TRIBUNAL REGIONAL ELEITORAL DE MATO GROSSO DO SUL

ESTUDO PRELIMINAR - CONTRATAÇÕES DE TIC

1. ESTUDO TÉCNICO PRELIMINAR - SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

1.1 SOLUÇÃO DE TI A CONTRATAR

Monitoramento de segurança dos dados que trafegam dentro do ambiente computacional interno do Regional, para prevenção de ataques cibernéticos, com adoção de tecnologias de análise de comportamento e inteligência artificial, a partir deste momento denominada apenas Solução.

1.2 EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

A equipe responsável pelo planejamento da contratação é composta pelos seguintes membros:

Tipo	Nome	Lotação	E-mail
Demandante	Antônio Mendes Barata Segundo	STI / ATSIC	antonio.barata@tre-ms.jus.br
Técnico	Robson Massaki Kobayashi	STI / CITIS / SGI	robson.kobayashi@tre-ms.jus.br
Técnico	Gustavo Leite Pinho	STI / ATSIC	gustavo.pinho@tre-ms.jus.br
Administrativo	Graziela Gonçalves Silva Jurado	SAOF / CRM / SLC	graziela.goncalves@tre-ms.jus.br
Administrativo-substituta	Sônia Aparecida Granja Anelli	SAOF / CRM / SLC	sonia.anelli@tre-ms.jus.br

1.3 DEFINIÇÃO E ESPECIFICAÇÃO DOS REQUISITOS E DA NECESSIDADE DA CONTRATAÇÃO

"Não se pode proteger o que não se conhece."

A Secretaria de Tecnologia da Informação tem por atribuição o provimento de soluções informatizadas, que busquem prover segurança quanto aos riscos e ameaças internas e externas.

Porém, os desafios são enormes. A equipe de cibersegurança do TRE-MS é pequena frente às diversas frentes que compõem a segurança de um Órgão com ambiente computacional que há muito deixou de ser pequeno e é neste momento de porte médio.

Além disso, o cenário atual do Poder Judiciário Brasileiro reflete um processo acelerado de transformação digital, no qual as soluções tecnológicas se tornam imprescindíveis para uma prestação jurisdicional mais efetiva. Essa efetividade só ocorrerá com a devida e correspondente proteção de dados, informações e usuários.

Se por um lado, a presença do TRE-MS em soluções digitais tem aumentado com velocidade, por outro lado também têm aumentado a superfície de ataques, deixando o Regional mais vulnerável.

O cenário de crimes cibernéticos vem passando por um processo de grande sofisticação, com uma escalada de ataques amplamente divulgados pela mídia, Internet e redes sociais.

De acordo com o levantamento Panorama de Ameaças para a América Latina 2024, o Brasil é o segundo país com mais ataques cibernéticos no mundo. Com mais de 700 milhões de tentativas registradas em 12 meses (o equivalente a 1.379 por minuto), o país fica atrás apenas dos Estados Unidos. (Fonte: Agência Senado - Criação de agência contra ataques cibernéticos ganha força em subcomissão — Senado Notícias) [Acesso em 31/03/2025].

Esse ambiente hostil evoluiu a partir de suas origens baseadas na disseminação de malwares em conjunto com ataques mais sofisticados de Roubo de Identidades, Ransomware, Vazamento de Dados, Sequestro de Dispositivos, Phishing direcionado a pessoas chave ligadas à Instituição e Ameaças Avançadas Persistentes, que determinam um alvo e buscam todas as formas de invadi-lo até que tenham sucesso.

Os agentes maliciosos têm desenvolvido ferramentas e técnicas cada vez mais sofisticadas, utilizando mecanismos de ampliação e furtividade, e os serviços de defesa, precisam, por sua vez, cada vez mais utilizar-se de ferramentas mais rápidas e eficazes para tentar evitar ou conter danos.

De acordo com o Relatório de Ameaças Globais de 2025 da empresa CrowdStrike (https://go.crowdstrike.com/2025-global-threat-report-thank-you.html) [Acesso em 02/04/2025], estatísticas destacam a necessidade de utilização de estratégias de segurança que levem em conta o alcance global de operações maliciosas que adotam o comprometimento de identidade, a movimentação lateral e os vetores de ataque baseados em nuvem, ambos sem uso de um malware específico para ataque e isso tem sido uma tendência definidora nos últimos cinco anos.

Em 2024, a atividade sem malware foi responsável por 79% das detecções, um aumento significativo em relação aos 40% de 2019, conforme pode ser observado no gráfico a seguir:

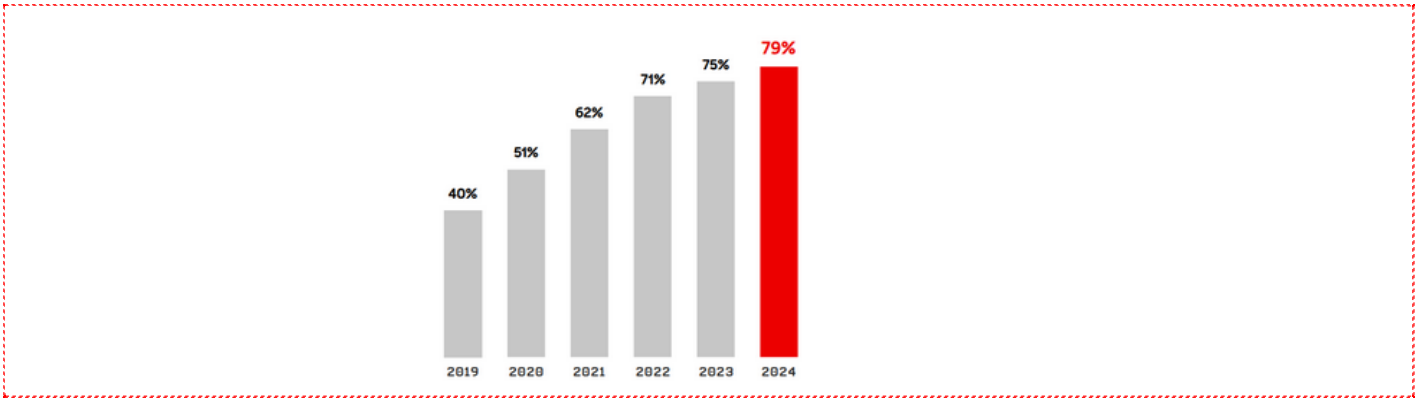

Gráfico 01: Percentual de detecções sem uso de malware

Tal crescimento está associado ao uso crescente da Inteligência Artificial – IA e Machine Learning – ML em ataques.

Ainda segundo o mesmo relatório, o tempo furtivo —tempo gasto para um ator malicioso começar a se mover lateralmente pela sua rede — atingiu o menor nível histórico em 2024. A média caiu para 48 minutos, com tempo de fuga mais rápido identificado de apenas 51 segundos, algo pouco provável de ser executado por um operador humano.

O uso da IA e ML vem desempenhando um papel fundamental em cibersegurança. Considerando o grande volume de dados e ativos, as capacidades avançadas de análise de dados da IA são cada vez mais utilizadas para identificar e prever ameaças cibernéticas e melhorar os sistemas de detecção precoce. Os algoritmos de ML estão evoluindo para melhor reconhecer e responder a novas ameaças, aprimorando as medidas defensivas ao longo do tempo.

O relatório do World Economic Forum em parceira com o Global Cyber Security Capacity Centre da Universidade de Oxford (WEF_Artificial_Intelligence_and_Cybersecurity_Balancing_Risks_and_Rewards_2025.pdf (weforum.org)[Acesso em 31/03/2025], apresenta como o impacto da IA na segurança cibernética pode ser considerado em três categorias amplas:

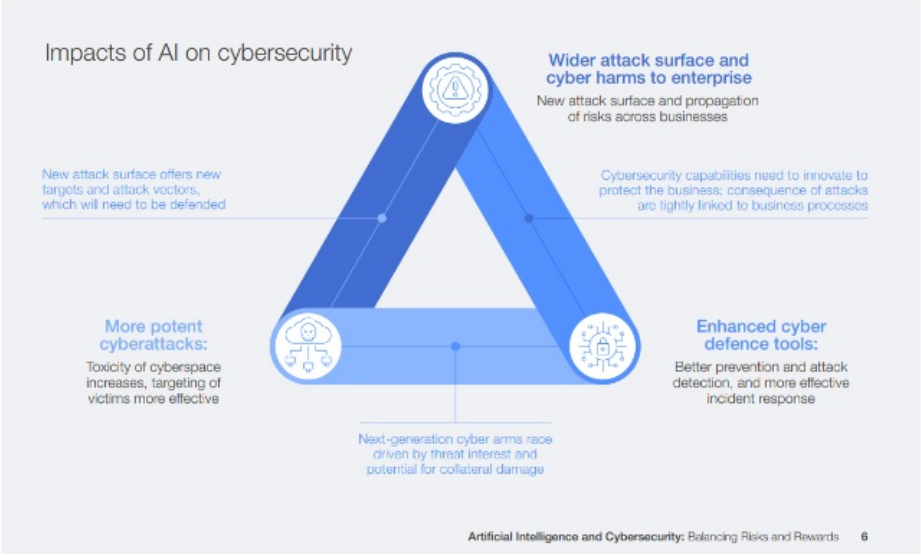

Figura 01 – Impactos do uso da IA em Cibersegurança

– O uso da IA por agentes de ameaças: os agentes de ameaças estão usando a IA para aprimorar suas capacidades e tornar suas táticas, técnicas e procedimentos mais potentes e os ataques mais eficazes.

– O uso de IA por defensores: paralelamente, os defensores cibernéticos estão aproveitando a IA para aprimorar os recursos de segurança cibernética, facilitando uma prevenção mais ampla, detecção de ameaças mais precisa, remediação autônoma e resposta a incidentes mais rápida e eficaz.

– Segurança cibernética para IA: O uso de IA está criando uma superfície de ataque expandida que pode ser explorada por agentes de ameaças. Os métodos existentes precisam ser estendidos para abordar novas vulnerabilidades que são inerentes à IA, mas que podem não ser tão relevantes para os sistemas de TI “clássicos”.

Podemos também testemunhar o surgimento de bots de segurança orientados por IA, programados para identificar e neutralizar de forma independente as ameaças cibernéticas, tornando a segurança da rede mais proativa e menos reativa. Estes desenvolvimentos significam uma mudança para sistemas de cibersegurança mais inteligentes e autônomos, impulsionados pelos avanços em IA e ML.

Os principais sistemas informatizados do TRE-MS utilizam a Internet como principal via de comunicação e acesso para usuários externos (público) e usuários internos (servidores e demais colaboradores da Justiça Eleitoral).

Estes sistemas informatizados são vitais para o desenvolvimento dos trabalhos executados nesta Instituição, tais como:

- Sistemas administrativos: SEI e SGRH, sistema de patrimônio ASI, sistema de pagamento, controle de ponto, dentre outros;
- Sistemas Eleitorais: Cadastro Nacional de Eleitores (ELO), Sistema Batimento Biométrico, dentre outros;
- Sistemas Jurisdicionais: PJe-TRE-MS, Jurisprudência, Nada consta com a Justiça Eleitoral, dentre outros;
- Sistemas de Comunicação: Ambientes TRE’s, tráfego de dados entre TSE e TRE’s, envio e recebimento de correio eletrônico (e-mails), plataformas com soluções de colaboração em nuvem, acesso ao sítio da Justiça Eleitoral, acesso à Internet e telefonia, dentre outros.

No que tange à responsabilidade da proteção de todos os sistemas informatizados existentes no ambiente de rede interna do TRE-MS, vale ressaltar que a simples adoção de soluções informatizadas em seu desenvolvimento apenas torna o trabalho mais eficiente.

Estes sistemas exigem uma camada adicional de proteção, principalmente contra ameaças cibernéticas que buscam incessantemente fragilidades ou falhas nas soluções informatizadas como forma de obter êxito em suas investidas.

A ausência de investimento na proteção aos sistemas informatizados poderá acarretar sérios prejuízos para todo o Órgão, por conta de possíveis demoras ou mesmo suspensão de importantes serviços prestados à sociedade, além de acarretar relevante impacto para a reputação e confiança do TRE-MS perante a sociedade de forma geral.

Além da carência de ferramentas para poder atuar nesse ambiente complexo, a Assessoria de Cibersegurança vêm buscando junto à Secretaria de Tecnologia da Informação a contratação de apoio especializado.

Ao mesmo tempo em que as soluções informatizadas existentes sofrem processos de modernização e atualização, as ameaças cibernéticas também acompanham de forma muito próxima este processo. Isto exige da Administração Superior uma atenção constante nas proteções a serem adotadas.

A telemetria de rede interna é uma fonte de dados rica que pode fornecer informações valiosas sobre quem está se conectando à organização e o que eles estão fazendo. Tudo toca a rede, de modo que essa visibilidade se estende entre todos os ativos/equipamentos a ela interligados.

Analisar esses dados pode ajudar a detectar ameaças que podem ter encontrado uma maneira de ignorar os controles existentes antes que eles possam ter um grande impacto.

Dessa forma, o resultado esperado com este processo é a preservação da integridade, disponibilidade e conformidade de todos os sistemas informatizados da Justiça Eleitoral, bem como a preservação da imagem institucional.

1.3.1 IDENTIFICAÇÃO DAS NECESSIDADES DE NEGÓCIO

- Implantação de Monitoramento Preventivo 24x7x365 conforme orienta a Estratégia Nacional de Cibersegurança;
- Implantação de Solução de Inovação, neste caso específico, na implantação de Inteligência Artificial e Aprendizado de Máquina na análise, detecção e resposta a incidentes de segurança;
- Colaboração com outros Órgãos/Tribunais na implantação de tais inovações relacionadas à segurança dos dados. Para atingir esta necessidade de negócio, nos unimos ao TRE-MG para realizar este pregão.

1.3.2 IDENTIFICAÇÃO DAS NECESSIDADES TECNOLÓGICAS

- Monitoramento da rede interna do Regional, voltado para análise, detecção e resposta a ameaças cibernéticas;
- Iniciar a implantação e consolidação da boa prática de segurança de realizar monitoramento preventivo de segurança, começando a substituir a prática de somente apagar incêndios, que até hoje, infelizmente, ainda é muito comum na administração pública em geral;
- Implantação de ferramenta de segurança que propicie a automação de processos de investigação de forma profunda; não somente processos que seriam realizados por pessoal de equipes de SOC Nível 1 (N1); mas, mais importante, que geralmente exigem pessoal qualificado de SOC Nível 2 (N2) e que são normalmente realizados de forma manual; para assim, prover agilidade na resposta e resolução de possíveis incidentes de segurança dentro do Regional;

1.3.3 DEMAIS REQUISITOS

Alguns dos requisitos iniciais necessários (serão apresentados todos os requisitos necessários no item "6. DA ESCOLHA E JUSTIFICATIVA DA STIC ESCOLHIDA") deste mesmo estudo.

REQUISITOS DE SERVIÇOS 24x7x365, GARANTIA E MANUTENÇÃO
Qualquer interface web da Solução de NDR ou integração entre a Solução de NDR com outra ferramenta de segurança deve obrigatoriamente, ser configurada para utilizar conexões criptografadas.

Monitoramento Preventivo 24x7x365.

REQUISITOS LEGAIS
Observância à Lei 13.853/2019 – Lei Geral de Proteção de Dados Pessoais.

Resolução CNJ N° 182/2013, dispõe sobre diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação pelos órgãos submetidos ao controle administrativo e financeiro do Conselho Nacional de Justiça (CNJ).

CNJ nº 370/2021, institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD).

Resolução CNJ nº 396/2021, institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

Lei n° 14.133/2021, que institui normas para licitações e contratos da Administração Pública.

REQUISITOS DE METODOLOGIA DE TRABALHO
A Solução deverá ser instalada nas dependências da CONTRATANTE e em seu Site Backup.

REQUISITOS SOCIAIS, AMBIENTAIS E CULTURAIS
Documentação preferencialmente no idioma português do Brasil – PT-BR ou Inglês e fornecidos em meio digital.

REQUISITOS DE IMPLANTAÇÃO
Não serão necessários ajustes no ambiente computacional do CONTRATANTE que venha a acarretar algum impacto financeiro ou de pessoal.

REQUISITOS DE DESINSTALAÇÃO DA SOLUÇÃO
Ao final do período contratual, os dados colhidos pela Solução deverão ser sanitizados ou excluídos de forma definitiva e irreversível.

REQUISITOS DE GARANTIA
Será exigida garantia dos artigos 96 e seguintes da Lei nº 14.133, de 2021.

REQUISITOS QUANTO À POSSIBILIDADE DE SUBCONTRATAÇÃO

Não será admitida a subcontratação do objeto contratual.

REQUISITOS DE PROVA DE CONCEITO
Será solicitada Prova de Conceito. Será exigida a POC conforme Termo de Referência desta contratação.

REQUISITOS DE EXPERIÊNCIA PROFISSIONAL DA EQUIPE DA CONTRATADA
Os requisitos detalhados de experiência profissional da equipe conforme item específico presente no Termo de Referência desta contratação.

2. ESTIMATIVA DA DEMANDA - QUANTIDADE DE BENS E SERVIÇOS, COM JUSTIFICATIVA PARA A QUANTIDADE

Monitoramento de segurança dos dados que trafegam dentro do ambiente computacional interno do Regional, para prevenção de ataques cibernéticos, com adoção de tecnologias de análise de comportamento e inteligência artificial, para 2500 ativos. Essa quantidade de ativos é a soma de computadores, celulares, impressoras, checkpoints, switches, roteadores,servidores virtuais e servidores físicos.

Quantidade é igual à prevista no DOD?

( ) Sim

(X) Não. Justifique: Quando da criação do DOD, havia a possibilidade de adesão a uma Ata de Registro de Preços na época capitaneada pelo TRE-DF. Porém, neste momento essa adesão não é mais possível, logo a demanda e o quantitativo, que na época era uma estimativa genérica uma vez que não houve tempo hábil para nos debruçarmos no levantamento necessário, são consequentemente diferentes. Diante disso, neste estudo, após extenso levantamento, possuímos uma demanda com escopo reduzido (sem monitoramento externo) e quantitativos mais ajustados à real necessidade do Órgão. Durante a realização deste estudo descobrimos que é melhor se concentrar no monitoramento interno primeiro; e somente após um bom monitoramento interno implantado, realizando um procedimento de boa prática de melhoria contínua e expandir o monitoramento para a parte externa.

( ) Não se aplica

3. ANÁLISE DE SOLUÇÕES POSSÍVEIS

3.1 IDENTIFICAÇÃO DAS DIFERENTES SOLUÇÕES DE TIC

Id	Descrição da Solução (ou cenário)
1	Apenas Software Livre com mão de obra do próprio Regional
2	Software Livre com fornecimento de serviços por empresa especializada
3	Contratação de empresa especializada para fornecimento de bens e serviços, **no formato de prestação de serviço**, para monitoramento da rede interna, voltados para análise, detecção e resposta de ameaças cibernéticas em escala 24x7x365, com equipe de monitoramento remota e adoção de tecnologias de análise de comportamento e inteligência artificial (machine learning não supervisionado, supervisionado e deep learning). Instalação, configuração, treinamento remoto, suporte técnico, garantia e manutenção.
4	Contratação de empresa especializada para fornecimento de bens e serviços, c**om aquisição de permanentes e serviços** de instalação, configuração e monitoramento da rede interna, voltados para análise, detecção e resposta de ameaças cibernéticas em escala 24x7x365, com equipe de monitoramento remota e adoção de tecnologias de análise de comportamento e inteligência artificial (machine learning não supervisionado, supervisionado e deep learning). Instalação, treinamento remoto, suporte técnico, garantia e manutenção.

3.2 ANÁLISE COMPARATIVA DE SOLUÇÕES

Solução 1 (considerada inviável, vide item 4 abaixo):
"Apenas Software Livre com mão de obra do próprio Regional"

Solução 2 (considerada inviável, vide item 4 abaixo):
"Software Livre com fornecimento de serviços por empresa especializada"

Solução 3:
"Contratação de empresa especializada para fornecimento de bens e serviços, **no formato de prestação de serviço**, para monitoramento da rede interna, voltados para análise, detecção e resposta de ameaças cibernéticas em escala 24x7x365, com equipe de monitoramento remota e adoção de tecnologias de análise de comportamento e inteligência artificial (machine learning não supervisionado, supervisionado e deep learning). Instalação, configuração, treinamento remoto, suporte técnico, garantia e manutenção."

Solução 4:
"Contratação de empresa especializada para fornecimento de bens e serviços, c**om aquisição de permanentes e serviços** de instalação, configuração e monitoramento da rede interna, voltados para análise, detecção e resposta de ameaças cibernéticas em escala 24x7x365, com equipe de monitoramento remota e adoção de tecnologias de análise de comportamento e inteligência artificial (machine learning não supervisionado, supervisionado e deep learning). Instalação, treinamento remoto, suporte técnico, garantia e manutenção."

A cibersegurança é uma área extremamente complexa, pois precisa defender sistemas, redes e dados contra uma vasta gama de ameaças digitais que evoluem constantemente, como invasões hackers, roubos de informações e sabotagens virtuais. Para tentar entender o quão complexo é para proteger todo esse ambiente, a equipe de cibersegurança do Regional têm que lidar com milhares de formas diferentes que os atacantes podem usar para

invadir, se esconder e causar danos – é como um jogo de xadrez onde o adversário tem milhões de movimentos possíveis.

Para se ter uma ideia da complexidade desse cenário, podemos nos basear no "framework" MITRE ATT&CK [Figura 2 abaixo], que cataloga os comportamentos dos agentes maliciosos observados no mundo real. A versão mais recente desse "framework" (de abril de 2025) inclui **14 táticas principais** (como reconhecimento e exfiltração de dados), **211 técnicas** (métodos gerais de ataque) e impressionantes **468 sub-técnicas** (variações mais específicas), **além de milhares de procedimentos** (que são exemplos reais de como essas técnicas são aplicadas por grupos cibercriminosos ou malwares, totalizando mais de **10 mil exemplos reais** documentados de softwares e ataques cibernéticos da vida real).

Esses números expressivos demonstram que a cibersegurança não se trata apenas de um ato isolado de instalar um antivírus e mantê-lo atualizado, mas de uma batalha contínua contra um ecossistema de ameaças cada vez mais sofisticadas e em constante expansão, exigindo conhecimento profundo e ferramentas avançadas para qualquer defesa minimamente eficaz.

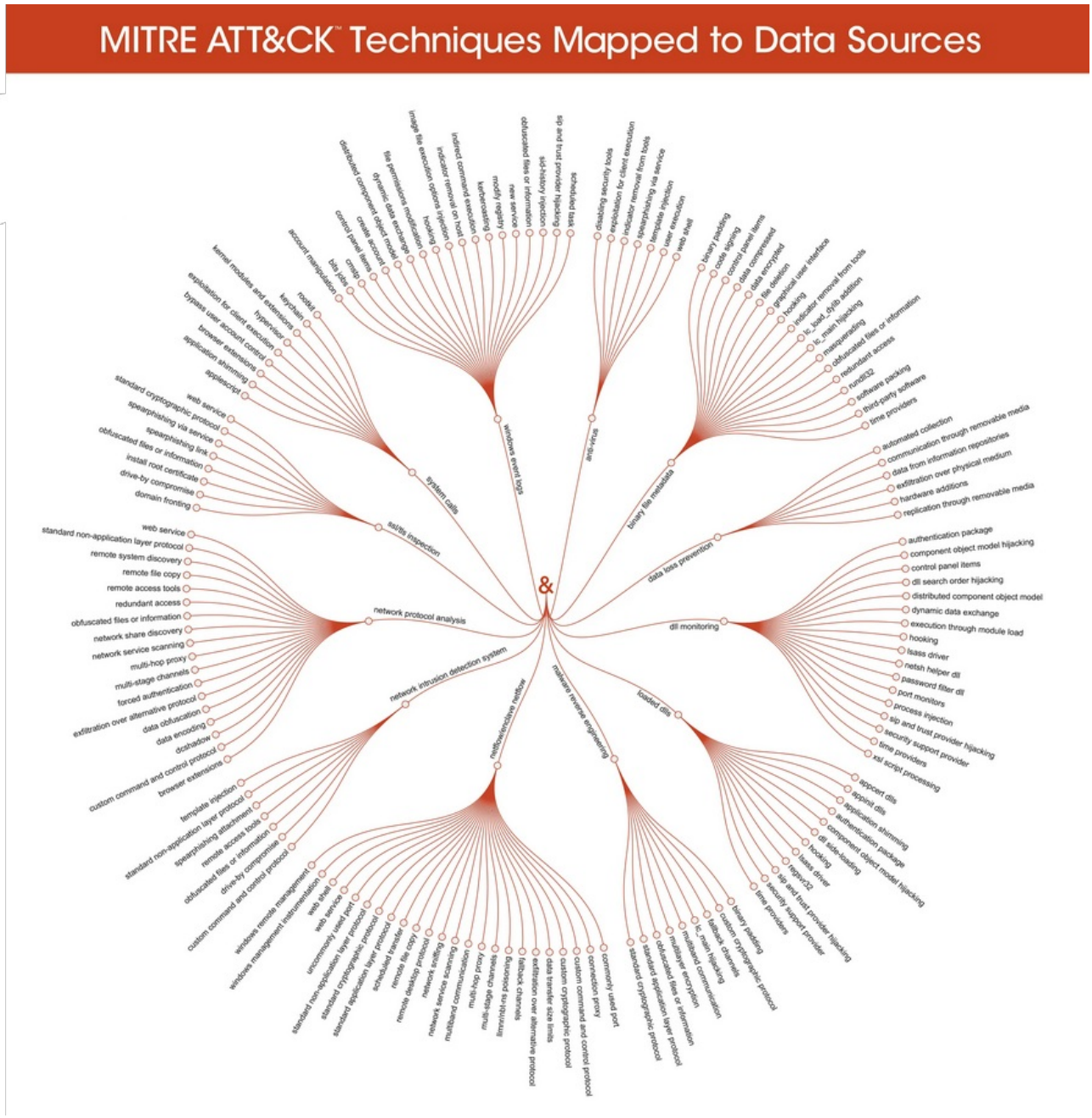

Figura 2 – Representação Gráfica de uma parte do Framework de Segurança MITRE ATT&CK

Tudo isso sem contar os aspectos não técnicos da Segurança da Informação. A segurança da informação vai muito além da cibersegurança técnica (como firewalls e antivírus) e inclui dimensões humanas, organizacionais e comportamentais. Isso abrange políticas de governança, treinamentos de conscientização, gerenciamento de riscos, conformidade regulatória e controle de acessos físicos. Esses elementos focam em pessoas e processos, não em ferramentas tecnológicas.

Considerando a pequena equipe técnica disponível para atuar nesse cenário extremamente desafiador, torna-se essencial a utilização de ferramentas de varredura e detecção automatizadas para o monitoramento de segurança.

É nesse contexto que surge a demanda pela Solução em estudo.

O monitoramento interno da segurança do Órgão pode ser realizado por duas ferramentas: o NDR e o SIEM.

O SIEM é vital para o monitoramento centralizado de logs, garantindo conformidade e fornecendo uma visão abrangente do cenário de segurança por meio da agregação e análise de dados de logs de várias fontes na infraestrutura de TI. Isso permite vigilância contínua e detecção oportuna de incidentes de segurança. Enquanto isso, o NDR oferece monitoramento em tempo real do tráfego de rede, utilizando análises avançadas para detectar anomalias e ameaças sofisticadas que podem escapar de sistemas baseados em logs. Juntos, o SIEM e o NDR proporcionam monitoramento robusto e contínuo, abordando as limitações um do outro e apoiando a conformidade com requisitos regulatórios rigorosos. Dada a natureza sensível dos dados governamentais e a sofisticação das ameaças cibernéticas, a implementação de ambos, SIEM e NDR, é uma necessidade estratégica para aumentar a resiliência em cibersegurança.

Um sistema de Detecção e Resposta em Rede (NDR) é necessário porque um sistema de Gerenciamento de Informações e Eventos de Segurança (SIEM) sozinho não é capaz de identificar todas as ameaças, principalmente aquelas que não deixam registros ou que atuam fora dos limites tradicionais de segurança. Embora os SIEMs sejam eficientes em coletar e correlacionar logs para fins de conformidade e análise histórica, eles geralmente têm dificuldade em detectar, em tempo real, ataques sofisticados, especialmente em ambientes de rede dinâmicos ou com tráfego criptografado. O NDR complementa o SIEM ao analisar o tráfego de rede e detectar ameaças que podem passar despercebidas pelo SIEM, como aquelas relacionadas a dispositivos não gerenciados, tráfego criptografado ou movimentação lateral.

A partir deste ponto, apenas a Solução de NDR será analisada, uma vez que a necessidade de um SIEM já está prevista para ser atendida por um processo que está elencado na Proposta Orçamentária do TRE-MS para 2026.

É consenso na equipe de contratação de que a Equipe de Cibersegurança precisa passar a ter uma ferramenta de NDR que auxilie a cibersegurança do Regional a atingir as necessidades de negócio do Órgão e, de quebra, permita aos analistas de segurança rastrear a progressão dos incidentes de segurança com precisão, reduzindo assim o tempo de resposta e implementando remediações eficazes com base em um contexto rico e bem estruturado.

É preciso que essa ferramenta de NDR realize não só tarefas automatizadas de Nível 1 (N1) de um SOC; mas prioritariamente, realize tarefas automatizadas e investigações profundas que seriam realizadas somente por uma equipe especializada de SOC Nível 2 (N2).

O NDR (Detecção e Resposta de Rede) é uma tecnologia de segurança cibernética que monitora e analisa o tráfego de rede interna da Instituição na busca de identificação de ameaças em tempo real, sendo uma camada adicional de segurança. Pode ser integrado com outras tecnologias de segurança cibernética, como EDR (Detecção e Resposta de Endpoint) e XDR (Detecção e Resposta Estendida), para fornecer uma defesa abrangente.

O NDR pode ser implementado por meio de:

- Dispositivos de hardware e software
- Software local
- SaaS
- Inteligência artificial (IA)
- Aprendizado de máquina (ML)
- Análise de dados

De modo geral, soluções de NDR analisam continuamente as atividades da rede interna para criar uma linha de base do comportamento normal da rede.

Em seguida, ele usa essa linha de base, juntamente com análises avançadas não baseadas em assinaturas que incluem algoritmos de modelagem comportamental e aprendizado de máquina, bem como inteligência de ameaças globais para identificar anomalias e detectar e responder a ameaças em tempo real.

Foram analisadas documentações e sites das soluções de NDR abaixo, além de terem sido feitas reuniões com

fornecedores da:

- Darktrace;
- Trend Micro;
- Extrahop; e
- VectraAI

Conforme a “Figura 3” abaixo, a maioria das ferramentas analisadas encontram-se em posição de destaque no mercado segundo o relatório do Quadrante Mágico do Gartner 2025.

Apesar da Solução da Trend Micro de NDR não estar posicionada em um local de destaque mercadológico segundo o Gartner, a equipe técnica do TRE-MS entendeu que seria interessante avaliar a Solução, pois o TRE-MS possui contrato vigente para a solução de EDR da Trend Micro, popularmente mais conhecido como "Antivírus"; e uma integração poderia trazer benefícios técnicos.

Figura 3 – Quadrante Mágico do Gartner para soluções de NDR (2025).

OBS. 1: Os representantes das soluções Zerum e OpManager também apresentaram suas soluções, mas, no entendimento da equipe técnica, os produtos não se enquadravam dentro das características de uma ferramenta de NDR. Diante do que foi exposto durante essas apresentações e pelo conteúdo pesquisado pela equipe de contratação no site das soluções/empresas, foi constatado que as ferramentas não tem características relacionadas a automações e investigações profundas que automatizem processos que seriam realizados por pessoal capacitado trabalhando em um SOC Nível 2 (N2), apenas possuindo caracaterísticas de automações e investigações, porém não profundas, voltadas a automatizar procedimentos que normalmente são realizados por pessoal que trabalha em um SOC Nível 1 (N1).

CARACTERÍSTICAS COMUNS DAS SOLUÇÕES NDR AVALIADAS:

Detecção Baseada em Comportamento e IA/ML: Todas utilizam inteligência artificial e aprendizado de máquina

(machine learning) para analisar o tráfego de rede e identificar anomalias ou comportamentos suspeitos que fogem do padrão, sem depender exclusivamente de assinaturas conhecidas. Além disso, utilizam-se dessa tecnologia para realizar investigações automatizadas profundas em cima dos dados coletados da rede.

Visibilidade de Rede: Fornecem visibilidade aprofundada sobre o que está acontecendo na rede, monitorando o tráfego de forma contínua para identificar ameaças internas e externas.

Modelo de Licenciamento: Predominantemente operam sob um modelo de licenciamento por assinatura (Opex), o que se alinha com a flexibilidade orçamentária do setor público, evitando grandes investimentos de capital inicial (Capex).

Requisitos de Implantação: Geralmente requerem a instalação de sensores (appliances físicas ou virtuais) em pontos estratégicos da rede (utilizando SPAN/TAP) para coletar e analisar o tráfego. A complexidade de implantação é moderada.

Integração com Ecossistema de Segurança: Apresentam alta capacidade de integração com outras ferramentas de segurança, como SIEM (Security Information and Event Management), SOAR (Security Orchestration, Automation and Response) e EDR (Endpoint Detection and Response), frequentemente via APIs robustas, para orquestrar a resposta e enriquecer o contexto de segurança.

Suporte e Serviços Gerenciados: Oferecem suporte técnico 24x7 com níveis de serviço definidos e possuem uma rede de parceiros MSSP (Managed Security Service Providers) que podem prover a Solução como um serviço gerenciado.

Aderência a Padrões de Segurança: Contribuem significativamente para a conformidade com regulamentações e padrões como LGPD (proteção de dados), ISO 27001 (gestão de segurança da informação) e NIST CSF (identificar, proteger, detectar, responder, recuperar).

Otimização de Operações de Segurança: Visam melhorar a postura de segurança, aumentar a eficiência operacional das equipes de SOC (Security Operations Center) e reduzir o Tempo Médio de Resposta (MTTR) a incidentes.

Escalabilidade: São projetadas para escalar e suportar ambientes de rede de grande porte e alto volume de tráfego, adequadas para a expansão de órgãos públicos.

Custo Total de Propriedade (TCO) e Retorno sobre Investimento (ROI): Embora o custo inicial e recorrente possa ser considerado alto em relação a ferramentas de segurança tradicionais, o ROI é justificado pela capacidade de prevenir violações de dados, reduzir perdas financeiras e proteger a reputação.

CARACTERÍSTICAS DIFERENCIAIS DE CADA SOLUÇÃO DE NDR:

Embora compartilhem muitas funcionalidades essenciais, cada Solução de NDR possui características distintivas que a tornam mais adequada para perfis específicos de necessidades e estratégias de segurança.

Darktrace:
A principal diferenciação da Darktrace reside em sua abordagem de IA autônoma e não supervisionada, que opera como um "sistema imunológico" para a rede.

IA de Autoaprendizado: A Darktrace se destaca por sua inteligência artificial não supervisionada, que aprende o "normal" de cada usuário, dispositivo e conexão na rede sem a necessidade de pré-configurações ou regras manuais. Isso permite a detecção de ameaças de dia zero e anomalias sutis que outras soluções baseadas em assinaturas ou regras não identificariam.

Antigena (Resposta Autônoma): Possui uma capacidade de resposta autônoma, chamada Antigena, que pode conter ameaças em tempo real, aplicando ações de mitigação (ex: isolar dispositivo, bloquear conexão) sem intervenção humana, minimizando o impacto de um ataque.

Independência de Assinaturas: Não depende de feeds de inteligência de ameaças baseados em assinaturas para a detecção primária, adaptando-se continuamente às novas ameaças.

Visibilidade Abrangente: Fornece insights sobre o comportamento de rede, incluindo dispositivos IoT/OT e sistemas legados, que podem ser difíceis de monitorar por outras ferramentas.

Trend Micro Vision One (Componente NDR):

O componente NDR da Trend Micro se diferencia por ser parte integrante de uma plataforma XDR (Extended Detection and Response) mais ampla, proporcionando uma visão e resposta correlacionadas.

Correlação Multivetorial: Sua maior força é a capacidade de correlacionar eventos e telemetria de múltiplos vetores de segurança – rede, endpoint, e-mail, cloud e servidores – em uma única console, permitindo a detecção de ameaças complexas que se espalham por diferentes camadas.

Insights Unificados (Storylines): Apresenta "storylines" de ataque que conectam os eventos de diferentes fontes, simplificando a investigação e reduzindo a fadiga de alertas para as equipes de segurança.

Inteligência de Ameaças Global: Beneficia-se da vasta e atualizada inteligência de ameaças da Trend Micro (Smart Protection Network), que enriquece suas capacidades de detecção.

Resposta Orquestrada: Permite uma resposta unificada e orquestrada em diversos pontos de controle, facilitando a remediação rápida em todo o ambiente.

Eficiência para Usuários Existentes: Pode ser mais custo-eficaz e de mais fácil integração para organizações que já utilizam outros produtos da Trend Micro.

Extrahop Reveal(x):

A Extrahop se destaca pela profundidade de visibilidade de rede, especialmente em relação ao tráfego criptografado, e por suas robustas capacidades de análise forense.

Decriptografia SSL/TLS: É uma das poucas soluções que oferece a capacidade de decifrar o tráfego SSL/TLS em tempo real para inspeção profunda, permitindo a detecção de ameaças ocultas em comunicações criptografadas (sujeito às políticas de privacidade do órgão).

Telemetria Rica e Captura de Pacotes: Coleta e analisa metadados de rede altamente granulares e, se necessário, oferece captura de pacotes brutos para investigações forenses extremamente detalhadas.

Análise de Comportamento de Ativos Não Gerenciados: Possui forte capacidade de identificar e monitorar o comportamento de dispositivos não gerenciados, como IoT (Internet of Things) e OT (Operational Technology), oferecendo visibilidade crítica em ambientes complexos.

Performance de Rede: Além da segurança, Extrahop também pode fornecer insights valiosos sobre a performance da rede, ajudando a otimizar as operações de TI.

Vectra AI:

A Vectra AI se diferencia pelo seu foco em detectar as TTPs (Táticas, Técnicas e Procedimentos) dos atacantes e pela priorização inteligente de ameaças baseada em IA.

Detecção de TTPs de Atacantes: Utiliza IA para identificar padrões de comportamento que indicam fases específicas de um ataque (como movimento lateral, persistência, exfiltração de dados, comando e controle), em vez de apenas alertas individuais.

Análise de Tráfego Criptografado sem Decriptografia: É capaz de analisar o tráfego criptografado (SSL/TLS) sem decifrá-lo, inspecionando metadados e padrões de fluxo para detectar atividades maliciosas, o que é valioso para ambientes com restrições de privacidade.

Priorização Baseada em Risco (Scores): Atribui scores de risco a hosts e usuários com base na gravidade e confiança da detecção, permitindo que as equipes de segurança foquem nos alertas mais críticos e complexos.

Detecção de Campanha: Agrupa detecções relacionadas em "campanhas" de ataque, fornecendo uma visão clara da progressão de uma intrusão, desde o reconhecimento inicial até a exfiltração de dados.

Inteligência Focada em Adversários: Sua inteligência é fortemente orientada pela pesquisa de comportamento de adversários e pela modelagem de cenários de ataque reais.

QUADRO COMPARATIVO DAS SOLUÇÕES:

	Solução			
Critério	**Darktrace**	**Trend Micro Vision One (Componente NDR está embutido)**	**Extrahop Reveal(x)**	**Vectra AI**
Custo (Relativo)	Alto	Médio-Alto (depende da integração XDR)	Alto	Alto
Foco Principal	IA Autônoma, Comportamento de Rede, Detecção de Dia Zero	XDR Unificado, Correlação Multivetorial	Visibilidade Profunda, Descriptografia SSL/TLS, Forense	IA para TTPs de Atacantes, Movimento Lateral
Aderência a Normas (LGPD, ISO, NIST)	Forte	Muito Forte (pela abrangência XDR)	Forte	Forte
Requisitos de Infraestrutura	Sensores (Físicos/Virtuais)	Sensores de Rede (Físicos/Virtuais)	Sensores (Físicos/Virtuais)	Sensores (Físicos/Virtuais)
Complexidade de Implantação	Moderada	Moderada	Moderada	Moderada
Compatibilidade com SIEM/SOAR/EDR	Alta (APIs)	Alta (APIs/Nativa)	Alta (APIs/Nativa)	Alta (APIs/Nativa)
Aquisição (Capex/Opex)	Principalmente Opex (assinatura)	Principalmente Opex (assinatura)	Principalmente Opex (assinatura)	Principalmente Opex (assinatura)
Modelos de Deployment	On-premises, Híbrido, Cloud	SaaS, On-premises, Híbrido	On-premises, SaaS (controle)	On-premises, Híbrido
Suporte e MSSP	24x7, Ampla rede MSSP	24x7, Vasta rede MSSP	24x7, Parceiros MSSP	24x7, Parceiros MSSP

Fontes de Dados Primárias	Tráfego Bruto, Metadados	Tráfego Rede, Logs Endpoint/Cloud/Email	Tráfego Bruto (c/ decripto), Metadados	Metadados, NetFlow, Logs Autenticação
Capacidade de Resposta	Autônoma (Antigena), Integração SOAR	Orquestrada XDR, Integração SOAR	Integração SOAR/SIEM	Integração SOAR/SIEM
Análise Forense	Detalhada (Tráfego Bruto)	Detalhada (Correlacionada XDR)	Muito Detalhada (Tráfego/Metadados)	Detalhada (Metadados/Eventos)
Escalabilidade	Alta	Alta	Alta	Alta
Risco de Vendor Lock-in	Moderado-Alto	Moderado	Moderado	Moderado
Nota Gartner PeerInsights	4,7 *	4,6 **	4,5 ***	4,7 ****

* No contexto do estudo realizado pelo Gartner PeerInsights a Darktrace recebeu nota "4,7",onde o máximo era "5,0", com 386 avaliações. https://www.gartner.com/reviews/market/network-detection-and-response/vendor/darktrace/product/darktrace-network [Acesso em 15/04/2025]

** No contexto do estudo realizado pelo Gartner PeerInsights a Trend Micro Vision One NDR recebeu nota "4,6", onde o máximo era "5,0", com 97 avaliações. https://www.gartner.com/reviews/market/extended-detection-and-response/vendor/trend-micro/product/trend-vision-one-endpoint-security [Acesso em 15/04/2025]

*** No contexto do estudo realizado pelo Gartner PeerInsights a Extrahop recebeu nota "4,5" onde o máximo era "5,0", com 217 avaliações. https://www.gartner.com/reviews/market/network-detection-and-response/vendor/extrahop/product/extrahop-reveal-x [Acesso em 15/04/2025]

**** No contexto do estudo realizado pelo Gartner PeerInsights a Vectra AI recebeu nota "4,7", onde o máximo era "5,0", com 423 avaliações. https://www.gartner.com/reviews/market/network-detection-and-response/vendor/vectra-ai/product/vectra-ai-platform [Acesso em 15/04/2025]

OBSERVAÇÕES:
O Gartner Peer Insights foi utilizado como parâmetro de avaliação entre as soluções, sendo uma plataforma online gratuita para análise e classificação de softwares e serviços de TI.

O Gartner Peer Insights não possuia uma entrada em seu banco de dados que fosse apenas para o componente NDR da Trend Micro, portanto neste estudo, foi utilizada a entrada no Garner Peer Insights para o Trend Vision One, que inclui o componente NDR "on-premise".

O Gartner Peer Insights é uma comunidade para profissionais de TI e tomadores de decisão em tecnologia compartilharem insights e aprimorarem produtos.

Recursos Avaliações: As avaliações são anônimas e verificadas pelo Gartner.

Discussões: Os líderes podem discutir tópicos e tecnologias em alta.

Informações: As avaliações fornecem informações reais sobre os clientes.

Pesquisa: O Gartner utiliza as informações do Peer Insights em suas pesquisas, incluindo os Quadrantes Mágicos, que é um recurso de informação referencial de mercado.

Benefícios:

- Ajuda os líderes de TI a tomar decisões de compra
- Auxilia os provedores de tecnologia a aprimorar seus produtos
- Ajuda os clientes a expandir seus negócios, e
- Conecta os clientes a profissionais de TI experientes.

Quem pode usar: Qualquer pessoa pode ler e analisar avaliações, sem precisar de uma assinatura do Gartner. Fornecedores podem listar produtos e obter avaliações sem precisar de uma assinatura do Gartner.

O que está incluído: Avaliações de softwares e serviços empresariais.

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		
	Solução 4	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	

3.3 PESQUISA DE PREÇOS DE MERCADO

Id	Descrição da Solução (ou cenário)
3	Contratação de empresa especializada para fornecimento de bens e serviços, **no formato de prestação de serviço**, para monitoramento da rede interna, voltados para análise, detecção e resposta de ameaças cibernéticas em escala 24x7x365, com equipe de monitoramento remota e adoção de tecnologias de análise de comportamento e inteligência artificial (machine learning não supervisionado, supervisionado e deep learning). Instalação, configuração, treinamento remoto, suporte técnico, garantia e manutenção.
4	Contratação de empresa especializada para fornecimento de bens e serviços, **com aquisição de permanentes e serviços** de instalação, configuração e monitoramento da rede interna, voltados para análise, detecção e resposta de ameaças cibernéticas em escala 24x7x365, com equipe de monitoramento remota e adoção de tecnologias de análise de comportamento e inteligência artificial (machine learning não supervisionado, supervisionado e deep learning). Instalação, treinamento remoto, suporte técnico, garantia e manutenção.

4. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

Solução 1:
"Apenas Software Livre com mão de obra do próprio Regional"

Conforme explicitado anteriormente, o TRE não possui pessoal suficiente para realizar uma implantação de software livre com essa complexidade, como o software livre "Zeek", por exemplo, muito menos mantê-la atualizada e segura. Além disso, esta opção não possibilita que o Órgão contrate empresa terceirizada para atender a demanda de monitoramento 24x7.

Solução 2:
"Software Livre com fornecimento de serviços por empresa especializada"

Apesar de possível, esta Solução se mostrou inviável durante os Estudos pois não foi encontrada nenhuma Empresa com essas características que entregue esse tipo de Solução no mercado nacional.

Esta era uma Solução possível, desde que alguma empresa comercializasse uma Solução como uma Solução de NDR de software livre de forma profissional, que fornecesse por exemplo, suporte e garantia e que ainda atendesse às especificações e demandas solicitadas pela equipe técnica. Essa exigência de ser uma Solução profissional, visa evitar "gambiarras" que não trarão o benefício esperado de aumento da segurança dos dados para o Órgão. A única Empresa/Solução que encontramos com essas características é a "Corelight", que utiliza software livre para fornecer o seu NDR corporativo (utilizando por baixo o software livre chamado "Zeek", informado pela própria "Corelight"). A empresa "Corelight " está inclusive em 4º lugar no Quadrante Mágico 2025 do Gartner para NDR. Esse é um exemplo de que é possível utilizar software livre da forma correta, aberta e profissional. Porém, infelizmente, não conseguimos análisá-la na pesquisa de mercado/pesquisa de preço abaixo, pois não conseguimos identificar um representante no Brasil.

5. ANÁLISE E COMPARAÇÃO ENTRE OS CUSTOS TOTAIS DAS STICs

5.1 CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE

LINHA DO TEMPO DA PESQUISA DE PREÇOS
Os e-mails solicitando os orçamentos foram enviados respectivamente em 03/09/2025 e 22/09/2025 (reforço), SEI nº (1928411) e SEI nº (1928429), para 4 empresas que representam as fabricantes analisadas neste estudo.

Das 4 fabricantes analisadas neste estudo, todas as 4 forneceram orçamentos através de seus representantes.

Informamos ainda que a empresa Garage Tech forneceu apenas orçamento para a Solução 3 e a empresa Agility forneceu apenas orçamento para a Solução 4, como pode ser verificado nos seus respectivos orçamentos abaixo.

CONSTATAÇÕES REALIZADAS PELA EQUIPE DE PLANEJAMENTO APARTIR DOS ORÇAMENTOS E PLANILHA DE CUSTOS

Como pode ser visto em quaisquer dos orçamentos que se venha a analisar, Garage Tech: SEI nº (1928468), NTSEC: SEI nº (1930223), ALLTECH: SEI nº (1930225) ou AGILITY: SEI nº (1931307); há vantajosidade financeira no pagamento único em relação ao pagamento mensal.

Portanto, a fim de tornar a planilha de Cálculo dos Custos Totais de Propriedade mais simples de ser analisada, planilha SEI nº (1931298), dentro da referida planilha só constam os valores orçados no formato de pagamento único.

Pode-se ainda, na planilha de Cálculo dos Custos Totais de Propriedade mencionada acima, constatar que em uma comparação simples entre valores médios, referentes à "Solução 3" (Tudo como Serviço) e a opção "Solução 4" (Serviço + Permanentes), que a opção "Solução 3" (Tudo como Serviço), se mostra mais vantajosa financeiramente, seja em 1, 2 ou 3 Anos de contrato.

É importante salientar que a Solução 3 ajuda ainda a aumentar a segurança da contratação, devido ao fato de que, nesse formato "Tudo como Serviço" (Comodato), caso o volume de tráfego de rede durante o contrato aumente inesperadamente devido à implantação de algum serviço não previsto e o equipamento físico ("appliance") não suporte esse aumento, a CONTRATADA terá o dever de fornecer um novo equipamento capaz de lidar com esse aumento de tráfego. Esse novo equipamento que deverá ser fornecido pela CONTRATADA em caso de necessidade, deverá ser capaz de lidar com o aumento do tráfego no ambiente do Regional sem custo adicional — algo impossível no formato de contratação da Solução de tipo 4 (Aquisição de Permanentes + Serviços). Nesse formato de contratação do tipo 4 uma nova licitação completa para aquisição de um segundo equipamento físico mais adequado teria que ser realizada para resolver esse problema de aumento de tráfego de rede.

Além disso, durante a confecção da planilha de Cálculo dos Custos Totais de Propriedade, esta equipe de contratação pôde constatar que o pagamento único fica sempre mais vantajoso financeiramente para o Regional, desde que haja disponibilidade orçamentária reservada para tanto.

As equipes de planejamento do TRE-MS e do TRE-MG, baseados nos valores dos orçamentos, informam que possuem orçamento reservado suficiente para pelo menos 03 anos de contrato.

Solução 3:
Contratação de empresa especializada para fornecimento de bens e serviços, **no formato de prestação de serviço**, para monitoramento da rede interna, voltados para análise, detecção e resposta de ameaças cibernéticas em escala 24x7x365, com equipe de monitoramento remota e adoção de tecnologias de análise de comportamento e inteligência artificial (machine learning não supervisionado, supervisionado e deep learning). Instalação, configuração, treinamento remoto, suporte técnico, garantia e manutenção.

CONTRATAÇÕES PÚBLICAS SIMILARES (Solução 3)

O item abaixo não poderá ser aproveitado. Apesar de possuir muita similaridade com a contratação atual, é uma contratação com o número de ativos a serem monitorados muito discrepante (1000 ativos a menos sendo monitorados, além de possuir itens que extrapolam o escopo da contratação atual, por exemplo monitoramento externo). Além disso a vigência do contrato do TRE-DF era de apenas 02 anos:

TRE-DF:
Código da UASG: 70025 / Pregão Eletrônico: 08/2023 (Ata de Registro de Preços que o TRE-MS e TRE-MG participaram na época)
Vigência: 24 meses
Valor Total para o TRE-MS na época: R$ 2.861.549,20

Valor Total para o TRE-MG na época: R$ 6.051.753,50

Os itens abaixo não poderão ser aproveitados. Apesar de possuir similaridade com a contratação pretendida, são processos com mais de 2 anos:

Tribunal de Contas da União - TCU
Código da UASG: 30001 / Pregão Eletrônico: 034/2017
Vigência: 60 meses
Valor contratado: R$10.000.000,00

Conselho da Justiça Federal – CJF
Código da UASG: 90026 / Pregão Eletrônico: 001/2020
Vigência: 24 meses
•alor contratado: R$3.602.025,36

Supremo Tribunal Federal - STF
Código da UASG: 40001 / Pregão Eletrônico: 008/2023
Vigência: 12 meses
Valor contratado: R$3.522.999,92

Tribunal de Justiça do Estado do Rio de Janeiro - TJRJ
Código da UASG: 30100 / Pregão Eletrônico: 050/2022
Vigência: 24 meses
Valor contratado: R$45.608.000,00

Banco da Amazônia - BASA
Código da UASG: 179007 / Pregão Eletrônico: 043/2021
Vigência: 36 meses

Valor contratado: R$11.636.999,44

Instituto Brasileiro de Geografia e Estatística - IBGE
Código da UASG: 114637 / Pregão Eletrônico: 011/2021
Vigência: 24 meses
Valor contratado: R$3.229.999,68

Solução 4:
Contratação de empresa especializada para fornecimento de bens e serviços, **com aquisição de permanentes** e serviços de instalação, configuração e monitoramento da rede interna, voltados para análise, detecção e resposta de ameaças cibernéticas em escala 24x7x365, com equipe de monitoramento remota e adoção de tecnologias de análise de comportamento e inteligência artificial (machine learning não supervisionado, supervisionado e deep learning). Instalação, treinamento remoto, suporte técnico, garantia e manutenção.

CONTRATAÇÕES PÚBLICAS SIMILARES (Solução 4)

Apesar desta contratação do STJ abaixo ser de NDR o uso desta contratação na composição de preço médio não é possível, uma vez que essa contratação não possui um item primordial à este estudo/contratação: o serviço de monitoramento 24x7x365 com equipe remota da CONTRATADA; fazendo com que os preços sejam muito divergentes, o que inviabiliza sua utilização.

Superior Tribunal de Justiça:
Código da UASG: 50001 / Pregão Eletrônico Nº 90089/2024
Vigência: 24 meses
Valor contratado: R$ 5.768.000,00 (possui item NPB que não faz parte deste estudo)

5.2 MAPA COMPARATIVO DOS CUSTOS TOTAIS DE PROPRIEDADE

O comparativo entre os Custos Totais de Propriedade pela quantidade de ano(s) a ser(em) contratado(s), pode ser feito analisando-se as médias disponíveis no final das abas "ORÇAMENTOS (Serviços+Permanente)" e "ORÇAMENTOS (Tudo como Serviços)" da planilha SEI nº (1931298).

6. DA ESCOLHA E JUSTIFICATIVA DA STIC ESCOLHIDA

A equipe da contratação, diante do exposto até aqui, vislumbra que a Solução 3 se mostrou mais vantajosa financeiramente, e por isso optou pela sua escolha: **Solução 3** (prazo de **03 Anos** para ambos os Regionais: **TRE-MS** e **TRE-MG**, com pagamento único). Ao mesmo tempo, essa escolha aumenta a segurança do futuro contrato pelo exposto no item 5.1 acima. Um resumo da opção escolhida:

Contratação de empresa especializada para fornecimento de bens e serviços, **no formato de prestação de serviço**, para monitoramento da rede interna, voltados para análise, detecção e resposta de ameaças cibernéticas em escala 24x7x365, com equipe de monitoramento remota e adoção de tecnologias de análise de comportamento e inteligência artificial (machine learning não supervisionado, supervisionado e deep learning). Instalação, configuração, treinamento remoto, suporte técnico, garantia e manutenção.

6.1 DESCRIÇÃO DA SOLUÇÃO de TIC A SER CONTRATADA

REQUISITOS DE SERVIÇOS 24x7x365, GARANTIA E MANUTENÇÃO

A prestação de serviços deve abranger o fornecimento completo da Solução, incluindo licenciamento, software, hardware e serviços correlatos. O escopo da prestação de serviços deve contemplar:

O serviço de monitoramento da rede interna do Regional, deverá prover análise, detecção e resposta a ameaças cibernéticas (com uso de software e hardware NDR e pessoal qualificado remoto trabalhando em turnos na análise dos dados coletados e investigados pela ferramenta), com uso de inteligência artificial e machine learning (machine learning não supervisionado, supervisionado e deep learning); sendo fornecido em cartáter ininterrupto, operando 24 horas por dia, 7 dias por semana e 365 dias por ano (24x7x365). Isso garante a vigilância constante do ambiente de rede, essencial para a identificação e mitigação de ameaças a qualquer momento.

A Solução de NDR deverá ser dimensionada de forma a suportar simultaneamente todos os requisitos mínimos presentes na tabela de perfil do Regional, presente no Termo de Referência. Não serão aceitas soluções que dimensionem a Solução para suportar apenas um dos itens da tabela, e sim, deverá ser dimensionada para suportar todos os itens.

A Solução deverá ter garantia/suporte pelo período definido na tabela de perfil do Regional, disponível no Termo de Referência, incluindo software, hardware, atualizações e, se necessário, substituição de peças e equipamentos.

O serviço de monitoramento remoto realizado por pessoal qualificado da CONTRATADA deverá monitorar em período integral (24x7x365) a ferramenta de NDR e deverá contatar o Regional, em qualquer horário, em caso de incidentes de alta críticidade de segurança. Incidentes de segurança de baixa e média criticidade poderão ser alertados em horário comercial. Esse contato se dará utilizando os canais oficiais de troca de documentações/informações definidos nesta especificação. Esta exigência é necessária uma vez que o Regional não tem pessoal necessário para realizar monitoramento de segurança fora do horário de expediente.

A CONTRATADA deverá ainda entregar relatórios mensais com análise de segurança que abranja esse período, a fim de auxiliar na melhoria da segurança do Regional. A CONTRATADA deve fornecer os relatórios através do canal oficial de troca de documentações/informações do Regional, informado nesta especificação.

O canal oficial para contato e troca de documentações/informações entre a equipe de monitoramento remoto da CONTRATADA e a CONTRATANTE, durante o dia a dia do contrato; bem como apresentação de relatórios e demais ações correlatas, deverá ser exclusivamente através do Ambiente de Colaboração já adquirido pela CONTRATANTE, por exemplo, Google Workspace (com o uso do “Google Drive” e “Google Chat”) ou Microsoft 365 (com o uso do “One Drive” e “Teams”). O Ambiente de Colaboração utilizado pela CONTRATANTE será informado na tabela de perfil do Regional no Termo de Referência.

Deverão ser fornecidos todos os licenciamentos, softwares e hardwares necessários para a plena operação da Solução e atendimento das especificações técnicas definidas, durante todo o período contratual.

A CONTRATADA assegurará a garantia do direito de uso integral de toda a tecnologia envolvida na Solução por parte da CONTRATANTE, sempre na versão mais recente publicada pelo desenvolvedor/fabricante.

A natureza crítica da segurança cibernética exige disponibilidade contínua e tempos de resposta ágeis.

Para a comunicação e solicitação de suporte, a CONTRATADA deverá disponibilizar múltiplos canais:

- Telefone: Um número de telefone dedicado (ex: 0800 ou chamada local) para abertura e acompanhamento de chamados técnicos, disponível 24x7x365.

- Portal Web: Uma plataforma online segura para abertura de chamados, acompanhamento do status, acesso a bases de conhecimento. Este portal deverá ser acessível via interface web, protegida por senha e conexão segura (HTTPs).

- E-mail: Endereço de e-mail dedicado para comunicação não urgente e envio de informações complementares relacionadas a chamados.

A CONTRATADA designará um preposto formal, com capacidade gerencial, que atuará como interlocutor principal. Este profissional será responsável por receber, diligenciar, encaminhar e responder a todas as questões técnicas, legais e administrativas relativas ao contrato. As informações de contato (nome, telefone, e-mail) deste preposto serão fornecidas formalmente no início do contrato.

Além do preposto, uma equipe de atendimento técnico estará disponível através dos canais de suporte (telefone, portal web). Esta equipe será responsável por triar os chamados, iniciar o tratamento e escalar para especialistas quando necessário. Em casos de urgência extrema, meios alternativos de comunicação (ex: aplicativos de mensagens) poderão ser utilizados, desde que formalizados posteriormente.

Serão realizadas reuniões periódicas (ex: mensais) entre a equipe de gestão da CONTRATANTE e a CONTRATADA para análise de resultados, discussão de incidentes, planejamento de atividades e alinhamento estratégico.

Tempos de Resposta e Solução (Acordo de Nível de Serviço — ANS) para o início do atendimento e para a Solução dos problemas serão definidos por níveis de severidade, garantindo a priorização adequada de cada incidente.

Severidade 1 (ALTA): Problemas que afetam de forma crítica a Solução contratada, causando impactos significativos no desempenho ou interrupção. Início do atendimento: Até 2 horas após a abertura do chamado. Solução (esforço concentrado): Até 6 horas a partir do início do atendimento. Se não solucionado, atendimento presencial obrigatório.

Severidade 2 (MÉDIA): Problemas que criam restrições à operação do sistema, mas não causam interrupções críticas na Solução contratada (ex: erros na configuração, divergências com especificações). Início do atendimento: Até 6 horas após a abertura do chamado. Solução: Até 24 horas a partir do início do atendimento.

Severidade 3 (BAIXA): Solicitações de esclarecimentos ou resolução de problemas que não impactam diretamente a operação da Solução contratada. Início do atendimento: Até o primeiro dia útil seguinte à solicitação. Solução: Até 2 dias úteis a partir do início do atendimento.

Informações que a CONTRATADA tiver acesso deverão ser utilizadas somente nos processos envolvidos para execução do objeto contratado.

A Solução deverá proporcionar a disponibilidade, a integridade e a segurança de todas as informações da CONTRATANTE por ela gerenciadas.

A Solução deve apresentar conformidade com a Lei Geral de Proteção de Dados – LGPD.

A CONTRATADA assinará no ato da entrega da Solução e do início dos serviços, Termo de Confidencialidade e Sigilo antes do início dos serviços, em que se comprometerá a não acessar, não divulgar e a proteger todos os dados de infraestrutura e de vulnerabilidades da CONTRATANTE a que tiver acesso, que abrangerá todos os seus colaboradores e terceiros.

A CONTRATADA deverá informar imediatamente à CONTRATANTE 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.

A CONTRATADA deverá submeter-se aos procedimentos de segurança existentes no ambiente da CONTRATANTE ou que possam ser criados durante a vigência do contrato. Os procedimentos deverão ser observados sempre que for necessário o acesso presencial ou remoto à infraestrutura da CONTRATANTE.

A CONTRATADA e seus profissionais deverão respeitar as diretrizes constantes da Política de Segurança da Informação da Justiça Eleitoral (Resolução TSE Nº 23.644, de 1º de julho de 2021 e da CONTRATANTE ou suas versões mais atuais), obrigando-se a manter sigilo a respeito de quaisquer informações, dados, processos, fórmulas, códigos, cadastros, fluxogramas, diagramas lógicos, dispositivos, modelos ou outros materiais de propriedade da CONTRATANTE aos quais tiver acesso em decorrência do objeto da presente contratação, ficando terminantemente proibida de fazer uso ou revelação destes sob quaisquer justificativas.

A quebra do sigilo acarretará em sanções administrativas, civis e criminais, conforme a legislação vigente (LGPD, Lei Anticorrupção, etc.).

A CONTRATADA deverá adotar boas práticas de governança e controle de acesso para garantir que apenas profissionais autorizados e necessários tenham acesso às informações sensíveis.

A CONTRATADA deverá manter uma comunicação clara e proativa, gerenciando as expectativas do contratante. Isso inclui informar sobre o andamento das atividades, potenciais desafios, e novas funcionalidades ou tendências de segurança que possam beneficiar o ambiente.

A CONTRATADA deverá atuar na melhoria contínua da Solução e dos processos de segurança. Isso se traduz em proposições de ajustes, atualizações de firmware/software, otimização de configurações e análise periódica das práticas internas para garantir a adequação às melhores práticas de mercado e às necessidades em constante evolução da CONTRATANTE.

A flexibilidade e a capacidade de adaptação são fundamentais. Para situações inesperadas ou emergências que possam exigir intervenção on-site ou fora do horário comercial, a CONTRATADA deve ter planos de contingência, com equipes preparadas para atuar rapidamente, minimizando interrupções.

A CONTRATADA deve assegurar o cumprimento integral de todas as legislações e normativas aplicáveis à sua atividade e à prestação de serviços, incluindo aspectos tributários, trabalhistas, ambientais e de privacidade de dados.

A Solução deverá ser ofertada com garantia e manutenção do fabricante e deverá ser prestado na modalidade 24 horas por dia, 7 dias por semana e 365 do ano (24x7x365).

A garantia deverá cobrir falhas no serviço de instalação e configuração da Solução, fornecimento de correções de software, substituição de hardware defeituoso e fornecimento de atualizações corretivas e evolutivas de software e hardware.

O contrato poderá ser prorrogado por até 10 anos, conforme previsão do art. 107 da Lei 14.133/2021.

REQUISITOS DE HARDWARE/SOFTWARE DA SOLUÇÃO

Formato da Contratação: O(s) appliance(s) da Solução de NDR deverá(ão) ser fornecidos em regime de comodato (serviço).

A Solução deverá ser instalada nas dependências da CONTRATANTE e em seu Site Backup.

Tipos de Dispositivos: O(s) dispositivo(s) responsável(eis) pela captura e processamento do tráfego deve(m) ser do tipo appliance físico, purpose-built para a função, e instalado(s) no(s) datacenter(s) do Regional. Não serão aceitas soluções similares baseadas em switches, roteadores, firewalls, balanceadores, servidores ou soluções híbridas.

Processamento e Gerenciamento Local (On-Premise): Todas as operações de processamento de dados e a interface de gerenciamento da Solução deverão ser locais. Adicionalmente, será permitido que somente algumas informações sejam enviados para a nuvem da fabricante apenas para processamento avançado de IA/ML, desde que sejam apenas metadados que tenham passado previamente por um processo de "anonimização" ou "desidentificação" e não o conteúdo completo do(s) pacote(s) de rede. É vedado quaisquer outro envio de dados, sem o tratamento como o acima discriminado, para fora da rede do Regional para que a Solução funcione em sua plenitude.

Integração com Fontes de Inteligência de Ameaças: A Solução deve suportar integração com fontes de inteligência de ameaças (Threat Intelligence) por meio de protocolos e linguagens padronizados.

De modo a preservar os recursos computacionais do datacenter da CONTRATANTE, serão aceitos somente appliances físicos para fornecimento da Solução de NDR.

O uso de recurso virtualizado para Solução de NDR será aceito somente caso a CONTRATADA forneça o host hospedeiro em conjunto com a Solução virtualizada.

Qualquer interface web da Solução de NDR ou integração entre a Solução de NDR com outras ferramentas de segurança deve obrigatoriamente, ser configurada para utilizar conexões criptografadas.

A Solução deve possuir capacidade de resposta a comportamentos anômalos ou suspeitos de forma que consiga realizar bloqueios automatizados, mesmo que para realizar essa funcionalidade seja necessário integração com outras ferramentas de segurança, como o firewall de borda já adquirido pelo Regional.

Captura de Tráfego Virtualizado: Visando possibilitar a captura dos tráfegos de dados existentes na infraestrutura de virtualização de servidores e entre o ambiente de containers, será aceito o uso de sensores ou agentes virtualizados utilizando os recursos computacionais da CONTRATANTE, exclusivamente para essa finalidade.

A Solução deverá ser instalada de forma a coletar o tráfego de rede de modo espelhado ("Out-of-Band"), não podendo acarretar impacto operacional no tráfego de dados da rede dos datacenters da CONTRATANTE.

A Solução será composta pela Solução de NDR, serviço de monitoramento 24x7x365, serviço de operação assistida sob demanda e treinamento no uso da Solução da CONTRATANTE e fornecido pela CONTRATADA.

A Solução deve ser dotada de tecnologia baseada em Inteligência Artificial – IA e Aprendizado de Máquina (machine learning) a fim de identificar anomalias de comportamento e ataques não identificados pelas tecnologias tradicionais de segurança da informação.

A Solução não deve exigir pré-configurações específicas da rede do Regional para identificar associações entre múltiplos elementos da rede e detectar anomalias comportamentais.

Métodos de Detecção: A Solução não deve ser baseada exclusivamente em detecção por assinatura (e.g., IDS, IPS, formato de assinatura de vírus). Deve implementar, adicionalmente, métodos de detecção de anomalias de segurança baseados em comportamento e inteligência artificial por aprendizado de máquina.

Capacidades de Inteligência Artificial e Análise Comportamental: A Solução deve incorporar tecnologia baseada em Inteligência Artificial (IA) para identificar anomalias comportamentais e ataques cibernéticos sofisticados que não são detectados por tecnologias de segurança tradicionais. Deve, no mínimo, empregar os seguintes métodos de IA para a criação de perfis de uso e a detecção de desvios comportamentais na rede: Aprendizado de Máquina Não Supervisionado (Unsupervised Machine Learning), Aprendizado de Máquina Supervisionado (Supervised Machine Learning) e aprendizado Profundo (Deep Learning).

Capacidades de Investigação, Threat Hunting e Forense: A Solução deve viabilizar a implementação de processos de investigação, threat hunting e forense de rede, com base nos metadados gerados pela Solução e suas funcionalidades de detecção e investigação.

Investigação Aprofundada: A Solução de NDR deve ser capaz de viabilizar investigações aprofundadas, como identificar automaticamente o "paciente zero", o ponto de "comprometimento inicial" ou ainda o "primeiro ponto de entrada". Encontrar esse ponto/alvo é crucial para uma investigação aprofundada, pois é apartir dessa informação que a ferramenta, por exemplo, poderá por conta própria, começar a correlacionar de forma automática diversos eventos de segurança, agrupando-os em um único incidente; e assim apresentá-lo de maneira gráfica e cronologicamente ordenada, com todos os detalhes do incidente do ponto/alvo inicial até o(s) ponto(s)/alvo(s) final(is), incluindo os eventos intermediários; agilizando sobremaneira a resolução de incidentes por parte do Regional. Uma investigação aprofundada, que poderia levar dias ou diversas semanas, dependendo da complexidade; e que precisaria ser realizada por uma equipe altamente especializada de um SOC Nível 2 (N2), podendo ainda ter resultados incertos; é realizada em tempo recorde de forma automatizada pela ferramenta.

A Solução de NDR deverá ser composta por um único fabricante, não sendo admitido uso de vários fornecedores ou serviços integrados, nem mesmo por meio de API's (Application Programming Interface). Esta exigência traz inúmeras vantagens para o Órgão, especialmente em termos de segurança, eficiência operacional e simplicidade, dentre elas: eliminação de problemas de compatibilidade; único ponto de contato para suporte técnico acelerando a solução de possíveis problemas técnicos futuros; menor complexidade operacional que ajuda a reduzir o tempo de treinamento da equipe de TI e segurança, além de minimizar erros humanos e prover segurança aprimorada. Uma vez que as dependências externas ou pontos de integração (como APIs) deixam de existir, há menos superfícies de ataque potenciais, logo menos riscos.

A Solução deve adotar uma abordagem proativa e realizar monitoramento contínuo do tráfego de rede, partindo do pressuposto de que ameaças podem estar presentes. O tráfego de rede deve ser a principal fonte para a identificação de rastros de ameaças e seus agentes.

Capacidades de Resposta Automatizada e Integração: A Solução deve ser capaz de iniciar ações autônomas de resposta a ameaças e/ou ataques cibernéticos, baseadas em seu mecanismo de inteligência artificial. Visando habilitar ações adicionais de contenção e bloqueio contra ataques cibernéticos, somente nestes casos, será permitido o uso de APIs para a integração com soluções de segurança de terceiros, ou seja, que não sejam do fabricante da Solução de NDR.

A Solução deve permitir a criação automática de relatórios executivos.

A console de gerenciamento deve ser única, desenvolvida pelo mesmo fabricante da Solução, e abranger o gerenciamento de todos os itens ativos e gerenciáveis da arquitetura.

Todas as funcionalidades da interface de gerenciamento devem ser compatíveis com os navegadores Google Chrome, Microsoft Edge e Mozilla Firefox, em suas configurações padrões.

Deve permitir o gerenciamento de todos os componentes da Solução, incluindo appliances físicos, sensores e ambientes virtualizados (se aplicável).

Deve possuir capacidade de implementar mecanismos de autenticação e autorização para acesso à Solução, integrados ao Microsoft Active Directory do Regional para uso de usuários e senhas contidos nesse repositório.

Sincronização de Horário (NTP): Deve suportar a atualização de horário por meio do protocolo NTP (Network Time Protocol).

Permitir a instalação em rack padrão EIA 19" (dezenove polegadas), acompanhado de todos os adaptadores, cabos e acessórios necessários para sua fixação.

Possuir ventilação tipo "front-to-back", onde a saída de ar quente ocorre pela traseira do equipamento.

Nos casos em que a Solução apresente mal funcionamento ou pare de operar, a rede de comunicação de dados da CONTRATANTE não poderá ser afetada. A Solução deverá operar em modo transparente, não afetando a rede de dados da CONTRATANTE.

Todos os conectores, cabos, interfaces e licenças necessárias para o correto funcionamento da Solução deverão ser fornecidos pela CONTRATADA.

A CONTRATADA deverá levar em consideração os requisitos de cada Regional no dimensionamento da Solução, seguindo as informações presentes na tabela de perfil de cada Regional disponível no Termo de Referência.

O(s) appliance(s) fornecido(s) deverá(ão) suportar a taxa de transferência ("Throughput") de rede, largura de banda, número de ativos e conexões por minuto instaladas no ambiente da CONTRATANTE, disponível na tabela de perfil do Regional, presente no Termo de Referência.

A taxa de transferência ("Throughput") de rede citado no item anterior será informado na tabela de perfil disponível no Termo de Referência e o(s) appliance(s) fornecido(s) pela CONTRATADA deverá(ão) operar com carga máxima de processamento de 80% considerando todo o tráfego informado pela CONTRATANTE.

A Solução deve ser capaz de receber, processar e analisar, em tempo real, todo o tráfego de rede capturado.

Caso o(s) appliance(s) apresente(m) uma taxa de operação superior à 80% (oitenta por cento) em relação aos valores informados no item anterior, a CONTRATADA deverá realizar adequação da Solução para que opere abaixo dessa taxa de operação, sem que essa adequação acarrete qualquer tipo de ônus para a CONTRATANTE.

O hardware fornecido para a Solução deverá possuir fontes de energia redundantes.

REQUISITOS DE OPERAÇÃO ASSISTIDA

O serviço contratado deverá possuir a modalidade de Operação Assistida ("Hands-On"), a ser realizada sob demanda da CONTRATANTE, com atendimento remoto ou presencial para Solução, para qualquer solicitação de esclarecimentos ou auxílio na operação da ferramenta.

O serviço de Operação Assistida será consumido em blocos contendo um número de horas a ser definido pela CONTRATANTE, que irá definir um bloco de horas padrão/mínimo, que julgar mais adequado para utilizar de forma eficientemente as horas contratadas.

Cada acionamento de bloco mínimo ocorrerá por intermédio de emissão de Ordem de Serviço (OS), utilizando os mesmos canais de solicitação para suporte para a Solução.

O regime de solicitação da Operação Assistida ocorrerá em horário comercial.

Todos os eventos relacionados à Operação Assistida que envolvam participação de integrantes da CONTRATANTE serão realizados durante os horários de expediente adotados, de segunda-feira a sexta-feira, exceto feriados, salvo casos de urgência e/ou acordo entre as partes, desde que tempestivamente informados e solicitados.

Este serviço de operação assistida, não deve ser confundido com os serviços de monitoramento, garantia, manutenção, sustentação e suporte da Solução, uma vez que eles se diferem principalmente pela obrigatoriedade dos últimos, obedecerem ao regime de 24x7x365 (vinte e quatro horas do dia, nos sete dias da semana, em todos os dias do ano).

O número total de horas previstas para a vigência do contrato referente à Operação Assistida, está disponível na tabela de perfil do Regional , que se encontra no Termo de Referência.

A solicitação do serviço de Operação Assistida ocorrerá sob demanda. O Regional irá designar a melhor forma de pagamento.

A CONTRATANTE deverá observar o empenho do valor relacionado a este serviço durante a vigência contratual.

O serviço será solicitado somente sob demanda da equipe técnica da CONTRATANTE e em caso de necessidade.

Poderá ser solicitado no mínimo 01 (um) bloco e até no máximo 06 (seis) blocos por dia para suporte na modalidade de Operação Assistida, considerando o total de 96 (noventa e seis) blocos durante toda vigência contratual.

O valor do bloco de horas para a Operação Assistida deverá ser informado como item discriminado dos demais serviços relacionados à Solução.

REQUISITOS DE CAPACITAÇÃO E TREINAMENTO

Deverá ser fornecido treinamento oficial para operação da Solução, que será alocada no ambiente do Regional, cujo conteúdo deverá ser suficiente para a perfeita compreensão e operação de todos os seus requisitos.

O treinamento deverá ser fornecido, por aluno, para servidores detentores de cargos efetivos da CONTRATANTE, com emissão de certificados e pesquisa de satisfação ao final do treinamento, sendo que a CONTRATADA estará sujeita a atingir uma qualidade mínima, sob pena de sanção aplicável, a ser definida no Termo de Referência;

Deverão ser disponibilizadas o número de vagas de acordo com a tabela do perfil do Regional, disponível no Termo de Referência.

O treinamento deverá ser realizado de forma remota, via videoconferência, na modalidade síncrona ("On-line"), objetivando agilizar a capacitação das equipes envolvidas, possibilitando atender de forma simultânea a equipe técnica que atua tanto na modalidade presencial quanto em teletrabalho.

O treinamento deverá ser gravado e permanecer disponível para consulta dos alunos por pelo menos 90 (noventa) dias após a sua realização.

Poderão ser indicados mais participantes na categoria de ouvintes, sem a exigência de fornecimento de certificado de participação e material por parte da CONTRATADA, limitando-se a 5 (cinco) participantes adicionais nessa modalidade.

Todas as despesas referentes à realização do treinamento ou ao custeio de insumos deverão estar discriminadas em item a parte do objeto principal.

REQUISITOS TEMPORAIS

Na contagem dos prazos estabelecidos neste Estudo Técnico, quando não expressados de forma contrária, excluir-se-á o dia do início e incluir-se-á o do vencimento.

Todos os prazos citados, quando não expresso de forma contrária, serão considerados em dias úteis.

Todos os eventos de trabalho que envolvam participação da equipe técnica da CONTRATANTE ou de integrantes da CONTRATADA em ambiente da CONTRATANTE serão realizados durante os horários de expediente adotados, de segunda-feira a sexta-feira, exceto feriados, salvo casos de urgência e/ou acordo entre as partes, desde que tempestivamente informados e solicitados.

Não será computado o tempo de atraso quando este tiver sido ocasionado pela CONTRATANTE ou por fatos supervenientes que impeçam ações da CONTRATADA, desde que devidamente justificado e aceito pela CONTRATANTE.

Não serão considerados casos ou fatos supervenientes as situações externas que possam ser contornadas ou mitigadas por ações de logísticas preventivas ou reativas da CONTRATADA.

REQUISITOS LEGAIS

Observância à Lei 13.853/2019 – Lei Geral de Proteção de Dados Pessoais.

Resolução CNJ N° 182/2013, dispõe sobre diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação pelos órgãos submetidos ao controle administrativo e financeiro do Conselho Nacional de Justiça (CNJ).

CNJ nº 370/2021, institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD).

Resolução CNJ nº 396/2021, institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

Lei n° 14.133/2021, que institui normas para licitações e contratos da Administração Pública.

REQUISITOS DE METODOLOGIA DE TRABALHO

Deverá ser apresentada documentação técnica detalhada contendo todas as informações referentes a instalação e a configuração de todos os itens que compõe a Solução (“As-Built”), com plano de ação detalhando as ações e procedimentos realizados.

A instalação e configuração da Solução só será considerada finalizada pelo Regional quando todas as VLANs ou correlatos apontados pelo Órgão como necessárias para inclusão no monitoramento, estiverem todos sendo monitorados; bem como, somente quando a Solução estiver configurada de forma a ter o mínimo de falsos positivos possibilitados pela ferramenta.

REQUISITOS SOCIAIS, AMBIENTAIS E CULTURAIS

Todos os manuais, guias de instruções e ajuda deverão ser disponibilizados preferencialmente no idioma português do Brasil – PT-BR ou Inglês e fornecidos em meio digital.

Os softwares aplicativos e interface do software devem ter a possibilidade de escolha de idioma pelo usuário. Será admitido o idioma inglês somente quando não existir uma versão no idioma em português do Brasil.

Os profissionais da CONTRATADA, quando nas dependências da CONTRATANTE, deverão apresentar-se com crachá de identificação, trajados de forma adequada ao ambiente de trabalho, evitando-se o vestuário que caracterize o comprometimento da boa imagem institucional da CONTRATANTE.

Os profissionais da CONTRATADA deverão zelar pela boa educação e tratar com urbanidade servidores, funcionários e colaboradores em qualquer posição hierárquica, preservando a comunicação e o relacionamento interpessoal construtivo.

REQUISITOS DE EXPERIÊNCIA PROFISSIONAL DA EQUIPE DA CONTRATADA

Demonstrar que a equipe de pessoas que irá atuar na implantação e operação da Solução possui a competência necessária para projetar, implementar e manter a Solução fornecida.

Apresentar a qualificação técnica necessária da equipe através de experiência técnica e profissional; além de certificações técnicas e atestados de capacidade técnica, compatíveis com os serviços a serem prestados pela CONTRATADA.

REQUISITOS DE PROPRIEDADE INTELECTUAL

A CONTRATADA cederá o direito à CONTRATANTE a todos os documentos e procedimentos operacionais produzidos em consequência dos serviços contratados, entendendo-se por documentos e procedimentos operacionais quaisquer estudos, relatórios, artefatos, descrições técnicas, protótipos, dados, esquemas, plantas, desenhos, diagramas, roteiros, tutoriais, scripts, fontes dos códigos de programas computacionais fornecidos pela CONTRATADA em qualquer mídia, páginas de Intranet e Internet e qualquer outra documentação produzida no escopo da presente contratação, em papel ou em mídia eletrônica, não precisando o Regional de autorização da CONTRATADA para reproduzir, distribuir e publicar em documentos públicos ou fornecer a terceiros quando a administração considerar necessário.

REQUISITOS DE IMPLANTAÇÃO

Infraestrutura tecnológica: Não serão necessários ajustes no ambiente computacional da CONTRATANTE que venha a acarretar algum impacto financeiro ou de pessoal.

Infraestrutura elétrica: A infraestrutura elétrica do ambiente da CONTRATANTE é capaz de suportar os serviços a serem contratados. Qualquer adequação no ambiente da CONTRATANTE para suportar os materiais, equipamentos, da CONTRATADA deverão ser suportados por ela.

Logística de implantação: Será provido pela CONTRATANTE o acesso físico às suas dependências aos diretamente envolvidos na prestação dos serviços. Assim como no caso do acesso físico, será fornecido o acesso lógico e os respectivos privilégios adequados nos sistemas, aplicações e ferramentas necessárias à perfeita execução dos serviços, exclusivamente para os profissionais diretamente envolvidos em sua execução.

Os acessos físicos e lógicos que tratam o item anterior deverão ocorrer de forma supervisionada pela equipe técnica da CONTRATANTE.

Espaço físico: A CONTRATANTE deverá disponibilizar espaço físico necessário para comportar a equipe de profissionais da CONTRATADA.

REQUISITOS DE DESINSTALAÇÃO DA SOLUÇÃO OU DESCOMISSIONAMENTO DA SOLUÇÃO

Ao final do período contratual, os dados colhidos pela Solução deverão ser sanitizados ou excluídos de forma definitiva e irreversível.

O processo de desinstalação da Solução de NDR deverá ser executado por profissional qualificado pela CONTRATADA e na presença de pelo menos um dos fiscais do contrato.

Um termo de sanitização do(s) appliance(s) envolvidos na Solução deverá ser emitido e assinado pelo representante legal da CONTRATADA.

Deverá ainda ser fornecido à CONTRATANTE um relatório final em forma de documento assinado, em meio físico e digital, com todas as evidências necessárias que comprovem futuramente a correta exclusão e sanitização, impedindo com que os dados sejam recuperados à posteriori, para que tal relatório seja anexado ao processo da contratação.

A ação de descomissionamento deverá ser realizada de forma presencial pela CONTRATADA e na presença dos Fiscais do Contrato da CONTRATANTE.

6.2 ALINHAMENTO DA SOLUÇÃO

PEI
Fortalecimento da Estratégia Nacional de TIC e de Proteção de Dados

PDTIC 2021-2026 (Objetivos Estratégicos)
Buscar a Inovação de Forma Colaborativa (Índice de Iniciativas realizadas em colaboração com outros órgãos do Judiciário) - (KR1 - 4.1)
Aprimorar a Segurança da Informação e a Gestão de Dados (Número de vulnerabilidades críticas e altas) - (KR1 - 7.1)

6.3 BENEFÍCIOS ESPERADOS

- Monitoramento contínuo e visibilidade em tempo real de possíveis ameaças cibernéticas;
- Monitoramento de segurança com baixa taxa de falsos positivos (decorrentes das análises aprofundadas realizada pela Solução escolhida), considerando a adoção de avançados recursos, tais como inteligência artificial, machine learning não supervisionado e análise comportamental da rede e de seus componentes de forma autônoma e contínua, adaptando-se às variações de comportamento;
- Menor interferência humana na atividade de monitoramento das ameaças a ser realizado, trazendo assim mais agilidade e segurança para o processo como um todo;
- Garantir a disponibilidade, desempenho e confiabilidade dos serviços prestados pelo Regional.

6.4 RELAÇÃO ENTRE A DEMANDA PREVISTA E A SER CONTRATADA

A previsão inicial, listada no DOD, era maior, com previsão de monitoramento externo e interno ao Regional.

Mas, durante o levantamento do presente Estudo Preliminar, verificou-se a importância de focar-se primeiro no monitoramento interno; e uma vez que este esteja consolidado, partir para a melhoria contínua e alçar vôos maiores, a fim de melhorar ainda mais a segurança do Regional.

6.5 ADEQUAÇÃO DO AMBIENTE

Infraestrutura tecnológica: Não serão necessários ajustes no ambiente computacional do Regional que venha a acarretar algum impacto financeiro ou de pessoal.

Infraestrutura elétrica: A infraestrutura elétrica do ambiente do TRE-MS é capaz de suportar os serviços a serem contratados. Qualquer adequação no ambiente do TRE-MS para suportar os materiais, equipamentos, da CONTRATADA deverão ser suportados por ela.

Logística de implantação: Será provido pelo TRE-MS o acesso físico às suas dependências aos diretamente envolvidos na prestação dos serviços. Assim como no caso do acesso físico, será fornecido o acesso lógico e os respectivos privilégios adequados nos sistemas, aplicações e ferramentas necessárias a perfeita execução dos serviços, exclusivamente para os profissionais diretamente envolvidos em sua execução.

Espaço físico: O TRE-MS disponibilizará sala com o espaço físico necessário para comportar a equipe de profissionais da contratada.

Mobiliário: O TRE-MS disponibilizará os materiais, como: mobiliário (cadeiras e mesas de escritório) necessário para comportar a equipe de profissionais da contratada.

Impacto Ambiental: Apesar do Plano de Logística Sustentável do TRE-MS prever, no tópico “Gestão de resíduos”, que o Tribunal deve “Promover a destinação ecologicamente correta dos resíduos gerados como lixo eletrônico, o objeto desta contratação não se enquadra na gestão de resíduo mencionada.

6.6 ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

O valor estimado da contratação é de **R$ 3.204.079,10** para o TRE-MS (por 3 Anos, Pagamento Único) e **R$ 6.785.378,17** para o TRE-MG (também por 3 Anos, Pagamento Único), totalizando **R$ 9.989.457,27.**

7. SUSTENTAÇÃO DO CONTRATO

7.1 RECURSOS NECESSÁRIOS À CONTINUIDADE DO NEGÓCIO DURANTE E APÓS A EXECUÇÃO DO CONTRATO

7.1.1 RECURSOS MATERIAIS

Todos os recursos materiais necessários para a implantação deverão ser fornecidos pela empresa contratada.

7.1.2 RECURSOS HUMANOS

Em relação aos Recursos Humanos, serão necessários:

- 03 (três) servidores do quadro para atuarem como gestores do contrato e fiscais demandante e técnico da contratação.

7.2 ESTRATÉGIA DE CONTINUIDADE CONTRATUAL

Os serviços objeto desta contratação são considerados essenciais e de natureza contínua, com possibilidade de prorrogação, por até 10 anos, pois devem ser realizados ininterruptamente, e sua paralisação acarretará suspensão ou o comprometimento das atividades prestadas pelos servidores e colaboradores do Regional.

A descontinuidade da prestação do serviço poderá afetar a disponibilização de sistemas providos pelo TRE-MS como através da rede da justiça eleitoral.

Havendo uma descontinuidade e em momento crítico, o Regional poderá proceder contratação imediata nos moldes permitidos na Lei nº 14.133/2021.

7.3 TRANSIÇÃO CONTRATUAL

O processo de transição do contrato se inicia a partir do momento em que a empresa assumir as responsabilidades, de forma gradual, pelos serviços prestados, preparando-se para o início efetivo da operação. Esse processo de transição contratual tem o propósito de preparar a empresa para assumir integralmente as obrigações advindas com o contrato, e será baseada em reuniões e repasse de documentos técnicos e/ou manuais específicos das soluções adquiridas.

Ao final do contrato de prestação dos serviços, a empresa deverá fornecer, pelo período de até 90 (noventa) dias corridos, todas as informações necessárias à transição para a empresa sucessora à prestação dos serviços, além de elaborar e atualizar toda a documentação que porventura não tenha sido devidamente gerada ou atualizada durante o período de vigência do contrato.

A empresa deverá se responsabilizar pela transição inicial e final dos serviços, absorvendo as atividades e documentando-as minuciosamente, para que os repasses de informações, conhecimentos e procedimentos, no final do contrato aconteçam de forma precisa e responsável.

7.4 ESTRATÉGIA DE INDEPENDÊNCIA TECNOLÓGICA

7.4.1 TRANSFERÊNCIA DE CONHECIMENTO

A empresa deverá realizar treinamento para gestão e operacionalização da Solução que será entregue, a todos servidores efetivos que forem definidos pelo Regional, para pleno conhecimento e entendimento da Solução.

Sempre que possível for, caberá também à empresa fazer o repasse de conhecimento em procedimentos e ações operacionais realizadas cotidianamente, desde que não impactem nas entregas mensais previstas, a fim de avaliarmos a qualidade dos serviços prestados.

7.4.2 DIREITOS DE PROPRIEDADE INTELECTUAL

Com essa contratação, o Regional irá adquirir serviços que compõe a Solução, não sendo detentor de propriedade intelectual de tais serviços. Ressalte-se que os direitos autorais dos fabricantes dos softwares e hardwares utilizados na Solução são resguardados e garantidos por legislação nacional e internacional.

Os direitos autorais e os direitos de propriedade intelectual da Solução de Tecnologia da Informação sobre os diversos artefatos e produtos produzidos ao longo do contrato, incluindo a documentação, os modelos de dados e as bases de dados, pertencerão ao Regional, devendo ser justificado os casos em que isso não ocorrer.

Portanto a empresa cederá os direitos de propriedade intelectual sobre os diversos artefatos produzidos ao longo do contrato, incluindo a documentação, modelos de dados e as bases de dados do Regional.

7.5 CRITÉRIOS DE SUSTENTABILIDADE

- Os documentos e/ou relatórios deverão ser entregues, sempre que possível, por via informatizada de forma a não utilizar papel ou outro insumo semelhante;
- Caso a impressão seja necessária, a empresa deve adotar práticas de impressão sustentáveis, como a utilização de papel reciclado, impressão frente e verso e a minimização do uso de tintas prejudiciais ao meio ambiente;
- Este Regional, quando da redação da cláusula que estipula os horários de realização dos serviços, deu preferência por conciliar com horários de funcionamento do órgão onde a energia e demais insumos já são utilizados.
- As embalagens a serem utilizadas na realização dos serviços, sempre que possível, deverão ser de material de baixo impacto ecológico.
- A empresa contratada deverá fornecer aos empregados os equipamentos de segurança que se fizerem necessários, para a execução de serviços.

8. ESTRATÉGIA PARA A CONTRATAÇÃO

8.1 NATUREZA DO OBJETO

Trata-se de contratação serviços comuns de Tecnologia da Informação, se submetendo à resolução CNJ 468/2022.

8.2 PARCELAMENTO DO OBJETO

Não haverá parcelamento do objeto, a contratação abrange serviços de monitoramento da rede interna, voltados para análise, detecção e resposta de ameaças cibernéticas em escala 24x7x365, com equipe de monitoramento remota e adoção de tecnologias de análise de comportamento e inteligência artificial (machine learning não supervisionado, supervisionado e deep learning); instalação, configuração, treinamento remoto, suporte técnico, garantia e manutenção, os quais podem ser oferecidos por diversos fornecedores.

A não fragmentação assegura maior eficiência e economicidade ao processo, garantindo que a responsabilidade pela entrega da Solução completa recaia sobre um único fornecedor, o que possibilita maior controle, coordenação e qualidade na prestação dos serviços.

Além disso, a execução fragmentada, com a contratação de diferentes fornecedores, não é viável, uma vez que os itens são interdependentes e a sua execução exige sinergia técnica e operacional. A separação do fornecimento poderia acarretar riscos significativos, como incompatibilidades técnicas, dificuldades de integração entre as partes e eventuais lacunas de responsabilidade, especialmente em casos de inexecução ou má execução por parte de um dos fornecedores.

Portanto, com base nos dispositivos legais aplicáveis e nas características específicas do objeto, a contratação será realizada de forma unificada, preservando os princípios da eficiência, da economicidade e da continuidade dos serviços públicos.

8.3 ADJUDICAÇÃO DO OBJETO

A adjudicação se dará à empresa que apresentar proposta que atenda a todos os requisitos do Edital, especificações do objeto e estejam habilitadas. Os itens que formam cada lote serão adjudicados a empresa que oferecer o menor valor global para o grupo.

8.4 MODALIDADE E TIPO DE LICITAÇÃO

A contratação dos serviços será realizada mediante licitação na modalidade de PREGÃO, em sua forma eletrônica, do tipo menor preço, nos termos do inciso XLI, art 6º e art. 29 da Lei 14.133/2021:

> Art. 6º [...]
>
> XLI - pregão: modalidade de licitação obrigatória para aquisição de bens e serviços comuns, cujo critério de julgamento poderá ser o de menor preço ou o de maior desconto;
>
> [...]
>
> Art. 29. A concorrência e o pregão seguem o rito procedimental comum a que se refere o art. 17 desta Lei, adotando-se o pregão sempre que o objeto possuir padrões de desempenho e qualidade que possam ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado. (grifo nosso)

Tendo em vista que se trata de uma contratação centralizada, onde o TRE/MS será o órgão gerenciador, adotarse-a o Sitema de Registro de Preços, comcom base no art. 3º, inciso III, do Decreto nº 11.462/2023, o qual traz os seguintes dizeres:

> Art. 3º O SRP poderá ser adotado quando a Administração julgar pertinente, em especial:
>
> I - quando, pelas características do objeto, houver necessidade de contratações permanentes ou frequentes;
>
> II - quando for conveniente a aquisição de bens com previsão de entregas parceladas ou contratação de serviços remunerados por unidade de medida, como quantidade de horas de serviço, postos de trabalho ou em regime de tarefa;
>
> III - quando for conveniente para atendimento a mais de um órgão ou a mais de uma entidade, inclusive nas compras centralizadas;
>
> IV - quando for atender a execução descentralizada de programa ou projeto federal, por meio de compra nacional ou da adesão de que trata o § 2º do art. 32; ou
>
> V - quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela Administração.

Por se tratar de registro de preços, conforme determina o art. 86 da Lei 14.133/2021, nos termos do regulamento do Decreto nº 11.462/2023, se faz necessária a realização de procedimento público de intenção de registro de preços (IRP), com a divulgação do Termo de Referência no sistema gov.br/compras e PNCP, pelo prazo de 8 (oito) dias úteis, que visa possibilitar a participação de outros órgãos e entidades da Administração Pública na Ata de Registro de Preços.

Será permitida apenas a participação do Tribunal Regional Eleitoral de Minas Gerais (TRE-MG), por se tratar de contratação centralizada, com a participação colaborativa estratégica desse Regional, cujos serviços a serem contratados estão adequados às suas necessidades do TRE/MS e TRE/MG de forma qualitativa e quantitativa. A simples soma de demandas de outros órgãos, sem uma análise prévia de compatibilidade e complexidade, geraria uma estimativa irreal e impraticável para qualquer licitante.

A contratação foi concebida, desde sua origem, como um arranjo colaborativo estratégico entre este TRE/MS e o TRE-MG em todo o projeto, não se tratando apenas de aquisição de um serviço.

Diante do exposto esta Equipe de Planejamento sugere a não aceitação da participação de outros órgãos, além do TRE-MG, no procedimento de Intenção de Registro de Preços (IRP) para assegurar a exequibilidade, a eficiência e a segurança da presente contratação, com a condução de um processo licitatório focado nas necessidades e na realidade dos órgãos partícipes originários.

8.5 CLASSIFICAÇÃO E INDICAÇÃO ORÇAMENTÁRIA

As despesas decorrentes do objeto desta licitação, serão custeadas com recursos aprovados pela Lei Orçamentária da União nº 115.080 de 30/12/2024, que estima a receita e fixa a despesa da União para o exercício financeiro 2025 (LOA).

Unidade 14112 – TRE-MS
Ação: 21EE – Gestão da Política de Segurança da Informação e Cibernética na Justiça Eleitoral
Programa de Trabalho 02.122.0033.21EE.0001
Elementos de Despesa: 33.90.40 - SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO – PJ
Subitem 21 – SERVIÇOS TÉCNICOS PROFISSIONAIS DE TIC.

As despesas que vierem a ocorrer nos exercícios futuros serão custeadas com recursos previstos nas respectivas Propostas Orçamentárias, e serão indicados oportunamente.

As informações acerca da disponibilidade orçamentária podem ser alteradas pela COPEG.

8.6 VIGÊNCIA DA PRESTAÇÃO DE SERVIÇO

O período de vigência desta contratação será de **3 (três) anos,** podendo ser prorrogado, nos termos do art. 107 da Lei 14.133/2021.

O prazo para início da execução será de no máximo 60 (sessenta) dias, contados **a partir da emissão da solicitação formal da fiscalização do contrato (abertura de ordem de serviço).**

8.7 EQUIPE DE APOIO À CONTRATAÇÃO (Art. 20 Resol. 468 CNJ)

A equipe que subsidiará a área de Licitações em suas dúvidas, respostas aos questionamentos, recursos e impugnações, bem como na análise e julgamento das propostas das licitantes pertence à Secretaria de Tecnologia da Informação, sendo os servidores Antônio Mendes Barata Segundo e Gustavo Leite Pinho, lotados na Assessoria Técnica de Segurança da Informação e Cibernética, Robson Massaki Kobayashi lotado na Seção de Gestão de Infraestrutura de TI e a servidora Graziela Gonçalves Silva Jurado, lotada na SAOF/Coordenadoria de Recursos Materiais/SLC.

8.8 EQUIPE DE GESTÃO DA CONTRATAÇÃO (Arts. 21e 24 Resol. 468 CNJ)

Gestora da Contratação: Luciana J. V. de Aguiar

Fiscal Demandante: Antônio Mendes Barata Segundo

Fiscal Técnico: Gustavo Leite Pinho

Fiscal Administrativo: a ser indicado pela Secretaria de Administração e Finanças

8.9 OBRIGATORIEDADE DE EXIGÊNCIA DE CONTRATAÇÃO DE EGRESSOS

A exigência não é aplicável ao presente objeto, por se tratar de serviços de tecnologia da informação, já excetuados pela Comissão do Projeto Começar de Novo deste TRE/MS (0589349).

8.10 ATESTADO DE CAPACIDADE TÉCNICA

Será exigido a apresentação de Atestado de Capacidade técnica emitido por pessoa jurídica de direito público ou privado que comprove a expertise/experiência/proficiência na gestão de serviços de monitoramento proativo e resposta a incidentes de segurança da informação, ou atestados de gestão em cibersegurança com discriminações dos serviços prestados que sejam similares ao mencionado neste item, em ambientes com no mínimo 2.000 (dois mil) ativos/dispositivos compreendidos no escopo do serviço prestado.

A comprovação de experiência mínima de 1 (um) ano na prestação de serviços de gestão de soluções de segurança da informação, ou atestados de gestão em cibersegurança com discriminações dos serviços prestados que sejam similares ao mencionado neste item, em ambientes com no mínimo 1.500 (mil e quinhentos) usuários.

Será permitido somatório de atestados.

9. ANÁLISE DE RISCOS

O Mapa de Gerenciamento de Riscos foi produzido pela equipe de planejamento e está registrado no processo sob ID nº (1814298).

10. DECLARAÇÃO DA VIABILIDADE DA CONTRATAÇÃO

A equipe de planejamento, diante dos dados expostos, entende que a contratação é viável e necessária, de monitoramento do ambiente computacional interno do Regional, com fins de implatanção de serviços de análise, detecção e resposta a ameaças cibernéticas.

Antônio Mendes Barata Segundo
Integrante Demandante

Robson Massaki Kobayashi
Integrante Técnico

Gustavo Leite Pinho
Integrante Técnico

Graziela Gonçalves Silva Jurado
Integrante Administrativa

Documento assinado eletronicamente por **GRAZIELA GONÇALVES SILVA JURADO**, **Chefe de Seção**, em 04/11/2025, às 14:32, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **GUSTAVO LEITE PINHO**, **Técnico Judiciário**, em 05/11/2025, às 08:11, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **ANTÔNIO MENDES BARATA SEGUNDO**, **Técnico Judiciário**, em 05/11/2025, às 15:12, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-ms.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1943856** e o código CRC **42B4CFDB**.