4.4.5.2. Reunião mensal;

4.4.5.2.1. Relatórios periódicos;

4.4.5.2.2. Acompanhamento de indicadores;

4.4.5.2.3. Melhoria contínua.

4.5. A lista de soluções constantes nos itens 2.13, 2.17, 2.18 e 2.19 não é exaustiva, de forma que, conforme houver evolução do parque tecnológico ao longo do contrato, a CONTRATADA deve, como parte da operação, sustentação e melhoria contínua da solução, realizar a configuração para o correto funcionamento de parsing (quando

houver), coleta, processamento e correlação de logs de eventos gerados pela novas soluções incluídas/alteradas no ambiente computacional.

5. ITENS 7 e 8 – Requisitos mínimos do serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos

5.1. Para o item 7, considera-se que o valor trata-se de custo fixo mensal referente à construção da infraestrutura mínima necessária para atendimento aos requisitos do item presentes neste edital, considerando 2.000 ativos por mês monitorados;

5.2. O item 8 refere-se ao monitoramento de ativos além da quantidade basal prevista para o item 7. A unidade de medida será mensurada em múltiplos de 1.000 ativos monitorados por mês, proporcional à quantidade de ativos monitorados. Por exemplo: uma contratação de 3200 ativos do item 1, implicam em 1 unidade do item 7 e 2 unidades do item 8;

5.3. Os serviços deverão ser prestados por meio do Centro de Operações de Segurança Cibernética (SOC) da CONTRATADA, em regime 24x7x365, que deverá atender os seguintes requisitos mínimos:

5.3.1. A prestação dos serviços deverá ser feita a partir de Centro de Operações de Segurança Cibernética especializado, sendo remoto às instalações do CONTRATANTE.

5.3.2. A equipe do SOC poderá, a critério da CONTRATADA, ser compartilhada com outros clientes, incluindo outros Órgãos da Justiça do Trabalho, de modo a otimizar os esforços, respeitando a confidencialidade das informações relativas ao objeto deste edital.

5.3.3. A solução contratada deve ter instância própria para o CONTRATANTE, exclusiva e dedicada para cada Tribunal e sem compartilhamento com outros clientes da CONTRATADA.

5.3.4. A CONTRATADA deve indicar, formalmente, quando da assinatura do contrato, PREPOSTO TITULAR e substituto que tenham capacidade gerencial para tratar de todos os assuntos previstos no instrumento contratual e coordenação da equipe para a execução dos serviços contratados.

5.3.5. O PREPOSTO deve, entre outras atividades, promover os contatos com o gestor do contrato bem como deve prestar atendimento aos profissionais em serviço, tais como:

5.3.5.1. Assegurar de que as determinações do CONTRATANTE sejam disseminadas junto aos profissionais alocados com vistas à execução dos serviços contratados;

5.3.5.2. Informar ao gestor do contrato sobre problemas de qualquer natureza que possam impedir o bom andamento dos serviços contratados;

5.3.5.3. Desenvolver atividades administrativas de responsabilidade

da CONTRATADA, principalmente quanto ao controle de informações relativas ao seu faturamento mensal e apresentação de documentos quando solicitado;

5.3.5.4. O PREPOSTO não pode ser contabilizado como profissional para execução dos serviços contratados.

5.3.6. Os serviços de operação e gestão da solução deverão ser fornecidos diretamente pela CONTRATADA, devendo a mesma ser autorizada ou ser parceira do fabricante da solução XDR para fornecer serviço de MDR (Managed Detection and Response).

5.3.7. O compartilhamento de profissionais não poderá comprometer capacidade, SLAs ou segregação lógica. A CONTRATADA manterá controles de acesso e menor privilégio.

5.3.8. A CONTRATADA deverá disponibilizar um canal de comunicação por telefone, celular ou 0800 com o serviço de SOC em regime 24x7;

5.4. A CONTRATADA deve possuir um "Computer Security Incident Response Team (CSIRT)", ou Grupo de Resposta a Incidentes de Segurança – grupo de pessoas com a responsabilidade de identificar, receber, analisar e investigar as notificações e atividades relacionadas a incidentes de segurança cibernética nos ativos monitorados e orientar o CONTRATANTE quanto ao que deve ser feito para resolver o incidente de segurança cibernética.

5.5. Os incidentes de segurança cibernética são os relacionados aos eventos de segurança dos ativos monitorados como: ataques de movimentação lateral, escalação de privilégios, acessos indevidos, instalações de códigos maliciosos, ataques por força bruta, ou qualquer outra ação passível de monitoramento pela solução proposta e que possa comprometer a confidencialidade, disponibilidade, integridade ou privacidade das informações do CONTRATANTE.

5.6. Um incidente de segurança é definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação do CONTRATANTE, levando à perda de um ou mais princípios básicos de segurança cibernética: confidencialidade, integridade, disponibilidade ou privacidade.

5.7. O processo de notificação de incidentes de segurança se inicia sempre que um evento adverso for submetido por qualquer ferramenta de segurança, podendo o corpo técnico de segurança deste CONTRATANTE a qualquer momento, abrir um incidente de segurança junto à CONTRATADA.

5.8. O CONTRATANTE deverá ser informado sobre os incidentes detectados através do Portal de Atendimento, e-mail e/ou por telefone, conforme previamente acordado com a CONTRATADA na fase de Planejamento e Projeto (item 4.4.1).

5.9. As solicitações de serviços e as notificações de incidentes de segurança cibernética reportadas pela solução proposta ou pelo CONTRATANTE deverão ser registradas no módulo de gestão de incidentes de segurança da solução ofertada (item 2.5.4).

5.10. Todo tipo de comunicação e documentação relacionados aos tratamentos de incidentes devem ser em Português.

OPERAÇÃO E SUSTENTAÇÃO

5.11. Os serviços de operação e sustentação da solução contemplam todas as atividades de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos identificados pela solução ofertada, bem como a sustentação da mesma, mediante a sua operação por parte da CONTRATADA.

5.12. Os seguintes serviços deverão ser realizados pela equipe da CONTRATADA para a operação da solução proposta:

5.12.1. Ativação e configuração dos módulos contratados;

5.12.2. Integração dos componentes contratados com o ambiente do CONTRATANTE;

5.12.3. Gestão do ciclo de vida da solução, contemplando a sua implantação e operação, além da inclusão, alteração e exclusão de ativos monitorados;

5.12.4. Abrir e fazer a triagem de chamados de segurança cibernética;

5.12.5. Fazer primeiro atendimento de reportes de incidentes de segurança cibernética;

5.12.6. Atender incidentes simples, os quais possuem instruções indicadas em playbooks (knowledge Base do ITSM);

5.12.7. Elaborar consultas(queries)/scripts de rastreamento quando necessário e/ou solicitados pelo CONTRATANTE;

5.12.8. Elaborar manual de usuário das atividades que se fizerem necessários e/ou solicitados pelo CONTRATANTE;

5.12.9. IPs externos deverão ser analisados e contextualizados conforme sua criticidade;

5.12.10. Fazer passagem de turno, acompanhar os incidentes e realizar “follow-ups”, de modo que haja acompanhamento integral dos tickets abertos;

5.12.11. Prestar suporte/apoio ao processo de automação das atividades relacionadas à resposta e tratamento de incidentes cibernéticos;

5.12.12. Desenvolvimento de playbooks de resposta a ataques cibernéticos;

5.12.13. Configuração de fontes de eventos;

5.12.14. Configuração de usuários VIP e usuários de serviço;

5.12.15. Criação de alertas customizados;

5.12.16. Configuração de coletores de eventos;

5.12.17. Configuração de monitoramento de arquivos e diretórios;

5.12.18. Liberação de acesso à solução para usuários autorizados pelo CONTRATANTE;

5.12.19. Geração de indicadores de performance (KPI) definidos neste documento e acordados na fase de Planejamento e Projeto (item 4.4.1);

5.12.20. Zelar e empregar todos os esforços necessários para garantir o

atendimento ao SLA estabelecido neste edital, tanto no que se refere aos serviços quanto às soluções contratadas;

5.12.21. Atualização da solução, quando necessário/aplicável e/ou solicitados pelo CONTRATANTE;

5.12.22. Resolução de chamados de suporte junto ao(s) fabricante(s) da solução.

5.13. A equipe da CONTRATADA deve ter, no mínimo, uma pessoa responsável pelos assuntos técnicos (líder técnico) e que será o ponto de contato com a equipe de segurança cibernética do CONTRATANTE. O líder técnico tem, entre outras responsabilidades:

5.13.1. Após a assinatura do contrato, conhecer o parque tecnológico e as atividades em andamento, visando à preparação da equipe que prestará os serviços, conhecer os modelos de serviços realizados, as normas internas, procedimentos de segurança e a definição dos requisitos necessários;

5.13.2. Fazer uma reunião semanal com a equipe do CONTRATANTE para acompanhamento dos resultados (a frequência da reunião poderá ser revista oportunamente, a critério do CONTRATANTE).

5.13.3. Fazer a entrega e apresentação dos relatórios mensais, conforme especificação técnica contida neste documento;

5.13.4. Esclarecer dúvidas em relação às requisições, alertas, incidentes, relatórios, prazos de atendimento e outras atividades de responsabilidade da equipe da CONTRATADA;

5.13.5. Estar disponível por telefone e e-mail, de segunda a sexta-feira, das 9 (nove) às 18 (dezoito) horas e acessível por contato telefônico em qualquer outro horário (incluindo sábados, domingos e feriados).

INTELIGÊNCIA DE AMEAÇAS

5.14. A equipe da CONTRATADA deve prover serviços de pesquisa e desenvolvimento de inteligência (threat intelligence) para proteção contra ataques cibernéticos, sendo responsável por:

5.14.1. Pesquisar novos tipos de ataques, vírus, malwares, botnets, vulnerabilidades e afins com intuito de melhoria contínua de detecção e mitigação destes males dentro dos serviços e ativos de segurança fornecidos pela CONTRATADA;

5.14.2. Criar, em colaboração com a equipe de segurança cibernética do CONTRATANTE, casos de uso (regras) que devem ser implementados na solução fornecida;

5.14.3. Revisar, sempre que necessário e/ou solicitados pelo CONTRATANTE, as regras da solução fornecida, realizando as adaptações e evoluções necessárias;

5.14.4. Produzir e entregar informação de inteligência acionável, na forma

de procedimentos para triagem de alertas e procedimentos para notificação de incidentes correspondentes às regras da solução ofertada;

5.15. A equipe da CONTRATADA deve fornecer serviço de Password e Credential Assessment (avaliação de credenciais em serviços de diretório e banco de dados):

5.15.1. A solução deve avaliar o nível de dificuldade de quebra de senhas.

5.15.2. A solução deve avaliar possíveis vazamentos de credenciais na Dark/Deep Web.

5.15.3. O serviço deve poder ser executado sob demanda.

5.15.4. O serviço deve ser executado sem que senhas sejam fornecidas.

MONITORAMENTO E DETECÇÃO DE AMEAÇAS E ATAQUES

5.16. A equipe da CONTRATADA deve atuar no monitoramento dos incidentes detectados pela solução e serviços propostos, sendo responsável por:

5.16.1. Monitorar equipamentos e softwares componentes das soluções de segurança do CONTRATANTE, envolvendo identificação, classificação e análise de eventos que possam comprometer a disponibilidade, integridade e confidencialidade dos serviços.

5.16.2. Focar suas ações nos eventos significativos, classificando-os corretamente conforme as categorias abaixo:

5.16.2.1. Informativos: são eventos que não requerem ação, utilizados para verificação de funcionalidades dos ativos monitorados, ou seja, tem por objetivo identificar se as ferramentas e soluções estão tendo o comportamento esperado. São úteis para gerar informações acerca do ambiente monitorado como, por exemplo, quantidade de eventos gerados nas últimas 24 (vinte e quatro) horas.

5.16.2.2. Avisos: são eventos utilizados para classificar comportamentos anômalos comparados à linha de base de operação do ambiente, porém que ainda não gerou impacto ao ambiente do CONTRATANTE como, por exemplo, espera-se que ocorram 10 bloqueios de um determinado hash diariamente e, entretanto, nos últimos 2 (dois) dias ocorreram 100 bloqueios, sendo que a ferramenta de antivírus continua bloqueando sem que haja qualquer impacto ou degradação no ambiente.

5.16.2.3. Exceções: são eventos que podem indicar que houve impacto em um ou mais dos pilares da segurança da informação (confidencialidade, integridade e disponibilidade) como, por exemplo, a ferramenta de antivírus não bloqueou a ação de um ransomware e dados do CONTRATANTE foram criptografados. Caso um evento seja classificado como

"Exceção", o processo de resposta a incidentes de segurança deve ser iniciado imediatamente.

5.16.3. Comunicar, à equipe de segurança cibernética do CONTRATANTE, as informações iniciais sobre o incidente de segurança e quais serão as linhas de atuação para sua resolução.

5.16.4. Informar ao CONTRATANTE, através do Portal de Atendimento, e-mail e/ou por telefone, conforme previamente acordado com a CONTRATADA na fase de Planejamento e Projeto (item 4.4.1), sobre os incidentes detectados.

5.16.5. Emitir relatórios mensais, provendo, no mínimo, as seguintes informações ao CONTRATANTE:

5.16.5.1. Alertas e notificações;

5.16.5.2. Quantidade de incidentes por categoria;

5.16.5.3. Quantidade de incidentes por criticidade (severidade);

5.16.5.4. Quantidade de incidentes que geraram crise;

5.16.5.5. Porcentagem dos incidentes originários do monitoramento;

5.16.5.6. Quantidade de incidentes tratados/fechados;

5.16.5.7. Quantidade de incidentes registrados.

5.16.6. Relativo ao monitoramento de Deep/Dark Web, a CONTRATADA deverá prover, no mínimo, os seguintes serviços:

5.16.6.1. Monitoramento e envio de notificações para a equipe técnica do CONTRATANTE contendo os alertas identificados no regime 24x7 (vinte e quatro horas por dia, sete dias por semana);

5.16.6.2. Serviço de investigação pela equipe técnica da CONTRATADA, contendo os alertas identificados e sugestões de mitigação, em regime 8x5 (oito horas por dia, cinco dias por semana);

5.16.6.3. Envio de um relatório ao fim do mês ao CONTRATANTE contendo, no mínimo, as informações a seguir:

5.16.6.3.1. Vazamento de dados do CONTRATANTE que foram encontrados na Deep/Dark Web, através do monitoramento de domínios, IPs, e e-mails.

5.16.6.3.2. Descrição do ambiente avaliado;

5.16.6.3.3. Tabela resumo de serviços descobertos, detecções e alertas;

5.16.6.3.4. Descrição detalhada dos alertas;

5.16.6.3.5. Descrição, evidências, screenshots relevantes e recomendações para mitigação dos riscos;

5.16.6.3.6. Testes executados e relatórios técnicos das ferramentas;

5.16.6.3.7. Apresentação técnica dos resultados, incluindo o

detalhamento dos eventos identificados.

RESPOSTA E INVESTIGAÇÃO A INCIDENTES CIBERNÉTICOS

5.17. A equipe da CONTRATADA deve atuar no processo de resposta a incidentes detectados pela solução proposta, sendo responsável por:

5.17.1. Analisar, recomendar ações de remediação e contenção e documentar os eventos de segurança que, após analisados, demonstraram ser um ataque ao ambiente do CONTRATANTE, tendo sido categorizados como "Eventos de Exceção" e, portanto, acionado o processo de resposta a incidentes cibernéticos.

5.17.2. Analisar, após um incidente de segurança ser aberto, os logs e artefatos enviados/coletados a fim de, no primeiro instante, identificar as fontes geradoras de tais eventos.

5.17.3. Identificar, uma vez realizadas as análises iniciais do incidente, quais foram os principais vetores de ataque ao ambiente do CONTRATANTE.

5.17.4. Definir, junto à equipe de segurança cibernética do CONTRATANTE, a severidade do incidente de segurança, que será obtida por meio de uma matriz GUT (Gravidade, Urgência e Tendência).

5.17.4.1. A matriz GUT será definida na fase de Planejamento e Projeto (item 4.4.1) pela CONTRATADA em conjunto à equipe de segurança cibernética do CONTRATANTE.

5.17.5. Apoiar a equipe técnica do CONTRATANTE nos processos de mitigação, contenção de ataques e restauração do seu ambiente tecnológico.

5.17.6. Realizar, após análises iniciais do incidente e a definição de severidade, uma análise aprofundada do incidente baseando-se no comportamento do ataque e/ou artefato (malware).

5.17.7. Documentar todo o processo de análise e resultado no módulo de gestão de incidentes de segurança da solução ofertada (item 2.5.4) para que a equipe de segurança cibernética do CONTRATANTE acompanhe os passos para a solução do incidente de segurança.

5.17.8. Definir e documentar, uma vez identificado o comportamento e os principais vetores de ataque, uma estratégia para a mitigação e contenção do ataque em questão e notificá-la ao CONTRATANTE.

5.17.8.1. Qualquer tipo de alteração no parque computacional do CONTRATANTE para contenção e mitigação de incidentes de severidade alta ou crítica, deverá ser executada pelo próprio CONTRATANTE com o suporte da CONTRATADA, que deverá sugerir a melhor maneira de implantar a estratégia definida por ela para a resposta ao ataque, até a efetiva resolução do incidente.

5.17.9. Iniciar, mitigado o incidente de segurança, o processo de compilação de todas e quaisquer evidências e identificação dos serviços afetados. Tais evidências serão utilizadas até a finalização do processo para execução de eventual análise forense do incidente de segurança.

5.17.9.1. A necessidade de análise forense será indicada pelo CONTRATANTE, seguindo os seus processos internos de gestão de incidentes de segurança, a serem apresentados na fase de Planejamento e Projeto (item 4.4.1).

5.17.9.2. Os dados coletados devem ser reunidos durante o processo de tratamento de incidente para subsidiar futura e eventual análise forense, seguindo as etapas de preservação, extração, análise e laudo. Tal análise deve ser realizada com o objetivo de identificar pessoas, locais ou eventos, correlacionando todas as informações reunidas e gerando como produto final um laudo sobre o incidente de segurança em questão.

5.17.10. Reconstruir o ataque, caso seja necessário e/ou solicitado pelo CONTRATANTE. Esta ação deve ser realizada pela CONTRATADA em ambiente controlado (como um sandbox), utilizando mecanismos de segurança para separar programas em execução, geralmente utilizado em um esforço para mitigar falhas de sistema ou vulnerabilidades de segurança cibernética.

5.17.11. Documentar, no módulo de gestão de incidentes de segurança da solução ofertada (item 2.5.4), as lições aprendidas do incidente de segurança em questão, formando, durante todo o período de vigência do contrato, uma grande base de conhecimento sobre ataques adversos.

5.17.11.1. A solução deve permitir a exportação da base de conhecimentos para formato Word ou PDF.

5.18. O regime de execução dos serviços deve ser 24x7x365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias ao ano).

CONFIDENCIALIDADE E DESCARTE DE INFORMAÇÕES

5.19. Confidencialidade**:**

5.19.1. A CONTRATADA deve ser responsável pelo ciclo de vida das informações coletadas pela solução proposta, atendendo aos critérios definidos pelo CONTRATANTE, devendo processar, armazenar e, após o término da sua finalidade, descartar os dados de maneira segura.

5.19.1.1. A CONTRATADA obriga-se a tratar como “segredos

comerciais e confidenciais” quaisquer informações, dados, processos, fórmulas, códigos, obtidos em consequência ou por necessidade desta contratação, utilizando-os apenas para as finalidades previstas no contrato, não podendo revelá-los ou facilitar a revelação a terceiros, mediante assinatura dos Termo de Compromisso com a Segurança da Informação (Anexo II);

5.19.2. Ao final do contrato, o descarte das informações deve ser realizado com o emprego de medidas que impossibilitem a sua reconstrução, de acordo com as necessidades do suporte físico ou digital.

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

Anexo II

TERMO DE COMPROMISSO COM A SEGURANÇA DA INFORMAÇÃO

A empresa _____, parte CONTRATADA no contrato___/____, neste ato representado pelo(a) Sr.(a)_____, portador(a) da CI/RG n.º _____ e do CPF nº _____, compromete-se, por intermédio do presente termo, a não divulgar sem prévia autorização informações confidenciais pertencentes ou custodiadas pelo **TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO (TRT4)** às quais tiver acesso em decorrência da prestação do objeto do citado contrato, em conformidade com as seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA: Consideram-se informações confidenciais aquelas referentes a dados pessoais e dados pessoais sensíveis existentes no ambiente tecnológico ou físico do TRT4 ou por ele contratado, bases de dados, topologias, planos, políticas, processos, códigos-fonte, serviços e sistemas tecnológicos vinculados ao TRT4.

§ 1º Em relação aos dados pessoais e dados pessoais sensíveis do TRT4, a CONTRATADA deverá realizar o tratamento de acordo com o disposto nas cláusulas *de Proteção de Dados* do instrumento contratual.

§ 2º – Em caso de dúvida acerca da confidencialidade de determinada informação, a CONTRATADA deverá tratar a mesma sob sigilo até que venha a ser autorizada por escrito pelo TRT4 a tratá-la diferentemente. De forma alguma se interpretará o silêncio do TRT4 como a liberação do compromisso de manter o sigilo da informação.

§ 3º Excluem-se das disposições desta Cláusula informações que já estiverem comprovadamente disponíveis ao público em geral de qualquer forma que não em decorrência de sua revelação pela CONTRATADA.

CLÁUSULA SEGUNDA: A CONTRATADA concorda que as informações às quais terá acesso serão utilizadas exclusivamente no desempenho das atividades necessárias para execução do objeto contratado, em conformidade com o presente TERMO.

CLÁUSULA TERCEIRA: A CONTRATADA obriga-se a conhecer e observar a Política de Segurança da Informação disponível no site do TRT4.

CLÁUSULA QUARTA: A CONTRATADA compromete-se a aplicar boas práticas de mercado relacionadas à segurança da informação (como, por exemplo, ABNT NBR 27002:2022, CIS *Controls*, OWASP, NIST *Cybersecurity Framework*, dentre outras), pertinentes ao serviço prestado, para garantir a segurança do seu ambiente tecnológico de forma a atender os Acordos de Níveis de Serviços (ANS) e os Acordos de Nível Operacional (ANO) estabelecidos em contrato, bem como garantir a proteção da confidencialidade, integridade e disponibilidade das informações do TRT4 que vierem a ser tratadas em seu ambiente tecnológico.

CLÁUSULA QUINTA: A CONTRATADA determinará a todos os seus representantes - assim considerados, diretores, administradores, sócios, empregados, prepostos, agentes,

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

colaboradores e prestadores de serviço a qualquer título (incluindo consultores e assessores) que estejam, direta ou indiretamente, envolvidos com a prestação de serviços - a observância do presente Termo, adotando todas as precauções e medidas para que as obrigações oriundas do presente instrumento sejam efetivamente observadas.

CLÁUSULA SEXTA: Caso a CONTRATADA seja obrigada, em decorrência de intimação de autoridade judiciária ou fiscal, a revelar quaisquer informações, notificará por escrito ao TRT4, em até 24 horas, acerca da referida intimação, de forma a permitir que o TRT4 possa optar entre interpor a medida cabível contra a ordem judicial ou administrativa ou consentir, por escrito, com a referida revelação.

CLÁUSULA SÉTIMA: A CONTRATADA obriga-se a informar ao TRT4, em até 24 horas, qualquer violação das regras de sigilo ora estabelecidas que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo, bem como de seus empregados, prepostos e prestadores de serviço.

CLÁUSULA OITAVA: A CONTRATADA obriga-se a informar, em até 24 horas, ao TRT4 a ocorrência de incidentes, tecnológicos ou não, que possam comprometer (ou possam ter comprometido) a confidencialidade, integridade ou a disponibilidade das informações do TRT4 que são tratadas em seu ambiente tecnológico ou o cumprimento de ANS e ANO, bem como as medidas adotadas para contenção, tratamento, resposta e erradicação dos incidentes.

CLÁUSULA NONA: O descumprimento de quaisquer das cláusulas do presente Termo acarretará a responsabilidade civil e criminal dos que, comprovadamente, estiverem envolvidos no descumprimento ou violação.

Porto Alegre, ___ de _____ de 20__.

_____

Assinatura do Representante Legal

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

versão janeiro/2026

Anexo III - FORMULÁRIO DE PESQUISA DE PREÇOS

Objeto:	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.

Unidade Requisitante:	SGTI	**Responsável(is) pela pesquisa de preços:**	Maurício Antonioli Schmitz Alberto Daniel Müller

Observações:
1. A pesquisa de preços deve ser realizada de acordo com as recomendações do Guia de Pesquisa de Preços do TRT4.
2. Devem ser indicadas as páginas (folhas) que ratificam os preços lançados em cada uma das fontes utilizadas.
3. Não há necessidade de indicação do nome das fontes que originaram o valor estimado.
4. Na coluna “Metodologia de Cálculo”, deve ser indicada a metodologia utilizada para o valor estimado de cada um dos itens da contratação (média, mediana ou menor preço, etc).
5. A unidade requisitante poderá adaptar o presente formulário a sua necessidade, devendo atentar para a apresentação, no processo administrativo, em arquivo único, devidamente identificado.
6. O valor estimado (unitário e total) deve constar no Termo de Referência da contratação.
7. A data do orçamento estimado refere-se à data de análise das fontes de pesquisa, escolha da metodologia de cálculo e formação do valor total estimado da contratação.
8. O Código do Catálogo Comprasnet deve ser obtido no seguinte link: https://catalogo.compras.gov.br/cnbs-web/busca

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

PODER JUDICIÁRIO

JUSTIÇA DO TRABALHO

TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO

VALORES ESTIMADOS PARA TODOS OS TRTs PARTICIPANTES:

							Fonte 01 (DOC. 4)	Fonte 02 (DOC. 5)	Fonte 03 (DOC. 6)	Fonte 4 (DOC. 7)	Fonte 5 (DOC. 8)	Fonte 6 (DOC. 9)	VALOR ESTIMADO		
Item	Descrição	CATMAT/ CATSERV	Classificação da Despesa	Unidade	Quantidade de compra inicial	Quantidade total do registro	Valor unitário	Valor unitário	Valor unitário	Valor unitário	Valor unitário	Valor unitário	Metodologia de cálculo	Valor unitário estimado	Valor total estimado
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	61.500	*1.836,00*	*541,74*	*755,43*	*1.049,00*	*1.227,72*	*1.320,00*	Média dos 2 menores valores	648,59	39.888.285,00
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	54.850	*216,59*	*154,17*	*101,96*	-	-	*975,00*	Média dos 2 menores valores	128,07	7.024.639,50
3	Módulo de solução Agêntica para resposta, orquestração e triagem de eventos e incidentes	26972	33904000 Serviços de TIC - PJ	Tokens	0	748.300	*15,66*	*21,45*	*7,31*	-	-	-	Média dos 2 menores valores	11,49	8.597.967,00
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	9.590	*12.511,80*	*930,49*	*6.680,00*	-	-	-	Menor valor	930,49	8.923.399,10
5	Serviço de treinamento na solução proposta	3840	33904020 Treinamento/capacitação em TIC	Serviço único, por turma de treinamento	0	21	*27.000,00*	*48.459,08*	*35.000,00*	*30.823,33*	-	*30.510,05*	Média dos 3 menores valores	29.444,46	618.333,66
6	Serviço de implantação da solução proposta	26972	33904000 Serviços de TIC - PJ	Serviço único por contratante	0	17	*32.400,00*	*254.864,77*	*54.500,00*	-	-	*63.588,87*	Média dos 2 menores valores	43.450,00	738.650,00
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	17	*2.700,00*	*28.201,35*	*5.750,00*	*5.300,33*	*4.400,00*	*12.480,37*	Média, excluindo o menor e maior valor	6.982,68	4.273.400,16
8				Serviço para 1000 ativos adicionais monitorados por mês	0	33	*2.160,00*	*6.635,61*	*3.450,00*	-	-	-	Média	4.081,87	4.849.261,56
														VALOR TOTAL ESTIMADO COMPRA INICIAL	**R$ 0,00**
														VALOR TOTAL ESTIMADO REGISTRO	**R$ 74.913.935,98**
														DATA DO ORÇAMENTO ESTIMADO	**22/10/2023**

* Fonte 1: Os valores foram orçados em dólar, para comparativo de preços foi utilizado o dólar estimado pela empresa de R$ 5,40.
* Fonte 5: no contrato o valor unitário do item 1 está para 30 meses, desta forma foi feito cálculo proporcional para 36 meses
* Fonte 6: as subscrições são para 1 ano, desta forma foi multiplicado por 3 para completar os 36 meses.

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

PODER JUDICIÁRIO

JUSTIÇA DO TRABALHO

TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO

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
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
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
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
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
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
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
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
8				Serviço para 1000 ativos adicionais monitorados por mês	0	5	4.081,87	734.736,60
							VALOR TOTAL ESTIMADO COMPRA INICIAL	0,00
							VALOR TOTAL ESTIMADO REGISTRO	7.608.927,54

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

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

Justificativa pela eventual não obtenção de 3 valores de mercado: [1]
Não se aplica

Justificativa pela eventual não utilização de painel de preços ou de contratos similares de outros órgãos na pesquisa de preços:
Não se aplica

Justificativa da escolha dos fornecedores que participaram da pesquisa de preços:
(x) Fornecedores que atuam no ramo empresarial relativo ao objeto da contratação;
( ) Fornecedores que mantém contrato vigente com o Tribunal;
( ) Fornecedores cadastrados no Tribunal e/ou que tenham fornecido no passado objeto similar;
( ) Fornecedores que venceram licitações de objetos similares em outros órgãos públicos;
( ) Outra:

[1] Neste campo, o requisitante deverá informar a situação que inviabilizou a obtenção de três orçamentos, mencionar as tentativas de consulta de preço empreendidas, informando os fornecedores contatados (nome e telefone) e anexando mensagens eletrônicas que tenha enviado, bem como demais documentos que entender relevantes para demonstrar tal fato, ou, ainda, informar acerca da inexistência de outros fornecedores para o objeto.

PROAD n. 6891/2026 DOC 42
Cadastrado por CARLOS COSTA JORDÃO em 23/10/2026
Juntado em 23/10/2026

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.

PROAD n. 6891/2026 DOC 42 - Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.GKDM.QTGV:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

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.

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

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).

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

versão janeiro/2026

CONTRATAÇÃO DE TIC

INSTITUIÇÃO DA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

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. VINCULAÇÃO AO PLANO DIRETOR DE TIC

A contratação atende a alguma ação do Plano Diretor de TI?

(x) Sim – Qual?
A contratação pretendida consta no Plano de Contratações de TIC, que faz parte do PDTIC.
Números do Item no Plano de Contratações: SGTI-18/2026 e 67/2026

( ) Não.

3. APROVAÇÃO DO COMITÊ DE GOVERNANÇA DE TIC

(Caso a contratação não tenha sido previamente aprovada, deverá ser encaminhada para aprovação)

A contratação foi aprovada pelo Comitê de Governança de TIC?

(x) Sim
Data da aprovação: 19.09.2025
Forma de aprovação: Plano de Contratações 2026
Proad: 2097/2025

4. EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

Integrante		Unidade/Setor
Demandante	Carlos Costa Jordão	Coordenadoria de Segurança da Informação e Proteção de Dados
Técnico	Maurício Antonioli Schmitz	Coordenadoria de Segurança da Informação e Proteção de Dados
Substituto Técnico	Carlos Augusto Nantes de Castilho Rivilino	Coordenadoria de Segurança da Informação e Proteção de Dados
Administrativo da SGTI/ Requisitante	Alberto Daniel Müller	Coordenadoria de Gestão e Apoio à Governança de TIC
Administrativo da SA	Geovane Dutra de Souza	Assessoria de Gestão de Projetos

CARLOS COSTA JORDÃO 23/10/2026 10:56
MAURICIO ANTONIOLI SCHMITZ 23/10/2026 11:09
NATACHA MORAES DE OLIVEIRA 23/10/2026 11:55
GEOVANE DUTRA DE SOUZA 23/10/2026 12:21
JOAO HENRIQUE CARVALHO DE LIMA RIBAS 23/10/2026 13:48
ALBERTO DANIEL MULLER 23/10/2026 16:36
CARLOS AUGUSTO NANTES DE CASTILHO RIVILINO 23/10/2026 18:33
CAROLINE ROCHA MOLINA 23/10/2026 19:44

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

Atendidos os pressupostos até o momento, indicam-se os integrantes relacionados acima, e autoriza-se o prosseguimento do planejamento da contratação.

Documento assinado digitalmente NATACHA MORAES DE OLIVEIRA Secretária-Geral de Tecnologia e Inovação	*Documento assinado digitalmente* JOÃO HENRIQUE CARVALHO DE LIMA RIBAS Autoridade competente da área Administrativa

Equipe de Planejamento da Contratação

Os integrantes da equipe de planejamento da contratação declaram:
- Ter ciência da sua nomeação, bem como possuir conhecimento de suas competências e das regras e diretrizes consignadas na Instrução Normativa n° 5/2017 do Ministério do Planejamento, Desenvolvimento e Gestão, na Lei nº 14.133/2021 e na Resolução CNJ 468/2022;
- Conhecer o Código de Conduta e Valores Éticos do TRT4 e, em especial, as vedações contidas no art. 7º, incisos I e V, e artigo 9º da Portaria nº 4.573/2023.

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

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

versão janeiro/2026

CONTRATAÇÃO DE TIC

INDICAÇÃO E CIÊNCIA DE EQUIPE DE GESTÃO E FISCALIZAÇÃO DE CONTRATO

Solução de TIC:	**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.**

Integrante	Titular	Substituto	Unidade
Gestor:	Carlos Costa Jordão	Charles Ferreira Falcao	Coordenadoria de Segurança da Informação e Proteção de Dados
Fiscal Técnico:	Maurício Antonioli Schmitz	Carlos Augusto Nantes de Castilho Rivilino	Coordenadoria de Segurança da Informação e Proteção de Dados
Fiscal Demandante:	Rodrigo Zarth	Mateus Both	Coordenadoria de Segurança da Informação e Proteção de Dados
Fiscal Administrativo:	Alberto Daniel Müller	Ricardo Krause Kurylenko	Coordenadoria de Gestão e Apoio à Governança de TIC

AUTORIDADE COMPETENTE

Documento assinado digitalmente
NATACHA MORAES DE OLIVEIRA
Secretária-Geral de Tecnologia e Inovação

DECLARAÇÃO

Os servidores designados, e seus substitutos, declaram:

- Ciência da sua indicação para compor equipe de gestão e fiscalização da contratação a ser formalizada para o objeto descrito acima;
- Conhecer suas atribuições descritas no instrumento contratual, no Manual de Gestão e Fiscalização de Contratos Administrativos do Tribunal e nas regras e diretrizes consignadas na Lei 14.133/2021 e na Resolução CNJ 468/2022;
- Conhecer o Código de Conduta e Valores Éticos do TRT4 e, em especial, a vedação de atuar como gestor ou fiscal de contratação formalizada com pessoa física ou jurídica com quem mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil, ou que seja ou tenha em seu quadro societário seu cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive;
- Compreender que suas funções englobam aferir o cumprimento dos resultados previstos pela Administração para os produtos/serviços contratados, verificar a regularidade das obrigações previdenciárias, fiscais e trabalhistas, quando for o caso, bem como prestar apoio à instrução processual, dentre outras;
- Ciência de que suas atribuições na presente contratação permanecerão até o final da vigência de quaisquer serviços ou obrigações acessórias da contratada, independente da vigência contratual;
- Que comunicarão eventuais impedimentos após a assinatura do contrato.

CARLOS COSTA JORDÃO 23/10/2026 10:56
CHARLES FERREIRA FALCAO 23/10/2026 10:58
MATEUS BOTH 23/10/2026 11:00
RICARDO KRAUSE KURYLENKO 23/10/2026 11:05
MAURICIO ANTONIOLI SCHMITZ 23/10/2026 11:09
NATACHA MORAES DE OLIVEIRA 23/10/2026 11:55
ALBERTO DANIEL MULLER 23/10/2026 16:36
CARLOS AUGUSTO NANTES DE CASTILHO RIVILINO 23/10/2026 18:33
RODRIGO ZARTH 23/10/2026 19:31
CAROLINE ROCHA MOLINA 24/10/2026 12:38

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

FERNANDO MOTTER KESSLER
23/11/2026 11:07

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

[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).

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

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

5. CONTRATAÇÕES CORRELATAS OU INTERDEPENDENTES

- 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 órgãos submetidos ao controle

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

		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.

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

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. 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. 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. 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

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. 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. 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. 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. 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. 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.
	Pagamento anual das subscrições	Durante a elaboração dos Estudos Técnicos Preliminares, foi solicitado às empresas consultadas o envio de propostas comerciais contemplando as modalidades de pagamento das subscrições mensal e anual. Na primeira rodada de orçamentos, a modalidade anual apresentou valores aproximadamente 20% inferiores aos da modalidade mensal. Nas rodadas posteriores de consulta de preços, as empresas informaram que seria possível conceder condições comerciais significativamente mais vantajosas, com descontos ainda mais expressivos, exclusivamente para a modalidade de pagamento anual. Nesse contexto, a comparação entre o

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

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

		orçamento inicialmente encaminhado pela Fonte 2, na modalidade mensal, e a proposta final negociada, com pagamento anual, demonstrou uma redução de aproximadamente 50% no valor da contratação. Tal condição é plenamente compatível com o modelo atual de licenciamento de software por assinatura, onde o valor da licença é normalmente pago de uma única vez para toda a vigência do contrato, ou em parcelas anuais. Dessa forma, considerando a expressiva economia obtida e a maior vantajosidade econômica, optou-se pela modalidade de pagamento anual das subscrições.
	Garantia Contratual	Considerando que o pagamento das subscrições deverá ser feito anualmente de forma antecipada, deverá ser prevista garantia contratual, em atendimento ao disposto no inciso IV do art. 40 da Portaria TRT4 Nº 1.737/2023. Considerando que o pagamento será realizado somente após a comprovação, pelo fabricante, da efetiva vigência das licenças, e que os serviços de manutenção corretiva e atualização do software serão prestados diretamente pelo mesmo fabricante, que pertence ao mercado especializado de fabricantes de soluções de segurança digital de reconhecida solidez e atuação consolidada no mercado de tecnologia da informação, entende-se que o risco de inexecução contratual é reduzido. Dessa forma, considera-se suficiente a exigência de garantia contratual de 5% do valor do contrato, percentual proporcional aos riscos envolvidos e adequado para resguardar a Administração quanto ao cumprimento das obrigações contratuais.
Capacitação e experiência	Dispor de equipe técnica comprovadamente qualificada e certificada para implantação,	Uma solução altamente automatizada ainda exige profissionais capazes de interpretar evidências, calibrar regras,

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

profissional da equipe	operação e resposta a incidentes.	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. As certificações e qualificações profissionais constituem meios de comprovação da capacitação técnica da equipe responsável pela execução dos serviços, cuja natureza 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.
	Dispor de pelo menos 3 (três) profissionais da equipe técnica responsáveis pela implantação e sustentação da solução com certificação oficial do fabricante da solução proposta de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Esta exigência justifica-se pela necessidade de assegurar que a equipe técnica efetivamente os conhecimentos técnicos específicos e indispensáveis para a implantação e sustentação da solução ofertada ao TRT. A implantação envolve atividades de configuração, integração, parametrização, testes e adequação da solução ao ambiente tecnológico do Tribunal, enquanto a sustentação exige capacidade para administrar seus recursos, identificar e solucionar problemas e realizar ajustes necessários à continuidade dos serviços. A certificação oficial do fabricante constitui meio objetivo de comprovação do domínio técnico sobre a solução proposta, pois é resultado de testes e avaliações padronizadas do conhecimento do

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

		profissional, reduzindo riscos de configurações inadequadas, falhas de integração e dificuldades operacionais. É importante destacar que a certificação técnica distingue-se da apresentação de certificados de participação em cursos ou workshops, uma vez que tais documentos, isoladamente, não comprovam a aferição dos conhecimentos técnicos do profissional pelo fabricante. O quantitativo mínimo de três profissionais é necessário paa assegurar que esse conhecimento esteja distribuído na equipe responsável pela execução contratual, mitigando a dependência de um único especialista.
	Dispor de profissionais da equipe técnica responsáveis pela detecção, notificação e investigação de ataques cibernéticos, sendo exigida, em conjunto, a comprovação de pelo menos 3 (três) certificações distintas em segurança ofensiva, dentre as relacionadas a seguir, admitida a distribuição entre os integrantes da equipe, observado o limite máximo de 2 (duas) certificações por profissional: CompTIA PenTest+; EC-Council Licensed Penetration Tester (LPT); IACRB Certified Expert Penetration Tester (CEPT); GIAC Exploit Researcher and Advanced Penetration Tester (GXPN); GIAC Reverse Engineering Malware (GREM); Offensive Security Certified Professional (OSCP); Ethical Hacking Post Exploitation (EHPX);	A exigência justifica-se pela necessidade de que a equipe possua conhecimentos sobre técnicas, ferramentas e metodologias utilizadas por agentes maliciosos para comprometer ambientes tecnológicos. O domínio dessas técnicas permite compreender o comportamento dos atacantes, reconhecer indicadores de comprometimento, identificar vulnerabilidades exploradas, analisar códigos maliciosos e reconstruir as etapas de uma intrusão, contribuindo para maior precisão e efetividade nas atividades de detecção e investigação. As certificações relacionadas foram selecionadas por sua aderência a essas competências, abrangendo conhecimentos em testes de intrusão (Penetration Testing), exploração de vulnerabilidades, pesquisa e desenvolvimento de exploits, engenharia reversa e análise de malware, técnicas de pós-exploração, segurança de aplicações web e operações de Red Team. São qualificações que contemplam diferentes técnicas e perspectivas de atuação ofensiva, permitindo que os profissionais compreendam os métodos empregados em ataques

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

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

	Offensive Security Experienced Penetration Tester (OSEP); Offensive Security Web Expert (OSWE); Certified Red Team Expert (CRTE); Offensive Security Certified Expert (OSCE) ou OSCE³; Certified Ethical Hacker (CEH).	reais e utilizem esse conhecimento para identificar, analisar e investigar ameaças ao ambiente institucional. Destaca-se que a certificação técnica, diferentemente da mera participação em treinamentos ou eventos, pressupõe avaliação baseada em critérios objetivos, destinada a comprovar os conhecimentos e as competências específicas do profissional na tecnologia exigida, conferindo maior segurança quanto à sua qualificação para a execução das atividades contratadas. Por sua vez, A exigência de pelo menos 3 (três) certificações, admitida sua distribuição entre os profissionais da equipe, com o limite de 2 (duas) por profissional, busca assegurar a diversidade e a distribuição dos conhecimentos técnicos necessários às atividades, evitando a concentração da qualificação em um único integrante.
	Dispor de profissionais da equipe técnica responsáveis pela resposta a ataques cibernéticos, sendo exigida, em conjunto, a comprovação de pelo menos 3 (três) certificações distintas em segurança cibernética e resposta a incidentes, dentre as relacionadas a seguir, admitida a distribuição entre os integrantes da equipe, observado o limite máximo de 2 (duas) certificações por profissional: Certified Information Security Manager (CISM); GIAC Experienced Cybersecurity Specialist (GX-CS); GIAC Reverse Engineering Malware (GREM); Ethical Hacking Post Exploitation (EHPX); CompTIA Security+;	A exigência de certificações em segurança defensiva para os profissionais responsáveis pela resposta a ataques cibernéticos justifica-se pela necessidade de assegurar conhecimentos técnicos para analisar incidentes, avaliar riscos, definir estratégias de contenção, executar medidas de mitigação e recuperação e reduzir os impactos de eventos de segurança sobre o ambiente tecnológico do Tribunal. As certificações relacionadas foram selecionadas por contemplarem competências pertinentes à proteção de ambientes tecnológicos, à análise e gestão de riscos, à identificação de ameaças, à gestão de segurança da informação e à resposta a incidentes. Abrangem conhecimentos em gestão de segurança da informação (CISM e CISSP), fundamentos e implementação de controles de segurança (Security+ e CASP),

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

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

	CompTIA Advanced Security Practitioner; EC-Council Security Analyst (ECSA) ou CPENT (Certified Penetration Testing Professional); Certified Information Systems Security Professional (CISSP); CompTIA CYSA+ - Cybersecurity Analyst.	análise e monitoramento de ameaças (CySA+), análise de segurança e testes especializados (ECSA e CPENT), além de engenharia reversa de códigos maliciosos (GREM) e técnicas de pós-exploração (EHPX). A certificação GX-CS também contempla conhecimentos especializados em segurança cibernética. A diversidade das qualificações admitidas busca contemplar competências complementares necessárias à atuação defensiva, desde a identificação e compreensão das ameaças até a definição e execução de ações de resposta, contribuindo para a condução adequada dos incidentes e a preservação da segurança e da disponibilidade dos serviços institucionais. Destaca-se que a certificação técnica, diferentemente da mera participação em treinamentos ou eventos, pressupõe avaliação baseada em critérios objetivos, destinada a comprovar os conhecimentos e as competências específicas do profissional na tecnologia exigida, conferindo maior segurança quanto à sua qualificação para a execução das atividades contratadas. Por sua vez, a exigência de pelo menos 3 (três) certificações, admitida sua distribuição entre os profissionais da equipe, com o limite de 2 (duas) por profissional, busca assegurar que os conhecimentos necessários à resposta a incidentes estejam distribuídos entre os integrantes da equipe, evitando a concentração da qualificação em um único profissional.

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

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

	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. 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.
	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.

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

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

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. 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.
	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. 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

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

		que demandam atuação simultânea sobre diferentes componentes da solução. 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. 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 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**. 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.

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

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
Equipamentos: ( ) Distribuição e racionalização do uso ( ) Custo total de propriedade ( ) Ciclo de vida do produto ( ) Composição ( ) Descarte e resíduos ( ) Embalagens ( ) Emissões ( ) Consumo elétrico	
Suprimentos e consumíveis: ( ) Embalagens ( ) Durabilidade ( ) Logística reversa	
Softwares: ( ) Transformação digital ( ) 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.
(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

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

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? (x) Sim ( ) Não atende ao requisito
Estimativa do valor da contratação (a eventual falta de estimativa de valor da solução deve ser justificada)	<u>Valor estimado</u>: ➢ 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.

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

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

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 técnica e econômica 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 comandos de resposta.

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

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

	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. 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. 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 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

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

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

	fabricantes pode ocasionar perda de informação ou impossibilidade de correlação. 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. 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. O resultado esperado é um ambiente com menos pontos de falhas operacionais, maior agilidade e custo total administrável. 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. ( ) Não - Justificativa:

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

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? ( ) 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:. ➢ 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. R$ 4.498.684,04 para 36 meses Memória de cálculo: ➢ Informar preços unitários referenciais, memórias de cálculo e documentos que lhe dão suporte. Valores do contrato atual: Subscrições: R$ 1.162.672,40 anual por 3 anos = R$ 3.488.017,20 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: ( ) **Sim - Justificativa técnica e econômica 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. (x) Não - Justificativa: 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. 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. 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. 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. 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. 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

<table>
<tr><td></td><td>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.

Pelas motivações acima expostas, a prorrogação do contrato atual mostra-se inviável para o atendimento das necessidades institucionais.</td></tr>
<tr><td>Descrição da Solução 3</td><td>Contratação de solução XDR e ITDR separadamente</td></tr>
<tr><td>Atendimento aos Requisitos</td><td>A solução atende a todos os requisitos da contratação especificados neste documento?

( ) Sim (x) Não atende a pelo menos os requisitos de integração operacional e de console única</td></tr>
<tr><td>Estimativa do valor da contratação
(a eventual falta de estimativa de valor da solução deve ser justificada)</td><td><u>Valor estimado</u>:.
➢ 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.

Valor total estimado somente para a solução ITDR: R$ 2.623.247,50

<table>
<tr><th>Nº Item</th><th>Descrição</th><th>Quant.</th><th>Unidade</th><th>Fonte 1 Valor Unitário</th><th>Fonte 2 Valor Unitário</th><th>Fonte 3 Valor Unitário</th><th>Fonte 4 Valor Unitário</th><th>Fonte 5 Valor Unitário</th><th>Metodologia de Cálculo</th><th>Valor Unit. Estimado</th><th>Valor Total Estimado</th></tr>
<tr><td>1</td><td>Subscrição de uso de solução de proteção de identidades para 36 meses</td><td>4500</td><td>Contas de usuários ativas</td><td>438,18</td><td>795,66</td><td>783,68</td><td>517,66</td><td>3.565,50</td><td>média 2 menores valores</td><td>477,92</td><td>2.150.637,00</td></tr>
<tr><td>2</td><td>Serviço de implantação de solução de proteção de identidades</td><td>1</td><td>serviço</td><td>55.430,00</td><td>84.006,98</td><td>20.900,00</td><td>185.000,00</td><td>38.852,00</td><td>média 3 menores valores</td><td>38.394,00</td><td>38.394,00</td></tr>
<tr><td>3</td><td>Serviço gerenciado da solução de proteção de identidades</td><td>36</td><td>mês</td><td>34.038,10</td><td>11.455,50</td><td>2.500,00</td><td>40.000,00</td><td>4.496,00</td><td>mediana</td><td>11.455,50</td><td>412.398,00</td></tr>
<tr><td>4</td><td>Treinamento</td><td>1</td><td>turma</td><td>180.900,00</td><td>7.637,00</td><td>-</td><td>40.000,00</td><td>36.000,00</td><td>média 2 menores valores</td><td>21.818,50</td><td>21.818,50</td></tr>
<tr><td colspan="5">VALOR TOTAL ESTIMADO PARA REGISTRO DE PREÇOS</td><td>3.433.511,60</td><td>4.084.511,98</td><td></td><td>3.994.464,00</td><td>16.281.458,00</td><td></td><td></td><td>2.623.247,50</td></tr>
<tr><td colspan="11">DATA DO ORÇAMENTO ESTIMADO</td><td>29/05/2026</td></tr>
</table>
</td></tr>
</table>

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

	Memória de cálculo: ➢ Informar preços unitários referenciais, memórias de cálculo e documentos que lhe dão suporte. 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: ( ) **Sim - Justificativa técnica e econômica 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. (x) Não - Justificativa: 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. 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. 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

	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. 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. 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. 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.

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

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

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. 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.
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 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: 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. 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. 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

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.

Considerando tratar-se de contratação a ser realizada por meio do Sistema de Registro de Preços, com critério de julgamento de menor preço por grupo de itens, cabe esclarecer que todos os itens da contratação possuem relação de **interdependência técnica e operacional, sendo o item 1 do objeto** (Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos) **o componente principal da solução,** e os demais itens (2 a 8), componentes complementares e acessórios que não podem ser utilizados sem a contratação do primeiro item.

Diante disso, foi previsto que na hipótese de serem celebrados contratos posteriores para qualquer item ou serviço diverso do Item 1, a vigência desses contratos se findará na mesma data de encerramento do contrato do Item 1.

Portanto, o item 1 do objeto deverá ser adquirido na primeira contratação da ARP, podendo ou não ser acompanhado dos demais itens complementares.

Diante do exposto, entende-se que a contratação de item em separado a partir da segunda contratação durante a vigência da ata de registro de preços, não se caracteriza como “item isolado”, previsto na alínea “b” do inciso III do § 1º do Art. 90 da Portaria TRT4 Nº 1.737/2023, pois tal componente somente poderá ser adquirido se o item 1 estiver contratado.

Sugere-se, portanto, que para a compra de item em separado, durante a vigência da ata de registro de preços, cujo preço registrado não representar o melhor lance válido obtido na disputa, seja analisada a totalidade das contratações já realizadas e as proporções de seus quantitativos, a fim de afastar a possibilidade de prejuízo ao erário e eventual jogo de planilhas.

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

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.
(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	

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

( ) 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.

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

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

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		
( ) 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.

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

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.) A transferência de conhecimento se dará por meio do acompanhamento das atividades de instalação e implantação; e na realização do treinamento.
( ) 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.

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

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 ( ) Não	Justificativa: 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 CARLOS COSTA JORDÃO Integrante Demandante	*Documento assinado digitalmente* MAURÍCIO ANTONIOLI SCHMITZ Integrante Técnico
Documento assinado digitalmente GEOVANE DUTRA DE SOUZA Integrante Administrativo da Secretaria de Administração	*Documento assinado digitalmente* ALBERTO DANIEL MÜLLER 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

			Quantidade total para registro																TOTAL
Item	Descrição	Unidade	TRT1	TRT3	TRT4	TRT5	TRT6	TRT7	TRT9	TRT10	TRT11	TRT14	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	2.700	2.000	1.600	1.500	2.700	1.500	1.500	2.000	1.000	6.000	61.500
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	3.200	1.200	1.300	1.100	2.700	1.300	1.300	2.000	900	5.000	54.850
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	36.000	25.200	13.500	30.000	25.200	14.400	60.000	748.300
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	400	450	25	100	150	15	1.000	9.590
5	Serviço de treinamento na solução proposta	Serviço único, por turma de treinamento	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	3	21
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	17
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	17
8		Serviço para 1000 ativos adicionais monitorados por mês	5	5	5	5	2	1	4	1	0	0	0	1	0	0	0	0	4	33

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

SECRETARIA DE ADMINISTRAÇÃO
GOVERNANÇA DE CONTRATAÇÕES

MAPA DE RISCOS | CONTRATAÇÕES

1. OBJETO:	Solução integrada de Detecção e Resposta Estendidas a ataques cibernéticos (XDR) e Detecção e Resposta a Ameaças de Identidade (ITDR)
Link deste mapa:	Formulário	Mapa de Riscos
Última Atualização:	Depois do Termo de Referência

2. IDENTIFICAÇÃO DOS RISCOS				3. ANÁLISE E AVALIAÇÃO DOS RISCOS										4. TRATAMENTO DOS RISCOS						5. MONITORAMENTO DOS RISCOS		
ETAPA	EVENTO	CAUSA	CONSEQUÊNCIA	PROBABILIDADE (P)		IMPACTO (I)		PxI	NÍVEL DE RISCO INERENTE (NRI)	CONTROLES EXISTENTES	AVALIAÇÃO DA EFICÁCIA DOS CONTROLES		NRI x FEC	NÍVEL DE RISCO RESIDUAL (NRR)	RESPOSTA AO RISCO	JUSTIFICATIVA (apenas para os casos em que a resposta não seja compatível com o nível de risco)	AÇÃO PREVENTIVA	RESPONSÁVEL	AÇÃO DE CONTINGÊNCIA	RESPONSÁVEL	STATUS	OCORREU	DESCRIÇÃO DAS MEDIDAS ADOTADAS
Planejamento da Contratação	Atraso no encaminhamento da contratação	Atraso na realização do Estudo Técnico Preliminar, na pesquisa de preços ou na elaboração do Termo de Referência e demais documentos da contratação	Descumprimento do cronograma de contratações e não contratação da solução	Alta	6	Muito relevante	8	48	Extremo	Plano de Contratações de TIC	Satisfatório	0,4	19	Médio	Aceitar		Iniciar o Estudo Técnico Preliminar no prazo previsto no Plano de Contratações de TIC; Encaminhar o processo de contratação no prazo previsto no Plano de Contratações de TIC.	Equipe de Planejamento da Contratação	Monitorar junto a CLC o andamento da contratação na fase de seleção do fornecedor.	Equipe de Planejamento da Contratação	Fechado	Sim	
Planejamento da Contratação	Divergência entre os preços de referência e aqueles praticados no mercado	Pesquisa de Preços inadequada	Atraso na contratação; Sobrepreço ou subpreço.	Baixa	2	Muito relevante	8	16	Médio	Guia de Pesquisa de Preços do TRT4	Satisfatório	0,4	6	Baixo	Aceitar		Elaboração de pesquisa de preços seguindo as diretrizes do Guia de Pesquisa de Preços do TRT4.	Equipe de Planejamento da Contratação	Ajuste na pesquisa de preços e republicação do Edital. Anulação da licitação, rescisão contratual e realização de nova contratação.	Equipe de Planejamento da Contratação	Aberto		
Seleção do Fornecedor	Atraso na contratação	Atraso no planejamento da contratação ou atraso na tramitação da licitação	Descumprimento do cronograma de contratações e não contratação da solução	Alta	6	Muito relevante	8	48	Extremo	Plano de Contratações Anual	Satisfatório	0,4	19	Médio	Aceitar		Monitorar os prazos da contratação na fase de seleção do fornecedor; Agilizar as análises de propostas e eventuais recursos.	Equipe de Planejamento da Contratação	Verificar a necessidade de prorrogação emergencial do contrato atual	Equipe de Planejamento da Contratação	Aberto		
Seleção do Fornecedor	Licitação deserta ou fracassada	Inconsistência na especificação dos requisitos da contratação ou na pesquisa de preços em relação ao mercado	Atraso na contratação	Baixa	2	Muito relevante	8	16	Médio	Estudo Técnico Preliminar; Guia de Pesquisa de Preços do TRT4	Satisfatório	0,4	6	Baixo	Aceitar		Realizar o Estudo Técnico Preliminar detalhado das especificações e preços de mercado; Definir critérios razoáveis de aceitabilidade do produto/serviço; Encaminhar a contratação com tempo hábil para repetição; Consulta à fornecedores do mercado para análise prévia dos requisitos da contratação; Elaboração da pesquisa de preços de acordo com o Guia de Pesquisa de Preços do TRT4.	Equipe de Planejamento da Contratação	Repetir a licitação, sanando eventuais falhas que possam ter criado obstáculos na seleção dos fornecedores.	Equipe de Planejamento da Contratação	Aberto		
Seleção do Fornecedor	Contratação de empresa inexperiente para prestação do objeto	Inconsistência na especificação dos requisitos de seleção do fornecedor	Baixa qualidade na prestação dos serviços; Dano ao erário; Suscetibilidade a ataques cibernéticos	Baixa	2	Muito relevante	8	16	Médio	Estudo Técnico Preliminar	Satisfatório	0,4	6	Baixo	Aceitar		Exigir requisitos de qualificação técnica que demonstrem a experiência da empresa na prestação de objeto compatível com o da contratação.	Equipe de Planejamento da Contratação	Encaminhar processo para aplicação de sanções previstas para quaisquer descumprimentos do contrato.	Equipe de Gestão e Fiscalização do Contrato	Aberto		
Seleção do Fornecedor	Contratação de produto de baixa qualidade	Inconsistência na especificação dos requisitos do objeto	Baixa qualidade na prestação dos serviços; Dano ao erário; Suscetibilidade a ataques cibernéticos	Baixa	2	Muito relevante	8	16	Médio	Estudo Técnico Preliminar	Satisfatório	0,4	6	Baixo	Aceitar		Realizar o estudo técnico preliminar detalhado dos requisitos e especificações de mercado.	Equipe de Planejamento da Contratação	Encaminhar processo para aplicação de sanções cabíveis. Realizar outra contratação.	Equipe de Gestão e Fiscalização do Contrato e Equipe de Planejamento da Contratação	Aberto		
Gestão Contratual	Não atendimento dos prazos e condições contratados	Não cumprimentos das obrigações contratuais pela contratada	Baixa qualidade na prestação dos serviços; Indisponibilidade dos serviços e produtos vinculados ao objeto.	Baixa	2	Muito relevante	8	16	Médio	Estabelecimento de Sanções Administrativas	Mediano	0,6	10	Baixo	Aceitar		Prever sanções administrativas pelo descumprimento das obrigações contratuais. Monitorar o cumprimento dos prazos de atendimento, alertando a contratada sobre a possível aplicação de sanções em caso de não cumprimento.	Equipe de Planejamento da Contratação e Equipe de Gestão e Fiscalização do Contrato	Acionar a garantia contratual, se aplicável; Encaminhar processo para aplicação de sanções cabíveis.	Equipe de Gestão e Fiscalização do Contrato	Aberto		
Gestão Contratual	Equipe técnica do TRT permanece dependente do fornecedor para operações básicas	Treinamento ministrado de forma genérica ou material didático de baixa qualidade	Incapacidade da equipe interna de realizar ajustes finos ou interpretar alertas críticos de segurança	Baixa	2	Relevante	5	10	Médio	Especificação robusta; Fiscalização adequada; Solicitação de realização de novo treinamento.	Satisfatório	0,4	4	Baixo	Aceitar		Prever sanções administrativas pelo descumprimento das obrigações contratuais.	Equipe de Planejamento da Contratação e Equipe de Gestão e Fiscalização do Contrato	Exigir a repetição do treinamento de acordo com os requisitos da contratação como condição para pagamento.	Equipe de Gestão e Fiscalização do Contrato	Aberto		

Acesse aqui o Tutorial | Preenchimento Mapa de Riscos em Contratações

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

CARLOS COSTA JORDÃO
23/10/2026 18:44

MAURICIO ANTONIOLI SCHMITZ
23/10/2026 18:50

GEOVANE DUTRA DE SOUZA
23/10/2026 18:56

ALBERTO DANIEL MULLER
23/10/2026 21:41

CAROLINE ROCHA MOLINA
24/10/2026 12:36

PROAD n. 6891/2026 DOC 45. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.KGST.QVTZV:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

MINUTA

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO
COORDENADORIA DE LICITAÇÕES E CONTRATOS
PROAD 6891/2026

ANEXO II DO EDITAL

ATA DE REGISTRO DE PREÇOS Nº @/202@

Pregão Eletrônico nº 27/2026
COMPRAS.GOV Nº 316/2026

O **TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO**, com sede na Av. Praia de Belas, n°. 1100, em Porto Alegre/RS, inscrito no C.N.P.J.M.F. sob o nº 02.520.619/0001-52, neste ato representado pelo Exmo. Presidente, Desembargador **ALEXANDRE CORRÊA DA CRUZ** e a empresa listada abaixo, classificada em **primeiro** lugar no **Pregão Eletrônico nº 27/2026**, conforme homologação do resultado divulgado no Portal Nacional de Contratações Públicas (PNCP) no dia @**, resolvem REGISTRAR OS PREÇOS**, nos termos da Lei nº 14.133/2021, Decreto nº 11.462/2023 e das demais disposições que seguem:

DO OBJETO

1. O objeto desta Ata é o registro de preços para eventual **aquisição de solução integrada de detecção e resposta estendidas a ataques cibernéticos (XDR) e detecção e resposta a ameaças de identidade (ITDR)**, visando atender às necessidades dos Tribunais, nas quantidades estabelecidas abaixo e em conformidade com as condições e especificações técnicas constantes no Anexo I do Edital do Pregão Eletrônico nº 27/2026, e seus anexos.

Grupo	Item	Descrição	Unidade	Órgão	Quant. Total a registrado por órgão	Quant. total para registro	Preço Unitário (R$)	Preço Total (R$)
1	1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos (XDR). **Fabricante/Modelo:** —	Ativo monitorado	**TRT1**	7.000	**61.500**		
				TRT3	6.500			
				TRT4	6.500			
				TRT5	6.500			
				TRT6	4.000			
				TRT7	2.500			
				TRT9	6.000			

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

				TRT10	2.700			
				TRT11	2.000			
				TRT14	1.600			
				TRT16	1.500			
				TRT18	2.700			
				TRT19	1.500			
				TRT20	1.500			
				TRT21	2.000			
				TRT22	1.000			
				TST	6.000			
	2	Subscrição do Módulo de Detecção e Resposta a Ameaças de Identidade (ITDR).	Usuários ativos	**TRT1**	6.000	**54.850**		
				TRT3	9.450			
				TRT4	4.500			
				TRT5	5.000			
				TRT6	2.500			
				TRT7	2.400			
				TRT9	5.000			
				TRT10	3.200			
				TRT11	1.200			
				TRT14	1.300			
				TRT16	1.100			
				TRT18	2.700			
				TRT19	1.300			
				TRT20	1.300			
				TRT21	2.000			
				TRT22	900			
				TST	5.000			
	3	Módulo de solução Agêntica para resposta, orquestração e triagem de eventos e incidentes.	Tokens	**TRT1**	72.000	**748.300**		
				TRT3	72.000			
				TRT4	72.000			
				TRT5	72.000			

MINUTA

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

				TRT6	36.000			
				TRT7	36.000			
				TRT9	72.000			
				TRT10	36.000			
				TRT11	40.000			
				TRT14	36.000			
				TRT16	36.000			
				TRT18	25.200			
				TRT19	13.500			
				TRT20	30.000			
				TRT21	25.200			
				TRT22	14.400			
				TST	60.000			
	4	Ingestão de logs externos.	Franquia de Gigabyte por dia	**TRT1**	1.000	**9.590**		
				TRT3	1.000			
				TRT4	1.000			
				TRT5	1.000			
				TRT6	150			
				TRT7	500			
				TRT9	1.000			
				TRT10	1.000			
				TRT11	400			
				TRT14	400			
				TRT16	400			
				TRT18	450			
				TRT19	25			
				TRT20	100			
				TRT21	150			
				TRT22	15			
				TST	1.000			
	5	Serviço de treinamento na	Serviço único, por	**TRT1**	2	**21**		

MINUTA

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

		solução proposta.	turma de treinamento	**TRT3**	2			
				TRT4	1			
				TRT5	1			
				TRT6	1			
				TRT7	1			
				TRT9	1			
				TRT10	1			
				TRT11	1			
				TRT14	1			
				TRT16	1			
				TRT18	1			
				TRT19	1			
				TRT20	1			
				TRT21	1			
				TRT22	1			
				TST	3			
	6	Serviço de implantação da solução proposta	Serviço único por contratante	**TRT1**	1	**17**		
				TRT3	1			
				TRT4	1			
				TRT5	1			
				TRT6	1			
				TRT7	1			
				TRT9	1			
				TRT10	1			
				TRT11	1			
				TRT14	1			
				TRT16	1			
				TRT18	1			
				TRT19	1			
				TRT20	1			
				TRT21	1			

MINUTA

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

				TRT22	1			
				TST	1			
	7	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Serviço fixo para 2000 ativos monitorados por mês	**TRT1**	36	**612***		
				TRT3	36			
				TRT4	36			
				TRT5	36			
				TRT6	36			
				TRT7	36			
				TRT9	36			
				TRT10	36			
				TRT11	36			
				TRT14	36			
				TRT16	36			
				TRT18	36			
				TRT19	36			
				TRT20	36			
				TRT21	36			
				TRT22	36			
				TST	36			
	8	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Serviço para 1000 ativos adicionais monitorados por mês	**TRT1**	180	**1.188***		
				TRT3	180			
				TRT4	180			
				TRT5	180			
				TRT6	72			
				TRT7	36			
				TRT9	144			
				TRT10	36			
				TRT18	36			
				TST	144			
PREÇO GLOBAL DO GRUPO 1 REGISTRADO PARA 36 MESES (R$)								

* ***A quantidade dos itens 7 e 8 decorrem da multiplicação da quantidade para registro de preços de cada Regional participante por 36 meses previsto para a contratação.***

MINUTA

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

Empresa	
C.N.P.J.M.F.	
Endereço	
Telefone	
E-mail	
Representante	
C.P.F	

1.1. A contratação com a detentora do(s) preço(s) registrado(s) será formalizada por meio de instrumento contratual, de acordo com o previsto no Edital Pregão Eletrônico nº 27/2026.

1.2. As demais condições de fornecimento constam no Edital Pregão Eletrônico nº 27/2026, e seus Anexos, que passam a fazer parte da presente Ata, independentemente de transcrição.

1.3. A presente ata de registro de preços **não** poderá ser utilizada por órgãos ou entidades não participantes, considerando o critério de julgamento adotado, pelo menor preço global, a fim de afastar a possibilidade de prejuízo ao erário, em consonância com o entendimento proferido pelo Acórdão nº 1.347/2018 do Plenário do TCU.

DOS ÓRGÃOS PARTICIPANTES

2. O órgão gerenciador da presente Ata será o Tribunal Regional do Trabalho da 4ª Região.

2.1. Figuram como participantes os seguintes órgãos:

a) Tribunal Regional do Trabalho da 1ª Região;
b) Tribunal Regional do Trabalho da 3ª Região;
c) Tribunal Regional do Trabalho da 5ª Região;
d) Tribunal Regional do Trabalho da 6ª Região;
e) Tribunal Regional do Trabalho da 7ª Região;
f) Tribunal Regional do Trabalho da 9ª Região;
g) Tribunal Regional do Trabalho da 10ª Região;
h) Tribunal Regional do Trabalho da 11ª Região;
i) Tribunal Regional do Trabalho da 14ª Região;
j) Tribunal Regional do Trabalho da 16ª Região;
k) Tribunal Regional do Trabalho da 18ª Região;
l) Tribunal Regional do Trabalho da 19ª Região;
m) Tribunal Regional do Trabalho da 20ª Região;
n) Tribunal Regional do Trabalho da 21ª Região;
o) Tribunal Regional do Trabalho da 22ª Região;
p) Tribunal Superior do Trabalho.

DA VIGÊNCIA DA ATA DE REGISTRO DE PREÇOS

3. O prazo de vigência da ata de registro de preços será de **01 (um) ano, contado do primeiro dia útil subsequente à data de divulgação no PNCP**, e poderá ser prorrogado **por igual período**, desde que comprovado o preço vantajoso, nos termos do art. 84 da Lei nº 14.133/2021 e do art. 22 do Decreto nº 11.462/2023.

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

3.1. A prorrogação do prazo de vigência da ata de registro de preços implicará, nos termos do art. 96, § 3º, inciso II, da Portaria TRT4 nº 1.737/2023, a renovação, tão-somente, dos quantitativos remanescentes do primeiro ano de vigência (saldos dos itens).

3.1.1. No caso de prorrogação da vigência da ata, os preços registrados poderão ser reajustados, mediante solicitação do fornecedor, com base no Índice de Custo da Tecnologia da Informação (ICTI), estabelecido no guia da Resolução CNJ nº 468/2022, com data base vinculada à elaboração do orçamento estimado (**22/10/2026**), aplicando-se sua variação a partir da referida data, na forma do item 11.9 do Edital do Pregão Eletrônico nº 27/2026.

DA GESTÃO E DA FISCALIZAÇÃO

4. A gestão e a fiscalização das contratações decorrentes deste instrumento serão exercidas pelos seguintes servidores:

Integrante	Titular	Substituto	Unidade
Gestor:	Carlos Costa Jordão	Charles Ferreira Falcao	Coordenadoria de Segurança da Informação e Proteção de Dados
Fiscal Técnico:	Maurício Antonioli Schmitz	Carlos Augusto Nantes de Castilho Rivilino	Coordenadoria de Segurança da Informação e Proteção de Dados
Fiscal Demandante:	Rodrigo Zarth	Mateus Both	Coordenadoria de Segurança da Informação e Proteção de Dados
Fiscal Administrativo:	Alberto Daniel Müller	Ricardo Krause Kurylenko	Coordenadoria de Gestão e Apoio à Governança de TIC

DO CADASTRO RESERVA

5. O registro dos licitantes interessados em aderir ao cadastro de reserva e que aceitaram cotar os bens ou serviços com preços iguais ao do licitante vencedor ou interessados em aderir ao cadastro de reserva com a manutenção dos preços de sua proposta original, na sequência da classificação do certame, é o seguinte:

Grupo / Item	CNPJ	Razão Social	Pelo preço do adjudicatário	Pelo preço da sua proposta original
Não houve cadastro reserva				

DAS DISPOSIÇÕES GERAIS

6. O inteiro teor da presente Ata de Registro de Preços será publicado no PNCP, conforme disposto no artigo 174, § 2º, IV, da Lei nº 14.133/2021 e no artigo 18, § 4º, do Decreto nº 11.462/2023, bem como divulgado no site *www.trt4.jus.br.*

7. Integram esta Ata, independentemente de transcrição, o Edital e Anexos do Pregão Eletrônico nº 27/2026.

8. Fica eleito o Foro da Justiça Federal, Seção Judiciária do Rio Grande do Sul, Subseção Judiciária de Porto Alegre, com esteio no artigo 109, inciso I, da Constituição Federal, para

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

dirimir quaisquer dúvidas decorrentes da presente ata, renunciando a qualquer outro, por mais privilegiado que seja.

E, por estarem justas e acordadas, as partes assinam eletrônica/digitalmente o presente instrumento, considerando-se efetivamente formalizado a partir da data da última assinatura.

Assinantes:

Pelo Tribunal:

Documento assinado digitalmente
ALEXANDRE CORRÊA DA CRUZ
Presidente do TRT da 4ª Região

Pela detentora do(s) preço(s) registrado(s):

Documento assinado digitalmente
@@@@@@@@@@@@@@@
CPF nº @@@@@@@
(Nome da vencedora)

MINUTA

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

TRT da 4ª Região
Pregão Eletrônico nº 27/2026
COMPRAS.GOV.BR Nº 316/2026

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

ANEXO III DO EDITAL

FORMULÁRIO PARA MANIFESTAÇÃO DE INTERESSE NO CADASTRO DE RESERVA DE ATA DE REGISTRO DE PREÇOS

PROCEDIMENTO LICITATÓRIO	
Pregão Eletrônico TRT4 n	
Objeto	
Grupo(s)/Item(ns)	

DADOS DA EMPRESA	
Razão Social	
CNPJ	
Endereço	
Representante Legal/Contato	
Telefone	
E-mail	

	Solicito o registro da empresa no cadastro de reserva da Ata de Registro e aceito fornecer o objeto por preço(s) igual(is) ao(s) do adjudicatário, observada a classificação na licitação, conforme previsto no art. 18 do Decreto 11.462/2023.
OU	
	Solicito o registro na empresa no cadastro de reserva da Ata de Registro e aceito fornecer o objeto pelo preço proposto no âmbito do procedimento licitatório.

Local e data	
Assinatura	

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO
COORDENADORIA DE LICITAÇÕES E CONTRATOS

ANEXO IV DO EDITAL - MODELO DE PROPOSTA

Grupo	Item	Descrição	Unidade	Quantidade total a registrar	Preço Unitário (R$)	Preço Total (R$)
1	1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos (XDR). **Fabricante/Modelo: _____**	Ativo monitorado	**61.500**		
	2	Subscrição do Módulo de Detecção e Resposta a Ameaças de Identidade (ITDR).	Usuários ativos	**54.850**		
	3	Módulo de solução Agêntica para resposta, orquestração e triagem de eventos e incidentes	Tokens	**748.300**		
	4	Ingestão de logs externos	Franquia de Gigabyte por dia	**9.590**		
	5	Serviço de treinamento na solução proposta	Serviço único, por turma de treinamento	**21**		
	6	Serviço de implantação da solução proposta	Serviço único por contratante	**17**		
	7	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Serviço fixo para 2000 ativos monitorados por mês	**612***		
	8	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Serviço para 1000 ativos adicionais monitorados por mês	**1.188***		
PREÇO GLOBAL DO GRUPO 1 PARA 36 MESES (R$)						

* ***A quantidade dos itens 7 e 8 decorrem da multiplicação da quantidade para registro de preços de cada Regional participante por 36 meses previsto para a contratação.***

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

DADOS DA LICITANTE:

Razão social:_____

CNPJ:_____

Endereço (*CEP, cidade, estado*):_____

E-mail:_____

Telefone:_____

Falar com:_____

Assinatura do representante da empresa

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

CONTRATO TRT4 Nº ___/202@

CONTRATO DE AQUISIÇÃO DE **SOLUÇÃO INTEGRADA DE DETECÇÃO E RESPOSTA ESTENDIDAS A ATAQUES CIBERNÉTICOS (XDR) E DETECÇÃO E RESPOSTA A AMEAÇAS DE IDENTIDADE (ITDR),** QUE ENTRE SI FAZEM O **TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO** E _____**.**

O **TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO**, inscrito no C.N.P.J.M.F. sob o nº 02.520.619/0001-52, com sede na Av. Praia de Belas, n° 1.100, em Porto Alegre/RS, doravante denominado CONTRATANTE, neste ato representado pelo Exmo. Presidente, Desembargador **ALEXANDRE CORRÊA DA CRUZ**, e, de outro lado,_____, inscrita no C.N.P.J.M.F. sob o nº _____, com sede na _____, doravante denominada CONTRATADA, neste ato representada por _____, inscrito no C.P.F.M.F. sob o nº _____, ajustam entre si este contrato, o qual reger-se-á pelas condições adiante discriminadas.

DO OBJETO

CLÁUSULA PRIMEIRA. O presente instrumento tem por objeto a 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, sob o regime de empreitada por preço unitário, em decorrência da Ata de Registro de Preços nº @/202@ (oriunda do Pregão Eletrônico nº 27/2026), conforme especificações técnicas constantes no Anexo I - Termo de Referência, e seus anexos, de referido Pregão, no quantitativo que segue:

Item	Descrição	Unidade	Quantidade
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos (XDR).	Ativo monitorado	@
2	Subscrição do Módulo de Detecção e Resposta a Ameaças de Identidade (ITDR).	Usuários ativos	@
3	Módulo de solução Agêntica para resposta, orquestração e triagem de eventos e incidentes	Tokens	@
4	Ingestão de logs externos	Franquia de Gigabyte por dia	@
5	Serviço de treinamento na solução proposta	Serviço único, por turma de treinamento	@
6	Serviço de implantação da solução proposta	Serviço único por contratante	@

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: 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	@
8	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Serviço para 1000 ativos adicionais monitorados por mês	@

Parágrafo Primeiro. 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.

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

Parágrafo Terceiro. 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.

Parágrafo Quarto. As especificações técnicas constam no **Anexo I** deste instrumento.

DA VIGÊNCIA E DOS PRAZOS

CLÁUSULA SEGUNDA. A vigência deste contrato tem início com sua assinatura e encerra-se no prazo de **36 meses** contados do início da prestação dos serviços (data do recebimento definitivo do objeto), podendo ser prorrogado, na forma dos artigos 106 e 107 da Lei n° 14.133/2021.

Parágrafo Primeiro. A prorrogação de que trata esta Cláusula é condicionada ao ateste, pela autoridade competente, de que as condições e os preços permanecem vantajosos para a Administração, permitida a negociação com o contratado.

Parágrafo Segundo. O contrato pode ser extinto antes do prazo nele fixado, sem ônus para o CONTRATANTE, quando este não dispuser de créditos orçamentários para sua continuidade ou quando entender que o contrato não mais lhe oferece vantagem, na forma do artigo 106, inciso III e § 1º da Lei nº 14.133/2021 e dos §§ 7º e 8º do artigo 112 da Portaria GP.TRT4 nº 1.737/2023.

Parágrafo Terceiro. A prorrogação do prazo de vigência deste instrumento implica a renovação dos quantitativos contratados nos itens @, @, @ e @ do *caput* da Cláusula Primeira.

CLÁUSULA SEGUNDA. A vigência deste contrato tem início com sua assinatura e encerra-se em @@, podendo ser prorrogado, na forma dos artigos 106 e 107 da Lei n° 14.133/2021. *(obs: Usar esta cláusula na hipótese de serem celebrados contratos oriundos da Ata*

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

de Registro de Preços, posteriores para qualquer item ou serviço diverso da primeira contratação do Item 1, quando a vigência desses contratos se findarão no mesmo dia de encerramento do contrato que originou a primeira compra do Item 1)

CLÁUSULA TERCEIRA. A disponibilização das subscrições e serviços (itens 1, 2, 3 e 4), e a execução completa da Implantação da Solução (item 6) devem ocorrer em até **60 dias** a contar da assinatura do contrato.

CLÁUSULA QUARTA. A vigência das subscrições dos itens 1 e 2 será de **36 meses**, contados a partir da data de emissão do Termo de Recebimento Definitivo do objeto, após a conclusão da implantação e a entrada da solução em produção, em pleno funcionamento, de acordo com as especificações do fabricante da solução e em conformidade com os requisitos da contratação.

Parágrafo Primeiro. As subscrições poderão ser disponibilizadas de forma anual, hipótese em que cada disponibilização deverá assegurar o período de vigência correspondente, observadas as condições estabelecidas na contratação.

Parágrafo Segundo. Durante a etapa de implantação, é facultado à CONTRATADA o uso de licenças temporárias (trial), visando não onerá-la antes da efetiva entrada em produção, evitando o cômputo precoce do prazo de vigência das subscrições, desde que tais licenças não apresentem limitações ao uso inicial da solução.

Parágrafo Terceiro. Eventuais atrasos na implantação motivados pelo CONTRATANTE não postergarão o início da vigência das subscrições já adquiridas e disponibilizadas, desde que estas estejam efetivamente disponíveis para uso, conforme as condições estabelecidas na contratação.

Parágrafo Quarto. As subscrições e os serviços correspondentes aos itens 2, 3, 4, 7 e 8, quando contratados conjuntamente com o item 1 na primeira contratação, observarão o mesmo marco temporal de referência e a mesma data de encerramento estabelecida para a vigência inicial do item 1 (36 meses), respeitadas as condições específicas de execução de cada item.

Parágrafo Quinto. Na hipótese prevista no parágrafo anterior, o valor dos itens será calculado proporcionalmente ao período efetivo de sua vigência, com base no preço unitário contratado.

Parágrafo Sexto. O serviço gerenciado (itens 7 e 8) terá início imediatamente após o recebimento definitivo do objeto e possuirá vigência de **36 meses**.

Parágrafo Sétimo. O serviço de Treinamento (item 5), caracterizado como serviço contratado por escopo, deverá ser integralmente executado e concluído no prazo máximo de 180 (cento e oitenta) dias, contados da assinatura do primeiro contrato referente ao item 1, observadas as condições estabelecidas no Termo de Referência.

DA GARANTIA E DO SUPORTE TÉCNICO

Da Garantia

CLÁUSULA QUINTA. A solução como um todo, englobando software, módulos, coletores, sensores, integrações e serviços associados, deverá contar com garantia e suporte integrais prestados pela CONTRATADA com respaldo do fabricante (Garantia Compreensiva), durante todo o período de vigência contratual.

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

Parágrafo Primeiro. A garantia deve cobrir a correção de quaisquer bugs, falhas de funcionamento, erros de código, atualizações de assinaturas, atualizações de versão (major e minor releases), patches e hotfixes, sem nenhum custo adicional para o CONTRATANTE.

Parágrafo Segundo. A assistência técnica em garantia deve assegurar o fornecimento de acesso irrestrito (24 horas por dia, 7 dias da semana) do CONTRATANTE à área de suporte do fabricante, especialmente ao endereço eletrônico (web site) e a toda a documentação técnica pertinente (guias de instalação e configuração atualizados, FAQ's, bases de conhecimento e bases de soluções, com pesquisa efetuada através de ferramentas de busca).

Do Serviço de Suporte Técnico

CLÁUSULA SEXTA. O suporte técnico inclui todos os serviços técnicos necessários para assegurar o pleno funcionamento da solução conforme as especificações do objeto, sem qualquer custo adicional para o CONTRATANTE.

Parágrafo Primeiro. Os serviços de suporte deverão ser corretivos, proativos e consultivos, envolvendo atividades como: auxílio na configuração de políticas e administração da solução; garantia do fornecimento e da instalação de novas versões, patches e hotfixes (tanto de componentes on premises quanto em nuvem); análise de dúvidas sobre melhores práticas de configuração, entre outros.

Parágrafo Segundo. A abertura de chamados pelo CONTRATANTE deve poder ser efetuada:
I - Pela plataforma web, em sistema de atendimento da CONTRATADA;
II - Pelo envio de mensagem de correio eletrônico;
II - Por meio do módulo de gestão de incidentes de segurança da solução ofertada;
IV - Por telefone.

Parágrafo Terceiro. O atendimento aos chamados deve estar disponível em regime 24x7x365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias ao ano).

Parágrafo Quarto. Não poderá haver qualquer restrição de quantidade de abertura de chamados no suporte técnico.

Parágrafo Quinto. Todas as comunicações e documentação relacionada aos atendimento de chamados deverão ser realizadas ou disponibilizadas em Português.

Parágrafo Sexto. Para a aferição e a avaliação dos níveis de serviço, a CONTRATADA deverá apresentar mensalmente à fiscalização do contrato um relatório gerencial de serviços, até o quinto dia útil do mês subsequente ao da prestação do serviço. O relatório deverá conter, entre outras informações, a medição dos indicadores/metas de níveis de serviço, recomendações técnicas, e demais informações relevantes para a gestão contratual.

Parágrafo Sétimo. Os prazos de solução dos chamados deverão atender aos seguintes critérios:

Severidade	Classificação	Prazo de Solução

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

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

A0 - Crítica	Chamados referentes a situações de emergência ou problema crítico, caracterizados pela existência de ambiente paralisado.	2 horas a contar da abertura do chamado
A1 - Alta	Chamados associados a situações de alto impacto, incluindo os casos de degradação severa de desempenho.	6 horas a contar da abertura do chamado
A2 - Média	Chamados referentes a situações de baixo impacto ou para aqueles problemas que se apresentem de forma intermitente.	2 dias úteis a contar da abertura do chamado
A3 - Baixa	Chamados com objetivo de sanar dúvidas quanto ao uso ou à implementação do produto, dúvidas, problemas na utilização, esclarecimentos da documentação, sugestões, impacto mínimo para os usuários.	5 dias úteis a contar do próximo dia útil da abertura do chamado
A4 - Pesquisa	Chamados com objetivo de melhorar a ferramenta, implantar novas funcionalidades ou configurações que demandem tempo e planejamento	10 dias úteis a contar do próximo dia útil da abertura do chamado

Do Serviço de Suporte a Incidentes

CLÁUSULA SÉTIMA. O serviço de operação e gestão da solução deverá classificar os incidentes de segurança conforme a seguir:

Prioridade	Descrição do impacto	Peso
P0 - Crítico	Alertas de invasão de ativos classificados como críticos; Comprometimento em massa de dados sensíveis; Comprometimento de credenciais administrativas; Movimentação lateral no ambiente;	**4**
P1 - Alto	Degradação de ativos classificados como críticos; Comprometimento parcial de dados sensíveis; Comprometimento de credenciais não administrativas;	**3**
P2 - Médio	Comprometimento ou degradação de ativos classificados como não críticos; Comprometimento de dados não sensíveis;	**2**
P3 - Baixo	Comprometimento ou degradação de ativos classificados como de baixa relevância. Representa uma oportunidade de melhoria no ambiente.	**1**

**'Dado pessoal sensível' terá o significado da LGPD. A criticidade da informação observará adicionalmente a política de segurança da informação do CONTRATANTE.*

Parágrafo Primeiro. Os seguintes Indicadores de Nível de Serviço de incidentes de segurança serão considerados:

Prioridade	Tempo máximo de percepção do incidente de segurança (MTTD)	Tempo máximo de resposta ao incidente de segurança	Tempo máximo de contenção (MTTR)

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

P0 - Crítico	15 min	35 min	90 min
P1 - Alto	30 min	90 min	150 min
P2 - Médio	2 horas	6 horas	10 horas
P3 - Baixo	4 horas	12 horas	24 horas

Parágrafo Segundo. Tempo máximo de percepção do incidente de segurança: é o limite contratual (SLA) que estabelece o tempo máximo aceitável para que a plataforma ou serviço correlacione a telemetria e identifique uma atividade maliciosa, medindo o intervalo entre a primeira evidência técnica do ataque no ambiente e a geração do alerta qualificado para os analistas. Essa métrica atua como o teto para o tempo de detecção (MTTD), visando minimizar a permanência velada do atacante na rede (dwell time) e servindo como parâmetro objetivo de conformidade e aplicação de penalidades ao fornecedor.

Parágrafo Terceiro. Tempo máximo de resposta ao incidente de segurança: é o limite contratual de tempo (SLA) exigido para que, a partir do momento em que uma ameaça é detectada e qualificada, sejam executadas as medidas operacionais e automatizadas de contenção e mitigação interrompendo ativamente a progressão do ataque e minimizando o impacto no ambiente antes que a remediação definitiva seja concluída.

Parágrafo Quarto. Tempo Máximo de Contenção: é o limite temporal estabelecido para que a equipe de analistas investigue, realize a triagem e confirme a veracidade de um alerta gerado pela plataforma, medindo o intervalo entre a emissão do alerta e a sua classificação definitiva como um incidente real (verdadeiro positivo) ou um alarme falso (falso positivo).

Parágrafo Quinto. Todos os tempos serão contados a partir do início do incidente de segurança. O tempo de início é medido a partir do momento em que houver registros das atividades maliciosas ou a partir do momento que houver impacto resultante da atividade maliciosa - o que ocorrer primeiro.

Parágrafo Sexto. Os tempos serão aferidos com base nos registros de data e hora do sistema de gestão de incidentes, relacionados aos registros da plataforma, disponibilizados para auditoria.

Parágrafo Sétimo. Quando o atendimento de um incidente depender de providência a cargo do CONTRATANTE, a contagem do tempo para cumprimento do SLA será suspensa durante o período de efetiva dependência dessa providência, sendo retomada a partir de seu atendimento pelo CONTRATANTE.

Parágrafo Oitavo. A suspensão da contagem somente será admitida quando houver dependência objetiva de providência do CONTRATANTE, devidamente registrada pela CONTRATADA, com indicação da ação requerida, da data e hora do acionamento, das evidências correspondentes e da data e hora do atendimento da solicitação pelo CONTRATANTE. Não será admitida a suspensão retroativa da contagem.

Parágrafo Nono. Quando o período de suspensão ultrapassar o dobro do tempo máximo previsto para validação e houver mais de um acionamento do CONTRATANTE para a mesma finalidade, a justificativa para a duração da suspensão deverá ser formalmente registrada e submetida à validação do CONTRATANTE. A suspensão somente será considerada válida se comprovada a efetiva necessidade do tempo utilizado para as validações, não sendo admitida sua utilização indevida para afastar ou reduzir a responsabilidade da CONTRATADA pelo cumprimento dos níveis de serviço estabelecidos.

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

MINUTA

Parágrafo Décimo. Não serão incluídos na contagem de totais os incidentes abertos e fechados de forma automática. Em caso de um incidente fechado de forma automática se mostrar como verdadeiro-positivo, este será tratado como se houvesse descumprimento de SLA.

Parágrafo Décimo Primeiro. O descumprimento de qualquer um dos tempos descritos nos Indicadores de Nível de Serviço será considerado como incidente de segurança não atendido no prazo.

Parágrafo Décimo Segundo. O descumprimento dos níveis descritos implicará em glosa a ser aplicada sobre a parcela total mensal dos itens 7 e 8, conforme tabela a seguir:

I - Periodicidade de medição: Mensal
II - Fórmula: somatória ponderada dos incidentes que descumpriram o SLA dividida pela somatória ponderada de todos os chamados.

III - ICSLA = (QTin / Tin) * 100

IV - ICSLA = Índice de Conformidade de SLA

V - QTin = Quantidade de incidentes de segurança atendidos nos prazos: $\Sigma_{\text{Incidentes com SLA cumprido}}$(P0 * peso P0 + P1 * peso P1 + P2 * peso P2 + P3 * peso P3)

VI - Tin = Total de incidentes de segurança registrado: $\Sigma_{\text{incidentes}}$(P0 * peso P0 + P1 * peso P1 + P2*peso P2 + P3 * peso P3)

VII - Apuração e Glosa:

Faixa	Níveis Alcançados	Glosa
1	ICSLA => 95%	Sem glosa
2	90% <= ICSLA < 95%	5%
3	85% <= ICSLA < 90%	10%
4	ICSLA < 85%	20%

VIII - Todo incidente do tipo P0 e P1 (crítico e alto) deverá ser comunicado por telefone, além do registro no sistema de tíquetes.

IX - Para P0/P1, a CONTRATADA apresentará relatório com linha do tempo, vetor, MITRE ATT&CK quando aplicável, ativos afetados, evidências, causa-raiz/hipóteses, contenção, remediação, impacto, lições, recomendações, responsáveis e prazos.

X - A classificação A0–A4 aplica-se exclusivamente ao suporte técnico. P0–P3 aplica-se aos incidentes de segurança. Em sobreposição, prevalecerá a classificação de incidente de segurança.

DO ÍNDICE DE DISPONIBILIDADE

CLÁUSULA OITAVA. A disponibilidade mensal da solução será apurada com base nos registros da própria plataforma e, quando disponível, em mecanismo independente de

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

monitoramento. A perda de coleta de dados, de telemetria ou de cobertura dos ativos monitorados deverá ser aferida por indicadores próprios.

Parágrafo Primeiro. O índice mensal de disponibilidade da solução deverá ser igual ou superior a 99,8% (noventa e nove inteiros e oito décimos por cento).

Parágrafo Segundo. Caso o índice mensal de disponibilidade seja inferior a **99,8%** (noventa e nove inteiros e oito décimos por cento), será aplicada glosa no percentual correspondente a 10 vezes a diferença entre a disponibilidade medida no mês e a disponibilidade mínima contratada, sobre o valor mensal dos itens 7 e 8.

DO PREÇO

CLÁUSULA NONA. Pela execução do objeto deste contrato, o CONTRATANTE pagará à CONTRATADA o valor total de R$ @@(@@).

Item	Descrição	Unidade	Quant.	Valor Unitário	Pagto	Forma	Valor Total (R$)
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos (XDR) pelo período de 36 meses	Ativo monitorado	@	@	Anual	**3 parcelas de R$:** @.@@	@
2	Subscrição do Módulo de Detecção e Resposta a Ameaças de Identidade (ITDR) pelo período de 36 meses	Usuários ativos	@	@	Anual	**3 parcelas de R$:** @.@@	@
3	Módulo de solução Agêntica para resposta, orquestração e triagem de eventos e incidentes	Tokens	@	@	Mensal	R$: @,@@ por mês (@ meses)	@
4	Ingestão de logs externos	Franquia de Gigabyte por dia	@	@	Anual	**3 parcelas de R$:** @.@@	@
5	Serviço de treinamento na solução proposta	Serviço único, por turma de treinamento	1	@	Único	-	@
6	Serviço de implantação da solução proposta	Serviço único por contratante	1	@	Único	-	@
7	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Serviço fixo para 2000 ativos monitorados por mês	@	@	Mensal	R$: @,@@ por mês (@ meses)	@
8	Serviço de monitoramento, detecção, notificação,	Serviço para 1000 ativos adicionais monitorados	@	@	Mensal	R$: @,@@ por mês	@

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

	investigação e resposta a ataques cibernéticos	por mês				(@ meses)	
Valor total da contratação por 36 meses (**R$**)							@,@@

DO PAGAMENTO

CLÁUSULA DÉCIMA. O pagamento será realizado mediante crédito em conta corrente bancária até o décimo dia útil após a entrega do documento fiscal correspondente ao objeto, devidamente atestado pela fiscalização, conforme critérios de medição e pagamento abaixo, sendo efetuada a retenção na fonte dos tributos e contribuições elencados na legislação em vigor, tais como IR, CSLL, COFINS e PIS/PASEP e, se for o caso, ISS:

Item	Descrição	Forma de Recebimento	Prazo	Forma de pagamento
1	Entrega das subscrições de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Termo de Recebimento Definitivo	60 dias da assinatura do contrato	Pagamento anual após o recebimento definitivo do objeto
2	Entrega das subscrições de Módulo de Detecção e Resposta a Ameaças de Identidade (ITDR)	Termo de Recebimento Definitivo	60 dias da assinatura do contrato	Pagamento anual após o recebimento definitivo do objeto
3	Módulo de solução Agêntica para resposta, orquestração e triagem de eventos e incidentes	Ateste na nota fiscal	mensal	Pagamento mensal
4	Disponibilização da ingestão de logs externos	Termo de Recebimento Definitivo	60 dias da assinatura do contrato	Pagamento anual após o recebimento definitivo do objeto
5	Realização do Treinamento	Ateste na nota fiscal	180 dias da assinatura do contrato	Pagamento único após a realização do treinamento
6	Conclusão do serviço de implantação	Termo de Recebimento Definitivo	60 dias da assinatura do contrato	Pagamento único após o recebimento definitivo do objeto
7 e 8	Prestação do serviço mensal de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Ateste na nota fiscal	mensal	Pagamento mensal após a realização do serviço

Parágrafo Primeiro. A presente contratação permite a antecipação de pagamento (itens 1, 2 e 4) que ocorrerá com prazo não superior a 30 dias contados do prazo estabelecido para o início do fornecimento/prestação do serviço.

Parágrafo Segundo. Os itens 1, 2 e 4 serão pagos em 3 (três) parcelas anuais, de igual valor, condicionadas à disponibilização anual das respectivas licenças e observados os seguintes marcos de pagamento: a primeira parcela será paga após a emissão do respectivo Termo de Recebimento Definitivo; a segunda, em até 12 (doze) meses após o

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

pagamento da primeira; e a terceira, em até 12 (doze) meses após o pagamento da segunda. A segunda e a terceira parcelas são reajustáveis pelo ICTI (Índice de Custo de Tecnologia da Informação).

Parágrafo Terceiro. O item 3 será pago mensalmente com base em um dos seguintes critérios:

I - Quantidade de tokens consumidos no período de apuração, de acordo com os registros de consumo da solução, devendo a CONTRATADA apresentar a memória de cálculo juntamente com o relatório mensal de medição;

II - Quantidade de tokens previamente estimados pela fiscalização do contrato para consumo no período de apuração.

Parágrafo Quarto. O faturamento ficará limitado ao consumo efetivamente registrado no período e ao quantitativo máximo contratado, sendo vedada a cobrança de tokens não utilizados.

Parágrafo Quinto. O pagamento dos itens 7 e 8 será realizado mensalmente, após a execução dos serviços e entrega ao CONTRATANTE, pela CONTRATADA, dos resultados dos indicadores apurados.

Parágrafo Sexto. O documento fiscal deverá ser obrigatoriamente registrado no Portal do SIGEO - JT para ateste, liquidação e pagamento.

CLÁUSULA DÉCIMA PRIMEIRA. Para todos os fins, considera-se como data do pagamento, o dia da emissão da ordem bancária.

CLÁUSULA DÉCIMA SEGUNDA. No caso de os documentos apresentados para atendimento ao disposto no subitem 12.2 do Edital Pregão Eletrônico nº 27/2026 estarem vencidos quando da apresentação do documento fiscal, a CONTRATADA deverá providenciar a regularização.

CLÁUSULA DÉCIMA TERCEIRA. Na eventualidade de atraso no pagamento, entre a data do vencimento e a data do efetivo pagamento, serão devidos pelo CONTRATANTE:

a) juros de mora de 0,5% a.m. (cinco décimos por cento ao mês) ou 6% a.a. (seis por cento ao ano), por dia de atraso na efetivação do pagamento;

b) multa moratória no percentual de 1% (um por cento) do valor da fatura em atraso; e

c) atualização financeira pelo IGP-DI.

Parágrafo Único. Não serão devidas quaisquer taxas de atualização financeira, juros ou multa moratória nas hipóteses em que houver a concorrência da CONTRATADA para o atraso no pagamento.

DO CRÉDITO

CLÁUSULA DÉCIMA QUARTA. As despesas oriundas do presente Contrato correrão à conta dos recursos orçamentários consignados ao CONTRATANTE nos exercícios de 202@ a 202@, Programa de Trabalho @, Elemento @.

DO REAJUSTAMENTO

CLÁUSULA DÉCIMA QUINTA. O reajustamento ocorrerá, mediante solicitação da CONTRATADA, a cada período de 12 meses contados a partir da data do orçamento

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

estimado (**22/10/2026**) com base no índice de Custo da Tecnologia da Informação (ICTI), estabelecido no guia da Resolução CNJ nº 468/2022, aplicando-se sua variação a partir da referida data.

CLÁUSULA DÉCIMA QUINTA. Nos contratos oriundos de Ata de Registro de Preços, já reajustadas, nos termos do subitem 11.9 do Edital do Pregão Eletrônico nº 27/2026, os reajustes subsequentes respeitarão o interregno mínimo de 12 meses, contados a partir dos efeitos financeiros do último reajuste.(no caso em que a ata já tiver sido prorrogada)

Parágrafo Primeiro. O reajustamento será calculado mediante a aplicação da variação acumulada do índice de reajuste sobre os preços praticados à época de sua concessão.

Parágrafo Segundo. O reajustamento incidirá sobre os preços unitários.

Parágrafo Terceiro. Será aplicado o índice acumulado do mês correspondente à data-base.

Parágrafo Quarto. Caso a variação acumulada no período seja positiva, o reajuste será concedido mediante requerimento da CONTRATADA à Fiscalização do contrato e o valor resultante da aplicação do índice poderá ser objeto de negociação entre as partes.

Parágrafo Quinto. Caso a variação acumulada no período seja negativa, o valor total do contrato será diminuído, automaticamente, com base na aplicação do índice.

Parágrafo Sexto. A prorrogação da vigência do contrato sem prévio requerimento dos valores de reajuste implicará na preclusão do direito da CONTRATADA. Também ensejará a preclusão do direito ao reajuste a extinção do contrato sem a prévia apresentação de requerimento da CONTRATADA.

Parágrafo Sétimo. Na hipótese de legislação superveniente reduzir ou aumentar o prazo de suspensão de aplicação de reajuste aos contratos, adequar-se-á o instrumento de contrato para refletir tal circunstância.

DA GARANTIA

CLÁUSULA DÉCIMA SEXTA. Como condição para início da execução do objeto, a CONTRATADA deverá, no prazo de **20 dias consecutivos**, contados da assinatura do contrato, prestar garantia no percentual de **5% (cinco por cento)** do valor da contratação, nos moldes do art. 96 da Lei nº 14.133/2021, mediante opção por uma das seguintes modalidades:

a) caução em dinheiro ou títulos da dívida pública;

a.1) na hipótese da garantia ser em dinheiro, deverá ser depositada na Caixa Econômica Federal em conta específica (operação 010) com correção monetária, em favor do Tribunal Regional do Trabalho da 4ª Região;

a.2) no caso da caução ser em títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Economia.

b) seguro-garantia,nos termos do art. 97 da Lei nº 14.133/2021;

c) fiança bancária.

c.1) no caso de garantia na modalidade de fiança bancária, deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

d) título de capitalização custeado por pagamento único, com resgate pelo valor total.

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

Parágrafo Primeiro. A garantia prestada pela CONTRATADA deverá viger durante todo o período de execução do objeto e 90 dias após o término da vigência contratual.

Parágrafo Segundo. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada à nova situação ou renovada, seguindo os mesmos parâmetros e prazos utilizados quando da contratação.

Parágrafo Terceiro. Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, a CONTRATADA obriga-se a fazer a respectiva reposição no prazo máximo de 10 dias úteis, prorrogáveis por igual período, contados da data em que for notificada.

Parágrafo Quarto. Na hipótese de inexecução e/ou atraso na execução do objeto, a garantia somente será devolvida após a apuração da aplicabilidade de sanção administrativa, descontados os valores correspondentes a eventuais multas aplicadas.

Parágrafo Quinto. Sem prejuízo da responsabilidade por perdas e danos, a garantia reverterá ao TRT da 4ª Região no caso de rescisão contratual por culpa exclusiva da CONTRATADA.

Parágrafo Sexto. O não cumprimento do disposto no *caput* da presente cláusula caracteriza descumprimento total da obrigação, sujeitando a CONTRATADA às sanções administrativas previstas no presente instrumento.

Parágrafo Sétimo. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:
a) prejuízo advindo do não cumprimento do objeto do contrato;
b) prejuízos causados à Administração, decorrentes de culpa ou dolo durante a execução do contrato; e
c) as multas moratórias e punitivas aplicadas pela Administração à CONTRATADA.

Parágrafo Oitavo. A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados nas alíneas *"**a**"* a *"**c**"* do parágrafo anterior, observada a legislação que rege a matéria.

DAS OBRIGAÇÕES DA CONTRATADA

CLÁUSULA DÉCIMA SÉTIMA. São obrigações da CONTRATADA:

a) Indicar um preposto para o contrato, sendo este o interlocutor da CONTRATADA junto ao CONTRATANTE para os assuntos relativos ao cumprimento das cláusulas contratuais e para participar de reuniões de acompanhamento, sempre que solicitado pelo CONTRATANTE;

b) Responsabilizar-se técnica e administrativamente pelo objeto contratado, não sendo aceita, sob qualquer pretexto, a transferência de responsabilidade a outras entidades, sejam fabricantes, técnicos ou quaisquer outros;

c) Responder integralmente por perdas e danos que vier a causar ao CONTRATANTE ou a terceiros em razão de ação ou omissão, dolosa ou culposa, sua ou dos seus prepostos, independentemente de outras cominações contratuais ou legais a que estiver sujeita;

d) Fornecer a seus empregados todos os instrumentos necessários à execução dos serviços;

e) Informar a relação dos empregados que prestarão serviços nas dependências do CONTRATANTE;

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

f) Responder pelas despesas relativas a encargos trabalhistas, de seguro de acidentes, impostos, contribuições previdenciárias e quaisquer outras que forem devidas e referentes aos serviços executados por seus empregados, uma vez que estes não têm nenhum vínculo empregatício com o CONTRATANTE.

g) Responder por valores adicionais ao valor do contrato, tais como custos de deslocamento, alimentação, transporte, alojamento, trabalho em sábados, domingos, feriados ou em horário noturno, bem como qualquer outro valor adicional;

h) Garantir o mais rigoroso sigilo sobre quaisquer dados, informações, documentos e especificações a que venham a ter acesso em razão dos serviços prestados, não podendo, sob qualquer pretexto, revelá-los, divulgá-los ou reproduzi-los, conforme o Termo de Compromisso com a Segurança da Informação (**Anexo II** deste contrato).

i) Manter, durante toda a vigência do contrato, as condições de habilitação exigidas na contratação;

j) Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual.

k) Propiciar todos os meios necessários à fiscalização do contrato pelo CONTRATANTE, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, sempre que considerar a medida necessária;

l) Quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de Tecnologia da Informação e Comunicação (TIC).

Parágrafo Primeiro. A CONTRATADA deverá promover, no prazo máximo de 3 (três) meses, a atualização das certificações de seus profissionais caso haja atualização de versão ou migração para uma nova solução de TI devido à modernização do ambiente tecnológico do CONTRATANTE. Este prazo se iniciará a partir da comunicação formal do CONTRATANTE.

Parágrafo Segundo. A CONTRATADA, o preposto e os empregados, vinculados à presente contratação, deverão conhecer e observar a Resolução Administrativa TRT4 nº 11/2025, que regulamenta o tratamento das notícias de assédio moral, assédio sexual e discriminação no âmbito da Justiça do Trabalho da 4ª Região, de acordo com a Política de Prevenção e Combate ao Assédio Moral na Justiça do Trabalho de 1º e 2º graus e com a Política de Prevenção e Enfrentamento do Assédio Moral, do Assédio Sexual e da Discriminação.

Parágrafo Terceiro. A CONTRATADA não poderá permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos, nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre.

Parágrafo Quarto. A CONTRATADA deverá cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas na legislação.

Parágrafo Quinto. A CONTRATADA deverá comprovar a reserva de cargos a que se refere o parágrafo acima, quando solicitado pelo fiscal do contrato.

Parágrafo Sexto. A CONTRATADA deverá efetuar o cadastro no Portal do SIGEO - JT para apresentação dos documentos fiscais (notas fiscais) com vistas à liquidação e pagamento, por meio do link https://portal.sigeo.jt.jus.br/portal-externo.

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

MINUTA

Parágrafo Sétimo. A CONTRATADA terá acesso a um guia detalhado das funcionalidades do sistema SIGEO - JT pelo link *https://sigeo.jt.jus.br/ajuda.*

DAS OBRIGAÇÕES DO CONTRATANTE

CLÁUSULA DÉCIMA OITAVA. São obrigações do CONTRATANTE:

a) Proporcionar as facilidades indispensáveis à boa execução dos serviços;

b) Relatar, por escrito, com a devida comprovação, as eventuais irregularidades na prestação de serviços;

c) Sustar a execução de quaisquer trabalhos por estarem em desacordo com o especificado ou por qualquer outro motivo que caracterize a necessidade de tal medida;

d) Efetuar os pagamentos devidos.

DO RECEBIMENTO DO OBJETO

CLÁUSULA DÉCIMA NONA. Em conformidade com o artigo 140 da Lei n° 14.133/2021, o objeto deste contrato será recebido da seguinte forma:

a) Provisoriamente, com verificação posterior da conformidade do objeto com os requisitos da contratação, e;

b) Definitivamente, após a verificação do atendimento dos requisitos da contratação.

Parágrafo Primeiro. A fiscalização recusará o recebimento provisório do objeto, caso haja qualquer inconformidade com as normas, com a legislação vigente afeta ao serviço/objeto, com as especificações técnicas ou com qualquer disposição do presente contrato.

Parágrafo Segundo. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança da obra ou serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato, nos limites estabelecidos pela lei ou pelo contrato.

DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

CLÁUSULA VIGÉSIMA. Comete infração administrativa, nos termos da Lei nº 14.133/2021, o contratado que:

a) der causa à inexecução parcial do contrato;

b) der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;

c) der causa à inexecução total do contrato;

d) ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;

e) apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;

f) praticar ato fraudulento na execução do contrato;

g) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

h) praticar ato lesivo previsto no art. 5º da Lei nº 12.846/2013.

Parágrafo Primeiro. Serão aplicadas ao contratado que incorrer nas infrações acima descritas as seguintes sanções:

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

I - Advertência, quando o contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §2º, da Lei nº 14.133/2021 e art. 4º da Portaria GP.TRT4 nº 2.714/2022);

II - Impedimento de licitar e contratar, quando praticadas as condutas descritas nas alíneas "b", "c" e "d" do *caput* desta Cláusula, sempre que não se justificar a imposição de penalidade mais grave (art. 156, § 4º, da Lei nº 14.133/2021 e art. 5º da Portaria GP.TRT4 nº 2.714/2022);

III - Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nas alíneas "e", "f", "g" e "h" do *caput* desta Cláusula, bem como nas alíneas "b", "c" e "d", que justifiquem a imposição de penalidade mais grave (art. 156, §5º, da Lei nº 14.133/2021 e art. 6º da Portaria GP.TRT4 nº 2.714/2022).

IV - Multa:

a) Na hipótese de atraso na disponibilização das subscrições e serviços **(itens 1, 2, 3, 4, 7 e 8)** e na execução da implantação da solução (**item 6)**, a CONTRATADA estará sujeita a multa diária de 0,5% (cinco décimos por cento) sobre o valor da obrigação objeto do atraso, limitada a 10% (dez por cento) do respectivo valor.

b) Na hipótese de atraso na solução dos chamados de suporte técnico, a CONTRATADA estará sujeita a multa nos percentuais descritos a seguir, sobre o valor mensal dos itens 7 e 8, limitada a 10% (dez por cento) do respectivo valor:

b.1) Severidade A0 (crítica): 1% (um por cento) por hora de atraso;

b.2) Severidade A1 (alta): 0,5% (cinco décimos por cento) por hora de atraso;

b.3) Severidade A2 (média): 0,5% (cinco décimos por cento) por día útil de atraso;

b.4) Severidade A3 (baixa): 0,2% (dois décimos por cento) por dia útil de atraso;

b.5) Severidade A4 (pesquisa): 0,1% (um décimo por cento) por dia útil de atraso.

c) Na hipótese de atraso na realização do treinamento (**item 5**), a CONTRATADA estará sujeita a multa diária de 0,5% (cinco décimos por cento) sobre o valor do item em atraso, limitada a 10% (dez por cento) do respectivo valor

d) Na hipótese de inexecução total ou parcial do objeto, a CONTRATADA estará sujeita à aplicação de multa compensatória de 10% (dez por cento) do valor da parcela não executada**.**

e) Na hipótese de descumprimento total da obrigação, além da multa prevista na alínea ***"d"*** e da possibilidade de aplicação da sanção administrativa de impedimento de licitar e contratar com a União prevista no inciso II do parágrafo primeiro supra, ficará a CONTRATADA obrigada a restituir ao CONTRATANTE o valor total da contratação dos **itens 1, 2 e 4**. Em caso de execução parcial do objeto, o valor a ser devolvido corresponderá ao montante da(s) parcela(s) não executada(s).

Parágrafo Segundo. A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao CONTRATANTE (art. 156, §9º, da Lei nº 14.133/2021 e art. 3º, §1º, da Portaria GP.TRT4 nº 2.714/2022)

Parágrafo Terceiro. Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa (art. 156, §7º, da Lei nº 14.133/2021 e art. 3º, §2º, da Portaria GP.TRT4 nº 2.714/2022).

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

I - Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação (art. 157 da Lei nº 14.133/2021 e art. 18 da Portaria GP.TRT4 nº 2.714/2022)

II - Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo CONTRATANTE à CONTRATADA, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente (art. 156, §8º, da Lei nº 14.133/2021 e art. 12 da Portaria GP.TRT4 nº 2.714/2022).

III - Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de 10 (dez) dias úteis, a contar da data do recebimento da comunicação enviada pela autoridade competente (art. 12, II, da Portaria GP.TRT4 nº 2.714/2022).

Parágrafo Quarto. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa à CONTRATADA, observando-se o procedimento previsto no *caput* e parágrafos do art. 158 da Lei nº 14.133/2021 e Portaria GP.TRT4 nº 2.714/2022, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

Parágrafo Quinto. Na aplicação das sanções serão considerados (art. 156, §1º, da Lei nº 14.133/2021):

a) a natureza e a gravidade da infração cometida;

b) as peculiaridades do caso concreto;

c) as circunstâncias agravantes ou atenuantes;

d) os danos que dela provierem para o CONTRATANTE;

e) a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

Parágrafo Sexto. Os atos previstos como infrações administrativas na Lei nº 14.133/2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846/2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei (art. 159).

Parágrafo Sétimo. A personalidade jurídica da CONTRATADA poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com a CONTRATADA, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia (art. 160 da Lei nº 14.133/2021 e art. 8º da Portaria GP.TRT4 nº 2.714/2022).

Parágrafo Oitavo. O CONTRATANTE deverá, no prazo máximo 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal. (Art. 161 da Lei nº 14.133/2021 e art. 31 da Portaria GP.TRT4 nº 2.714/2022).

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

Parágrafo Nono. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133/2021 e art. 36 da Portaria GP.TRT4 nº 2.714/2022.

Parágrafo Décimo. Os débitos da CONTRATADA para com a Administração CONTRATANTE, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes deste mesmo contrato ou de outros contratos administrativos que a CONTRATADA possua com o CONTRATANTE, na forma da Instrução Normativa SEGES/ME nº 26/2022.

Parágrafo Décimo Primeiro. Da decisão proferida pela administração caberá recurso administrativo, que deverá ser apresentado no prazo de 15 dias úteis, contados da data da intimação, e encaminhado exclusivamente por e-mail para o endereço dg@trt4.jus.br.

Parágrafo Décimo Segundo. A apuração dos descumprimentos e a eventual cominação de sanções administrativas observarão o disposto na Portaria GP.TRT4 nº 2.714/2022.

Parágrafo Décimo Terceiro. A defesa escrita e os recursos administrativos deverão ser encaminhados exclusivamente por meio eletrônico para o endereço dg@trt4.jus.br.

DA GESTÃO E FISCALIZAÇÃO DO CONTRATO

CLÁUSULA VIGÉSIMA PRIMEIRA. A gestão e a fiscalização do contrato será exercida pelos seguintes servidores:

Integrante	Titular	Substituto	Unidade
Gestor:	Carlos Costa Jordão	Charles Ferreira Falcao	Coordenadoria de Segurança da Informação e Proteção de Dados
Fiscal Técnico:	Maurício Antonioli Schmitz	Carlos Augusto Nantes de Castilho Rivilino	
Fiscal Demandante:	Rodrigo Zarth	Mateus Both	
Fiscal Administrativo:	Alberto Daniel Müller	Ricardo Krause Kurylenko	Coordenadoria de Gestão e Apoio à Governança de TIC

Parágrafo Primeiro. O gestor do contrato ficará responsável por:

a) Organizar a reunião inicial;
b) Encaminhar alterações contratuais;
c) Controlar prazos e indicadores contratuais;
d) Atestar notas fiscais;
e) Tratar eventuais irregularidades constatadas na execução contratual;
f) Realizar o recebimento definitivo, emitindo o respectivo termo;
g) Verificar as obrigações previstas no encerramento do contrato.

Parágrafo Segundo. O fiscal administrativo do contrato ficará responsável por:

a) Participar da reunião inicial;
b) Conferir cumprimento de prazos contratuais;
c) Conferir o atendimento dos níveis de serviços contratados;

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

MINUTA

d) Conferir documentação exigida no contrato;
e) Verificar a conformidade do faturamento do objeto contratado;
f) Informar ao gestor do contrato qualquer irregularidade na execução do objeto ou descumprimento dos níveis de serviços contratados.

Parágrafo Terceiro. O fiscal demandante do contrato ficará responsável por:
a) Participar da reunião inicial;
b) Acompanhar a execução do objeto de acordo com o contrato;
c) Monitorar cumprimento de prazos contratuais;
d) Encaminhar demandas para a CONTRATADA por meio de ordens de serviço e/ou chamados;
e) Aferir as entregas da execução em relação ao objeto contratado;
f) Atestar se os requisitos de negócio da contratação foram atendidos;
g) Informar ao gestor do contrato qualquer irregularidade na execução do objeto ou descumprimento dos níveis de serviços contratados.

Parágrafo Quarto. O fiscal técnico do contrato ficará responsável por:
a) Participar da reunião inicial;
b) Acompanhar a execução do objeto de acordo com o contrato;
c) Monitorar cumprimento de prazos contratuais;
d) Encaminhar demandas para a CONTRATADA por meio de ordens de serviço e/ou chamados;
e) Aferir as entregas da execução em relação ao objeto contratado;
f) Atestar se os requisitos técnicos da contratação foram atendidos;
g) Assinar o ateste de fiscalização do contrato, quando cabível;
h) informar ao gestor do contrato qualquer irregularidade na execução do objeto ou descumprimento dos níveis de serviços contratados.

Parágrafo Quinto. No prazo máximo de 10 dias, contados da assinatura do contrato, será realizada uma reunião inicial do contrato com a participação obrigatória do preposto e um integrante da equipe técnica da CONTRATADA, do gestor e fiscais do contrato. A pauta da reunião deverá abordar o planejamento detalhado da implantação da solução contratada, além das condições contratuais.

Parágrafo Sexto. O mecanismo formal de comunicação utilizado no contrato será o e-mail, conforme detalhamento a seguir:

Assunto	E-mail
Envio de notas fiscais	Deve ser feito através do sistema SIGEO-JT
Informações sobre faturamento	sgti.contratos@trt4.jus.br
Informações técnicas	setic.csipd@trt4.jus.br

DAS HIPÓTESES DE EXTINÇÃO DO CONTRATO

CLÁUSULA VIGÉSIMA SEGUNDA. A extinção deste contrato poderá ser:

I - Determinada por ato unilateral e escrito do CONTRATANTE, exceto no caso de descumprimento decorrente de sua própria conduta;

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

MINUTA

II - consensual, por acordo entre as partes, por conciliação, por mediação ou por comitê de resolução de disputas, desde que haja interesse da Administração CONTRATANTE;

III - determinada por decisão arbitral, em decorrência de cláusula compromissória ou compromisso arbitral, ou por decisão judicial.

Parágrafo único. A extinção contratual será formalmente motivada nos autos do respectivo processo, assegurado o contraditório e a ampla defesa, nos termos dos artigos 137, 138 e 139 da Lei nº 14.133/2021.

DA VINCULAÇÃO AO INSTRUMENTO CONVOCATÓRIO

CLÁUSULA VIGÉSIMA TERCEIRA. Ficam fazendo parte do presente contrato, independentemente de transcrição, a íntegra do Edital do Pregão Eletrônico nº 27/2026 e seus anexos, bem como a proposta apresentada na licitação pela CONTRATADA, nos termos em que esta não for contrária ao referido instrumento convocatório.

DA LEGISLAÇÃO APLICÁVEL

CLÁUSULA VIGÉSIMA QUARTA. Aplicam-se à execução deste contrato a Lei n° 14.133/2021 e a legislação complementar, vigente e pertinente à matéria.

DOS CRITÉRIOS DE SUSTENTABILIDADE

CLÁUSULA VIGÉSIMA QUINTA. A solução a ser contratada promove a transformação digital ou racionalização de serviços atualmente realizados por meio de análise humana, especificamente através de recursos de inteligência artificial para a correlação de eventos e geração de relatórios.

Parágrafo Primeiro. 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.

Parágrafo Segundo. Assinatura digital é um ato de transformação digital, portanto, sustentável.

Parágrafo Terceiro. A realização de treinamentos de forma remota racionaliza o consumo de recursos orçamentários do CONTRATANTE e evita o deslocamento dos servidores, contribuindo para a sustentabilidade nesses dois aspectos.

DA PROMOÇÃO DA EQUIDADE DE GÊNERO, RAÇA E DIVERSIDADE

CLÁUSULA VIGÉSIMA SEXTA. A CONTRATADA, em consonância com os princípios e normas constantes na Política de Equidade de Gênero, Raça e Diversidade do TRT4, instituída pela Resolução Administrativa nº 03/2017, deverá implementar, sempre que possível, na execução do objeto da contratação, políticas que respeitem e valorizem a diversidade, garantindo tratamento equânime e repudiando preconceitos e discriminações de gênero, raça, etnia, orientação sexual, identidade de gênero, geracional e de pessoas com deficiência.

Parágrafo único. Sem prejuízo da responsabilidade da CONTRATADA em ter ciência e cumprir as disposições da Política de Equidade de Gênero, Raça e Diversidade do TRT4, a fiscalização ou a gestão contratual deverá, no início da execução do contrato, encaminhar à

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

CONTRATADA cópia do referido documento, a fim de assegurar a plena ciência de seu conteúdo.

DA PROTEÇÃO DE DADOS

CLÁUSULA VIGÉSIMA SÉTIMA. As partes envolvidas deverão observar as disposições da Lei nº 13.709/2018, Lei Geral de Proteção de Dados, quanto ao tratamento dos dados pessoais que lhes forem confiados, em especial quanto à finalidade e boa-fé na utilização de informações pessoais para consecução dos fins a que se propõe o presente contrato.

Parágrafo Primeiro. O CONTRATANTE figura na qualidade de Controlador dos dados quando fornecidos à CONTRATADA para tratamento, sendo esta enquadrada como Operador dos dados. A CONTRATADA será Controlador dos dados com relação a seus próprios dados e suas atividades de tratamento.

Parágrafo Segundo. As partes estão obrigadas a guardar o mais completo sigilo por si, por seus empregados ou prepostos, nos termos da Lei Complementar nº 105/2001 e da Lei Geral de Proteção de Dados (LGPD), cujos teores declaram ser de seu inteiro conhecimento, em relação aos dados, informações ou documentos de qualquer natureza, exibidos, manuseados ou que por qualquer forma ou modo venham tomar conhecimento ou ter acesso, em razão deste contrato, ficando, na forma da lei, responsáveis pelas consequências da sua divulgação indevida e/ou descuidada ou de sua incorreta utilização, sem prejuízo das penalidades aplicáveis nos termos da lei.

Parágrafo Terceiro. Em caso de necessidade de coleta de dados pessoais indispensáveis à própria prestação do serviço, esta será realizada mediante prévia aprovação do CONTRATANTE, responsabilizando-se a CONTRATADA por obter o consentimento dos titulares (salvo nos casos em que opere outra hipótese legal de tratamento). Os dados assim coletados só poderão ser utilizados na execução dos serviços especificados neste contrato, e em hipótese alguma poderão ser compartilhados ou utilizados para outros fins.

I. Eventualmente, as partes podem ajustar que o CONTRATANTE será responsável por obter o consentimento dos titulares, observadas as demais condicionantes deste parágrafo.

Parágrafo Quarto. A CONTRATADA dará conhecimento formal aos seus empregados das obrigações e condições acordadas nesta Cláusula, inclusive no tocante à Política de Privacidade e Proteção de Dados Pessoais do CONTRATANTE (Portaria TRT4 nº 2.036/2021), cujos princípios deverão ser aplicados à coleta e tratamento dos dados pessoais de que trata esta Cláusula.

Parágrafo Quinto. Os dados pessoais tratados e operados serão eliminados após o término do objeto deste contrato, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

a) Cumprimento de obrigação legal ou regulatória pelo controlador;

b) Estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

c) Uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

Parágrafo Sexto. O Encarregado indicado pela CONTRATADA manterá contato formal com o Encarregado pelo contrato indicado pelo CONTRATANTE, no prazo de 24 (vinte e quatro) horas da ocorrência de qualquer incidente que implique violação ou risco de violação de

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

dados pessoais, para que este possa adotar as providências devidas, na hipótese de questionamento das autoridades competentes.

Parágrafo Sétimo. Os casos omissos em relação ao tratamento dos dados pessoais que forem confiados à CONTRATADA, e não puderem ser resolvidos com amparo na LGPD, deverão ser submetidos à Fiscalização para que decida previamente sobre a questão.

DAS DISPOSIÇÕES GERAIS

CLÁUSULA VIGÉSIMA OITAVA. Na forma do inciso XVI do artigo 92 da Lei nº 14.133/2021, a CONTRATADA obriga-se a manter, durante toda a execução do contrato, em compatibilidade com as obrigações por ele assumidas, todas as condições exigidas para a habilitação na licitação.

Parágrafo Primeiro. Caso o CONTRATANTE verifique a não manutenção das condições habilitatórias, a CONTRATADA será notificada para regularizar a situação, o que deverá ocorrer no prazo máximo de 10 dias úteis.

Parágrafo Segundo. Em caso de não atendimento à determinação constante no Parágrafo anterior, a CONTRATADA incorrerá em inexecução contratual, hipótese que poderá ensejar a rescisão do contrato e a execução da garantia.

CLÁUSULA VIGÉSIMA NONA. A CONTRATADA obriga-se a manter seu endereço e telefone atualizados durante toda a vigência da contratação, mediante envio de mensagem eletrônica para o endereço *dlic@trt4.jus.br*.

CLÁUSULA TRIGÉSIMA. As alterações de quaisquer condições do presente Contrato deverão sempre ser procedidas por meio de termos aditivos.

CLÁUSULA TRIGÉSIMA PRIMEIRA. Na execução dos serviços, a CONTRATADA cumprirá todos os padrões de segurança e regras de uso e de controle de acesso às instalações do CONTRATANTE. A CONTRATADA se compromete a manter sigilo acerca das informações obtidas e geradas no decorrer do trabalho, mediante assinatura de Termo de Compromisso com a Segurança da Informação (**Anexo II** do presente contrato).

CLÁUSULA TRIGÉSIMA SEGUNDA. Durante a execução dos serviços, a CONTRATADA deverá observar as Políticas de Controle de Acesso definidas pelo CONTRATANTE.

CLÁUSULA TRIGÉSIMA TERCEIRA. A CONTRATADA ficará obrigada a aceitar, nas mesmas condições propostas, os acréscimos ou supressões que se fizerem no objeto desta licitação, até o limite de 25% (vinte e cinco por cento) do valor contratado.

CLÁUSULA TRIGÉSIMA QUARTA. É vedada a subcontratação do objeto contratual, não sendo considerada subcontratação a atuação do fabricante da solução nas atividades inerentes ao fornecimento, operação, manutenção, atualização e suporte técnico especializada da plataforma, permanecendo a CONTRATADA integralmente responsável pelo cumprimento das obrigações contratuais.

CLÁUSULA TRIGÉSIMA QUINTA. Até a data do início dos serviços, a CONTRATADA deverá comprovar que os profissionais que prestarão os serviços, indicados na alínea ***"c.1"*** do subitem 7.1 do edital Pregão Eletrônico nº 27/2026, integram o quadro de pessoal permanente da CONTRATADA. A comprovação deverá ser feita mediante apresentação de:

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

MINUTA

I) Documento que comprove vínculo de emprego; ou
II) Documento que comprove ser o profissional sócio da empresa; ou
III) Contrato civil de prestação de serviços.

Parágrafo único. Excepcionalmente, a CONTRATADA poderá substituir o(s) profissional(is) para a execução dos serviços, desde que comprovadas as condições de qualificação exigidas, condicionadas à prévia avaliação dos requisitos de qualificação e aceite por parte do CONTRATANTE.

CLÁUSULA TRIGÉSIMA SEXTA. É vedada a manutenção, aditamento ou prorrogação do presente contrato, caso a empresa CONTRATADA venha a admitir empregados que sejam cônjuges, companheiros ou parentes em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de:
I - servidores que tenham participado do planejamento da contratação ou que desempenhem função na área de licitações e contratos do TRT4;
II - servidores ocupantes de cargos ou funções de direção, chefia ou assessoramento vinculados à Secretaria de Administração, à Diretoria-Geral, à Assessoria Jurídica da Presidência, à Secretaria-Geral da Presidência e às demais unidades envolvidas no procedimento licitatório;
III - o Presidente do Tribunal ou o desembargador que estiver no exercício da Presidência do TRT4;
IV - o Diretor da Escola Judicial do TRT4 ou o desembargador que estiver no exercício do cargo, em relação às contratações da referida unidade;
V - os membros ou juízes vinculados a este Tribunal (conforme o art. 3º da Resolução CNJ nº 7/2005).

CLÁUSULA TRIGÉSIMA SÉTIMA. Incumbirá ao CONTRATANTE divulgar o presente instrumento no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no art. 94 da Lei 14.133/2021, bem como no respectivo sítio oficial na Internet, em atenção ao art. 8º, §2º, da Lei n. 12.527/2011, c/c art. 7º, §3º, inciso V, do Decreto n. 7.724/2012.

CLÁUSULA TRIGÉSIMA OITAVA. Fica eleito o Foro da Justiça Federal, Seção Judiciária do Rio Grande do Sul, Subseção Judiciária de Porto Alegre, com esteio no artigo 109, inciso I, da Constituição Federal, para dirimir quaisquer dúvidas decorrentes do presente contrato, renunciando a qualquer outro, por mais privilegiado que seja.

E, por estarem justas e acordadas, as partes assinam eletrônica/digitalmente o presente instrumento, considerando-se efetivamente formalizado a partir da data da última assinatura.

Assinantes:

Pelo CONTRATANTE:

Documento assinado digitalmente
ALEXANDRE CORRÊA DA CRUZ
Presidente do TRT da 4ª Região

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

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

MINUTA

Pela CONTRATADA:

Documento assinado digitalmente
@@@@@@@@@@@@@@@
CPF nº @@@@@@@

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

MINUTA

CONTRATO TRT4 nº @/202@ - Anexo I

ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO

1. Definições para fins desta especificação:

1.1. Define-se “Ativo monitorado” como sendo uma estação de trabalho, notebook, dispositivo móvel, servidor, container, firewall, ativo de rede ou qualquer equipamento similar ao listado que possua endereço IP próprio e distinto e que deverá ser monitorado pela solução proposta. Poderá ser físico ou virtual e poderá estar hospedado em ambiente local (on-premise) ou em nuvem.

1.1.1. Relativo a container, deverá ser contabilizado como “Ativo monitorado” o host que hospeda o(s) container(s), para efeito de subscrição.

1.1.2. As licenças para *container* estarão limitadas a 4% de todos os ativos contratados.

1.2. Caso o ativo possua mais de um endereço IP, será contabilizado um único “Ativo monitorado” para efeito de subscrição.

1.3. Para os dados do ambiente do CONTRATANTE que serão coletados pela solução proposta, adotam-se as seguintes definições:

1.3.1. “Dados de logs”, “logs de evento” ou simplesmente “log”: informações produzidas sobre eventos ocorridos nos sistemas operacionais, aplicações, servidores, endpoints, ativos de rede ou outros componentes do ambiente computacional.

1.3.2. “Dados de telemetria”: informações produzidas pelos agentes a serem instalados nos ativos monitorados (quando a solução fizer uso de agentes).

1.3.3. “Dados de rede”: informações sobre o tráfego de rede.

1.4. Tokens: Unidades de consumo de Inteligência Artificial, utilizados em agentes inteligentes para automação de tarefas.

1.5. Usuários ativos: usuários que fazem uso dos recursos do Active Directory, pertencentes a uma organização ou restritos a uma ou mais OUs (Unidades Organizacionais) dentro da subárvore do Active Directory.

1.6. Define-se “Área de Armazenamento” como sendo a área disponibilizada por meio da solução contratada para armazenamento dos logs em ambiente SaaS, coletados pela solução.

1.7. Será utilizada a métrica de GB/dia (gigabytes por dia) para a ingestão de logs no SIEM da solução contratada, sendo que:

1.7.1. O volume de logs ingeridos no SIEM a partir dos demais módulos da solução do fabricante ofertadas na proposta não deverão ser contabilizados;

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

1.7.2. Serão contabilizados a ingestão de apenas fontes externas vindas de outros fabricantes, cuja cobrança será baseado no consumo médio de GB/dia;

1.7.3. Caberá à CONTRATADA estimar e controlar o volume de logs de fontes externas ingeridos na solução, se desejar fazer uso deste recurso;

1.7.4. A ingestão de logs externos no volume de até 10 GB/dia será considerado isento de cobrança;

1.7.5. Considera-se o arredondamento bancário para as frações de GB/dia aferidas.

1.8. Os itens 2, 3 e 4 estão vinculados à contratação do item 1 e não podem ser contratados separadamente.

2. ITENS 1 a 4 – Requisitos mínimos da solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos

2.1. A solução contratada visa o monitoramento contínuo e ininterrupto dos ativos computacionais do CONTRATANTE (supramencionados como “Ativos monitorados”) por meio das etapas de, mas não se limitando à, coleta, processamento e correlação de logs de eventos, dados de telemetria e/ou de rede de tais ativos, com o objetivo de, após análise contextualizada das etapas mencionadas, identificar eventos suspeitos ou incomuns, direcionados ao CONTRATANTE e permitir ações de proteção de forma automatizada ou manual.

2.2. A solução deve possuir as características mínimas constantes nesta especificação, devendo ser constituída de softwares, licenças, subscrições e garantias, de tal forma que haja a total compatibilidade entre seus componentes.

2.3. A CONTRATADA deve prover, ao ambiente, soluções de segurança cibernética que permitam a visibilidade de logs, dados de telemetria, tráfego de rede e de informações correlatas, capazes de identificar eventos suspeitos ou incomuns que possam comprometer os serviços tecnológicos do CONTRATANTE, por meio da coleta, processamento e correlação dos logs de eventos, dados de telemetria e/ou de rede dos ativos monitorados e do tráfego de rede.

2.4. Para a prestação desse serviço, deve ser utilizada uma solução de Monitoramento, Detecção, Notificação, Investigação e Resposta a Ataques Cibernéticos, com capacidades de Coleta e Correlacionamento de Logs e Mecanismos de Detecção de Comportamento Anômalo de Usuários e Aplicações (UEBA – User and Entity Behavior Analytics). Neste caso,

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

entende-se por “Aplicações” como sendo os softwares instalados nos ativos monitorados.

2.5. A solução permitirá monitorar em regime 24x7 (vinte e quatro horas por dia, sete dias por semana) eventos de segurança cibernética, identificando incidentes relativos a ataques, violações de conformidade e comportamento suspeito nas aplicações, rede e ativos computacionais do CONTRATANTE, compreendendo:

2.5.1. Analisar, classificar, categorizar, correlacionar e notificar os eventos e incidentes classificados como ameaças à segurança cibernética, ou que sejam considerados relevantes de acordo com diretrizes estabelecidas pelo CONTRATANTE;

2.5.2. Registrar e comunicar os incidentes de segurança cibernética para o CONTRATANTE, com as respectivas recomendações para tratamento e mitigação das ameaças, conforme especificação técnica contida neste documento;

2.5.3. Elaborar procedimentos padronizados contendo as melhores práticas para tratamento e resposta dos incidentes confirmados, que serão posteriormente executados pelas equipes responsáveis do CONTRATANTE;

2.5.4. Registrar os incidentes no módulo de gestão de incidentes da solução ofertada, cujo acesso deverá estar disponível para o CONTRATANTE.

2.5.4.1. O módulo de gestão de incidentes deverá ser nativo da solução ofertada ou ser implementado por meio de ferramenta de ITSM (IT Service Management), complementar e integrado à solução ofertada. As funcionalidades do módulo ou da ferramenta devem conter os dados dos alertas, incidentes e chamados além de informações sobre SLA para acompanhamento do tratamento dos chamados.

2.5.4.1.1. O módulo ou ferramenta deve ser capaz de, minimamente:

2.5.4.1.1.1. Permitir a criação e acompanhamento de incidentes cibernéticos, de forma manual e automática, com no mínimo as seguintes características:

2.5.4.1.1.1.1. Sumário do incidente, incluindo título, sumário, detalhes, e a fonte geradora do incidente. Também deverá incluir o status do incidente, incluindo data de criação, de modificação, de fechamento, tempo em que o chamado está aberto, número de alertas agregados e, opcionalmente, prioridade e analistas envolvidos;

2.5.4.1.1.1.2. Classificação inicial da ameaça, incluindo categoria, origem (interna/externa), possibilidade de modificação manual da prioridade e justificativa, além de informações específicas para subsidiar o relatório de incidentes e possibilidade de inclusão de documentação adicional através da anexação de arquivos;

2.5.4.1.1.1.3. Possibilidade de manter o histórico de atividades realizadas pelos

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

PROAD n. 6891/2026 DOC 43
Cadastrado por lfarias - LEDIANE FERNANDES DE FARIAS
Juntado em 24/11/2026

analistas, tais como criação de registros, atualização de campos, etc;

2.5.4.1.1.1.4. Permitir inserir comentários dos analistas no incidente, de tal forma a possibilitar o registro de todas as atividades de análise;

2.5.4.1.1.1.5. Permitir inserir evidências coletadas de eventual análise forense de host e rede como um complemento da análise do incidente;

2.5.4.1.1.1.6. Permitir registrar ações de remediação que incluam contenção, erradicação, educação de usuários e melhorias no programa do SOC;

2.5.4.1.1.1.7. Permitir registrar os resultados de um Incidente incluindo sua confirmação, categoria de ataque, identificação de técnicas utilizadas, detalhes sobre o alvo dos ataques e eficácia dos controles de detecção, prevenção e investigação.

2.5.4.1.1.2. Permitir o recebimento de alertas de segurança, de forma automática, com no mínimo as seguintes características:

2.5.4.1.1.2.1. Nome do alerta, fonte geradora, prioridade, data de criação, data original do alerta, categoria, ação, tipo, nível de severidade, descrição, serviço afetado, e detalhes do alerta;

2.5.4.1.1.2.2. Dados de origem e destino: IPs e portas; quando disponível, informações de contexto de negócio de cada dispositivo de origem e destino: domínios, endereços MAC, nomes dos dispositivos, tipos, unidades de negócio, geolocalização, índices de criticidade e conformidade e proprietários;

2.5.4.1.1.2.3. Capacidade de incluir arquivos anexos, de acordo com a necessidade de aprofundamento de detalhes dos alertas.

2.5.4.1.1.3. Gerar relatórios mensais do acordo de nível de serviço (SLA – Service Level Agreement).

2.5.4.1.1.3.1. Os relatórios gerados deverão ser encaminhados para o CONTRATANTE.

2.5.5. O módulo ou ferramenta de ITSM deverá estar licenciado para o CONTRATANTE, devendo ser hospedado em regime SaaS (Software as a Service) pela CONTRATADA, bem como deve estar protegido por autenticação do tipo MFA - Multi-Factor Authentication e acesso criptografado ponto a ponto.

2.6. A solução deve ser fornecida no modelo Software as a Service (SaaS) permitindo a instalação de múltiplos coletores e agentes on-premises e em nuvem, a fim de realizar a implantação distribuída da arquitetura.

2.6.1. Deve ter instância própria para cada CONTRATANTE, isto é, exclusiva e dedicada para cada Tribunal e sem compartilhamento com outros clientes da CONTRATADA.

2.6.2. Todas as licenças e subscrições necessárias para o pleno funcionamento da solução deverão ser fornecidas pela CONTRATADA, conforme as quantidades e faixas discriminadas nesta especificação.

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

2.6.3. Coletores de logs: o software dos coletores de logs, bem como os respectivos sistemas operacionais, sistemas gerenciadores de banco de dados, entre outros componentes eventualmente necessários para a coleta e centralização de logs de eventos e/ou dados de telemetria deverão ser fornecidos pela CONTRATADA;

2.6.4. O CONTRATANTE disponibilizará, no máximo, os seguintes recursos em ambiente virtual a serem usados pelos coletores de logs (os recursos podem ser distribuídos entre diversas máquinas virtuais - uma para cada coletor, se necessário):

2.6.4.1. 12 vCPUs;

2.6.4.2. 32Gb vRAM;

2.6.4.3. 200GB de espaço em disco.

2.6.5. Caso os recursos em ambiente virtual necessários para o pleno funcionamento da solução extrapolem os recursos disponibilizados pelo CONTRATANTE, a CONTRATADA deve demonstrar, por meio de documento técnico do fabricante e/ou de boas práticas, a necessidade de aumento dos recursos, que serão disponibilizados pelo CONTRATANTE conforme comprovação apresentada. Caso não haja comprovação, a critério do CONTRATANTE, a CONTRATADA deverá providenciar, sem custos adicionais para o CONTRATANTE, a entrega da infraestrutura (total ou remanescente) e em conformidade com a estrutura computacional do CONTRATANTE.

2.6.6. Agentes: software de baixo consumo de processamento que é instalado nos ativos suportados para centralizar e monitorar os dados de segurança cibernética. O agente oferece visibilidade e detecção de ataques nos endpoints, coletando informações on-line do sistema, incluindo informações básicas de identificação de ativos, processos em execução, logs e outros dados de telemetria e enviando essas informações à solução para análise.

2.6.7. O console de gerência deve ser acessado via web, de forma segura (HTTPS) e deve possuir compatibilidade com, no mínimo, os seguintes navegadores:

2.6.7.1. Google Chrome;

2.6.7.2. Microsoft Edge

2.6.8. O console de gerência deve estar disponível no ambiente do próprio fabricante, que é responsável pelas manutenções, atualizações e disponibilidade da solução.

2.6.8.1. Os ambientes utilizados pela solução, inclusive os do fabricante, devem estar localizados no Brasil ou em país que confira grau de proteção de dados pessoais adequado ao previsto na Lei nº 13.709/2018 (LGPD), assim

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

entendido o país que possua legislação geral de proteção de dados pessoais de conteúdo equivalente à LGPD ou ao Regulamento (UE) 2016/679 (GDPR) e autoridade de controle independente com poderes de fiscalização e sanção.

2.6.8.2. É vedado utilizar dados, logs, telemetria, incidentes, prompts ou resultados para treinamento, ajuste ou desenvolvimento de modelos próprios ou de terceiros, salvo autorização expressa do CONTRATANTE. Subprocessadores deverão ser previamente informados.

2.6.9. O console de gerência deve possuir a capacidade de autenticação multifator (MFA - Multi-Factor Authentication).

2.7. A solução deve ser fornecida dimensionada para a quantidade de ativos a serem monitorados de forma a abranger o escopo completo de ativos do CONTRATANTE, conforme conceito apresentado nesta especificação técnica.

2.8. 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;

2.8.1. As análises realizadas e alertas devem estar disponíveis de forma integral por pelo menos 90 dias.

2.8.2. Retenção de logs de auditoria da plataforma e de artefatos coletados pelos agentes por período mínimo de 180 (cento e oitenta) dias.

2.8.3. Os logs do SIEM deverão ser armazenados por 30 dias para correlação com os dados de telemetria.

2.8.4. Em caso de encerramento do contrato, substituição da solução ou mediante solicitação do CONTRATANTE durante o processo de transição, a CONTRATADA deverá permitir a exportação em lote de todos os logs, dados de telemetria, eventos e dados de rede do CONTRATANTE que ainda estejam armazenados na solução e abrangidos pelo período de retenção contratado, em 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.

2.8.5. A solução não deve possuir mecanismos que limitem ou onerem o CONTRATANTE com base na quantidade/volume de dados a serem exportados.

2.9. A solução deve possuir capacidade de monitorar e identificar o comportamento de usuários que representar ameaça (UEBA - User and Entity Behavior Analytics), em nível de ativos monitorados ou em nível de logs de eventos, do Microsoft Active Directory e do OpenLDAP, monitorando

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

MINUTA

diferentes vetores de ataque, como:

2.9.1. Movimentação lateral com uso de credenciais locais de máquina;

2.9.2. Ataques de força bruta em contas locais de máquinas;

2.9.3. Usuários locais que tentam apagar arquivos de evento dos registros da máquina.

2.9.4. Adicionalmente, para ambientes com Microsoft Active Directory:

2.9.4.1. Movimentação lateral com uso de credenciais de domínio;

2.9.4.2. Ataques de força bruta em contas de domínio;

2.9.4.3. Usuários de domínio que tentem apagar arquivos de evento dos registros da máquina;

2.10. A solução deve permitir, para ambientes com Microsoft Active Directory, monitorar ações de todos os usuários, permitindo campanhas de caças a ameaças, auditoria e criação de alertas para usuários específicos.

2.11. A solução deve monitorar qualquer tipo de acesso de usuário:

2.11.1. Em máquinas com credenciais locais – monitoramento com uso de agente da própria solução;

2.11.2. Com credenciais do domínio – monitoramento do Microsoft Active Directory;

2.11.3. Ingress Authentication – como VPN, Google Workspace/Google Apps e Office 365;

2.11.3.1. Para autenticações vindas de fora do ambiente – Ingress Authentication – a solução deve identificar e correlacionar a informações da origem do acesso – minimamente data, hora e IP.

2.12. A solução deve suportar IPv4 ou IPv4/IPv6.

2.13. Para detectar incidentes, a solução deverá implementar o recebimento e análise de logs, dados de telemetria e/ou de rede de, no mínimo:

2.13.1. Firewalls;

2.13.2. Web Application Firewalls;

2.13.3. IPS (Intrusion Prevention System) / IDS (Intrusion Detection System);

2.13.4. Web filtering;

2.13.5. Antivírus;

2.13.6. Microsoft Active Directory;

2.13.7. Open LDAP;

2.13.8. IAM (Identity and Access Management) / PAM (Privileged Access Management);

2.13.9. Servidores HTTP (HTTP Servers);

2.13.10. Balanceadores de Carga (Load Balancers);

2.13.11. DNS;

2.13.12. DHCP;

2.13.13. ELK Stack;

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

MINUTA

2.13.14. Sistemas Operacionais.

2.14. A solução que fizer uso de parsers para análise dos dados recebidos deve permitir a ingestão de fontes de eventos por meio de, no mínimo, o protocolo Syslog.

2.14.1. A solução deve permitir a leitura de logs e arquivos nos formatos CSV, XML, JSON e texto puro, de forma a permitir a inclusão de outras fontes de evento que não tenham conectores nativos.

2.14.2. A solução deve possuir módulo nativo (já incluso) para realização de parsers customizados.

2.14.2.1. A solução deve permitir utilização de expressões regulares (regex) nos parsers.

2.14.2.2. A solução deve prover identificação de eventos com erro de parsing e de eventos sem suporte de coleta.

2.15. A solução deve ter funcionalidade de coleta de eventos de auditoria de bancos de dados por meio de conectores nativos, coleta de logs, dados de telemetria e/ou de rede.

2.16. Para detectar incidentes, a solução também deverá suportar o recebimento e processamento de eventos de tráfego de rede e, opcionalmente, flow de rede.

2.17. 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:

2.17.1. De forma nativa (sem a necessidade de customização de parsers):

2.17.1.1. Checkpoint para proteção de perímetro (Firewall);

2.17.1.2. Fortinet FortiGate para proteção de perímetro (Firewall);

2.17.1.3. Forcepoint para proteção de perímetro (Firewall);

2.17.1.4. Microsoft Active Directory para serviços de diretório.

2.17.2. De forma nativa (sem a necessidade de customização de parsers) ou não:

2.17.2.1. Open LDAP para serviços de diretório;

2.17.2.2. OpenVPN;

2.17.2.3. Citrix;

2.17.2.4. RDP e RDPWeb;

2.17.2.5. Senha Segura para serviços de gerenciamento de acesso privilegiado;

2.17.2.6. Cyberark para serviços de gerenciamento de acesso privilegiado

2.17.2.7. Hashicorp Vault e Hashicorp Boundary para serviços de gerenciamento de acesso privilegiado;

2.17.2.8. Keycloak para gerenciamento de identidade e acesso;

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

MINUTA

2.17.2.9. midPoint para segurança de identidades (identity security);
2.17.2.10. ForeScout CounterACT (eyeSight e eyeControl) para serviços de NAC (Network Access Control);
2.17.2.11. Loqed;
2.17.2.12. Varonis;
2.17.2.13. IBM Spectrum Protect Plus para proteção de dados;
2.17.2.14. Kaspersky para proteção de endpoint;
2.17.2.15. Blackberry Cylance para proteção de endpoint.
2.17.2.16. Check Point Harmony para proteção de endpoint;
2.17.2.17. Tenable One para gerenciamento de exposição (exposure management platform);
2.17.2.18. Tenable.ep / Nessus para gerenciamento de vulnerabilidades;
2.17.2.19. Tenable.ad para proteção do Active Directory;
2.17.2.20. Trivy para varredura de vulnerabilidades;
2.17.2.21. VMware/vCenter para virtualização de máquinas;
2.17.2.22. VMware/Horizon para virtualização de estações de trabalho;
2.17.2.23. Hyper-V para virtualização de máquinas;
2.17.2.24. Ovirt para virtualização de máquinas;
2.17.2.25. Docker e Kubernetes;
2.17.2.26. Apache HTTP Server;
2.17.2.27. HAProxy;
2.17.2.28. Ingress;
2.17.2.29. Nginx;
2.17.2.30. Switches Cisco MDS;
2.17.2.31. Switches H3C;
2.17.2.32. Switches HP;
2.17.2.33. Switches Huawei;
2.17.2.34. Roteadores Cisco;
2.17.2.35. Roteadores Juniper;
2.17.2.36. Roteadores MikroTik;
2.17.2.37. Access Points Aruba;
2.17.2.38. Access Points Ruckus;
2.17.2.39. Controladoras Virtuais Aruba;
2.17.2.40. Bacula para serviços de backup;
2.17.2.41. Commvault (software de backup);
2.17.2.42. Veeam (software de backup);
2.17.2.43. Storage Huawei;
2.17.2.44. Storage IBM;
2.17.2.45. TSM Server IBM Spectrum Protect para serviços de backup;
2.17.2.46. Dell EMC Data Domain;

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

MINUTA

2.17.2.47. Dell EMC Isilon.

2.18. A solução deve ser capaz de coletar e processar fontes de eventos oriundas dos seguintes serviços de Cloud:

2.18.1. De forma nativa (sem a necessidade de customização de parsers):

2.18.1.1. AWS CloudTrail, via SQS ou API;

2.18.1.2. Google Cloud Platform, via API;

2.18.1.3. Google Workspace/Google Apps, via API;

2.18.1.4. Microsoft Office 365, via API.

2.19. A solução deve suportar e implementar a coleta e o processamento de fontes de eventos oriundas, no mínimo, dos seguintes sistemas operacionais. Para as soluções que fazem uso de agentes ou outro software externo/nativo do sistema operacional, eles devem ser compatíveis com as versões 32 e 64 bits dos sistemas operacionais (quanto existirem). Caso a solução não faça uso de agentes, os dados devem ser obtidos por meio da coleta do tráfego de rede.

2.19.1. De forma nativa (sem a necessidade de customização de parsers):

2.19.1.1. Windows 10;

2.19.1.2. Windows 11;

2.19.1.3. Windows Server 2016;

2.19.1.4. Windows Server 2019;

2.19.1.5. Windows Server 2022;

2.19.1.6. Windows Server 2025;

2.19.1.7. Red Hat Enterprise Linux / Oracle Enterprise Linux / Rocky Linux 8.4;

2.19.1.8. Red Hat Enterprise Linux / Oracle Enterprise Linux / Rocky Linux 8.5;

2.19.1.9. Red Hat Enterprise Linux / Oracle Enterprise Linux / Rocky Linux 9.0;

2.19.1.10. Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 7;

2.19.1.11. Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 8.0;

2.19.1.12. Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 8.1;

2.19.1.13. Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 8.2;

2.19.1.14. Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 8.3;

2.19.1.15. Amazon Linux;

2.19.1.16. Debian Linux;

2.19.1.17. Ubuntu Linux.

2.20. Para os itens 2.13, 2.17, 2.18 e 2.19, as listas de soluções são do tipo "não exaustivas", devendo ser considerada pela CONTRATADA, por meio de configuração da solução, a possibilidade de inclusão ou alteração de produtos em decorrência da evolução do parque tecnológico do CONTRATANTE.

2.20.1. A inclusão ou alteração de tecnologias pertencentes ao escopo ordinário será realizada sem custo adicional. Ampliações substanciais dependerão de formalização contratual.

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

2.21. A solução deve ser capaz de detectar comportamentos caracterizados como maliciosos de acordo com o MITRE ATT&CK Framework levando-se em consideração os dados recebidos dos ativos monitorados e gerados pelo coletor de tráfego de rede.

2.22. A solução deve cobrir detecções nativas de, ao menos, os grupos de atacantes categorizados pelo MITRE ATT&CK.

2.23. A solução deverá informar com qual técnica e tática do MITRE ATT&CK Framework o ataque está relacionado, além de possuir link direto para o site da organização.

2.24. A solução deve possuir de maneira nativa detecções de, no mínimo, os seguintes vetores de ataque:

2.24.1. Requisição a domínio suspeito;

2.24.2. Execução de processos suspeitos;

2.24.3. Requisição de dados de registro do sistema de nome de domínio (DNS);

2.24.4. Comunicação com servidores Command & Control;

2.24.5. Tentativa de desabilitar recursos de Sysmon;

2.24.6. Execução de processos LSASS (Local Security Authority Subsystem Service) com objetivo de detectar dump de memória para acessar possíveis credenciais armazenadas;

2.24.7. Detecção do uso de msrsc.exe - Microsoft Terminal Services Client;

2.24.8. Detecção do uso de comandos estruturados consistentes pela ferramenta Impacket e Impacket-Obfuscation;

2.24.9. Detecção de atividade de linha de comando da execução da função GetSystem, usada pelo Meterpreter ou Cobalt Strike;

2.24.10. Detecção de execução do Mimikatz e variações;

2.24.11. Detecção de processos que utilizam resultados do comando wget via Bash, Perl e Python;

2.24.12. Detecção de tentativas de criação de reverse shells para Command & Control.

2.25. A solução deve possuir a capacidade de identificar e monitorar o comportamento de atacantes baseados em IoC's (Indicators of Compromise) do próprio fabricante e de terceiros (threat intelligence).

2.26. A solução deve possuir listas de terceiros com informações de IoC's com, no mínimo, IPs, domínios, URLs e hashes da família SHA e, opcionalmente, MD5.

2.27. A solução deve possuir a capacidade de integração e/ou ingestão de dados de outras ferramentas de threat intelligence, de maneira manual ou por API, importando arquivos com base CSV ou STIX (Structured Threat Information Expression), através de assinatura de feeds de inteligência de

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

ameaças de terceiros, aceitando, no mínimo, os seguintes tipos: IPs, domínios, URLs e hashes da família SHA e, opcionalmente, MD5.

2.28. A solução deve disponibilizar informações a respeito dos principais ataques que estão ocorrendo no mundo, quais plataformas e países são afetados, além de links para obter mais informações.

2.29. A solução deve possui Inteligência de ameaças própria, reconhecida no quadrante mágico "2026 Gartner® Magic Quadrant™ for Cyberthreat Intelligence Technologies" ou permitir o enriquecimento de dados relacionados a endereços IPs, buscando informações adicionais em fontes de OSINT (Open Source Intelligence)

2.30. A solução deve prover relatórios de inteligência de ameaças avançadas mais recentes e indicadores de comprometimento para ajudar na defesa proativa contra ameaças.

2.30.1. A solução deve integrar relatórios de inteligência criados por especialistas em ameaças do fabricante e de terceiros para ajudar na identificação de ameaças.

2.30.2. Após análise dos relatórios de ameaças pela CONTRATADA, deverá ser feita uma investigação dentro do ambiente computacional do CONTRATANTE e registrado um incidente caso sejam identificadas atividades presentes nos relatórios.

2.30.3. Cada relatório deve possuir, no mínimo, informações como: região/país alvo, plataforma alvo e campanhas de ataques relacionadas aos dados do relatório.

2.31. Ter capacidade de Gerenciamento de Superfície de Ataque e Exposição de Ameaças (ASM):

2.31.1. Capacidade de realizar o mapeamento contínuo e sem necessidade de agentes adicionais de todos os ativos da organização expostos à internet pública (endereços IP, domínios, serviços, portas e recursos em nuvem), combinado com a identificação automatizada de ativos internos e não gerenciados (*Shadow IT*) realizada pela telemetria nativa da plataforma;

2.31.2. Funcionalidade de identificação automatizada e sem interrupção de vulnerabilidades conhecidas (CVEs), portas de alto risco expostas e configurações inadequadas de segurança em tempo real, dispensando o agendamento manual ou a execução de varreduras (*scans*) invasivas tradicionais;

2.31.3. Mapeamento e visualização gráfica automatizada das rotas potenciais de exploração, identificando de forma clara como um invasor pode se aproveitar de uma exposição externa ou

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

vulnerabilidade local para realizar movimentação lateral e comprometer sistemas e dados críticos (*crown jewels*);

2.31.4. Cálculo dinâmico do nível de risco das exposições identificadas, correlacionando pontuação CVSS, aplicabilidade técnica no ambiente, criticidade do ativo e dados de inteligência de ameaças em tempo real (existência de exploits ativos no mundo real) para ordenar as vulnerabilidades que exigem correção imediata;

2.31.5. Integração direta entre o módulo de exposição e os fluxos de automação nativos da própria plataforma (XDR/SOAR), permitindo o disparo de ações imediatas ou guiadas de mitigação (como isolamento de host, bloqueio de portas ou alteração de políticas) diretamente a partir da console central;

2.31.6. Disponibilização de painéis consolidados em tempo real com métricas de postura de segurança, histórico de redução da superfície de ataque, cálculo de tendência de risco e exportação de relatórios executivos para suporte a auditorias e conformidade;

2.32. O serviço deve gerar um relatório mensal que indique como corrigir os problemas que venham a ser encontrados.

2.33. A solução que fizer uso de agentes deve permitir sua instalação de forma “silenciosa” nos ativos a serem monitorados.

2.34. A solução deve possuir as funcionalidades de:

2.34.1. Monitoramento de comportamento (behavior monitor);

2.34.2. Controle de aplicação;

2.34.3. Monitoramento de eventos;

2.34.4. Auditoria de alterações no sistema;

2.34.5. Resposta automatizada a ameaças com a possibilidade de, mas não se limitando a, executar as ações propostas no item 2.61.

2.34.6. Capacidade de fornecer proteção contra malware desconhecido sem exigir uma conexão com o console de gerenciamento ou com a Internet;

2.34.7. Capacidade de proteção contra malware sem a necessidade de assinaturas, utilizando padrões e/ou heurísticas;

2.35. A solução deve monitorar os ativos em tempo real, estando eles dentro ou fora do domínio.

2.36. Os agentes devem poder coexistir com outras soluções de proteção, como antivírus, instaladas nos ativos monitorados sem que gerem conflito nem incompatibilidade entre os softwares.

2.36.1. Serão aceitas apenas soluções de NGAV/EDR cujo motor primário de detecção e prevenção opere por meio de análise comportamental contínua de

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

processos e aprendizado de máquina (Machine Learning), capaz de avaliar tanto o comportamento de execução de arquivos quanto de atividades em memória (*fileless*). A solução deverá ser capaz de detectar e bloquear ameaças mesmo quando não houver assinatura, hash, indicador de comprometimento ou conhecimento prévio específico da ameaça;

2.36.2. Não serão aceitas soluções que possuam apenas mecanismos de detecção baseados em assinaturas, hashes, reputação ou indicadores de comprometimento previamente conhecidos. A existência de módulos baseados em assinaturas será aceita como camada complementar de proteção, desde que a solução também possua, de forma nativa e habilitada, mecanismos de análise comportamental e Machine Learning para detecção e prevenção de ameaças conhecidas e desconhecidas, mesmo que tais módulos possam ser desabilitados ou parametrizados nas configurações do produto para simular o uso exclusivo do motor comportamental.

2.36.3. 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;

2.36.4. Capacidade de fornecer proteção contra malware desconhecido sem exigir uma conexão com o console de gerenciamento ou com a Internet;

2.37. Os agentes devem executar de maneira que não haja impacto na performance ou disponibilidade dos ativos monitorados.

2.37.1. Durante a implantação será estabelecido *baseline* de CPU, memória, disco e rede; degradação superior aos limites acordados será não conformidade.

2.38. Os agentes e os coletores devem, em caso de desconexão com o console, manter as informações sendo coletadas a fim de serem enviadas quando a conexão for restabelecida.

2.39. Os agentes e coletores devem enviar os dados para o console de maneira:

2.39.1. Segura e criptografada;

2.39.2. Que não haja impacto na performance ou disponibilidade da rede do CONTRATANTE.

2.40. Os agentes e coletores, ao enviarem os dados para o console, não devem degradar o tráfego de saída da rede do CONTRATANTE.

2.41. A solução deve monitorar, no mínimo:

2.41.1. Força bruta no ativo (brute force – asset);

2.41.2. Força bruta em conta local (brute force – local account);

2.41.3. Detecção de evasão - Deleção de log de evento (detection evasion – event log deletion);

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

2.41.4. Detecção de evasão - Deleção de log de evento local (detection evasion – local event log deletion);

2.41.5. Correspondência de Threat Intel (endpoint threat intelligence match);

2.41.6. Exploração mitigada (exploit mitigated);

2.41.7. Hash sinalizado no ativo (flagged hash on asset) - a solução deve permitir cadastrar um hash qualquer para gerar um alerta quando for acessado no ativo;

2.41.8. Processo sinalizado no ativo (flagged process on asset);

2.41.9. Exploração de elevação de privilégio Kerberos (kerberos privilege elevation exploit);

2.41.10. Movimentação lateral com personificação de administrador local (lateral movement – local administrator impersonation);

2.41.11. Movimentação lateral com credenciais locais (lateral movement – local credentials);

2.41.12. Tentativa de escalação de privilégio em honey credential local (local honey credential privilege escalation attempt);

2.41.13. Hash malicioso no ativo (malicious hash on asset) - a solução deve gerar um alerta quando um hash já conhecido como malicioso é acessado no ativo;

2.41.14. Criação de nova conta de usuário local (new local user account created);

2.42. A solução deve ser capaz de fornecer uma listagem dos ativos sendo monitorados.

2.43. A solução deve ser capaz de fornecer uma listagem dos ativos que estejam se comunicando no ambiente computacional do CONTRATANTE e que não estejam sendo monitorados.

2.44. A solução deve ser capaz de identificar acessos a URLs maliciosas além das portas padrão 80 e 443.

2.44.1. A solução deverá permitir classificar alertas relacionados a URLs em exceção para redução de falsos-positivos.

2.45. A solução deve correlacionar logs e/ou dados de telemetria/de rede dos ativos monitorados para:

2.45.1. Identificar comportamentos anômalos que aconteçam localmente no ativo monitorado;

2.45.2. Identificar quais eventos devem gerar alertas;

2.45.3. A solução deverá permitir classificar alertas relacionados a usuários e ativos em exceção para redução de falsos-positivos.

2.46. O console de correlacionamento deve estar disponível no ambiente do próprio fabricante, que é responsável pelas manutenções, atualizações e disponibilidade da solução.

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

2.47. A solução deve fazer uso de inteligência de ameaças do fabricante para analisar e correlacionar os dados recebidos.

2.48. A solução deve detectar ameaças conhecidas usando casos de uso de detecção constantemente atualizados, e desconhecidas por meio de conjuntos de dados aprendidos.

2.49. A solução deve prover funcionalidade de detecção de padrões em eventos coletados:

2.49.1. A solução deve prover detecção de padrões de ataque em todas as suas fases, com base no modelo Cyber Kill Chain, MITRE ou NIST;

2.50. A solução deve permitir a criação de alertas customizados baseados em um comportamento específico ou em um contexto de combinação de eventos.

2.51. Os modelos de detecção deverão possuir níveis de severidade (score) individuais para cada modelo em pelo menos os seguintes níveis:

2.51.1. Crítico;

2.51.2. Alto;

2.51.3. Médio;

2.51.4. Baixo.

2.52. A solução deve consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento.

2.53. A solução deve informar qual o escopo de impacto ou dimensionar o impacto em servidores, estações de trabalho e usuários, indicando a quantidade de componentes afetados no ataque.

2.53.1. Essas informações podem ser disponibilizadas por interação humana após investigação.

2.54. A solução deve permitir a visualização da correlação entre usuários, servidores, processos/comandos, arquivos e demais componentes correlacionados em determinado ataque.

2.55. A solução deve permitir o encerramento remoto de processos ativos executados nas estações de trabalho e servidores sob sua gestão.

2.56. A solução deve ser capaz de isolar uma estação de trabalho, desconectando-a da rede e permitindo se comunicar exclusivamente com a central da solução.

2.56.1. A solução deve ser capaz de restaurar a conectividade da estação de trabalho com a rede.

2.57. A solução deve ser capaz de realizar as ações dos itens 2.55. e 2.56. sem a necessidade de fornecimento de credenciais de usuário administrativo, o que não significa que o agente (caso a solução faça uso) não possa ser instalado com direitos administrativos.

2.58. A solução deve possuir a capacidade de monitorar a integridade de

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

MINUTA

arquivos (FIM – File Integrity Monitoring) nos servidores monitorados.

2.58.1. Nativamente, para os seguintes formatos de arquivos, no mínimo:

2.58.1.1. .bat

2.58.1.2. .cfg

2.58.1.3. .conf

2.58.1.4. .config

2.58.1.5. .dll

2.58.1.6. .exe

2.58.1.7. .ini

2.58.1.8. .sys

2.58.2. A solução deve permitir a inclusão de novos formatos de arquivos diferentes dos nativos.

2.59. O serviço de segurança cibernética de Caça a Ameaças (Threat Hunting) deverá ser prestado diretamente pelo fabricante da solução ou pela CONTRATADA, desde que sua equipe possua certificações oficiais emitidas pelo fabricante. Em ambos os casos, deverão ser observados os níveis mínimos de serviço (SLA) estabelecidos para as atividades de Detecção e Resposta Gerenciadas (MDR) e Threat Hunting, os quais deverão ser validados ou auditados pelo fabricante;

2.60. A solução deve, junto com o monitoramento do tráfego de rede (ou por meio de agentes), implementar regras de detecção de intrusão para correlacionar e trazer as informações sobre possíveis anomalias e ataques no nível de rede.

2.60.1. A solução deve permitir a criação de regras e/ou fornecer um conjunto de regras pré definidas.

2.60.1.1. No caso da solução possuir regras pré-definidas, deve haver sua atualização periódica cobrindo as informações de novas ameaças.

2.61. A solução deve possuir funcionalidade de automação na resposta de incidentes com playbooks de resposta já funcionais, devendo suportar, no mínimo, a automação das seguintes tarefas:

2.61.1. Envio de e-mails.

2.61.2. Com a utilização de agentes (não deve haver a necessidade de fornecimento de credenciais de usuário administrativo, o que não significa que o agente não possa ser instalado com direitos administrativos) ou outro mecanismo que a solução utilize para a automação:

2.61.2.1. Isolamento de uma máquina – caso seja detectado uma ameaça ou comportamento anômalo em uma máquina, deve ser possível isolá-la da rede;

2.61.2.2. Encerrar um processo malicioso – caso o agente detecte algum processo malicioso na máquina, a solução deve ter a capacidade de finalizar esse processo;

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

2.61.3. Com integrações para as soluções nativas indicadas no item 2.17.1:

2.61.3.1. Alertas relacionados a usuários do Microsoft Active Directory – se um alerta for gerado associado a uma credencial de domínio, a solução deve desabilitar o usuário para conter a ameaça de maneira rápida;

2.61.3.2. Sugerir e/ou criar regras no firewall – se um alerta for gerado associado a uma consulta DNS a um domínio considerado malicioso, a solução deve possibilitar a criação de regras de bloqueio no firewall ou sugerir qual regra deve ser criada para tal.

2.61.4. A solução deve permitir que cada tarefa nos playbooks de resposta de incidentes possa ser configurada de forma a:

2.61.4.1. Ser totalmente automática;

2.61.4.2. Aguardar uma interação humana para ser realizada.

2.62. Em casos de identificação de uma ameaça, a solução deve ter a capacidade de bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do sistema operacional ou demais aplicações instaladas no ativo.

2.63. A solução deve conter regras pré-definidas para detecção de ransomware e as principais famílias deste tipo de malware.

2.64. A solução deve possuir módulo de investigação e detecção integrados.

2.65. A solução deve apresentar os alertas de ameaças consolidados e correlacionados para melhor investigação e resposta aos incidentes.

2.66. A solução deve permitir configuração de notificações por e-mail (SMTP) e Webhooks (do Google Workspaces, no mínimo) para envio de alertas e notificações.

2.66.1. As notificações podem ser nativas ou, caso necessário, serem desenvolvidas pela CONTRATADA, sem custo para o CONTRATANTE, para viabilizar sua integração.

2.67. A solução deve permitir que as detecções sejam correlacionadas com dados recebidos dos ativos monitorados.

2.68. A solução deve, através dos dados do alerta, permitir a criação de um incidente e vinculá-lo ao alerta, possibilitando a definição da gravidade do incidente com dados de gravidade da fonte do alerta.

2.69. A solução deve permitir visualizar uma lista de incidentes e suas descrições, solicitar enriquecimentos e executar ações sobre os incidentes.

2.70. A solução deve criar uma linha do tempo (timeline) do ataque detectado, incluindo as evidências sobre cada alerta gerado e informando qual ativo gerou aquela evidência.

2.70.1. A solução deve prover visualização em linha do tempo com informações dos eventos monitorados em cada estação de trabalho.

2.71. A solução deve ser capaz de classificar a relevância dos eventos,

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

minimamente, em “crítico”, “alto”, “médio” e “baixo”.

2.72. A solução deve permitir a alteração do status dos incidentes de acordo com seu tratamento e indicar falsos positivos para a plataforma.

2.73. A solução deve permitir visualizar as atividades suspeitas de forma a sinalizar a causa raiz, seguindo as categorias do MITRE ATT&CK.

2.74. A solução deve permitir investigar os alertas gerados pelos modelos de detecção por meio de análise de impacto e análise de causa raiz.

2.74.1. Deve ser possível ativar ou desativar qualquer modelo de detecção.

2.74.2. A solução deverá possuir todos os módulos de detecção completamente licenciados, sem custo para o CONTRATANTE, independentemente da quantidade de modelos de detecção que venham a ser disponibilizados futuramente.

2.74.3. A solução deve permitir a análise automatizada de causa raiz de qualquer alerta, incluindo os alertas de rede, se os dados do endpoint estiverem disponíveis;

2.74.4. Visualização das cadeias de execução que levam a um alerta;

2.74.5. Visualização da cadeia de execução de eventos não envolvidos com alertas (Caça de ameaça - Threat Hunt);

2.74.6. Visualização de análise da linha do tempo para ver todas as ações e alertas em uma linha do tempo;

2.74.7. Consulta de indicadores de comprometimento (IoCs) e comportamentos de endpoint;

2.74.8. Para investigação em estações ou servidores deverá ser possível o registro minimamente dos seguintes itens:

2.74.8.1. Processo executado, incluindo datas e horários;

2.74.8.2. Atividades realizadas em arquivos;

2.74.8.3. Criação e encerramento de processos;

2.74.8.4. Threads de processo;

2.74.8.5. Protocolos de rede utilizados: solicitações DNS, conexão HTTP, desconexão HTTP;

2.74.8.6. Estatísticas de rede: histórico de conexões realizadas e processos associados;

2.74.8.7. Alterações em valores do registro;

2.74.8.8. Sessões de usuários no sistema operacional.

2.75. A solução deve permitir a criação de listas de exceção de objetos para redução de falsos positivos.

2.76. A solução deve adicionar os logs, dados de telemetria e/ou de rede coletados/correlacionados aos incidentes/alertas detectados.

2.77. A solução deve permitir o registro de incidentes por demanda, sem a necessidade de a própria solução ter gerado um alerta.

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

2.78. A solução deve possibilitar que, para cada incidente gerado, um analista seja vinculado ao incidente e que ele possa criar anotações sobre como está a evolução da resposta deste incidente;

2.79. A solução deve permitir que incidentes possam ser fechados após atividades serem encerradas, permitir marcação como falsos positivos e, também, que possam ser reabertos.

2.80. A solução deve exibir os eventos de forma a priorizar os alertas mais críticos para que o analista realize a investigação, indicando criticidade e níveis de prioridade.

2.80.1.1. A classificação quanto ao nível de criticidade deve ser baseada nas regras do MITRE.

2.81. A solução deve ter a capacidade de realizar buscas avançadas para localizar dados ou objetos no ambiente para análise avançada de atividades ou detecções.

2.82. A solução deve permitir realizar buscas e filtros de objetos para possibilitar pesquisas e análises avançadas.

2.83. A solução deve possibilitar a interação com cada um dos objetos relacionados ao evento para análise avançada e resposta.

2.83.1.1. Ao clicar em quaisquer dos objetos, a solução deve permitir a realização de buscas específicas pelo objeto ou ainda executar ações como executar investigações mais aprofundadas.

2.84. A solução deve prover diferentes métodos de pesquisa, filtros e uma linguagem de consulta para identificar, categorizar e recuperar os resultados da pesquisa.

2.85. A solução deve permitir a realização de buscas através de strings parciais, exatas, valores nulos, coringas (wildcards) e caracteres especiais.

2.86. A solução deve permitir salvar pesquisas com os critérios de busca e operadores lógicos utilizados para futuras consultas.

2.87. A solução deve permitir a criação de dashboards e relatórios baseados em bibliotecas prontas ou, também, criar do zero.

2.87.1.1. Deve possuir dashboards pré-configurados e permitir sua customização ou mesmo a criação de novos para refletir necessidades específicas do CONTRATANTE.

2.87.1.2. Deve fornecer a possibilidade de criação de relatórios e dashboards para dados de todas as fontes de dados ingeridas (endpoints, rede, e-mail, nuvem, etc.), seja por meio de criação de consultas (queries) ou a partir de cliques com o mouse.

2.87.2. Deve possuir dashboards pré-configurados que permitam a

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

visualização executiva dos principais incidentes e atividades no ambiente com base em usuários, aplicações acessadas e estações de trabalho/servidores.

2.87.3. Deve possuir, ao menos, 15 (quinze) dashboards em sua biblioteca, incluindo dashboards de fácil visualização de:

2.87.3.1. Alertas e incidentes mais frequentes;

2.87.3.2. Nível de risco do ambiente;

2.87.3.3. Relatório dos últimos 30 (trinta) dias da detecção de incidentes;

2.87.3.4. Top 10 (dez) ativos com incidentes;

2.87.3.5. Os ativos que mais sofreram incidentes em um determinado período;

2.87.3.6. Os usuários que mais sofreram incidentes em um determinado período;

2.87.3.7. Ativos e contas descobertas;

2.87.3.8. Ameaças descobertas e classificadas conforme a cadeia de ataque.

2.87.4. Deve permitir configuração de atualização do tempo de cada dashboard.

2.87.5. Deve permitir exportação dos relatórios para os seguintes formatos:

2.87.5.1. Planilha: CSV e/ou Excel;

2.87.5.2. Texto: HTML e/ou PDF.

2.88. A solução deve permitir o gerenciamento de usuários, funções e permissões.

2.89. A solução deve permitir a criação de usuários com permissões distintas, contendo no mínimo, permissão total e permissão para realizar investigações.

2.90. A solução deve permitir uma gestão de usuários, com recursos de permissionamento RBAC, onde usuários podem ser excluídos da console sem prejuízos à auditoria ou a funcionalidades.

2.91. A solução deve registrar todas as atividades efetuadas pelos seus usuários, permitindo auditoria das ações realizadas.

2.91.1. Registros de auditoria de usuários, administradores e componentes integrarão os dados do CONTRATANTE e serão exportáveis ao encerramento.

2.92. A solução deve disponibilizar APIs, com documentação e sem custo adicional, para integração com outras soluções.

MONITORAMENTO DEEP/DARK WEB (MONITORAMENTO DE MARCA E AMEAÇAS GLOBAIS)

2.93. A CONTRATADA deverá realizar serviços de monitoramento de

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

Deep/Dark Web por meio da solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos ofertada (nativamente ou por meio de solução complementar). Os serviços e a respectiva solução utilizada para a realização do monitoramento de Deep/Dark Web devem atender às seguintes especificações mínimas:

2.93.1. A solução de monitoramento de Deep/Dark Web deve ter como objetivo principal o rastreamento de salas, blogs, fóruns e sites na Deep/Dark Web para identificar informações relativas ao CONTRATANTE e seus colaboradores como: credenciais roubadas e outros vazamentos de informações pessoais identificáveis.

2.93.2. A solução de monitoramento de Deep/Dark Web deve estar licenciada para monitorar até 6 (seis) domínios DNS do CONTRATANTE e uma quantidade de no mínimo 500 (quinhentos) termos por domínio.

2.93.3. O serviço de monitoramento de Deep/Dark Web deve ser prestado no regime 24x7 (vinte e quatro horas por dia, sete dias por semana).

2.93.4. A solução de monitoramento de Deep/Dark Web deve realizar buscas, no mínimo:

2.93.4.1. Na Darknet;

2.93.4.2. Em plataformas de compartilhamento de documentos;

2.93.4.3. Pelas seguintes categorias:

2.93.4.3.1. Por Bucket: Darknet TOR, Whois, Usenet, Leaks, Bot Logs, Wikileaks, Public Leaks, Dumpster, Sci-Hub;

2.93.4.3.2. Por Site Público: .com, .org, .net, .info, .eu.

2.93.4.3.3. Por Geolocalização.

2.93.5. A solução de monitoramento de Deep/Dark Web deve permitir a busca de termos:

2.93.5.1. Domínio DNS;

2.93.5.2. Endereço de e-mail;

2.93.5.3. IP e CIDR;

2.93.5.4. Número de telefone;

2.93.5.5. Número do cartão de crédito;

2.93.5.6. URL.

2.93.6. Deve detectar resultados de itens pesquisa duplicados, apresentando-os de forma consolidada, otimizando a busca por informações relevantes.

2.93.7. A solução de monitoramento de Deep/Dark Web deve ter a

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

capacidade de buscar dados pelo período mínimo de 1 (um) ano.

2.93.8. A solução de monitoramento de Deep/Dark Web deve ter a capacidade de filtrar e classificar os resultados das buscas:

2.93.8.1. Com base na data ou no tempo de publicação das informações encontradas (antigas e novas);

2.93.8.2. Com base nos domínios, e-mails e URLs encontrados;

2.93.8.3. Com base nos resultados mais relevante, menos relevante, mais recente e mais antigo;

2.93.8.4. Com capacidade de combinar ou excluir termos de pesquisa a fim de encontrar com eficiência informações relevantes no banco de dados.

2.93.9. A solução de monitoramento de Deep/Dark Web deve ter a capacidade de manter históricos de resultados de busca.

2.93.10. A solução de monitoramento de Deep/Dark Web deve contemplar os seguintes itens:

2.93.10.1. Monitoramento de atividades na Deep/Dark Web relacionadas às informações sobre domínios, URLs, IPs, hashes, credenciais, e-mails e informações sensíveis do CONTRATANTE.

2.93.10.2. Amplitude de rastreamento contemplando dados e informações disponibilizadas na Deep/Dark Web como:

2.93.10.2.1. Monitoramento das credenciais de funcionários em listas e bases de dados de credenciais vazadas na Deep/Dark Web, marketplaces, entre outros;

2.93.10.2.2. Monitoramento do Pastebin, incluindo posts deletados e outros sites, buscando por referências sobre a empresa, domínios ou endereços IP;

2.93.10.2.3. Monitoramento de documentos vazados ou roubados da empresa em páginas da Deep/Dark Web e fóruns hackers;

2.93.10.2.4. Monitoramento de referências aos sistemas em páginas da Deep/Dark Web e fóruns hackers, além de Threat Intelligence e listas de IoC’s;

2.93.10.2.5. Busca de informações sobre redes sociais e plataformas de divulgação de vulnerabilidades vazadas na Deep/Dark Web.

2.93.10.3. Deve ser possível encontrar marketplaces, fóruns e agentes de ameaças;

2.93.10.4. Deve ser capaz de realizar avaliação da exposição da

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

PROAD n. 6891/2026 DOC 43
Cadastrado por lfarias - LEDIANE FERNANDES DE FARIAS
Juntado em 24/11/2026

MINUTA

marca e vazamentos de informações na Deep/Dark Web, até um total de 20 marcas, submarcas ou nomenclaturas;

2.93.10.5. Investigação de origens de vazamentos de, no mínimo:

2.93.10.5.1. Grupos de hackers;

2.93.10.5.2. Ameaças em fóruns;

2.93.10.5.3. Salas de chats reservadas;

2.93.10.5.4. Carteira de bitcoins e endereços;

2.93.10.5.5. Registros históricos.

2.93.10.6. As investigações deverão ser realizadas por uma equipe especializada à medida que informações monitoradas forem identificadas na Deep/Dark Web.

2.93.10.7. Geração e notificação de alertas acompanhados da enumeração das ameaças e riscos relacionados e ações de mitigação sugeridas.

2.93.11. A coleta e tratamento serão limitados à finalidade de segurança cibernética, vedada utilização diversa e observados necessidade, segurança, prevenção e responsabilização.

2.94. A solução como um todo, bem como os seus componentes devem contar com garantia e suporte integrais conforme especificado neste documento.

2.95. O serviço de segurança cibernética de Caças Ameaças (Threat Hunting) deverá ser realizado através de análise humana e operar em caráter contínuo, regime 24 horas x 7 dias da semana, em busca de ameaças cibernéticas, anomalias, comportamentos suspeitos e ou maliciosos, análise e revisão da telemetria gerada pelos dispositivos e estratégias avançadas utilizadas por atores maliciosos, sem a dependência de alertas ou detecções. Ou seja, as atividades listadas devem ocorrer independente de alertas e detecções.

REQUISITOS PARA PROTEÇÃO DE IDENTIDADES

2.96. A solução deverá fornecer capacidades de Detecção e Resposta a Ameaças de Identidade (ITDR) integradas à plataforma XDR para ambientes Active Directory (on-premises) e Entra ID (nuvem), sendo capaz de avaliar continuamente vulnerabilidades e riscos em credenciais, detectar ataques em andamento (incluindo técnicas como Password Spray, DCSync, Pass-the-Hash e Skeleton Key), prevenir ou identificar movimentações laterais associadas ao uso indevido de protocolos de administração remota e investigar comportamentos anômalos nos fluxos e acessos de autenticação que envolvam os protocolos Kerberos e NTLM.

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

2.97. A solução deverá suportar a detecção e monitoramento de identidades não-humanas, incluindo contas de serviço, aplicações, APIs e identidades gerenciadas.

2.98. A ferramenta deverá analisar o comportamento de cada conta de usuário e conta de computador, além de estabelecer o perfil comportamental padrão dos acessos comuns, com o intuito de alertar ou bloquear condições anormais, utilizando técnicas de User and Entity Behavior Analytics (UEBA), incluindo técnicas de análise comportamental avançada, estatística e/ou aprendizado de máquina.

2.99. A solução deverá possuir capacidade de detecção baseada em anomalia de protocolo, identificando desvios em protocolos de autenticação e comunicação de diretório que não correspondam aos padrões documentados ou ao comportamento legítimo de sistemas operacionais homologados, independentemente da assinatura de um ataque específico.

2.100. A solução deverá identificar caminhos de ataque (attack paths) que permitam a elevação de privilégios ou comprometimento de ativos críticos a partir de identidades com menor privilégio.

2.101. A solução deverá permitir a execução de ações de contenção imediata diretamente a partir do console ou de seus componentes técnicos (sensores/coletores), incluindo, no mínimo, mecanismos de invalidação de credenciais e sessões de autenticação, tanto em ambientes on-premises quanto em nuvem, de forma imediata e centralizada, devendo abranger credenciais Kerberos, tokens de autenticação e sessões ativas.

2.102. A solução deverá analisar configurações inadequadas, detalhar os riscos, o que deve ser feito para remediar, além de listar todas as identidades afetadas, incluindo minimamente:

2.102.1. Contas com SPN vulneráveis;
2.102.2. Utilização de protocolos vulneráveis como NTLMv1;
2.102.3. Contas configuradas para nunca expirar a senha;
2.102.4. Contas configuradas como uma política de senhas fraca;
2.102.5. Contas inativas;
2.102.6. Domain Controllers com o serviço Print Spooler em execução;
2.102.7. Caminhos onde contas regulares podem adotar para se tornarem contas privilegiadas.
2.102.8. Usuários com Account Lockout;
2.102.9. Alterações de senhas;
2.102.10. Alterações em contas;
2.102.11. Usuários desabilitados;
2.102.12. Usuários com senhas há muito tempo sem trocar;
2.102.13. Principais falhas de login;

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

2.102.14. Contas vulneráveis a Kerberoasting;
2.102.15. Contas vulneráveis a DCSync e Pass the Hash;
2.102.16. Informar se a conta KRBTGT precisa ser alterada para mitigar ataques como Golden Ticket;
2.102.17. Conta oculta identificada (contas que possuem configurações que impedem administradores de encontrá-las em buscas no serviço de diretório);
2.102.18. Identificação de permissões excessivas que possibilitem usuários comuns manipular políticas de acesso e autenticação de contas privilegiadas;
2.102.19. Identificar alterações no objeto AdminSDHolder;
2.102.20. Contas sincronizadas com o Entra ID que possuam privilégios excessivos ou MFA desabilitado.

2.103. A detecção de ameaças deverá ocorrer em tempo real ou próximo de tempo real e permitir que ações sejam tomadas para evitar que futuros ataques aconteçam, incluindo, mas não se limitando a ataques e técnicas, tais como:

2.103.1. Golden Ticket;
2.103.2. Suspicious Protocol Implementation (Pass the Hash);
2.103.3. NTLM Relay;
2.103.4. Suspicious LDAP Search (Kerberos Misconfiguration);
2.103.5. Suspicious LDAP search (Accounts);
2.103.6. DCSync;
2.103.7. Ataque DCSync com conta MSOL;
2.103.8. Ataques de DCShadow (replicação fraudulenta de objetos);
2.103.9. Forged PAC Attack;
2.103.10. Suspicious Kerberos Ticket Reuse;
2.103.11. Password Brute Force;
2.103.12. Credential Scanning;
2.103.13. Bronze Bit exploit;
2.103.14. CredSSP Vulnerability;
2.103.15. Skeleton Key Attack;
2.103.16. Pass-the-Ticket;
2.103.17. Overpass-the-Hash;
2.103.18. Token replay e abuso de tokens de autenticação;
2.103.19. Injeção de SID-History em contas de usuário;
2.103.20. Acesso incomum a um endpoint;
2.103.21. Acesso excessivo a múltiplos endpoints;
2.103.22. Atividade excessiva de acesso a múltiplos endpoints;

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

MINUTA

2.103.23. Acesso de um IP envolvido com outros incidentes ou qualificado como danoso pelo sistema de inteligência.
2.103.24. Administradores de Domínio com SPN;
2.103.25. Contas com senhas em branco;
2.103.26. Escalação de Privilégio via Grupo;
2.103.27. Atividades recentes vindas de contas dormentes;
2.103.28. Conta de computador - abuso de Serviços Kerberos para Usuário (S4U);

2.104. Para cada ataque identificado, a solução deverá minimamente fornecer as seguintes informações e possibilidades:
2.104.1. Data e hora da detecção;
2.104.2. Descrição do ataque;
2.104.3. Severidade;
2.104.4. Tática e técnica associada ao framework MITRE ATT&CK;
2.104.5. Conta comprometida;
2.104.6. Host de origem, de onde o ataque foi realizado;
2.104.7. Host de destino, quando o ataque está relacionado a uma movimentação lateral;
2.104.8. Recomendações com ações que devem ser realizadas para conter tal ataque;
2.104.8.1. Marcar o ataque como resolvido;
2.104.8.2. Marcar o ataque como falso positivo e não alertar ataques similares.

2.105. A solução deverá permitir a configuração de políticas de acesso para minimamente os seguintes cenários:
2.105.1. Em caso de detecção de um ataque pré-definido (como DCSync ou Pass the Hash), a solução deverá automaticamente adicionar a conta comprometida a uma lista de contenção; e, em seguida, bloquear ou restringir autenticações e sessões desta mesma conta, mediante aprovação manual ou configuração prévia de políticas de automação baseadas em níveis de confiança, com o fim de interromper uma movimentação lateral;
2.105.2. Impedir a autenticação (Logon) de usuários incluídos em lista de contenção;
2.105.3. Alertar ou bloquear quando usuários privilegiados sejam utilizados em horários fora do normal (como fora do horário comercial).

2.106. A solução deverá fornecer capacidades de investigação de contas de usuários e acessos suspeitos, permitindo minimamente a visualização de:

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

2.106.1. Autenticações realizadas, incluindo sucesso e falha, com capacidade de filtragem por usuário, origem e destino;

2.106.2. Eventos de replicação de domínio, Account Lockout e acesso RPC;

2.106.3. Acessos realizados por contas de serviço e por contas com privilégios específicos (como Domain Admin);

2.106.4. Capacidade de listar em tempo real todas as sessões ativas de um usuário em múltiplos endpoints.

2.107. Deverá ser possível emitir relatórios para as funcionalidades de proteção de identidade minimamente dos seguintes indicadores:

2.107.1. Account Lockouts por endpoint;

2.107.2. Account Lockouts por usuário;

2.107.3. Uso de NTLM por usuário;

2.107.4. Uso de NTLM por endpoint;

2.107.5. Resumo de novos incidentes de segurança relacionados às identidades;

2.107.6. Top 10 incidentes por severidade;

2.107.7. Top 10 usuários com riscos significativos;

2.107.8. Usuários que nunca efetuaram Logon no domínio;

2.107.9. Administradores inativos;

2.107.10. Administradores com privilégios ocultos.

2.108. A solução deverá possuir capacidade de detectar, correlacionar, alertar e responder a ameaças relacionadas a autenticações e identidades em tempo real ou próximo de tempo real, utilizando mecanismos nativos, integrações ou ações automatizadas compatíveis com sua arquitetura.

2.109. A solução deverá permitir ações de contenção e resposta a incidentes relacionados a identidades, de forma automatizada ou manual, utilizando recursos nativos e/ou integração com plataformas de segurança, autenticação ou orquestração

2.110. As ações de bloqueio, restrição ou contenção de autenticação deverão ser executadas diretamente pela solução, não dependendo exclusivamente de integrações externas para sua efetivação.

2.110.1. As ações automatizadas serão classificadas como automáticas, dependentes de aprovação ou proibidas, conforme Matriz de Autonomia definida pelo CONTRATANTE.

2.111. A capacidade de detecção e resposta a ameaças de identidade deverá estar disponível de forma nativa, não dependendo da criação manual de regras ou correlações para identificação de ataques conhecidos.

2.112. A solução não deverá depender exclusivamente da instalação de agentes em endpoints para detecção de ameaças de identidade, devendo ser

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

capaz de analisar autenticações diretamente a partir de controladores de domínio, serviços de diretório ou tráfego de autenticação.

2.113. A solução deverá prover visibilidade e proteção de identidades mesmo em sistemas que não suportam instalação de agentes, incluindo sistemas legados, dispositivos de rede e aplicações, por meio da análise de autenticações e credenciais.

2.114. A solução deverá apresentar encadeamento de eventos (timeline) permitindo a visualização da cadeia de ataque relacionada a uma identidade comprometida.

2.115. A solução deverá correlacionar eventos provenientes de múltiplas fontes, incluindo diretórios, autenticações, endpoints e sistemas integrados, para identificação de ataques complexos.

2.116. A solução deverá permitir o monitoramento e a rastreabilidade de alterações relacionadas a identidades, grupos e permissões no ambiente de diretório, incluindo registro e consulta de eventos associados.

2.117. A solução deverá fornecer evidências e contexto detalhado para cada detecção, permitindo a rastreabilidade e compreensão do motivo do alerta.

2.118. A solução deverá permitir a priorização de incidentes com base em risco agregado, considerando múltiplos fatores, como comportamento, exposição e criticidade da identidade.

2.119. A solução deverá identificar quando um usuário desativado tenta autenticar;

2.120. A solução deverá possuir capacidade de identificar comportamentos anômalos relacionados à autenticação e acesso às identidades, incluindo desvios de comportamento, padrões incomuns de acesso ou eventos suspeitos correlacionados;

2.121. A solução deverá identificar tentativas suspeitas relacionadas à autenticação NTLM, destacando comportamentos anômalos, como coleta de credenciais e volume incomum de autenticações em hosts de destino, permitindo a análise desses eventos em diferentes janelas de tempo, incluindo a última hora;

2.122. A solução deverá identificar quando um host procura se registrar como um novo controlador de domínio e alertar quando houver tráfego de sincronização de dados de um controlador de domínio legítimo;

2.123. A solução deverá identificar quando um usuário tenta se autenticar em um host via NTLM e não o fez nos últimos 30 dias;

2.124. Realizar Análise de Caminhos de Ataque, que é o mapeamento de como um invasor poderia realizar elevação de privilégio ou fazer movimentação lateral;

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

2.125. A solução deverá identificar comportamento que caracteriza uma quantidade excessiva de logins;

2.126. A solução deverá possuir módulo que seja capaz de identificar Brute Force em usuário e senha;

2.127. A solução deverá identificar contas de usuário que possuem permissões administrativas diretas (ACLs) em objetos do serviço de diretório, sem que estas contas pertençam formalmente a grupos de administradores;

2.128. A solução deverá fornecer uma pontuação de Risco por Usuário, calculado com base no comportamento e nas exposições da identidade, permitindo priorizar a investigação de contas com maior probabilidade de comprometimento;

2.129. A detecção de ameaças não deverá depender exclusivamente da ingestão de logs, devendo a solução ser capaz de identificar atividades maliciosas de forma independente, inclusive em cenários de evasão, como limpeza, manipulação ou ausência de logs. Todas as comunicações entre componentes da solução e os Controladores de Domínio devem priorizar o uso de protocolos seguros (como Kerberos ou LDAPS), evitando a utilização de protocolos legados sempre que tecnicamente possível (como NTLM).

2.130. A solução deverá funcionar em sua plenitude (com todos os recursos), sem depender de reboots nos Domain Controllers.

2.131. A solução deverá possuir capacidade de integração com ferramentas de segurança e infraestrutura, como SIEM, SOAR, EDR/XDR e soluções de gestão de identidade, por meio de APIs ou conectores nativos.

2.132. A solução deve possuir APIs documentadas para integração com ferramentas de orquestração (SOAR), permitindo que ações de contenção sejam disparadas de forma externa;

2.133. A solução deverá possuir mecanismos para identificação de tentativas suspeitas de enumeração, acesso indevido, movimentação lateral ou abuso de credenciais privilegiadas, podendo utilizar recursos nativos de detecção, análise comportamental, correlação ou tecnologias complementares;

MÓDULO DE SOAR AGÊNTICO

2.134. A solução deve dispor de agentes virtuais baseados em Inteligência Artificial integrados à solução capazes de interpretar alertas, formular hipóteses de investigação e tomar decisões de roteamento sem a necessidade de fluxogramas totalmente pré-configurados.

2.134.1. A utilização de IA não transfere à Administração responsabilidade pelas ações da plataforma. A CONTRATADA responderá pela operação, controles e rastreabilidade dos agentes.

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

2.135. O uso de módulo de SOAR agêntico consumirá *tokens* para execução de suas funções;

2.136. A CONTRATADA deve fornecer exemplos de cenários de uso de agentes inteligentes e seu consumo estimado de tokens;

2.137. Deverá existir alertas graduais (p. ex: 50%, 80%, 90%) de consumo e a possibilidade de bloqueios automáticos no uso da ferramenta a fim de evitar oneração imprevista acima do teto estabelecido pelo CONTRATANTE;

2.138. A quantidade de tokens contratados poderá ser utilizada durante todo o período contratual, sendo que o faturamento será sobre o número de tokens mensais previamente contratados até o limite estabelecido.

2.139. A solução deve operar de forma integrada combinando automações determinísticas (playbooks de regras fixas para execução previsível) e automações agênticas (IA adaptativa baseada em objetivos).

2.139.1. Alterações de playbook decorrentes de mecanismo agêntico deverão ser versionadas e registradas e observar a política de autorização antes de ações de alto impacto.

2.140. Capacidade de criar, implantar e gerenciar múltiplos agentes de IA autônomos e especializados (ex: Agente de Triagem, Agente de Investigação de Nuvem, Agente de Threat Hunting e Agente de Remediação).

2.141. Os agentes virtuais de inteligência artificial devem ser capazes de colaborar entre si, compartilhando contexto, dividindo tarefas complexas e orquestrando o fluxo de trabalho do incidente do início ao fim.

2.142. A solução deve permitir a criação automática de playbooks ou adaptação do fluxo de resposta em tempo real com base no raciocínio da IA, eliminando a dependência de manutenção de regras estáticas.

2.143. A solução deve permitir análise automatizada do alerta no momento de sua geração, atribuindo um índice de confiança (*confidence score*) e determinando se o alerta corresponde a um falso positivo ou uma ameaça real.

2.144. O agente deve ter capacidade de investigar árvores de processos, logs de chamadas de API em nuvem (ex: AWS, Azure, GCP), eventos de rede e telemetria de identidade de forma automatizada para correlacionar o ataque.

2.145. A solução deve permitir a identificação e mapeamento automático das táticas, técnicas e procedimentos (TTPs) utilizados pelo atacante durante a investigação do incidente.

2.146. A solução deve permitir a geração automática de narrativas detalhadas e resumos executivos do incidente em Português (Brasil) ou Inglês, cobrindo causa-raiz, cronologia dos fatos, ativos e identidades impactadas.

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

2.146.1. Resultados automatizados de causa-raiz serão apresentados como hipótese, acompanhados das evidências, grau de confiança e validação do analista.

2.147. A solução deve prover interface conversacional de suporte ao analista que permite realizar perguntas operacionais e investigativas sobre o ambiente de segurança em linguagem natural em Português ou inglês;

2.148. A solução deve sugerir os próximos passos de mitigação e remediação mais adequados com base no contexto específico da infraestrutura.

2.149. A solução deve permitir mecanismos de governança para limitar o nível de autonomia que cada agente de IA possui sobre a infraestrutura.

2.150. A solução deve permitir a possibilidade de configurar travas operacionais obrigatórias para que ações de contenção/resposta de alto risco (ex: isolar servidor crítico, revogar acesso de usuário VIP) dependam de autorização prévia por um operador humano.

2.151. A solução manterá registro auditável dos eventos, entradas relevantes, regras/políticas, agente, ação, resultado, data/hora e justificativa operacional, sem exigir exposição de raciocínio interno proprietário do modelo.

3. ITEM 5 – Requisitos mínimos de treinamento na solução

3.1. Deve ser realizado treinamento de administração e de operação da solução para até 10 (dez) profissionais da CONTRATANTE, contemplando, ao menos, os seguintes temas: instalação, configuração, operação e utilização da solução contratada.

3.1.1. O treinamento deve contemplar todos os recursos e configurações existentes na solução ofertada.

3.2. O treinamento deverá proporcionar aos participantes condições de:

3.2.1. Compreender a arquitetura da solução;

3.2.2. Identificar e configurar os recursos disponibilizados no produto;

3.2.3. Configurar fontes de eventos;

3.2.4. Instalar e configurar agentes, coletores e outros módulos necessários para o perfeito funcionamento da solução;

3.2.5. Configurar funcionalidade de deception, quando a solução tiver essa capacidade;

3.2.6. Configurar regras;

3.2.7. Configurar alertas;

3.2.8. Configurar playbooks;

3.2.9. Investigar incidentes;

3.2.10. Pesquisar em logs;

3.2.11. Criar dashboards;

3.2.12. Criar relatórios e agendamento de relatórios;

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

MINUTA

3.2.13. Gerenciar usuários, funções e permissões;

3.2.14. Identificar as possíveis causas de problemas e atuar na sua resolução;

3.2.15. Monitorar o funcionamento da solução (analisar mensagens de log, efetuar acesso remoto, atualizar os componentes que fazem parte da solução, administração e utilização dos recursos disponibilizados);

3.2.16. Conhecer os procedimentos para abertura de chamados técnicos;

3.2.17. Conhecer os procedimentos para obtenção de atualizações de software.

3.3. O treinamento deve ser oficial ou autorizado pelo fabricante da solução, devendo ser realizado na plataforma online do fabricante ou do centro autorizado de treinamento.

3.3.1. O conteúdo do treinamento poderá seguir o padrão de treinamento utilizado pelo fabricante para os módulos ofertados na solução, enquanto demais conteúdos que extrapolem o contexto padronizado do fabricante podem ser complementados pela CONTRATADA através de treinamento próprio.

3.4. O treinamento deve ser ministrado por pessoa certificada na solução.

3.5. A CONTRATADA deverá apresentar, juntamente à documentação técnica, a programação, conteúdo programático e carga horária do curso, a fim de serem ajustados às necessidades do CONTRATANTE.

3.6. É de responsabilidade da CONTRATADA todo material audiovisual, didático e eletrônico para a realização do treinamento.

3.7. O treinamento deve ter duração mínima de 40 horas.

3.8. O treinamento deverá ser ministrado em horário definido pelo CONTRATANTE, em dias úteis.

3.8.1. A critério da CONTRATANTE e havendo disponibilidade da CONTRATADA, o treinamento poderá ser realizado em meio-turno ou turno inteiro.

3.9. O treinamento deverá ser ministrado em língua portuguesa do Brasil.

3.10. O material escrito (PDF, apresentações, imagens etc) deverá ser fornecido, preferencialmente, em Português (Brasil). Em caso de não disponibilidade dessa versão, a mesma deverá ser disponibilizada em Inglês.

3.11. Deve ser realizado na modalidade telepresencial síncrona.

3.12. O prazo para execução do treinamento é de até 180 dias após a assinatura do contrato.

3.13. A CONTRATADA deverá fornecer, ao término, certificado de realização, em português do Brasil, para cada participante, contendo, no mínimo: nome do curso, carga horária, conteúdo programático, nome do instrutor e período de realização.

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

3.14. A CONTRATANTE poderá solicitar, sem custo adicional, a repetição total ou parcial do treinamento quando forem identificadas, mediante critérios objetivos de avaliação, falhas no cumprimento da carga horária, conteúdo programático, condições de realização ou requisitos mínimos estabelecidos neste instrumento, devendo a CONTRATADA realizar a nova capacitação em prazo acordado entre as partes.

3.15. O treinamento será aceito após comprovação da carga horária, conteúdo, participação e entrega dos materiais.

4. ITEM 6 – Requisitos mínimos de implantação da solução

4.1. A fase de ativação dos serviços deverá ser conduzida e concluída nos primeiros 60 dias corridos contados a partir da assinatura do contrato, quando serão executados o planejamento para implantação das ferramentas e a adequação de processos de gestão de segurança cibernética que nortearão a prestação de serviços do Centro de Operações de Segurança Cibernética (SOC).

4.1.1. A CONTRATADA deve realizar o planejamento, a implantação, configuração e ativação dos serviços e soluções propostas no prazo de até 60 dias corridos, contados a partir da assinatura do contrato, conforme objetivos, escopo, requisitos, premissas e demais condições elencadas nesta especificação.

4.2. As atividades que propiciarão criar, alterar e manter controles de segurança cibernética, além de medir a eficiência e eficácia dos serviços de SOC quanto à sua utilização dentro do negócio, serão adequadas nesta fase de ativação do contrato, conforme parâmetros (baseline) a serem acordados entre as partes.

4.3. Os papéis e responsabilidades das partes nos processos de gestão de segurança cibernética, bem como indicadores necessários para medir e melhorá-los continuamente, serão definidos também com base nos referidos parâmetros (baseline).

4.4. As atividades de implantação e ativação do contrato poderão ocorrer de forma remota e deverão contemplar, no mínimo, as seguintes fases:

4.4.1. Planejamento e Projeto:

4.4.1.1. Reunião de kick-off;

4.4.1.2. Coleta de dados e requisitos complementares;

4.4.1.3. Detalhamento de cronograma;

4.4.1.4. Apresentação de parâmetros (baseline) e adequação de processos de gestão de segurança cibernética.

4.4.2. Implantação, Configuração e Ativação da solução:

4.4.2.1. Instalação e ativação da solução on-line e console de gerência;

4.4.2.2. Instalação e ativação dos agentes, coletores, console de

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

gerência e demais componentes da solução (pertinentes aos ativos monitorados) no ambiente computacional do CONTRATANTE: servidores, estações de trabalho, firewalls, servidores de diretório e cloud;

4.4.2.3. Instalação e ativação dos coletores de logs;

4.4.2.4. Configuração e o correto funcionamento da coleta, processamento e correlação de logs de eventos em que a solução possua conectores nativos, ou seja, que não necessitem de customização de parsers para tal funcionamento (os conectores nativos devem contemplar a coleta, processamento e correlação de logs para os ambientes que constam nos itens 2.17.1, 2.18.1 e 2.19.1);

4.4.2.5. Testes e homologação.

4.4.3. Definição de Processos e Outras Configurações:

4.4.3.1. Implementação dos processos e recursos propostos;

4.4.3.2. Desenvolvimento de playbooks de resposta a ataques cibernéticos;

4.4.3.3. Configuração e correto funcionamento da coleta, processamento e correlação de logs de eventos em que haja a necessidade de customização de parsers para tal funcionamento (item 2.17.2).

4.4.3.4. Testes e homologação;

4.4.3.5. Desenvolvimento de um plano de continuidade que contemple minimamente a exportação de:

4.4.3.5.1. Base de incidentes em aberto (em tratamento);

4.4.3.5.2. Playbooks implementados.

4.4.4. Treinamento de equipes.

4.4.5. Operação, Sustentação e Melhoria Contínua:

4.4.5.1. Sustentação/On-Going;

4.4.5.2. Reunião mensal;

4.4.5.2.1. Relatórios periódicos;

4.4.5.2.2. Acompanhamento de indicadores;

4.4.5.2.3. Melhoria contínua.

4.5. A lista de soluções constantes nos itens 2.13, 2.17, 2.18 e 2.19 não é exaustiva, de forma que, conforme houver evolução do parque tecnológico ao longo do contrato, a CONTRATADA deve, como parte da operação, sustentação e melhoria contínua da solução, realizar a configuração para o correto funcionamento de parsing (quando houver), coleta, processamento e correlação de logs de eventos gerados pela novas soluções incluídas/alteradas no ambiente computacional.

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

5. ITENS 7 e 8 – Requisitos mínimos do serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos

5.1. Para o item 7, considera-se que o valor trata-se de custo fixo mensal referente à construção da infraestrutura mínima necessária para atendimento aos requisitos do item presentes neste instrumento, considerando 2.000 ativos por mês monitorados;

5.2. O item 8 refere-se ao monitoramento de ativos além da quantidade basal prevista para o item 7. A unidade de medida será mensurada em múltiplos de 1.000 ativos monitorados por mês, proporcional à quantidade de ativos monitorados. Por exemplo: uma contratação de 3200 ativos do item 1, implicam em 1 unidade do item 7 e 2 unidades do item 8;

5.3. Os serviços deverão ser prestados por meio do Centro de Operações de Segurança Cibernética (SOC) da CONTRATADA, em regime 24x7x365, que deverá atender os seguintes requisitos mínimos:

5.3.1. A prestação dos serviços deverá ser feita a partir de Centro de Operações de Segurança Cibernética especializado, sendo remoto às instalações do CONTRATANTE.

5.3.2. A equipe do SOC poderá, a critério da CONTRATADA, ser compartilhada com outros clientes, incluindo outros Órgãos da Justiça do Trabalho, de modo a otimizar os esforços, respeitando a confidencialidade das informações relativas ao objeto deste instrumento.

5.3.3. A solução contratada deve ter instância própria para o CONTRATANTE, exclusiva e dedicada para cada Tribunal e sem compartilhamento com outros clientes da CONTRATADA.

5.3.4. A CONTRATADA deve indicar, formalmente, quando da assinatura do contrato, PREPOSTO TITULAR e substituto que tenham capacidade gerencial para tratar de todos os assuntos previstos no instrumento contratual e coordenação da equipe para a execução dos serviços contratados.

5.3.5. O PREPOSTO deve, entre outras atividades, promover os contatos com o gestor do contrato bem como deve prestar atendimento aos profissionais em serviço, tais como:

5.3.5.1. Assegurar de que as determinações do CONTRATANTE sejam disseminadas junto aos profissionais alocados com vistas à execução dos serviços contratados;

5.3.5.2. Informar ao gestor do contrato sobre problemas de qualquer natureza que possam impedir o bom andamento dos serviços contratados;

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

5.3.5.3. Desenvolver atividades administrativas de responsabilidade da CONTRATADA, principalmente quanto ao controle de informações relativas ao seu faturamento mensal e apresentação de documentos quando solicitado;

5.3.5.4. O PREPOSTO não pode ser contabilizado como profissional para execução dos serviços contratados.

5.3.6. Os serviços de operação e gestão da solução deverão ser fornecidos diretamente pela CONTRATADA, devendo a mesma ser autorizada ou ser parceira do fabricante da solução XDR para fornecer serviço de MDR (Managed Detection and Response).

5.3.7. O compartilhamento de profissionais não poderá comprometer capacidade, SLAs ou segregação lógica. A CONTRATADA manterá controles de acesso e menor privilégio.

5.3.8. A CONTRATADA deverá disponibilizar um canal de comunicação por telefone, celular ou 0800 com o serviço de SOC em regime 24x7;

5.4. A CONTRATADA deve possuir um "Computer Security Incident Response Team (CSIRT)", ou Grupo de Resposta a Incidentes de Segurança – grupo de pessoas com a responsabilidade de identificar, receber, analisar e investigar as notificações e atividades relacionadas a incidentes de segurança cibernética nos ativos monitorados e orientar o CONTRATANTE quanto ao que deve ser feito para resolver o incidente de segurança cibernética.

5.5. Os incidentes de segurança cibernética são os relacionados aos eventos de segurança dos ativos monitorados como: ataques de movimentação lateral, escalação de privilégios, acessos indevidos, instalações de códigos maliciosos, ataques por força bruta, ou qualquer outra ação passível de monitoramento pela solução proposta e que possa comprometer a confidencialidade, disponibilidade, integridade ou privacidade das informações do CONTRATANTE.

5.6. Um incidente de segurança é definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação do CONTRATANTE, levando à perda de um ou mais princípios básicos de segurança cibernética: confidencialidade, integridade, disponibilidade ou privacidade.

5.7. O processo de notificação de incidentes de segurança se inicia sempre que um evento adverso for submetido por qualquer ferramenta de segurança, podendo o corpo técnico de segurança deste CONTRATANTE a qualquer momento, abrir um incidente de segurança junto à CONTRATADA.

5.8. O CONTRATANTE deverá ser informado sobre os incidentes detectados através do Portal de Atendimento, e-mail e/ou por telefone, conforme previamente acordado

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

com a CONTRATADA na fase de Planejamento e Projeto (item 4.4.1).

5.9. As solicitações de serviços e as notificações de incidentes de segurança cibernética reportadas pela solução proposta ou pelo CONTRATANTE deverão ser registradas no módulo de gestão de incidentes de segurança da solução ofertada (item 2.5.4).

5.10. Todo tipo de comunicação e documentação relacionados aos tratamentos de incidentes devem ser em Português.

OPERAÇÃO E SUSTENTAÇÃO

5.11. Os serviços de operação e sustentação da solução contemplam todas as atividades de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos identificados pela solução ofertada, bem como a sustentação da mesma, mediante a sua operação por parte da CONTRATADA.

5.12. Os seguintes serviços deverão ser realizados pela equipe da CONTRATADA para a operação da solução proposta:

5.12.1. Ativação e configuração dos módulos contratados;

5.12.2. Integração dos componentes contratados com o ambiente do CONTRATANTE;

5.12.3. Gestão do ciclo de vida da solução, contemplando a sua implantação e operação, além da inclusão, alteração e exclusão de ativos monitorados;

5.12.4. Abrir e fazer a triagem de chamados de segurança cibernética;

5.12.5. Fazer primeiro atendimento de reportes de incidentes de segurança cibernética;

5.12.6. Atender incidentes simples, os quais possuem instruções indicadas em playbooks (knowledge Base do ITSM);

5.12.7. Elaborar consultas(queries)/scripts de rastreamento quando necessário e/ou solicitados pelo CONTRATANTE;

5.12.8. Elaborar manual de usuário das atividades que se fizerem necessários e/ou solicitados pelo CONTRATANTE;

5.12.9. IPs externos deverão ser analisados e contextualizados conforme sua criticidade;

5.12.10. Fazer passagem de turno, acompanhar os incidentes e realizar “follow-ups”, de modo que haja acompanhamento integral dos tickets abertos;

5.12.11. Prestar suporte/apoio ao processo de automação das atividades relacionadas à resposta e tratamento de incidentes cibernéticos;

5.12.12. Desenvolvimento de playbooks de resposta a ataques cibernéticos;

5.12.13. Configuração de fontes de eventos;

5.12.14. Configuração de usuários VIP e usuários de serviço;

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

5.12.15. Criação de alertas customizados;
5.12.16. Configuração de coletores de eventos;
5.12.17. Configuração de monitoramento de arquivos e diretórios;
5.12.18. Liberação de acesso à solução para usuários autorizados pelo CONTRATANTE;
5.12.19. Geração de indicadores de performance (KPI) definidos neste documento e acordados na fase de Planejamento e Projeto (item 4.4.1);
5.12.20. Zelar e empregar todos os esforços necessários para garantir o atendimento ao SLA estabelecido neste instrumento, tanto no que se refere aos serviços quanto às soluções contratadas;
5.12.21. Atualização da solução, quando necessário/aplicável e/ou solicitados pelo CONTRATANTE;
5.12.22. Resolução de chamados de suporte junto ao(s) fabricante(s) da solução.

5.13. A equipe da CONTRATADA deve ter, no mínimo, uma pessoa responsável pelos assuntos técnicos (líder técnico) e que será o ponto de contato com a equipe de segurança cibernética do CONTRATANTE. O líder técnico tem, entre outras responsabilidades:

5.13.1. Após a assinatura do contrato, conhecer o parque tecnológico e as atividades em andamento, visando à preparação da equipe que prestará os serviços, conhecer os modelos de serviços realizados, as normas internas, procedimentos de segurança e a definição dos requisitos necessários;
5.13.2. Fazer uma reunião semanal com a equipe do CONTRATANTE para acompanhamento dos resultados (a frequência da reunião poderá ser revista oportunamente, a critério do CONTRATANTE).
5.13.3. Fazer a entrega e apresentação dos relatórios mensais, conforme especificação técnica contida neste documento;
5.13.4. Esclarecer dúvidas em relação às requisições, alertas, incidentes, relatórios, prazos de atendimento e outras atividades de responsabilidade da equipe da CONTRATADA;
5.13.5. Estar disponível por telefone e e-mail, de segunda a sexta-feira, das 9 (nove) às 18 (dezoito) horas e acessível por contato telefônico em qualquer outro horário (incluindo sábados, domingos e feriados).

INTELIGÊNCIA DE AMEAÇAS

5.14. A equipe da CONTRATADA deve prover serviços de pesquisa e desenvolvimento de

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

inteligência (threat intelligence) para proteção contra ataques cibernéticos, sendo responsável por:

5.14.1. Pesquisar novos tipos de ataques, vírus, malwares, botnets, vulnerabilidades e afins com intuito de melhoria contínua de detecção e mitigação destes males dentro dos serviços e ativos de segurança fornecidos pela CONTRATADA;

5.14.2. Criar, em colaboração com a equipe de segurança cibernética do CONTRATANTE, casos de uso (regras) que devem ser implementados na solução fornecida;

5.14.3. Revisar, sempre que necessário e/ou solicitados pelo CONTRATANTE, as regras da solução fornecida, realizando as adaptações e evoluções necessárias;

5.14.4. Produzir e entregar informação de inteligência acionável, na forma de procedimentos para triagem de alertas e procedimentos para notificação de incidentes correspondentes às regras da solução ofertada;

5.15. A equipe da CONTRATADA deve fornecer serviço de Password e Credential Assessment (avaliação de credenciais em serviços de diretório e banco de dados):

5.15.1. A solução deve avaliar o nível de dificuldade de quebra de senhas.

5.15.2. A solução deve avaliar possíveis vazamentos de credenciais na Dark/Deep Web.

5.15.3. O serviço deve poder ser executado sob demanda.

5.15.4. O serviço deve ser executado sem que senhas sejam fornecidas.

MONITORAMENTO E DETECÇÃO DE AMEAÇAS E ATAQUES

5.16. A equipe da CONTRATADA deve atuar no monitoramento dos incidentes detectados pela solução e serviços propostos, sendo responsável por:

5.16.1. Monitorar equipamentos e softwares componentes das soluções de segurança do CONTRATANTE, envolvendo identificação, classificação e análise de eventos que possam comprometer a disponibilidade, integridade e confidencialidade dos serviços.

5.16.2. Focar suas ações nos eventos significativos, classificando-os corretamente conforme as categorias abaixo:

5.16.2.1. Informativos: são eventos que não requerem ação, utilizados para verificação de funcionalidades dos ativos monitorados, ou seja, tem por objetivo identificar se as ferramentas e soluções estão tendo o comportamento esperado. São úteis para gerar informações acerca do

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

ambiente monitorado como, por exemplo, quantidade de eventos gerados nas últimas 24 (vinte e quatro) horas.

5.16.2.2. Avisos: são eventos utilizados para classificar comportamentos anômalos comparados à linha de base de operação do ambiente, porém que ainda não gerou impacto ao ambiente do CONTRATANTE como, por exemplo, espera-se que ocorram 10 bloqueios de um determinado hash diariamente e, entretanto, nos últimos 2 (dois) dias ocorreram 100 bloqueios, sendo que a ferramenta de antivírus continua bloqueando sem que haja qualquer impacto ou degradação no ambiente.

5.16.2.3. Exceções: são eventos que podem indicar que houve impacto em um ou mais dos pilares da segurança da informação (confidencialidade, integridade e disponibilidade) como, por exemplo, a ferramenta de antivírus não bloqueou a ação de um ransomware e dados do CONTRATANTE foram criptografados. Caso um evento seja classificado como "Exceção", o processo de resposta a incidentes de segurança deve ser iniciado imediatamente.

5.16.3. Comunicar, à equipe de segurança cibernética do CONTRATANTE, as informações iniciais sobre o incidente de segurança e quais serão as linhas de atuação para sua resolução.

5.16.4. Informar ao CONTRATANTE, através do Portal de Atendimento, e-mail e/ou por telefone, conforme previamente acordado com a CONTRATADA na fase de Planejamento e Projeto (item 4.4.1), sobre os incidentes detectados.

5.16.5. Emitir relatórios mensais, provendo, no mínimo, as seguintes informações ao CONTRATANTE:

5.16.5.1. Alertas e notificações;

5.16.5.2. Quantidade de incidentes por categoria;

5.16.5.3. Quantidade de incidentes por criticidade (severidade);

5.16.5.4. Quantidade de incidentes que geraram crise;

5.16.5.5. Porcentagem dos incidentes originários do monitoramento;

5.16.5.6. Quantidade de incidentes tratados/fechados;

5.16.5.7. Quantidade de incidentes registrados.

5.16.6. Relativo ao monitoramento de Deep/Dark Web, a CONTRATADA deverá prover, no mínimo, os seguintes serviços:

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

5.16.6.1. Monitoramento e envio de notificações para a equipe técnica do CONTRATANTE contendo os alertas identificados no regime 24x7 (vinte e quatro horas por dia, sete dias por semana);

5.16.6.2. Serviço de investigação pela equipe técnica da CONTRATADA, contendo os alertas identificados e sugestões de mitigação, em regime 8x5 (oito horas por dia, cinco dias por semana);

5.16.6.3. Envio de um relatório ao fim do mês ao CONTRATANTE contendo, no mínimo, as informações a seguir:

5.16.6.3.1. Vazamento de dados do CONTRATANTE que foram encontrados na Deep/Dark Web, através do monitoramento de domínios, IPs, e e-mails.

5.16.6.3.2. Descrição do ambiente avaliado;

5.16.6.3.3. Tabela resumo de serviços descobertos, detecções e alertas;

5.16.6.3.4. Descrição detalhada dos alertas;

5.16.6.3.5. Descrição, evidências, screenshots relevantes e recomendações para mitigação dos riscos;

5.16.6.3.6. Testes executados e relatórios técnicos das ferramentas;

5.16.6.3.7. Apresentação técnica dos resultados, incluindo o detalhamento dos eventos identificados.

RESPOSTA E INVESTIGAÇÃO A INCIDENTES CIBERNÉTICOS

5.17. A equipe da CONTRATADA deve atuar no processo de resposta a incidentes detectados pela solução proposta, sendo responsável por:

5.17.1. Analisar, recomendar ações de remediação e contenção e documentar os eventos de segurança que, após analisados, demonstraram ser um ataque ao ambiente do CONTRATANTE, tendo sido categorizados como "Eventos de Exceção" e, portanto, acionado o processo de resposta a incidentes cibernéticos.

5.17.2. Analisar, após um incidente de segurança ser aberto, os logs e artefatos enviados/coletados a fim de, no primeiro instante, identificar as fontes geradoras de tais eventos.

5.17.3. Identificar, uma vez realizadas as análises iniciais do incidente, quais foram os principais vetores de ataque ao ambiente do CONTRATANTE.

5.17.4. Definir, junto à equipe de segurança cibernética do

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

CONTRATANTE, a severidade do incidente de segurança, que será obtida por meio de uma matriz GUT (Gravidade, Urgência e Tendência).

5.17.4.1. A matriz GUT será definida na fase de Planejamento e Projeto (item 4.4.1) pela CONTRATADA em conjunto à equipe de segurança cibernética do CONTRATANTE.

5.17.5. Apoiar a equipe técnica do CONTRATANTE nos processos de mitigação, contenção de ataques e restauração do seu ambiente tecnológico.

5.17.6. Realizar, após análises iniciais do incidente e a definição de severidade, uma análise aprofundada do incidente baseando-se no comportamento do ataque e/ou artefato (malware).

5.17.7. Documentar todo o processo de análise e resultado no módulo de gestão de incidentes de segurança da solução ofertada (item 2.5.4) para que a equipe de segurança cibernética do CONTRATANTE acompanhe os passos para a solução do incidente de segurança.

5.17.8. Definir e documentar, uma vez identificado o comportamento e os principais vetores de ataque, uma estratégia para a mitigação e contenção do ataque em questão e notificá-la ao CONTRATANTE.

5.17.8.1. Qualquer tipo de alteração no parque computacional do CONTRATANTE para contenção e mitigação de incidentes de severidade alta ou crítica, deverá ser executada pelo próprio CONTRATANTE com o suporte da CONTRATADA, que deverá sugerir a melhor maneira de implantar a estratégia definida por ela para a resposta ao ataque, até a efetiva resolução do incidente.

5.17.9. Iniciar, mitigado o incidente de segurança, o processo de compilação de todas e quaisquer evidências e identificação dos serviços afetados. Tais evidências serão utilizadas até a finalização do processo para execução de eventual análise forense do incidente de segurança.

5.17.9.1. A necessidade de análise forense será indicada pelo CONTRATANTE, seguindo os seus processos internos de gestão de incidentes de segurança, a serem apresentados na fase de Planejamento e Projeto (item 4.4.1).

5.17.9.2. Os dados coletados devem ser reunidos durante o processo de tratamento de incidente para subsidiar futura

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

e eventual análise forense, seguindo as etapas de preservação, extração, análise e laudo. Tal análise deve ser realizada com o objetivo de identificar pessoas, locais ou eventos, correlacionando todas as informações reunidas e gerando como produto final um laudo sobre o incidente de segurança em questão.

5.17.10. Reconstruir o ataque, caso seja necessário e/ou solicitado pelo CONTRATANTE. Esta ação deve ser realizada pela CONTRATADA em ambiente controlado (como um sandbox), utilizando mecanismos de segurança para separar programas em execução, geralmente utilizado em um esforço para mitigar falhas de sistema ou vulnerabilidades de segurança cibernética.

5.17.11. Documentar, no módulo de gestão de incidentes de segurança da solução ofertada (item 2.5.4), as lições aprendidas do incidente de segurança em questão, formando, durante todo o período de vigência do contrato, uma grande base de conhecimento sobre ataques adversos.

5.17.11.1. A solução deve permitir a exportação da base de conhecimentos para formato Word ou PDF.

5.18. O regime de execução dos serviços deve ser 24x7x365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias ao ano).

CONFIDENCIALIDADE E DESCARTE DE INFORMAÇÕES

5.19. Confidencialidade**:**

5.19.1. A CONTRATADA deve ser responsável pelo ciclo de vida das informações coletadas pela solução proposta, atendendo aos critérios definidos pelo CONTRATANTE, devendo processar, armazenar e, após o término da sua finalidade, descartar os dados de maneira segura.

5.19.1.1. A CONTRATADA obriga-se a tratar como “segredos comerciais e confidenciais” quaisquer informações, dados, processos, fórmulas, códigos, obtidos em consequência ou por necessidade desta contratação, utilizando-os apenas para as finalidades previstas no contrato, não podendo revelá-los ou facilitar a revelação a terceiros, mediante assinatura dos Termo de Compromisso com a Segurança da Informação (Anexo II);

5.19.2. Ao final do contrato, o descarte das informações deve ser

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

MINUTA

realizado com o emprego de medidas que impossibilitem a sua reconstrução, de acordo com as necessidades do suporte físico ou digital.

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

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

CONTRATO TRT4 nº @/202@ - Anexo II

TERMO DE COMPROMISSO COM A SEGURANÇA DA INFORMAÇÃO

A empresa _____, parte CONTRATADA no contrato___/____, neste ato representado pelo(a) Sr.(a)_____, portador(a) da CI/RG n.º _____ e do CPF nº _____, compromete-se, por intermédio do presente termo, a não divulgar sem prévia autorização informações confidenciais pertencentes ou custodiadas pelo **TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO (TRT4)** às quais tiver acesso em decorrência da prestação do objeto do citado contrato, em conformidade com as seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA: Consideram-se informações confidenciais aquelas referentes a dados pessoais e dados pessoais sensíveis existentes no ambiente tecnológico ou físico do TRT4 ou por ele contratado, bases de dados, topologias, planos, políticas, processos, códigos-fonte, serviços e sistemas tecnológicos vinculados ao TRT4.

§ 1º Em relação aos dados pessoais e dados pessoais sensíveis do TRT4, a CONTRATADA deverá realizar o tratamento de acordo com o disposto nas cláusulas *de Proteção de Dados* do instrumento contratual.

§ 2º – Em caso de dúvida acerca da confidencialidade de determinada informação, a CONTRATADA deverá tratar a mesma sob sigilo até que venha a ser autorizada por escrito pelo TRT4 a tratá-la diferentemente. De forma alguma se interpretará o silêncio do TRT4 como a liberação do compromisso de manter o sigilo da informação.

§ 3º Excluem-se das disposições desta Cláusula informações que já estiverem comprovadamente disponíveis ao público em geral de qualquer forma que não em decorrência de sua revelação pela CONTRATADA.

CLÁUSULA SEGUNDA: A CONTRATADA concorda que as informações às quais terá acesso serão utilizadas exclusivamente no desempenho das atividades necessárias para execução do objeto contratado, em conformidade com o presente TERMO.

CLÁUSULA TERCEIRA: A CONTRATADA obriga-se a conhecer e observar a Política de Segurança da Informação disponível no site do TRT4.

CLÁUSULA QUARTA: A CONTRATADA compromete-se a aplicar boas práticas de mercado relacionadas à segurança da informação (como, por exemplo, ABNT NBR 27002:2019, CIS *Controls*, OWASP, NIST *Cybersecurity Framework*, dentre outras), pertinentes ao serviço prestado, para garantir a segurança do seu ambiente tecnológico de forma a atender os Acordos de Níveis de Serviços (ANS) e os Acordos de Nível Operacional (ANO) estabelecidos em contrato, bem como garantir a proteção da confidencialidade, integridade e disponibilidade das informações do TRT4 que vierem a ser tratadas em seu ambiente tecnológico.

CLÁUSULA QUINTA: A CONTRATADA determinará a todos os seus representantes - assim considerados, diretores, administradores, sócios, empregados, prepostos, agentes, colaboradores e prestadores de serviço a qualquer título (incluindo consultores e assessores) que estejam, direta ou indiretamente, envolvidos com a prestação de serviços - a observância do presente Termo, adotando todas as precauções e medidas para que as obrigações oriundas do presente instrumento sejam efetivamente observadas.

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

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

CLÁUSULA SEXTA: Caso a CONTRATADA seja obrigada, em decorrência de intimação de autoridade judiciária ou fiscal, a revelar quaisquer informações, notificará por escrito ao TRT4, em até 24 horas, acerca da referida intimação, de forma a permitir que o TRT4 possa optar entre interpor a medida cabível contra a ordem judicial ou administrativa ou consentir, por escrito, com a referida revelação.

CLÁUSULA SÉTIMA: A CONTRATADA obriga-se a informar ao TRT4, em até 24 horas, qualquer violação das regras de sigilo ora estabelecidas que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo, bem como de seus empregados, prepostos e prestadores de serviço.

CLÁUSULA OITAVA: A CONTRATADA obriga-se a informar, em até 24 horas, ao TRT4 a ocorrência de incidentes, tecnológicos ou não, que possam comprometer (ou possam ter comprometido) a confidencialidade, integridade ou a disponibilidade das informações do TRT4 que são tratadas em seu ambiente tecnológico ou o cumprimento de ANS e ANO, bem como as medidas adotadas para contenção, tratamento, resposta e erradicação dos incidentes.

CLÁUSULA NONA: O descumprimento de quaisquer das cláusulas do presente Termo acarretará a responsabilidade civil e criminal dos que, comprovadamente, estiverem envolvidos no descumprimento ou violação.

Documento assinado digitalmente
@@@@@@@@@@@@@@@
CPF nº @@@@@@@

PROAD n. 6891/2026 DOC 43. Para verificar a autenticidade desta cópia, acesse o seguinte endereço eletrônico e informe o código 2026.WGLJ.QYGW: https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml