PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

Estudos Técnicos para Registro de Preços para contratação de solução de Monitoramento, Detecção, Notificação, Investigação e Resposta a Ataques Cibernéticos, pelo período de 24 meses.

PROAD Nº 9.605/2021

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

1 ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO

1.1 Contextualização

Situação Atual:

O monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos, bem como o gerenciamento de eventos e informações de segurança de TIC são essenciais para o rastreamento de atividades de usuários dos sistemas, sem o qual o uso abusivo (com desvio de finalidade) ou malicioso (malwares) de recursos computacionais tornam-se mais difíceis ou demorados para serem detectados e tratados.

Quando a Coordenadoria de Segurança de TIC foi instituída no TRT2, procurou-se estabelecer possíveis ferramentas que auxiliassem a equipe na visibilidade e tratamento de incidentes cibernéticos no parque computacional do Tribunal. Nesse ínterim, após várias reuniões com diferentes fornecedores, foi considerado que o custo de uma solução como essa seria muito elevado, para aquele momento, frente a maturidade da equipe, recém estabelecida, e que ainda angariava experiência na área de segurança da informação. Dessa forma, optou-se pelo uso ferramentas de código aberto como ELK (Elasticsearch, Logstash e Kibana - três ferramentas comumente usadas em conjunto e que permitem extrair logs, visualizá-los e consultá-los), além da criação de scripts em shell Linux para alguns monitoramentos, onde a forma de alerta seria o envio de e-mails. No entanto, pelo tamanho reduzido da equipe, essa construção foi sendo realizada aos poucos e até hoje controles são implementados dessa maneira. Ao longo do tempo, apesar de ter trazido amadurecimento para a equipe, essa forma de realizar o monitoramento demonstrou-se precária, insuficiente e onerosa para a equipe. Dentre os pontos de atenção em relação ao modelo em uso, destacam-se:

- Dificuldade de se configurar a ferramenta para tratar os diversos tipos de fontes de dados que podem ser enviados;
- Complexidade para se criar correlacionamentos diversos, mesmo entre os registros de um mesmo tipo de fonte de dado;
- Não possui um conjunto mínimo de regras de detecção e de correlação, ou seja, todas devem ser criadas integralmente, quando possível;
- Não possui suporte nativo a uma série de ferramentas de apoio como: registro de incidentes, criação e automação de playbooks, inteligência de ameaças, entre outras;

- Não possui suporte técnico, ainda mais quando se trata dos scripts em shell Linux que foram desenvolvidos;
- Em um ambiente com muitos equipamentos e heterogêneo como é o do TRT2, muitas são as origens dos registros de auditoria, o que demanda tempo para a visualização, filtragem e correlacionamento de eventos que permitem detectar e analisar os usos abusivos ou maliciosos.

Mais recentemente, o CNJ estabeleceu a ENSEC-JT (Estratégia Nacional de Segurança da Informação e Cibernética do Poder Judiciário) onde se determina, entre seus diversos pontos de importância:

> *Art. 11. Para elevar o nível de segurança das infraestruturas críticas, deve-se:*
>
> *IV – utilizar tecnologia que possibilite a análise consolidada dos registros de auditorias coletados em diversas fontes de ativos de informação e de ações de usuários, permitindo automatizar ações de segurança e oferecer inteligência à análise de eventos de segurança;*
>
> *V – utilizar tecnologia que permita a inteligência em ameaças cibernéticas em redes de informação; especialmente em fóruns, inclusive da iniciativa privada e comunidades virtuais da internet;*

Diante de oportunidade renovada, não só pela ENSEC-JT, mas também pelo estabelecimento de contratações nacionais por meio do Subcomitê Nacional de Segurança Cibernética do CSJT (SNSec), onde um “Serviço de Correlação de Logs de Segurança” ficou a cargo do TRT2, procurou-se restabelecer o contato com os fornecedores de SIEM. No entanto, durante a prospecção de mercado, levantou-se que a tecnologia avançou de SIEM para XDR (eXtended Detection and Response) e, desta forma, foram necessárias várias rodadas de reuniões com diversos fornecedores para que se estabelecesse um entendimento desse novo ferramental e que uma especificação fosse redigida de forma a, não somente haver a possibilidade de contratação de uma solução que atingisse as expectativas da Justiça do Trabalho, mas que também fosse possível de ser atendida pelo mercado.

Com a experiência obtida e diante ampla gama de especializações necessárias para o atingimento dos resultados esperados, também verificou-se que, além de uma ferramenta de XDR, seria importante que um serviço de SOC (Centro de Operações de Segurança, do inglês Security Operation Center) fosse contratado de forma que, além de haver um

monitoramento 24 horas por dia, 7 dias por semana, ele fosse feito por uma equipe de especialistas em cibersegurança, o que aumentou a complexidade da solução, exigindo, assim, um maior esforço na análise e consolidação dos requisitos.

Por conta dessa necessidade, o CSJT determinou a criação de um grupo de trabalho entre o TRT2 e membros do SNSec para a realização de uma análise mais criteriosa da especificação que havia sido redigida. Durante este trabalho houve a criação de um grupo no Google Space com a participação de outros Regionais e com o Tribunal Superior do Trabalho (TST), proporcionando a todos maior clareza da contratação que estava sendo efetuada, além de permitir que sugerissem alterações que julgassem importantes. Esse trabalho culminou em mais algumas reuniões, inclusive com novos fornecedores, que trouxeram ainda mais maturidade para o documento, permitindo a elaboração de uma especificação técnica completa e robusta, incluindo todas as necessidades levantadas por todos os Regionais e TST e permitindo a ampla competitividade entres os principais fornecedores do mercado que validaram as novas alterações propostas. Para permitir o levantamento de dados de dimensionamento (quantidade de ativos de cada Tribunal), foi aberto pelo CSJT o JIRA EGPTI-3212, onde todos os tribunais puderam se manifestar.

As atividades realizadas pelo grupo de trabalho permitiram o amadurecimento da compreensão de que por meio da implantação de uma solução de Monitoramento, Detecção, Notificação, Investigação e Resposta a Ataques Cibernéticos, é possível prover ao ambiente computacional, soluções de segurança cibernética que permitam a visibilidade de logs, dados de telemetria, tráfego de rede e de informações correlatas, capazes de identificar eventos suspeitos ou incomuns que possam comprometer os serviços tecnológicos do Tribunal, utilizando-se da coleta, processamento e correlação dos logs de eventos, dados de telemetria e/ou de rede dos ativos monitorados e do tráfego de rede.

Considerando que existe uma tendência preocupante para o cenário de segurança cibernética nas infraestruturas críticas e sistemas de informação governamentais, é imprescindível a disponibilização de serviço técnico especializado de monitoramento de ameaças cibernéticas em regime 24x7, com resposta a incidentes de segurança, de modo a minimizar os impactos de possíveis ocorrências de incidentes de segurança cibernética.

Nesse contexto, a consolidação do PJe vem proporcionando grandes avanços para a prestação jurisdicional da JT. Com o processo judicial existindo e tramitando exclusivamente

no meio eletrônico, além de vários outros sistemas utilizados, a tecnologia da informação passou a ser componente essencial para a continuidade dos serviços prestados pelo TRT2.

Aliado a isso, o cenário tecnológico atual coloca o Brasil como um dos principais alvos cibernéticos no mundo[1], tendo o governo como o principal alvo dos hackers[2]. Muitas notícias de ataques cibernéticos a órgãos governamentais foram veiculadas nos últimos anos, como o ataque ao STJ ocorrido em 2020[3], o ataque ao TRT-4 ocorrido em 2021[4] e o ataque ao TRT-17 ocorrido em 2022[5]. Pesquisas também apontam que os ataques de ransomware aumentaram 51% em um ano, colocando o país na primeira posição como sendo o mais atacado da América Latina[6]. Quando exitosos, estes ataques podem causar grande indisponibilidade nos sistemas computacionais, além de colocar em risco a integridade e o sigilo das informações armazenadas.

Considerando a tendência preocupante no cenário de segurança cibernética nas infraestruturas críticas e sistemas de informação governamentais, é fundamental a instituição de cenário seguro e compatível para defesa cibernética.

Reconhecendo este cenário, a implantação da solução proposta é congruente com as novas demandas de segurança da informação que enfrentamos atualmente, corroborada pela Resolução nº 396 de 07/06/2021 do CNJ.

1.2 Equipe de Planejamento da Contratação:

A Equipe de Planejamento da Contratação é formada pelos seguintes membros:

Integrante	Nome	Ramal	E-Mail (@trt2.jus.br)
Demandante Titular	Ramon Chiara	2737	incidentesseg-ti@trt2.jus.br

[1] https://www.cnnbrasil.com.br/tecnologia/por-que-o-brasil-e-um-dos-principais-alvos-de-ataques-ciberneticos-do-mundo/
[2] https://canaltech.com.br/seguranca/governo-e-o-principal-alvo-de-ataques-ciberneticos-no-brasil-revela-analise-189050/
[3] https://www.techtudo.com.br/listas/2020/11/ataque-hacker-ao-stj-seis-coisas-que-voce-precisa-saber-sobre-o-caso.ghtml
[4] https://www.trt4.jus.br/portais/trt4/modulos/noticias/474900
[5] https://g1.globo.com/es/espirito-santo/noticia/2022/02/21/tribunal-regional-do-trabalho-do-es-sofre-ataque-cibernetico.ghtml
[6] https://www.cisoadvisor.com.br/maioria-das-empresas-que-usam-rdp-estao-expostas-a-ransomware/

Demandante Substituto	Lucas Ihara Alves	2737	lucas.alves@trt2.jus.br
Técnico 1 Titular	Luciano de Souza Paiva	2070	luciano.paiva@trt2.jus.br
Técnico 1 Substituto	Leonardo Henrique Day de Toledo	2070	leonardo.toledo@trt2.jus.br
Técnico 2 Titular	Ramon Chiara	2737	incidentesseg-ti@trt2.jus.br
Técnico 2 Substituto	Lucas Ihara Alves	2737	lucas.alves@trt2.jus.br
Administrativo Titular	Bruno Thiago Pereira Pacelli	2807	bruno.pacelli@trt2.jus.br
Administrativo Substituto	Ricardo Brandão Longo	2807	ricardo.brandao@trt2.jus.br

1.3 Definição e Especificação dos Requisitos da Demanda

A presente demanda consiste na contratação de solução que seja capaz de apoiar a área demandante no monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos no ambiente computacional do TRT2, bem como serviços de treinamento, implantação e sustentação da solução proposta, este último sendo realizado por meio de um Centro de Operações de Segurança Cibernética (SOC) da contratada.

A solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos visa o monitoramento contínuo e ininterrupto dos ativos computacionais do Tribunal por meio das etapas de, mas, não se limitando à, coleta, processamento e correlação de logs de eventos, dados de telemetria e/ou de rede de tais ativos, com o objetivo de, após análise contextualizada das etapas mencionadas, identificar eventos suspeitos ou incomuns, direcionados ao Tribunal. A solução deve ter capacidade de Coleta e Correlacionamento de Logs e Mecanismos de Detecção de Comportamento Anômalo de Usuários e Aplicações (UEBA – User and Entity Behavior Analytics). Como ela deve ser fornecida no modelo Software as a Service (SaaS) é necessária uma subscrição para sua utilização. E, como forma de permitir um melhor dimensionamento em termos de propostas, a pedido dos fornecedores, optou-se por dividir em faixas de subscrição em relação às quantidades de ativos e tráfego de rede monitorados.

O treinamento da solução contempla a instalação, configuração, operação e utilização da solução contratada, com carga horária mínima de 40 (quarenta) horas e com fornecimento de certificados a todos os participantes.

A implantação da solução consiste no planejamento, implantação, configuração e ativação dos serviços e soluções propostas. Estão previstas fases de Planejamento e Projeto;

Implantação, Configuração e Ativação da solução; Definição de Processos e Outras Configurações; Treinamento de equipes; e Operação, Sustentação e Melhoria Contínua.

O serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos é um serviço técnico especializado de monitoramento do ambiente para prevenção de ameaças cibernéticas, com resposta a incidentes de segurança da informação. É comumente denominado SOC (Security Operation Center), termo que define de forma genérica um conjunto de operações de identificação de eventos de segurança, coleta, armazenamento, análise, reação e observação, por meio de ferramenta específica e mão de obra especializada.

As especificações técnicas detalhadas encontram-se listadas pelo Anexo A, mas em linhas gerais, a solução pretendida deverá ser capaz de:

Requisitos mínimos da solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernético

- A CONTRATADA deve prover, ao ambiente, soluções de segurança cibernética que permitam a visibilidade de logs, dados de telemetria, tráfego de rede e de informações correlatas, capazes de identificar eventos suspeitos ou incomuns que possam comprometer os serviços tecnológicos da CONTRATANTE, por meio da coleta, processamento e correlação dos logs de eventos, dados de telemetria e/ou de rede dos ativos monitorados e do tráfego de rede.
- A solução permitirá monitorar em regime 24x7 (vinte e quatro horas por dia, sete dias por semana) eventos de segurança cibernética, identificando incidentes relativos a ataques, violações de conformidade e comportamento suspeito nas aplicações, rede e ativos computacionais da CONTRATANTE;
- A solução deve ser fornecida no modelo Software as a Service (SaaS) permitindo a instalação de múltiplos coletores e agentes on-premises e em nuvem, a fim de realizar a implantação distribuída da arquitetura;
- A solução deve possuir capacidade de monitorar e identificar o comportamento de usuários que representar ameaça (UEBA - User and Entity Behavior Analytics), em nível de ativos monitorados ou em nível de logs de eventos, do Microsoft Active Directory e do Open LDAP, monitorando diferentes vetores de ataque;

- A solução deve possuir a capacidade de integração e/ou ingestão de dados de outras ferramentas de threat intelligence, de maneira manual ou por API, importando arquivos com base CSV ou STIX (Structured Threat Information Expression), através de assinatura de feeds de inteligência de ameaças de terceiros, aceitando, no mínimo, os seguintes tipos: IPs, domínios, URLs e hashes da família SHA e, opcionalmente, MD5;
- Os agentes devem poder coexistir com outras soluções de proteção, como antivírus, instaladas nos ativos monitorados sem que gerem conflito nem incompatibilidade entre os softwares;
- A solução deve possuir nativamente a capacidade de "deception" ou permitir que se implemente capacidade similar por meio de ferramenta complementar e integrada a solução proposta, possibilitando a marcação de ativos, credenciais, usuários e arquivos específicos como sendo "iscas" a fim de, quando acessados, gerarem alertas, facilitando o monitoramento e auditoria contínuos;
- Quando a solução não possuir capacidade de “deception”, a capacidade de “Breach and Attack Simulation” (BAS) pode ser apresentada;
- A solução deve possuir a capacidade de monitorar a integridade de arquivos (FIM – File Integrity Monitoring) nos servidores monitorados;
- A solução deve possuir funcionalidade de automação na resposta de incidentes com playbooks de resposta já funcionais;
- Deverá realizar serviços de monitoramento de Deep/Dark Web por meio da solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos ofertada (nativamente ou por meio de solução complementar).

Requisitos mínimos de treinamento na solução

- A CONTRATADA deve oferecer treinamento contemplando a perfeita instalação, configuração, operação e utilização da solução contratada com carga horária mínima de 40 (quarenta) horas e com fornecimento de certificados a todos os participantes.

Requisitos mínimos de implantação da solução

- A fase de ativação dos serviços deverá ser conduzida nos primeiros 45 (quarenta e cinco) dias corridos contados a partir da assinatura do contrato, quando serão

executados o planejamento para implantação das ferramentas e a adequação de processos de gestão de segurança cibernética que nortearão a prestação de serviços do Centro de Operações de Segurança Cibernética (SOC);

- As atividades que propiciarão criar, alterar e manter controles de segurança cibernética, além de medir a eficiência e eficácia dos serviços de SOC quanto à sua utilização dentro do negócio, serão adequadas nesta fase de ativação do contrato, conforme parâmetros (baseline) a serem acordados entre as partes;

Requisitos mínimos do serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos

- Os serviços deverão ser prestados por meio do Centro de Operações de Segurança Cibernética (SOC) da CONTRATADA, em regime 24x7x365;
- Os incidentes de segurança cibernética são os relacionados aos eventos de segurança dos ativos monitorados como: ataques de movimentação lateral, escalação de privilégios, acessos indevidos, instalações de códigos maliciosos, ataques por força bruta, ou qualquer outra ação passível de monitoramento pela solução proposta e que possa comprometer a confidencialidade, disponibilidade, integridade ou privacidade das informações da CONTRATANTE.
- Os serviços de operação e sustentação da solução contemplam todas as atividades de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos identificados pela solução ofertada, bem como a sustentação da mesma, mediante a sua operação por parte da CONTRATADA;
- A equipe da CONTRATADA deve prover serviços de pesquisa e desenvolvimento de inteligência (threat intelligence) para proteção contra ataques cibernéticos;
- A equipe da CONTRATADA deve fornecer serviço de Password e Credential Assessment (avaliação de credenciais em serviços de diretório e banco de dados).

1.3.1 Soluções Disponíveis no Mercado de Tecnologia da Informação

Em linhas gerais, o mercado de soluções de Monitoramento, Detecção, Notificação, Investigação e Resposta a Ataques Cibernéticos é composto por diversos tipos de ferramentas como:

- SIEM (Gerenciamento de Eventos e Informações de Segurança - em inglês, Security Information and Event Management), que costuma ser a principal ferramenta para ingestão, correlação e análise dos eventos de segurança;
- SOAR (Orquestração, Automação e Resposta de Segurança - do inglês, Security Orchestration, Automation and Response), que é a ferramenta que, uma vez que um eventos suspeito é detectado, permite a automação de uma resposta, proporcionando rapidez no tratamento de certos incidentes;
- NDR (Detecção e Resposta em Rede - do inglês, Network Detection and Response), também conhecido anteriormente como NTA (Análise de Tráfego de Rede - do inglês, Network Traffic Analysis), é a ferramenta que monitora o tráfego de rede em busca de ameaças e, uma vez que as encontra, permite uma resposta que possivelmente as contenham;
- EDR (Detecção e Resposta em Endpoint - do inglês, Endpoint Detection and Response), é uma ferramenta que, diferente de um antivírus que atua na detecção de um possível arquivo malicioso antes de sua execução, monitora o computador em busca de atividades anômalas e, uma vez que as encontra, permite uma resposta que possivelmente as contenham, como suspender a execução de um programa suspeito ou até o isolamento da máquina;
- XDR (Detecção e Resposta Estendida - do inglês, eXtended Detection and Response), é uma solução que atua na detecção e resposta a ameaças de segurança levando em conta todo o ambiente de uma organização e não apenas em pontos específicos da rede. Coletando e correlacionando dados de várias fontes, como endpoints, servidores, nuvem e redes, fornece uma visão abrangente das ameaças em todo o ambiente;
- UEBA (Análise de Comportamento de Usuários e Entidades - do inglês, User and Entity Behavior Analytics), é uma ferramenta que se concentra na detecção de ameaças com base no comportamento de usuários e entidades dentro de uma rede, procurando identificar desvios do comportamento típico e que podem ser indicativos de atividades maliciosas, como ataques de insider ou comprometimento de contas;
- Monitoramento de Marca e Ameaças Globais ou Monitoramento de Deep/Dark Web, que é realizado para identificar possíveis ameaças, vazamentos de informações, atividades criminosas ou qualquer outra informação relevante que possa afetar a segurança ou a reputação de uma organização, ajudando na prevenção e na resposta a incidentes cibernéticos.

Essas, entre outras ferramentas, costumam estar disponíveis para aumentar a segurança nos ambientes computacionais e, embora possam ser eficazes por conta própria, a integração de várias delas em uma solução unificada oferece vantagens significativas em termos de eficácia na segurança cibernética. Uma abordagem integrada para a segurança cibernética permite que as organizações aproveitem ao máximo essas ferramentas de várias maneiras:

1. Visão abrangente e correlação de ameaças: uma solução integrada pode coletar e correlacionar dados de várias fontes, como endpoints, redes, logs de eventos e comportamento de usuários. Isso resulta em uma visão mais completa e em tempo real das ameaças em todo o ambiente computacional.
2. Detecção aprimorada: a combinação de várias técnicas de detecção, como análises comportamentais, assinaturas de ameaças e análises avançadas de dados, pode aumentar a capacidade de detectar ameaças, mesmo as mais sofisticadas.
3. Resposta rápida: a automação e orquestração oferecidas pelo SOAR podem acelerar a resposta a incidentes, reduzindo o tempo de detecção, contenção e mitigação.
4. Redução de falsos positivos: a capacidade de correlacionar eventos em toda a infraestrutura ajuda a reduzir falsos positivos, permitindo que as equipes de segurança concentrem seus esforços nas ameaças mais críticas.
5. Simplificação da gestão: a administração e manutenção de uma única solução integrada é mais eficiente do que lidar com várias ferramentas independentes, economizando tempo e recursos.

Em última análise, a escolha de uma solução de segurança cibernética integrada não apenas reforça a postura de segurança de uma organização, mas também simplifica a complexidade da gestão de várias ferramentas isoladas.

Dessa forma, não se vislumbra solução de mercado alternativa à contratação de produto ou pacote de produtos específicos ao tema, sendo nesse último caso necessária a composição e integração de ferramentas por parte da CONTRATADA de modo a atingir os objetivos pretendidos pelo TRT2.

1.3.2 Contratações Públicas Similares

Foram localizadas as seguintes contratações públicas com características similares ao do objeto da pretendida contratação através de pesquisa nos seguintes sites:

www.bancodeprecos.com.br, paineldeprecos.planejamento.gov.br, google,com.br e www.gov.br/compras/pt-br/.

Órgão	Objeto	Identificação	Data	Valor Total
Instituto Nacional de Tecnologia da Informação	Contratação de serviços técnicos especializados de operação de infraestrutura de TIC, exclusivos para o ambiente de Assinaturas Eletrônicas Avançadas do ITI, com monitoramento por meio de NOC (Network Operations Center/Centro de Operações de Rede) e SOC (Security Operations Center/Centro de Operações de Segurança).	Pregão: 6/2022 UASG: 243001	26/07/2022	R$ 2.785.810,08
Tribunal Regional Federal da 3ª Região	Registro de Preços para contratação de empresa especializada na prestação de serviços de monitoramento de ambiente tecnológico, prevenção de ameaças cibernéticas e resposta à incidentes de segurança da informação através da implantação de NOC (Network Operations Center) e SOC (Security Operations Center).	Pregão: 44/2022 UASG: 90029	11/10/2022	R$ 7.829.800,00
Instituto de Tecnologia em Imunobiológicos Bio-Manguinhos/Fiocruz	Contratação de empresa especializada para o fornecimento de Serviço de Centro de Operações de Segurança (Security Operations Center - SOC) com funcionamento e suporte 24h por dia e 7 dias por semana, para o atendimento das necessidades da Divisão de Tecnologia da Informação de Bio-Manguinhos/Fiocruz.	Pregão: 368/2022 UASG: 254445	24/11/2022	R$ 900.000,00

Banco Central do Brasil	Contratação de serviços continuados sem dedicação exclusiva de mão-de-obra aplicados à segurança cibernética do Banco Central do Brasil - BCB, sendo composto por dois itens, quais sejam: serviço técnico especializado de segurança cibernética por meio de Centro de Operações de Segurança Cibernética (Cyber Security Operation Center - CSOC) e serviço técnico especializado de Inteligência de Ameaças Cibernéticas (Cyber Threat Intelligence – CTI)	Pregão: 5/2023 UASG: 179087	27/01/2023	R$ 4.959.252,32
Instituto Nacional de Estudos e Pesquisas Educacionais – INEP	Contratação de serviços técnicos especializados de Segurança Cibernética/(Security Operations Center - SOC), envolvendo a prestação de serviços de gerenciamento, de operação e resposta a requisições de segurança, monitoramento e resposta a incidentes de segurança, de gestão de vulnerabilidades, de gestão de risco e conformidade de segurança e privacidade, de inteligência aplicada à segurança, de testes de intrusão e conscientização.	Pregão: 2/2023 UASG: 153978	08/02/2023	R$ 9.199.920,00
Tribunal Regional do Trabalho da 17ª Região	Contratação de Serviço técnico especializado de monitoramento do ambiente para prevenção de ameaças cibernéticas, com resposta a incidentes de segurança da informação, normalmente denominado SOC - Security Operation Center, conforme especificações técnicas constantes do Anexo I e demais condições no Edital.	Pregão: 03/2023 UASG: 80019	15/03/2023	R$ 650.000,00

Entretanto, das contratações públicas encontradas, apenas a licitação realizada pelo TRT da 17ª Região possui características mais próximas às que se pretende contratar e por isso, os valores das demais contratações não poderão ser usados na composição da estimativa de custo.

1.3.3 Outras Soluções Disponíveis

Conforme o item 1.3.1, existem no mercado de Tecnologia da Informação, variadas soluções de diversos fabricantes com capacidade similar de atendimento à presente demanda.

No entanto, há de se citar a existência de soluções chamadas de MDR (Detecção e Resposta Gerenciada - do inglês, Managed Detection and Response), que são serviços de segurança cibernética que oferecem monitoramento em tempo real, detecção de ameaças e resposta a incidentes gerenciados por um provedor de serviços de segurança. O objetivo principal do MDR é ajudar as organizações a identificar, mitigar e responder a ameaças cibernéticas de forma eficaz, mesmo quando enfrentam recursos limitados de pessoal interno ou expertise em segurança.

Optou-se pela não especificação puramente de um MDR, uma vez que há a necessidade de se estabelecer requisitos específicos em termos de ferramental mínimo para garantir um alto grau de qualidade nas ferramentas utilizadas pelo serviço de Centro de Operações de Segurança (SOC). A qualidade das ferramentas desempenha um papel central na eficácia da detecção e resposta a ameaças cibernéticas e, portanto, é imperativo que haja essa definição, o que não é possível quando se contrata um MDR, pois o ferramental atrelado a ele já está definido na própria oferta da solução.

Diante desse cenário, procurou-se especificar de forma separada a solução e o serviço (SOC) de Monitoramento, Detecção, Notificação, Investigação e Resposta a Ataques Cibernéticos.

Reforça-se a importância da integração de várias delas em uma solução unificada como vantagem significativa em termos de eficácia na segurança cibernética. Em última análise, uma solução de segurança cibernética integrada não apenas reforça a postura de segurança, mas também simplifica a complexidade da gestão de várias ferramentas isoladas. Dessa forma, não se vislumbra solução de mercado alternativa à proposta.

1.3.4 Portal do *Software* Público Brasileiro

O Software Público Brasileiro é um tipo específico de software livre que atende às necessidades de modernização da administração pública de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios e é compartilhado sem ônus no Portal do Software Público Brasileiro, resultando na economia de recursos públicos e constituindo um recurso benéfico para a administração pública e para a sociedade.

Atualmente o Software Público Brasileiro está disciplinado pela Portaria N° 46 de 28 de setembro de 2016 do Ministério do Planejamento Desenvolvimento e Gestão, que dispõe sobre os procedimentos para o desenvolvimento, a disponibilização e o uso do Software Público Brasileiro. Não foi localizada no portal do Software Público Brasileiro uma solução com capacidade de atender a demanda.

1.3.5 Alternativas de *Software* no Mercado de Tecnologia da Informação

Foram localizadas soluções de diversos fabricantes com capacidade de atender parcialmente à atual demanda por solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos como: Cortex (Palo Alto), Insight IDR (Rapid7), Helix (Trellix), QRadar (IBM), ArcSight (MicroFocus), Trend Micro, Taegis (SecureWorks).

Não obstante serem soluções pertinentes ao tema, ressalva-se o fato de que algumas destas soluções não estão relacionadas somente a monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos e que há variações no conjunto das funcionalidades de cada solução listada, sendo que alguns dos requisitos da área técnica podem não estar contemplados em alguns dos produtos apresentados, sendo necessária a composição e integração de ferramentas por parte da CONTRATADA.

1.3.6 Modelo Nacional de Interoperabilidade – MNI

O MNI se destina a estabelecer as bases para o intercâmbio de informações de processos judiciais e assemelhados entre os diversos órgãos de administração da Justiça, e, além de servir de base para a implementação das funcionalidades pertinentes no âmbito do sistema processual de que trata o TCOT nº 073/2009, servindo como base de discussão para revisão do modelo já estabelecido em razão do acordo TAC n.º 58/2009. Desse modo, o MNI não é aplicável ao objeto do presente estudo.

1.3.7 Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil

A Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) é uma cadeia hierárquica e de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão. Por não exigir utilização de certificado digital este item não se aplica.

1.3.8 Modelo de Requisitos Moreq-Jus

O Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário (Moreq-Jus) refere-se aos requisitos que os documentos digitais produzidos pelo Judiciário e os sistemas informatizados de gestão documental deverão cumprir, no intuito de garantir a segurança e a preservação das informações, assim como a comunicação com outros sistemas, não sendo aplicável, portanto ao objeto deste estudo, pois não trata de processos nem de documentos judiciais.

1.3.9 Análise dos Custos Totais da Demanda

Para obtenção de uma estimativa atualizada de custos no mercado, foram contatadas, com o objetivo de garantir uma ampla pesquisa de mercado, as seguintes empresas prestadoras

dos serviços: Blue Eye, BRLink/Ingram Micro, Cisco, Claro, Compwire, Crowdstrike, EverCo, Fast Help, Future, Hillstone, Innovatex, Intelliway, ISH, IT Protect, Lanlink, LCM Consulting/FastHelp, Leadcomm, LTA-RH, MW Microware, Network Secure, NTSec, Oakmont, Petacorp, Sencinet, Service IT, Suporte Informática, Tecno-IT, Teletex e Viwsec, das quais, até o momento, enviaram propostas as empresas Intelliway, Petacorp, Service IT, Suporte Informática e Network Secure, conforme orçamentos anexos e demonstrativos abaixo. Para a escolha das empresas a serem consultadas para solicitação de propostas, foram consideradas as que participaram em outras contratações públicas similares, como a realizada pelo TRT da 17ª Região, potenciais fornecedores contatados em eventos de tecnologia da informação como o ENASTIC-JT, bem como aqueles consultados durante a fase de prospecção de mercado de outros projetos de TIC. Por se tratar de um projeto conduzido em nível nacional, o TRT2 recebeu diversos contatos de empresas interessadas em participar, indicadas por outros Tribunais, e que também foram consultadas durante a elaboração dos estudos para validação das especificações técnicas e para o envio de propostas comerciais.

Proposta Comercial - Intelliway

Item	Descrição	Faixa	Faixa de Subscrição por Ativo	Unidade de Medida	Qtde.	Valor Unitário	Valor Total (em 12 meses)	Valor Total – (em 24 meses)
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos	Ativo monitorado anualmente	994	R$ 249,14	R$ 247.645,16	R$ 495.290,32
		Tipo 2	De 1001 a 2000 ativos	Ativo monitorado anualmente	15182	R$ 242,10	R$ 3.675.562,20	R$ 7.351.124,40
		Tipo 3	De 2001 a 5000 ativos	Ativo monitorado anualmente	28292	R$ 227,01	R$ 6.422.566,92	R$ 12.845.133,84
		Tipo 4	De 5001 a 8000 ativos	Ativo monitorado anualmente	30960	R$ 222,39	R$ 6.885.194,40	R$ 13.770.388,80
		Tipo 5	De 8001 a 12000 ativos	Ativo monitorado anualmente	10846	R$ 216,22	R$ 2.345.122,12	R$ 4.690.244,24
		Rede	1Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	109	R$ 0,00	R$ 0,00	R$ 0,00
			10Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	6	R$ 0,00	R$ 0,00	R$ 0,00
2	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes para 251 alunos	Serviço pontual, por turma de treinamento (8 alunos por turma no máximo)	40	R$ 31.156,36	R$ 1.246.254,40	R$ 1.246.254,40
3	Serviço de implantação da solução proposta	-	Serviço de implantação e ativação da solução e seus componentes	Serviço pontual	25	R$ 81.282,92	R$ 2.032.073,00	R$ 2.032.073,00

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

4	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos monitorados	Serviço mensal	1	R$ 53.431,30	R$ 641.175,60	R$ 1.282.351,20
		Tipo 2	De 1001 a 2000 ativos monitorados	Serviço mensal	10	R$ 74.051,19	R$ 8.886.142,80	R$ 17.772.285,60
		Tipo 3	De 2001 a 5000 ativos monitorados	Serviço mensal	8	R$ 109.809,60	R$ 10.541.721,60	R$ 21.083.443,20
		Tipo 4	De 5001 a 8000 ativos monitorados	Serviço mensal	5	R$ 157.758,30	R$ 9.465.498,00	R$ 18.930.996,00
		Tipo 5	De 8001 a 12000 ativos monitorados	Serviço mensal	1	R$ 172.566,00	R$ 2.070.792,00	R$ 4.141.584,00
							Valor Total	**R$ 105.641.169,00**

Proposta Comercial - Petacorp

Item	Descrição	Faixa	Faixa de Subscrição por Ativo	Unidade de Medida	Qtde.	Valor Unitário	Valor Total (em 12 meses)	Valor Total – (em 24 meses)
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos	Ativo monitorado anualmente	994	R$ 469,12	R$ 466.305,28	R$ 932.610,56
		Tipo 2	De 1001 a 2000 ativos	Ativo monitorado anualmente	15182	R$ 399,41	R$ 6.063.842,62	R$ 12.127.685,24
		Tipo 3	De 2001 a 5000 ativos	Ativo monitorado anualmente	28292	R$ 364,32	R$ 10.307.341,44	R$ 20.614.682,88
		Tipo 4	De 5001 a 8000 ativos	Ativo monitorado anualmente	30960	R$ 382,61	R$ 11.845.605,60	R$ 23.691.211,20
		Tipo 5	De 8001 a 12000 ativos	Ativo monitorado anualmente	10846	R$ 359,65	R$ 3.900.763,90	R$ 7.801.527,80
		Rede	1Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	109	R$ 190.638,93	R$ 20.779.643,37	R$ 41.559.286,74
			10Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	6	R$ 300.638,93	R$ 1.803.833,58	R$ 3.607.667,16
2	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes para 251 alunos	Serviço pontual, por turma de treinamento (8 alunos por turma no máximo)	40	R$ 50.000,00	R$ 2.000.000,00	R$ 2.000.000,00
3	Serviço de implantação da solução proposta	-	Serviço de implantação e ativação da solução e seus componentes	Serviço pontual	25	R$ 180.000,00	R$ 4.500.000,00	R$ 4.500.000,00
4	Serviço de monitoramento, detecção, notificação, investigação e	Tipo 1	Até 1000 ativos monitorados	Serviço mensal	1	R$ 28.500,00	R$ 342.000,00	R$ 684.000,00
		Tipo 2	De 1001 a 2000 ativos monitorados	Serviço mensal	10	R$ 39.000,00	R$ 4.680.000,00	R$ 9.360.000,00

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

	resposta a ataques cibernéticos	Tipo 3	De 2001 a 5000 ativos monitorados	Serviço mensal	8	R$ 48.000,00	R$ 4.608.000,00	R$ 9.216.000,00
		Tipo 4	De 5001 a 8000 ativos monitorados	Serviço mensal	5	R$ 63.000,00	R$ 3.780.000,00	R$ 7.560.000,00
		Tipo 5	De 8001 a 12000 ativos monitorados	Serviço mensal	1	R$ 70.000,00	R$ 840.000,00	R$ 1.680.000,00
							Valor Total	**R$ 145.334.671,58**

Proposta Comercial - Service IT

Item	Descrição	Faixa	Faixa de Subscrição por Ativo	Unidade de Medida	Qtde.	Valor Unitário	Valor Total (em 12 meses)	Valor Total – (em 24 meses)
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos	Ativo monitorado anualmente	994	R$ 477,32	R$ 474.456,08	R$ 948.912,16
		Tipo 2	De 1001 a 2000 ativos	Ativo monitorado anualmente	15182	R$ 409,21	R$ 6.212.626,22	R$ 12.425.252,44
		Tipo 3	De 2001 a 5000 ativos	Ativo monitorado anualmente	28292	R$ 371,54	R$ 10.511.609,68	R$ 21.023.219,36
		Tipo 4	De 5001 a 8000 ativos	Ativo monitorado anualmente	30960	R$ 386,01	R$ 11.950.869,60	R$ 23.901.739,20
		Tipo 5	De 8001 a 12000 ativos	Ativo monitorado anualmente	10846	R$ 369,76	R$ 4.010.416,96	R$ 8.020.833,92
		Rede	1Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	109	R$ 192.456,97	R$ 20.977.809,73	R$ 41.955.619,46
			10Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	6	R$ 305.987,11	R$ 1.835.922,66	R$ 3.671.845,32
2	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes para 251 alunos	Serviço pontual, por turma de treinamento (8 alunos por turma no máximo)	40	R$ 60.000,00	R$ 2.400.000,00	R$ 2.400.000,00
3	Serviço de implantação da solução proposta	-	Serviço de implantação e ativação da solução e seus componentes	Serviço pontual	25	R$ 187.950,00	R$ 4.698.750,00	R$ 4.698.750,00
4	Serviço de monitoramento, detecção, notificação, investigação e	Tipo 1	Até 1000 ativos monitorados	Serviço mensal	1	R$ 30.100,00	R$ 361.200,00	R$ 722.400,00
		Tipo 2	De 1001 a 2000 ativos monitorados	Serviço mensal	10	R$ 41.240,00	R$ 4.948.800,00	R$ 9.897.600,00

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

	resposta a ataques cibernéticos	Tipo 3	De 2001 a 5000 ativos monitorados	Serviço mensal	8	R$ 52.185,00	R$ 5.009.760,00	R$ 10.019.520,00
		Tipo 4	De 5001 a 8000 ativos monitorados	Serviço mensal	5	R$ 64.890,00	R$ 3.893.400,00	R$ 7.786.800,00
		Tipo 5	De 8001 a 12000 ativos monitorados	Serviço mensal	1	R$ 72.280,00	R$ 867.360,00	R$ 1.734.720,00
							Valor Total	**R$ 149.207.211,86**

Proposta Comercial - Suporte Informática

Item	Descrição	Faixa	Faixa de Subscrição por Ativo	Unidade de Medida	Qtde.	Valor Unitário	Valor Total (em 12 meses)	Valor Total – (em 24 meses)
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos	Ativo monitorado anualmente	994	R$ 843,32	R$ 838.260,08	R$ 1.676.520,16
		Tipo 2	De 1001 a 2000 ativos	Ativo monitorado anualmente	15182	R$ 843,32	R$ 12.803.284,24	R$ 25.606.568,48
		Tipo 3	De 2001 a 5000 ativos	Ativo monitorado anualmente	28292	R$ 843,32	R$ 23.859.209,44	R$ 47.718.418,88
		Tipo 4	De 5001 a 8000 ativos	Ativo monitorado anualmente	30960	R$ 843,32	R$ 26.109.187,20	R$ 52.218.374,40
		Tipo 5	De 8001 a 12000 ativos	Ativo monitorado anualmente	10846	R$ 843,32	R$ 9.146.648,72	R$ 18.293.297,44
		Rede	1Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	109	R$ 23.308,74	R$ 2.540.652,66	R$ 5.081.305,32
			10Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	6	R$ 12.830,50	R$ 76.983,00	R$ 153.966,00
2	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes para 251 alunos	Serviço pontual, por turma de treinamento (8 alunos por turma no máximo)	40	R$ 24.000,00	R$ 960.000,00	R$ 960.000,00
3	Serviço de implantação da solução proposta	-	Serviço de implantação e ativação da solução e seus componentes	Serviço pontual	25	R$ 200.000,00	R$ 5.000.000,00	R$ 5.000.000,00
4	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos monitorados	Serviço mensal	1	R$ 15.950,00	R$ 191.400,00	R$ 382.800,00
		Tipo 2	De 1001 a 2000 ativos monitorados	Serviço mensal	10	R$ 31.900,00	R$ 3.828.000,00	R$ 7.656.000,00
		Tipo 3	De 2001 a 5000 ativos monitorados	Serviço mensal	8	R$ 79.950,00	R$ 7.675.200,00	R$ 15.350.400,00

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

		Tipo 4	De 5001 a 8000 ativos monitorados	Serviço mensal	5	R$ 127.600,00	R$ 7.656.000,00	R$ 15.312.000,00
		Tipo 5	De 8001 a 12000 ativos monitorados	Serviço mensal	1	R$ 191.400,00	R$ 2.296.800,00	R$ 4.593.600,00
							Valor Total	**R$ 200.003.250,68**

Proposta Comercial - Network Secure

Item	Descrição	Faixa	Faixa de Subscrição por Ativo	Unidade de Medida	Qtde.	Valor Unitário	Valor Total (em 12 meses)	Valor Total – (em 24 meses)
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos	Ativo monitorado anualmente	994	R$ 3.359,42	R$ 3.339.263,48	R$ 6.678.526,96
		Tipo 2	De 1001 a 2000 ativos	Ativo monitorado anualmente	15182	R$ 3.110,06	R$ 47.216.930,92	R$ 94.433.861,84
		Tipo 3	De 2001 a 5000 ativos	Ativo monitorado anualmente	28292	R$ 2.507,85	R$ 70.952.092,20	R$ 141.904.184,40
		Tipo 4	De 5001 a 8000 ativos	Ativo monitorado anualmente	30960	R$ 2.102,12	R$ 65.081.635,20	R$ 130.163.270,40
		Tipo 5	De 8001 a 12000 ativos	Ativo monitorado anualmente	10846	R$ 1.709,94	R$ 18.546.009,24	R$ 37.092.018,48
		Rede	1Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	25	R$ 850.000,00	R$ 21.250.000,00	R$ 42.500.000,00
			10Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente				
2	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes para 251 alunos	Serviço pontual, por turma de treinamento (8 alunos por turma no máximo)	40	R$ 680.000,00	R$ 27.200.000,00	R$ 27.200.000,00
3	Serviço de implantação da solução proposta	-	Serviço de implantação e ativação da solução e seus componentes	Serviço pontual	25	R$ 1.250.000,00	R$ 31.250.000,00	R$ 31.250.000,00
4	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos monitorados	Serviço mensal	1	R$ 78.975,00	R$ 947.700,00	R$ 1.895.400,00
		Tipo 2	De 1001 a 2000 ativos monitorados	Serviço mensal	10	R$ 131.625,00	R$ 15.795.000,00	R$ 31.590.000,00
		Tipo 3	De 2001 a 5000 ativos monitorados	Serviço mensal	8	R$ 210.600,00	R$ 20.217.600,00	R$ 40.435.200,00
		Tipo 4	De 5001 a 8000 ativos monitorados	Serviço mensal	5	R$ 263.250,00	R$ 15.795.000,00	R$ 31.590.000,00

		Tipo 5	De 8001 a 12000 ativos monitorados	Serviço mensal	1	R$ 315.900,00	R$ 3.790.800,00	R$ 7.581.600,00
							Valor Total	**R$ 624.314.062,08**

Obs.: A proposta comercial apresentada pela empresa Network Secure possui valor único para o monitoramento do tráfego de rede, independente do volume, pois conforme explicado pela empresa, a entrega de sua solução para atender a este item é com a instalação de uma subscrição de software de máquina virtual para cada Tribunal.

Há também os valores da licitação realizada pelo Tribunal Regional do Trabalho da 17ª Região em 15/03/2023, para contratação de solução similar a que se pretende contratar, pelo período de 6 meses, conforme segue abaixo:

Item	Descrição	Quantidade	Preço Unitário	Preço Total
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos, considerando um parque de até 2000 ativos monitorados.	Ativo monitorado semestralmente	N/A	R$ 350.000,00
2	Serviço de treinamento na solução proposta para 8 alunos.	1 turma	R$ 10.000,00	R$ 10.000,00
3	Serviço de implantação da solução proposta	1 execução	R$ 20.000,00	R$ 20.000,00
4	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos, considerando um parque de até 2000 ativos monitorados.	Mensal – vigência do contrato - 6 meses	R$ 45.000,00	R$ 270.000,00
			Total	**R$ 650.000,00**

Com o objetivo de atender a demanda de todos os Tribunais Regionais do Trabalho e do Tribunal Superior do Trabalho, recomenda-se que seja realizada licitação para geração de uma ata de registro de preços. Serão registrados 5 tipos de faixas, com diferentes quantitativos de ativos a serem monitorados. As quantidades totais a serem registradas foram obtidas através da planilha de dimensionamento da solução (Anexo II), que foi preenchida por todos os Tribunais.

Desta forma, uma estimativa de custo poderá ser elaborada considerando as médias dos valores das 3 menores propostas recebidas para os itens 1, 2, 3 e 4.

A análise dos valores recebidos nas propostas comerciais para o monitoramento do tráfego diário de rede apresentou uma significativa desproporcionalidade entre os custos para volume de tráfego de rede monitorado de 10Gbps (Gigabits por segundo) e de 1Gbps,

sendo que, de acordo com as propostas recebidas, a contratação de 2Gbps já representaria um custo superior em relação a contratação de 10Gbps.

No dimensionamento realizado pelos Regionais, apenas dois apresentaram demanda equivalente a 1Gbps, porém há de se considerar uma previsão de crescimento estimada em 20% no tráfego de rede em todos os Tribunais para os próximos anos, conforme planilha de dimensionamento da solução (Anexo II) e, desta forma, todos os Regionais demandariam, no mínimo, a contração de 2 subscrições de 1Gbps, ou a combinação de subscrições de 10Gbps e mais 2 de 1Gbps.

Partindo deste entendimento, o volume de tráfego apontado pelos Regionais foi reavaliado e adequado para aquisições exclusivas de subscrições de 10Gbps, totalizando a necessidade de 33 unidades ao invés das 109 subscrições de 1Gbps e 6 de 10Gbps anteriormente solicitados para fornecimentos de propostas.

Conforme será verificado nas tabelas a seguir, em relação a proposta comercial enviada pela empresa Network Secure, não haverá alteração de valores, pois possui valor único para o monitoramento do tráfego de rede, independente do volume, com a instalação de uma subscrição de software de máquina virtual para cada Tribunal.

Desta forma, as propostas comerciais das empresas Intelliway, Petacorp, Service IT e Suporte Informática passariam a ter os seguintes valores:

Proposta Comercial - Intelliway - Com quantidade ajustada referente ao monitoramento do tráfego de rede

Item	Descrição	Faixa	Faixa de Subscrição por Ativo	Unidade de Medida	Qtde.	Valor Unitário	Valor Total (em 12 meses)	Valor Total – (em 24 meses)
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos	Ativo monitorado anualmente	994	R$ 249,14	R$ 247.645,16	R$ 495.290,32
		Tipo 2	De 1001 a 2000 ativos	Ativo monitorado anualmente	15182	R$ 242,10	R$ 3.675.562,20	R$ 7.351.124,40
		Tipo 3	De 2001 a 5000 ativos	Ativo monitorado anualmente	28292	R$ 227,01	R$ 6.422.566,92	R$ 12.845.133,84
		Tipo 4	De 5001 a 8000 ativos	Ativo monitorado anualmente	30960	R$ 222,39	R$ 6.885.194,40	R$ 13.770.388,80
		Tipo 5	De 8001 a 12000 ativos	Ativo monitorado anualmente	10846	R$ 216,22	R$ 2.345.122,12	R$ 4.690.244,24
		Rede	10Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	33	R$ 0,00	R$ 0,00	R$ 0,00

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

2	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes para 251 alunos	Serviço pontual, por turma de treinamento (8 alunos por turma no máximo)	40	R$ 31.156,36	R$ 1.246.254,40	R$ 1.246.254,40
3	Serviço de implantação da solução proposta	-	Serviço de implantação e ativação da solução e seus componentes	Serviço pontual	25	R$ 81.282,92	R$ 2.032.073,00	R$ 2.032.073,00
4	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos monitorados	Serviço mensal	1	R$ 53.431,30	R$ 641.175,60	R$ 1.282.351,20
		Tipo 2	De 1001 a 2000 ativos monitorados	Serviço mensal	10	R$ 74.051,19	R$ 8.886.142,80	R$ 17.772.285,60
		Tipo 3	De 2001 a 5000 ativos monitorados	Serviço mensal	8	R$ 109.809,60	R$ 10.541.721,60	R$ 21.083.443,20
		Tipo 4	De 5001 a 8000 ativos monitorados	Serviço mensal	5	R$ 157.758,30	R$ 9.465.498,00	R$ 18.930.996,00
		Tipo 5	De 8001 a 12000 ativos monitorados	Serviço mensal	1	R$ 172.566,00	R$ 2.070.792,00	R$ 4.141.584,00
							Valor Total	**R$ 105.641.169,00**

Proposta Comercial - Petacorp - Com quantidade ajustada referente ao monitoramento do tráfego de rede

Item	Descrição	Faixa	Faixa de Subscrição por Ativo	Unidade de Medida	Qtde.	Valor Unitário	Valor Total (em 12 meses)	Valor Total – (em 24 meses)
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos	Ativo monitorado anualmente	994	R$ 469,12	R$ 466.305,28	R$ 932.610,56
		Tipo 2	De 1001 a 2000 ativos	Ativo monitorado anualmente	15182	R$ 399,41	R$ 6.063.842,62	R$ 12.127.685,24
		Tipo 3	De 2001 a 5000 ativos	Ativo monitorado anualmente	28292	R$ 364,32	R$ 10.307.341,44	R$ 20.614.682,88
		Tipo 4	De 5001 a 8000 ativos	Ativo monitorado anualmente	30960	R$ 382,61	R$ 11.845.605,60	R$ 23.691.211,20
		Tipo 5	De 8001 a 12000 ativos	Ativo monitorado anualmente	10846	R$ 359,65	R$ 3.900.763,90	R$ 7.801.527,80
		Rede	10Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	33	R$ 300.638,93	R$ 9.921.084,69	R$ 19.842.169,38

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

2	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes para 251 alunos	Serviço pontual, por turma de treinamento (8 alunos por turma no máximo)	40	R$ 50.000,00	R$ 2.000.000,00	R$ 2.000.000,00
3	Serviço de implantação da solução proposta	-	Serviço de implantação e ativação da solução e seus componentes	Serviço pontual	25	R$ 180.000,00	R$ 4.500.000,00	R$ 4.500.000,00
4	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos monitorados	Serviço mensal	1	R$ 28.500,00	R$ 342.000,00	R$ 684.000,00
		Tipo 2	De 1001 a 2000 ativos monitorados	Serviço mensal	10	R$ 39.000,00	R$ 4.680.000,00	R$ 9.360.000,00
		Tipo 3	De 2001 a 5000 ativos monitorados	Serviço mensal	8	R$ 48.000,00	R$ 4.608.000,00	R$ 9.216.000,00
		Tipo 4	De 5001 a 8000 ativos monitorados	Serviço mensal	5	R$ 63.000,00	R$ 3.780.000,00	R$ 7.560.000,00
		Tipo 5	De 8001 a 12000 ativos monitorados	Serviço mensal	1	R$ 70.000,00	R$ 840.000,00	R$ 1.680.000,00
							Valor Total	**R$ 120.009.887,06**

Proposta Comercial - Service IT - Com quantidade ajustada referente ao monitoramento do tráfego de rede

Item	Descrição	Faixa	Faixa de Subscrição por Ativo	Unidade de Medida	Qtde.	Valor Unitário	Valor Total (em 12 meses)	Valor Total – (em 24 meses)
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos	Ativo monitorado anualmente	994	R$ 477,32	R$ 474.456,08	R$ 948.912,16
		Tipo 2	De 1001 a 2000 ativos	Ativo monitorado anualmente	15182	R$ 409,21	R$ 6.212.626,22	R$ 12.425.252,44
		Tipo 3	De 2001 a 5000 ativos	Ativo monitorado anualmente	28292	R$ 371,54	R$ 10.511.609,68	R$ 21.023.219,36
		Tipo 4	De 5001 a 8000 ativos	Ativo monitorado anualmente	30960	R$ 386,01	R$ 11.950.869,60	R$ 23.901.739,20
		Tipo 5	De 8001 a 12000 ativos	Ativo monitorado anualmente	10846	R$ 369,76	R$ 4.010.416,96	R$ 8.020.833,92
		Rede	10Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	33	R$ 305.987,11	R$ 10.097.574,63	R$ 20.195.149,26
2	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes para 251 alunos	Serviço pontual, por turma de treinamento (8 alunos por turma no máximo)	40	R$ 60.000,00	R$ 2.400.000,00	R$ 2.400.000,00

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

3	Serviço de implantação da solução proposta	-	Serviço de implantação e ativação da solução e seus componentes	Serviço pontual	25	R$ 187.950,00	R$ 4.698.750,00	R$ 4.698.750,00
4	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos monitorados	Serviço mensal	1	R$ 30.100,00	R$ 361.200,00	R$ 722.400,00
		Tipo 2	De 1001 a 2000 ativos monitorados	Serviço mensal	10	R$ 41.240,00	R$ 4.948.800,00	R$ 9.897.600,00
		Tipo 3	De 2001 a 5000 ativos monitorados	Serviço mensal	8	R$ 52.185,00	R$ 5.009.760,00	R$ 10.019.520,00
		Tipo 4	De 5001 a 8000 ativos monitorados	Serviço mensal	5	R$ 64.890,00	R$ 3.893.400,00	R$ 7.786.800,00
		Tipo 5	De 8001 a 12000 ativos monitorados	Serviço mensal	1	R$ 72.280,00	R$ 867.360,00	R$ 1.734.720,00
							Valor Total	**R$ 123.774.896,34**

Proposta Comercial - Suporte Informática - Com quantidade ajustada referente ao monitoramento do tráfego de rede

Item	Descrição	Faixa	Faixa de Subscrição por Ativo	Unidade de Medida	Qtde.	Valor Unitário	Valor Total (em 12 meses)	Valor Total – (em 24 meses)
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos	Ativo monitorado anualmente	994	R$ 843,32	R$ 838.260,08	R$ 1.676.520,16
		Tipo 2	De 1001 a 2000 ativos	Ativo monitorado anualmente	15182	R$ 843,32	R$ 12.803.284,24	R$ 25.606.568,48
		Tipo 3	De 2001 a 5000 ativos	Ativo monitorado anualmente	28292	R$ 843,32	R$ 23.859.209,44	R$ 47.718.418,88
		Tipo 4	De 5001 a 8000 ativos	Ativo monitorado anualmente	30960	R$ 843,32	R$ 26.109.187,20	R$ 52.218.374,40
		Tipo 5	De 8001 a 12000 ativos	Ativo monitorado anualmente	10846	R$ 843,32	R$ 9.146.648,72	R$ 18.293.297,44
		Rede	10Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	33	R$ 12.830,50	R$ 423.406,50	R$ 846.813,00
2	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes para 251 alunos	Serviço pontual, por turma de treinamento (8 alunos por turma no máximo)	40	R$ 24.000,00	R$ 960.000,00	R$ 960.000,00
3	Serviço de implantação da solução proposta	-	Serviço de implantação e ativação da solução e seus componentes	Serviço pontual	25	R$ 200.000,00	R$ 5.000.000,00	R$ 5.000.000,00

4	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos monitorados	Serviço mensal	1	R$ 15.950,00	R$ 191.400,00	R$ 382.800,00
		Tipo 2	De 1001 a 2000 ativos monitorados	Serviço mensal	10	R$ 31.900,00	R$ 3.828.000,00	R$ 7.656.000,00
		Tipo 3	De 2001 a 5000 ativos monitorados	Serviço mensal	8	R$ 79.950,00	R$ 7.675.200,00	R$ 15.350.400,00
		Tipo 4	De 5001 a 8000 ativos monitorados	Serviço mensal	5	R$ 127.600,00	R$ 7.656.000,00	R$ 15.312.000,00
		Tipo 5	De 8001 a 12000 ativos monitorados	Serviço mensal	1	R$ 191.400,00	R$ 2.296.800,00	R$ 4.593.600,00
							Valor Total	**R$ 195.614.792,36**

Diante da ampla faixa de valores totais das propostas recebidas, buscou-se analisar a distribuição dos valores individuais de cada um dos itens nas propostas comerciais recebidas em relação aos valores totais cobrados, ou seja, a porcentagem que cada item representa no custo total da proposta.

Tendo em vista que a proposta da empresa Network Secure apresenta um valor 490% superior ao da menor proposta, considera-se que a mesma não pode ser considerada para a análise e estimativa de custo da demanda.

Desta forma, verifica-se que as propostas das empresas Petacorp, Service IT, Suporte Informática possuem porcentagens aproximadas se comparadas com a proposta da empresa Intelliway, que possui distribuição dos valores diferente das demais, conforme se demonstra nas tabelas a seguir:

Proposta Comercial - Intelliway - Com distribuição em percentual para cada um dos itens

Item	Descrição	Faixa	Faixa de Subscrição por Ativo	Unidade de Medida	Qtde.	Valor TOTAL – Intelliway	Porcentagem em relação ao valor total da solução Intelliway
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos	Ativo monitorado anualmente	994	R$ 495.290,32	0,47%
		Tipo 2	De 1001 a 2000 ativos	Ativo monitorado anualmente	15182	R$ 7.351.124,40	6,96%
		Tipo 3	De 2001 a 5000 ativos	Ativo monitorado anualmente	28292	R$ 12.845.133,84	12,16%
		Tipo 4	De 5001 a 8000 ativos	Ativo monitorado anualmente	30960	R$ 13.770.388,80	13,04%

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

		Tipo 5	De 8001 a 12000 ativos	Ativo monitorado anualmente	10846	R$ 4.690.244,24	4,44%
		Rede	10Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	33	R$ 0,00	0,00%
2	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes para 251 alunos	Serviço pontual, por turma de treinamento (8 alunos por turma no máximo)	40	R$ 1.246.254,40	1,18%
3	Serviço de implantação da solução proposta	-	Serviço de implantação e ativação da solução e seus componentes	Serviço pontual	25	R$ 2.032.073,00	1,92%
4	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos monitorados	Serviço mensal	1	R$ 1.282.351,20	1,21%
		Tipo 2	De 1001 a 2000 ativos monitorados	Serviço mensal	10	R$ 17.772.285,60	16,82%
		Tipo 3	De 2001 a 5000 ativos monitorados	Serviço mensal	8	R$ 21.083.443,20	19,96%
		Tipo 4	De 5001 a 8000 ativos monitorados	Serviço mensal	5	R$ 18.930.996,00	17,92%
		Tipo 5	De 8001 a 12000 ativos monitorados	Serviço mensal	1	R$ 4.141.584,00	3,92%
					TOTAIS	**R$ 105.641.169,00**	100,00%

Proposta Comercial - Petacorp - Com distribuição em percentual para cada um dos itens

Item	Descrição	Faixa	Faixa de Subscrição por Ativo	Unidade de Medida	Qtde.	Valor TOTAL – Petacorp	Porcentagem em relação ao valor total da solução Petacorp
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos	Ativo monitorado anualmente	994	R$ 932.610,56	0,78%
		Tipo 2	De 1001 a 2000 ativos	Ativo monitorado anualmente	15182	R$ 12.127.685,24	10,11%
		Tipo 3	De 2001 a 5000 ativos	Ativo monitorado anualmente	28292	R$ 20.614.682,88	17,18%
		Tipo 4	De 5001 a 8000 ativos	Ativo monitorado anualmente	30960	R$ 23.691.211,20	19,74%
		Tipo 5	De 8001 a 12000 ativos	Ativo monitorado anualmente	10846	R$ 7.801.527,80	6,50%

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

		Rede	10Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	33	R$ 19.842.169,38	16,53%
2	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes para 251 alunos	Serviço pontual, por turma de treinamento (8 alunos por turma no máximo)	40	R$ 2.000.000,00	1,67%
3	Serviço de implantação da solução proposta	-	Serviço de implantação e ativação da solução e seus componentes	Serviço pontual	25	R$ 4.500.000,00	3,75%
4	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos monitorados	Serviço mensal	1	R$ 684.000,00	0,57%
		Tipo 2	De 1001 a 2000 ativos monitorados	Serviço mensal	10	R$ 9.360.000,00	7,80%
		Tipo 3	De 2001 a 5000 ativos monitorados	Serviço mensal	8	R$ 9.216.000,00	7,68%
		Tipo 4	De 5001 a 8000 ativos monitorados	Serviço mensal	5	R$ 7.560.000,00	6,30%
		Tipo 5	De 8001 a 12000 ativos monitorados	Serviço mensal	1	R$ 1.680.000,00	1,40%
					TOTAIS	**R$ 120.009.887,06**	100,00%

Proposta Comercial - Service IT - Com distribuição em percentual para cada um dos itens

Item	Descrição	Faixa	Faixa de Subscrição por Ativo	Unidade de Medida	Qtde.	Valor TOTAL – Service IT	Porcentagem em relação ao valor total da solução Service IT
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos	Ativo monitorado anualmente	994	R$ 948.912,16	0,77%
		Tipo 2	De 1001 a 2000 ativos	Ativo monitorado anualmente	15182	R$ 12.425.252,44	10,04%
		Tipo 3	De 2001 a 5000 ativos	Ativo monitorado anualmente	28292	R$ 21.023.219,36	16,99%
		Tipo 4	De 5001 a 8000 ativos	Ativo monitorado anualmente	30960	R$ 23.901.739,20	19,31%
		Tipo 5	De 8001 a 12000 ativos	Ativo monitorado anualmente	10846	R$ 8.020.833,92	6,48%

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

		Rede	10Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	33	R$ 20.195.149,26	16,32%
2	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes para 251 alunos	Serviço pontual, por turma de treinamento (8 alunos por turma no máximo)	40	R$ 2.400.000,00	1,94%
3	Serviço de implantação da solução proposta	-	Serviço de implantação e ativação da solução e seus componentes	Serviço pontual	25	R$ 4.698.750,00	3,80%
4	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos monitorados	Serviço mensal	1	R$ 722.400,00	0,58%
		Tipo 2	De 1001 a 2000 ativos monitorados	Serviço mensal	10	R$ 9.897.600,00	8,00%
		Tipo 3	De 2001 a 5000 ativos monitorados	Serviço mensal	8	R$ 10.019.520,00	8,09%
		Tipo 4	De 5001 a 8000 ativos monitorados	Serviço mensal	5	R$ 7.786.800,00	6,29%
		Tipo 5	De 8001 a 12000 ativos monitorados	Serviço mensal	1	R$ 1.734.720,00	1,40%
					TOTAIS	**R$ 123.774.896,34**	100,00%

Proposta Comercial - Suporte Informática - Com distribuição em percentual para cada um dos itens

Item	Descrição	Faixa	Faixa de Subscrição por Ativo	Unidade de Medida	Qtde.	Valor TOTAL – Suporte Informática	Porcentagem em relação ao valor total da solução Suporte Informática
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos	Ativo monitorado anualmente	994	R$ 1.676.520,16	0,86%
		Tipo 2	De 1001 a 2000 ativos	Ativo monitorado anualmente	15182	R$ 25.606.568,48	13,09%
		Tipo 3	De 2001 a 5000 ativos	Ativo monitorado anualmente	28292	R$ 47.718.418,88	24,39%
		Tipo 4	De 5001 a 8000 ativos	Ativo monitorado anualmente	30960	R$ 52.218.374,40	26,69%
		Tipo 5	De 8001 a 12000 ativos	Ativo monitorado anualmente	10846	R$ 18.293.297,44	9,35%

		Rede	10Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	33	R$ 846.813,00	0,43%
2	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes para 251 alunos	Serviço pontual, por turma de treinamento (8 alunos por turma no máximo)	40	R$ 960.000,00	0,49%
3	Serviço de implantação da solução proposta	-	Serviço de implantação e ativação da solução e seus componentes	Serviço pontual	25	R$ 5.000.000,00	2,56%
4	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos monitorados	Serviço mensal	1	R$ 382.800,00	0,20%
		Tipo 2	De 1001 a 2000 ativos monitorados	Serviço mensal	10	R$ 7.656.000,00	3,91%
		Tipo 3	De 2001 a 5000 ativos monitorados	Serviço mensal	8	R$ 15.350.400,00	7,85%
		Tipo 4	De 5001 a 8000 ativos monitorados	Serviço mensal	5	R$ 15.312.000,00	7,83%
		Tipo 5	De 8001 a 12000 ativos monitorados	Serviço mensal	1	R$ 4.593.600,00	2,35%
					TOTAIS	**R$ 195.614.792,36**	100,00%

Após essa etapa, passou-se a analisar os custos totais de cada proposta, de forma que, para composição da média das propostas, também não foi considerada a proposta da empresa Suporte Informática por apresentar valor superior à 85% em relação a proposta de menor valor, da empresa Intelliway.

Após esse passo, definiu-se o valor total da contratação com base na média das propostas comerciais das empresas Intelliway, Petacorp e Service IT.

Com isso, com o objetivo de garantir a elaboração de uma estimativa de custo de forma mais equilibrada, sugere-se que seja elaborada uma média das porcentagens dos itens em relação aos valores totais das propostas recebidas das empresas, mesmo que a proposta da empresa Suporte Informática não tenha sido utilizada na composição dos valores médios estimados, pois verifica-se que possuem distribuição percentual dos itens semelhantes. Sendo assim, teríamos as seguintes porcentagens médias conforme segue na tabela abaixo:

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

Média das Porcentagens das propostas

Item	Descrição	Faixa	Faixa de Subscrição por Ativo	Unidade de Medida	Qtde.	Média das Porcentagens das Propostas
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos	Ativo monitorado anualmente	994	0,72%
		Tipo 2	De 1001 a 2000 ativos	Ativo monitorado anualmente	15182	10,05%
		Tipo 3	De 2001 a 5000 ativos	Ativo monitorado anualmente	28292	17,68%
		Tipo 4	De 5001 a 8000 ativos	Ativo monitorado anualmente	30960	19,70%
		Tipo 5	De 8001 a 12000 ativos	Ativo monitorado anualmente	10846	6,69%
		Rede	10Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	33	8,32%
2	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes para 251 alunos	Serviço pontual, por turma de treinamento (8 alunos por turma no máximo)	40	1,32%
3	Serviço de implantação da solução proposta	-	Serviço de implantação e ativação da solução e seus componentes	Serviço pontual	25	3,01%
4	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos monitorados	Serviço mensal	1	0,64%
		Tipo 2	De 1001 a 2000 ativos monitorados	Serviço mensal	10	9,13%
		Tipo 3	De 2001 a 5000 ativos monitorados	Serviço mensal	8	10,89%
		Tipo 4	De 5001 a 8000 ativos monitorados	Serviço mensal	5	9,58%
		Tipo 5	De 8001 a 12000 ativos monitorados	Serviço mensal	1	2,27%
					TOTAL	**100,00%**

Por fim, para a definição da estimativa de custo de cada item da contratação, aplicou-se a média das porcentagens obtidas, conforme a tabela acima, no valor total estimado da contratação obtido por meio da média das propostas comerciais das empresas Intelliway, Petacorp e Service IT, obtendo-se assim a estimativa a seguir:

Estimativa de custo total - Média das 3 menores propostas

Item	Descrição	Faixa	Faixa de Subscrição por Ativo	Unidade de Medida	Qtde.	Valor Unitário	Valor Total (em 12 meses)	Valor Total – (em 24 meses)
1	Subscrição de solução de monitoramento,	Tipo 1	Até 1000 ativos	Ativo monitorado anualmente	994	R$ 398,53	R$ 396.138,82	R$ 792.277,64

	detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 2	De 1001 a 2000 ativos	Ativo monitorado anualmente	15182	R$ 350,24	R$ 5.317.343,68	R$ 10.634.687,36
		Tipo 3	De 2001 a 5000 ativos	Ativo monitorado anualmente	28292	R$ 320,96	R$ 9.080.600,32	R$ 18.161.200,64
		Tipo 4	De 5001 a 8000 ativos	Ativo monitorado anualmente	30960	R$ 330,34	R$ 10.227.326,40	R$ 20.454.652,80
		Tipo 5	De 8001 a 12000 ativos	Ativo monitorado anualmente	10846	R$ 315,21	R$ 3.418.767,66	R$ 6.837.535,32
		Rede	10Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	33	R$ 202.208,68	R$ 6.672.886,44	R$ 13.345.772,88
2	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes para 251 alunos	Serviço pontual, por turma de treinamento (8 alunos por turma no máximo)	40	R$ 47.052,12	R$ 1.882.084,80	R$ 1.882.084,80
3	Serviço de implantação da solução proposta	-	Serviço de implantação e ativação da solução e seus componentes	Serviço pontual	25	R$ 149.744,31	R$ 3.743.607,75	R$ 3.743.607,75
4	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos monitorados	Serviço mensal	1	R$ 37.343,77	R$ 448.125,24	R$ 896.250,48
		Tipo 2	De 1001 a 2000 ativos monitorados	Serviço mensal	10	R$ 51.430,40	R$ 6.171.648,00	R$ 12.343.296,00
		Tipo 3	De 2001 a 5000 ativos monitorados	Serviço mensal	8	R$ 69.998,20	R$ 6.719.827,20	R$ 13.439.654,40
		Tipo 4	De 5001 a 8000 ativos monitorados	Serviço mensal	5	R$ 95.216,10	R$ 5.712.966,00	R$ 11.425.932,00
		Tipo 5	De 8001 a 12000 ativos monitorados	Serviço mensal	1	R$ 104.948,67	R$ 1.259.384,04	R$ 2.518.768,08
Valor Total Estimado para todos os Tribunais								**R$ 116.475.720,15**

Obs. 1: Os valores referentes aos itens 1, 2, 3 e 4 foram calculados com base na média dos valores das 3 menores propostas comerciais recebidas das empresas Intelliway, Petacorp e Service IT. Os valores das propostas comerciais recebidas das empresas Suporte Informática e Network Secure, como já desqualificada anteriormente, não foram utilizados na estimativa de custo por estarem muito superior em relação à proposta de menor valor recebida da empresa Intelliway.

Obs. 2: Recomenda-se que os valores referentes a licitação realizada pelo TRT17 não sejam utilizados nos cálculos da estimativa de custo, por se tratar de uma contratação com escopo bem menor da que se pretende realizar, sendo feita para atender apenas a necessidade daquele Regional, bem como por não ter todos os valores dos tipos de faixas

das subscrições e dos serviços de monitoramento e nem ter os valores do monitoramento do tráfego de rede.

Reforça-se esta possibilidade pelo fato de que na licitação da 17ª Região, a solução que sagrou-se vencedora foi a mesma que já estava em utilização naquele tribunal, o que pode influenciar drasticamente nos valores referentes a serviços e nos treinamentos, principalmente de instalação uma vez que solução já se encontrava instalada e o regional já possuía conhecimento da solução, e ainda, licenciamento de software, uma vez que a renovação pode custar menos que uma nova licença, podendo tornar inexequível a utilização parcial dessa proposta na composição de preços.

Aplicando-se as médias das porcentagens das propostas comerciais recebidas, conforme explicado acima, em relação ao valor total estimado de R$ 116.475.720,15, que foi calculado com base na média das 3 menores propostas, teremos os seguintes valores unitários e totais máximos dos itens conforme segue abaixo:

Estimativa de custo total para todos os Tribunais

Item	Descrição	Faixa	Faixa de Subscrição por Ativo	Unidade de Medida	Qtde.	Valor Unitário	Valor Total (em 12 meses)	Valor Total – (em 24 meses)
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos	Ativo monitorado anualmente	994	**R$ 398,53**	R$ 396.138,82	R$ 792.277,64
		Tipo 2	De 1001 a 2000 ativos	Ativo monitorado anualmente	15182	**R$ 350,24**	R$ 5.317.343,68	R$ 10.634.687,36
		Tipo 3	De 2001 a 5000 ativos	Ativo monitorado anualmente	28292	**R$ 320,96**	R$ 9.080.600,32	R$ 18.161.200,64
		Tipo 4	De 5001 a 8000 ativos	Ativo monitorado anualmente	30960	**R$ 330,34**	R$ 10.227.326,40	R$ 20.454.652,80
		Tipo 5	De 8001 a 12000 ativos	Ativo monitorado anualmente	10846	**R$ 315,21**	R$ 3.418.767,66	R$ 6.837.535,32
		Rede	10Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	33	**R$ 202.208,68**	R$ 6.672.886,44	R$ 13.345.772,88
2	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes para 251 alunos	Serviço pontual, por turma de treinamento (8 alunos por turma no máximo)	40	**R$ 47.052,12**	R$ 1.882.084,80	R$ 1.882.084,80
3	Serviço de implantação da solução proposta	-	Serviço de implantação e ativação da solução e seus componentes	Serviço pontual	25	**R$ 149.744,31**	R$ 3.743.607,75	R$ 3.743.607,75
4	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos monitorados	Serviço mensal	1	**R$ 37.343,77**	R$ 448.125,24	R$ 896.250,48
		Tipo 2	De 1001 a 2000 ativos monitorados	Serviço mensal	10	**R$ 51.430,40**	R$ 6.171.648,00	R$ 12.343.296,00
		Tipo 3	De 2001 a 5000 ativos monitorados	Serviço mensal	8	**R$ 69.998,20**	R$ 6.719.827,20	R$ 13.439.654,40

		Tipo 4	De 5001 a 8000 ativos monitorados	Serviço mensal	5	**R$ 95.216,10**	R$ 5.712.966,00	R$ 11.425.932,00
		Tipo 5	De 8001 a 12000 ativos monitorados	Serviço mensal	1	**R$ 104.948,67**	R$ 1.259.384,04	R$ 2.518.768,08
Valor Total Estimado para todos os Tribunais								**R$ 116.475.720,15**

Desta forma, o valor total estimado da contratação para todos o TRTs e para o TST é de R$ 116.475.720,15 (cento e dezesseis milhões, quatrocentos e setenta e cinco mil, setecentos e vinte reais e quinze centavos) pelo período de 24 (vinte e quatro) meses.

Já o valor total estimado somente para o TRT2 será conforme segue na tabela abaixo:

Estimativa de custo total para o TRT2

Item	Descrição	Faixa	Faixa de Subscrição por Ativo	Unidade de Medida	Qtde.	Valor Unitário (12 meses)	Valor Total (12 meses)	Valor Total – (24 meses)
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 5	De 8001 a 12000 ativos	Ativo monitorado anualmente	10846	R$ 315,21	R$ 3.418.767,66	R$ 6.837.535,32
		Rede	10Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	2	R$ 202.208,68	R$ 404.417,36	R$ 808.834,72
2	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes para 8 alunos	Serviço pontual, por turma de treinamento (8 alunos por turma no máximo)	1	R$ 47.052,12	R$ 47.052,12	R$ 47.052,12
3	Serviço de implantação da solução proposta	-	Serviço de implantação e ativação da solução e seus componentes	Serviço pontual	1	R$ 149.744,31	R$ 149.744,31	R$ 149.744,31
4	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 5	De 8001 a 12000 ativos monitorados	Serviço mensal	1	R$ 104.948,67	R$ 1.259.384,04	R$ 2.518.768,08
Valor Total Estimado para o TRT2								**R$ 10.361.934,55**

Para a composição dos quantitativos referente ao TRT2, estão sendo considerados um total de 10.846 ativos monitorados, sendo 10.170 estações de trabalho/notebooks, 615 servidores Linux e 61 servidores Windows, o que nos enquadra na faixa do tipo 5, que é de 8.001 a 12.000 ativos monitorados. Para o tráfego diário de rede monitorado anualmente, considerando que o nosso volume médio diário do tráfego da rede interna é de 17,04 Gbps,

já considerando um crescimento de 20% para os próximos anos, está sendo considerada a aquisição de 2 subscrições de 10Gbps.

Para a realização do treinamento, está sendo considerada a participação de 8 alunos, sendo necessária a contratação de 1 turma.

Para os serviços de implantação e de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos (itens 3 e 4), está sendo considerada a quantidade de 1 para cada Tribunal.

Desta forma, a estimativa de custo total para o TRT2 será de R$ 10.361.934,55 (dez milhões, trezentos e sessenta e um mil, novecentos e trinta e quatro reais e cinquenta e cinco centavos) pelo período de 24 (vinte e quatro) meses.

1.3.10 Escolha e Justificativa da Solução

A aquisição e implantação de uma solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos visa permitir a análise mais rápida e assertiva dos ativos de TIC envolvidos em incidentes de segurança da informação, além de visar a detecção, a análise e a atuação para evitar ou mitigar acessos indevidos e/ou maliciosos.

O aumento de investimentos na área da segurança cibernética tem se mostrado uma tendência tanto no Brasil quanto internacionalmente, devido ao aumento de ataques cibernéticos, tendo as organizações governamentais estado entre os principais alvos. Exemplo disso são os ataques sofridos pelo STJ, TRT4, TRF3 e TRT17, que acarretaram prejuízos tanto para a sociedade quanto para as próprias instituições.

Percebe-se, assim, a importância da priorização de investimentos em soluções que auxiliem na prevenção de incidentes.

A contratação deste tipo de solução se mostra viável se considerarmos os impactos negativos do ponto de vista operacional e financeiro que poderão ser causados em caso de um ataque cibernético. Não só para este Tribunal, mas também prejuízos imensuráveis para toda a sociedade como: falta de acesso à justiça, perda de informações, impactos na imagem do órgão, dentre outros. Se considerarmos que o custo diário da folha de pagamento de magistrados e servidores ativos mais as obrigações patronais é de aproximadamente R$ 5.000.000,00 (cinco milhões de reais), o equivalente a quase 1 ano de contratação da solução pretendida, entende-se que o custo-benefício da solução é extremamente vantajoso. Dependendo das proporções do ataque, é comum que a instituição fique alguns dias sem acesso aos seus sistemas, podendo eventualmente, em alguns casos, levar semanas para um serviço ser totalmente recuperado/restabelecido, como ocorreu com o Superior Tribunal de Justiça (STJ) que sofreu ataque hacker em e precisou trabalhar em regime de plantão por quase uma semana, conforme notícia[7] do

[7] https://www.nic.br/noticia/na-midia/ataques-no-mundo-digital/

NIC.br (Núcleo de Informação e Coordenação do Ponto BR). Durante o período, ficaram suspensas todas as sessões de julgamento por videoconferência e também as sessões virtuais destinadas à apreciação de recursos internos (agravos internos, agravos regimentais e embargos de declaração), bem como as audiências. Nove dias após o ataque, o STJ ainda mantinha os trabalhos de recuperação dos sistemas afetados.

O exposto se soma ao Acórdão 1.768/2022-TCU-Plenário, que apresenta o resultado obtido por meio de mapeamento da maturidade das organizações públicas federais quanto à implementação de controles críticos de segurança cibernética. Para isso, foram utilizados controles e medidas de segurança preconizados pelo CIS (Center for Internet Security - conjunto de práticas em segurança cibernética recomendadas internacionalmente). Como resultado, o TCU observou uma situação de alto risco para a segurança cibernética no setor público federal e, por isso, essa Corte sugeriu a implementação urgente de controles críticos indicados no CIS, os quais tratam, por exemplo, de inventário e controle de ativos, gestão de vulnerabilidades e gestão de resposta a incidentes.

Desse modo, vai ao encontro do Acórdão citado, a contratação de serviço técnico especializado de monitoramento e resposta a incidentes de segurança da informação, com o objetivo de minimizar os impactos de uma ocorrência de grande magnitude, assim como prevenir tentativas de acesso não autorizadas ao ambiente tecnológico deste Regional e dos demais Tribunais coparticipantes da licitação.

Além disso, há o Parecer do Subcomitê Nacional de Segurança Cibernética - SNSEC do CSJT (conforme Anexo I), no qual recomenda a contratação de solução de Monitoramento, Detecção, Notificação, Investigação e Resposta a Ataques Cibernéticos, soluções também conhecidas XDR, SOC/SIEM, que está em andamento neste Regional, para todos os órgãos da Justiça do Trabalho.

1.3.11 Descrição da Solução

Registro de Preços para contratação de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos, pelo período de 24 meses.

1.3.12 Alinhamento da Solução

Esta solução encontra-se alinhada com os seguintes objetivos:

PEI (Plano Estratégico Institucional) - 2021-2026:

- Objetivo 10: Aprimorar a Governança de TIC e a proteção de dados;

Também está de acordo com a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ):

- Art. 6º São objetivos da ENSEC-PJ:

  II – aumentar a resiliência às ameaças cibernéticas;

- Art. 9º São ações da ENSEC-PJ:

  I – fortalecer as ações de governança cibernética;

  II – elevar o nível de segurança das infraestruturas críticas.

E de acordo com a Estratégia Nacional de Tecnologia de Informação e Comunicação do Poder Judiciário (ENTIC-JUD):

- Objetivo 7: Aprimorar a Segurança da Informação e a Gestão de Dados.

1.3.13 Benefícios Esperados

O resultado pretendido é a contratação de uma solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos, com suporte e treinamento, no qual permitirá a atuação das equipes técnicas da SETIC de forma rápida e ágil frente aos diversos tipos de incidentes cibernéticos, tais como uso indevido de recursos computacionais, infecção de malwares, ransomwares, execução remota de código, entre outros, evitando ou minimizando os prejuízos ao Tribunal e aos magistrados, servidores e jurisdicionados.

1.3.14 Relação entre a Demanda Prevista e Solução a ser Contratada

A demanda prevista representa as limitações citadas no item 1.1, como a dificuldade de configuração, complexidade na criação de regras de correlações e de detecção prontas, ausência de suporte técnico e a falta de integração com ferramentas de apoio. Além disso, o ambiente heterogêneo e complexo do TRT2, com vários tipos diferentes de fontes de dados, torna ainda mais importante a contratação de uma solução que possa lidar com essa complexidade de forma eficaz.

Espera-se, com essa contratação, uma solução de segurança cibernética que permita a visibilidade de logs, dados de telemetria, tráfego de rede e de informações correlatas e capaz de identificar eventos suspeitos ou incomuns que possam comprometer os serviços tecnológicos da CONTRATANTE, por meio da coleta, processamento e correlação dos logs de eventos, dados de telemetria e/ou de rede de todos os ativos monitorados e do tráfego de rede, sendo atualmente 10.170 estações de trabalho/notebooks, 615 servidores Linux e 61 servidores Windows, além do tráfego de rede que apresenta volume médio diário da rede interna de 17,04 Gbps, já considerando um crescimento de 20% para os próximos anos.

A solução e o serviço de SOC permitirá monitorar em regime 24x7 (vinte e quatro horas por dia, sete dias por semana) eventos de segurança cibernética, identificando e prevenindo incidentes relativos a ataques, violações de conformidade e comportamento suspeito nas aplicações, redes e ativos computacionais do Tribunal.

A contratação de empresa especializada em prestação de serviço de SOC (Centro de Operações de Segurança) com solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos, com implantação, suporte e treinamento para o TRT da 2ª Região e demais Regionais coparticipantes da contratação pelo período de 24 (vinte e quatro) meses, atende a demanda prevista atualmente para incremento da segurança cibernética em todo o parque computacional do Tribunal.

Além disso, há um ganho colateral adicional: por ser uma contratação nacional, espera-se que haja um aumento na segurança cibernética da Justiça do Trabalho como um todo, uma vez que, havendo um monitoramento único para todos os Tribunais que compõem a JT, um incidente cibernética que ocorra em um órgão pode ter suas medidas de resposta a incidentes replicadas em todos os outros de maneira mais célere e eficaz.

1.3.15 Adequação do Ambiente

Tendo em vista que se trata de contratação de uma solução nova, que não é utilizada atualmente neste Regional, será necessário:

- Providenciar os treinamentos de todos os profissionais envolvidos;
- Disponibilizar eventuais acessos e permissões para os sistemas e profissionais da contratada;
- Implementar alterações de configurações que eventualmente sejam necessárias nos sistemas e servidores do TRT2 para operação em conjunto com a solução contratada;
- Apoiar a contratada na distribuição e instalação inicial de agentes e sensores no ambiente computacional do TRT2.

1.3.16 Requisitos Tecnológicos, Necessidades e Ações Adicionais necessárias ao pleno funcionamento da solução

Além das adequações já mencionadas, não foram identificadas ações adicionais necessárias ao pleno funcionamento da solução pretendida.

1.3.17 Orçamento Estimado

O orçamento estimado para a contratação dos serviços para todos os TRTs e o TST é de R$ 116.475.720,15 (cento e dezesseis milhões, quatrocentos e setenta e cinco mil, setecentos e vinte reais e quinze centavos) para um período de 24 meses. Já o orçamento estimado somente para o TRT2 é de R$ 10.361.934,55 (dez milhões, trezentos e sessenta e um mil, novecentos e trinta e quatro reais e cinquenta e cinco centavos) pelo período de 24 (vinte e quatro) meses. As despesas deverão estar previstas para constar nas programações orçamentárias de SETIC para os anos de 2024 e 2025.

2 SUSTENTAÇÃO DO CONTRATO

2.1 Recursos Materiais e Humanos

Na medida do necessário, serão disponibilizados recursos humanos da Coordenadoria de Segurança de TIC da SETIC para apoio durante a implantação da solução. Além disso, será necessário também alocar um grupo de servidores para a realização dos treinamentos e administração da solução.

2.2 Descontinuidade do Fornecimento

Em caso de eventual interrupção do fornecimento dos serviços, deverá ser iniciado um novo processo de contratação.

2.3 Transição Contratual

Ao término do contrato, seja por decurso de vigência ou por rescisão antecipada, a empresa contratada deverá promover a transição contratual com transferência de tecnologia e técnicas empregadas ao time do TRT2, sem que haja perda de informações e sem ônus adicional ao contratante.

2.4 Estratégia de Independência Tecnológica

Na presente contratação, não é possível criar uma relação de independência tecnológica, cabendo ao demandante da solução tomar medidas tempestivas para manter o serviço constante e evitar futuras ocorrências. Como forma de mitigação, todo conhecimento adquirido ou desenvolvido, bem como toda informação produzida e/ou utilizada para a execução dos serviços contratados deverão ser disponibilizados ao contratante ou empresa por ele designada, como: ativos configurados, parsers, IoC's (Indicators of Compromise), dados de threat intelligence, alertas customizados, lista de exceções, regras de detecção de intrusão, dashboards, relatórios, entre outras configurações.

Convém destacar que a própria especificação contempla mecanismos que auxiliam essa mitigação em seus itens 2.8 e 4.4.3.5:

> 2.8. A solução deve possuir retenção mínima de 03 (três) meses de registros prontamente acessíveis ("Logs Quentes"). Após este período, a solução deve suportar, no mínimo, 09 (nove) meses de registros arquivados ("Logs Frios") - totalizando 12 (doze) meses de registros - bem como permitir a exportação destes

logs/dados de telemetria/de rede para armazenamento em ambiente de propriedade da CONTRATANTE.

2.8.1. As análises realizadas e alertas devem estar disponíveis de forma integral por pelo menos 06 (seis) meses.

2.8.2. Deve haver a opção de exportação de logs/dados de telemetria/de rede em formato aberto (plain text) podendo ser abertos e lidos em editores de texto sem a necessidade de softwares proprietários ou plugins.

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

4.4.3.5. Desenvolvimento de um plano de continuidade que contemple minimamente a exportação de:

4.4.3.5.1. Base de incidentes em aberto (em tratamento);

4.4.3.5.2. Playbooks implementados.

3 ESTRATÉGIA PARA A CONTRATAÇÃO

3.1 Natureza do Objeto

O objeto a ser contratado possui características comuns e usuais encontradas atualmente no mercado de Tecnologia de Informação, cujos padrões de desempenho e de qualidade podem ser objetivamente definidos neste documento.

A descrição do objeto a ser contratado é Solução e Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos, incluindo suporte técnico, implantação e treinamento.

Conforme decreto nº 11.462, de 31 de março de 2023, Artigo 3º, incisos III e V, o Sistema de Registro de Preços poderá ser adotado quando a Administração julgar pertinente, em especial quando for conveniente para atendimento a mais de um órgão ou a mais de uma entidade, inclusive nas compras centralizadas e quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela Administração. O Tribunal poderá efetuar a contratação dos itens do objeto deste documento observando a viabilidade técnica na ocasião do vencimento da garantia vigente e disponibilidade orçamentária.

Com o objetivo de padronizar soluções, sistemas, ferramentas e contratações conjuntas, como meio de minimizar custos e maximizar a força de trabalho das equipes de TIC, será permitida a adesão/carona somente aos órgãos integrantes da Justiça do Trabalho.

3.2 Parcelamento do Objeto

Recomenda-se que o objeto não seja parcelado, uma vez que todos os produtos e serviços a serem fornecidos e prestados são componentes de uma única solução de TIC, a qual não pode ser desmembrada sem que haja perda de produtividade e economia de escala.

Cabe ressaltar também que não é viável o parcelamento dos serviços prestados, pois geraria riscos à continuidade da solução, dificultando a gestão de problemas diversos em diferentes itens da solução.

3.3 Adjudicação do Objeto

Para efeito de adjudicação do objeto, sugere-se que seja considerado o menor preço global, uma vez que todos os itens a serem fornecidos são componentes de uma única solução de TIC, a qual não pode ser desmembrada sem que haja perda de produtividade e economia de escala.

3.4 Modalidade e Tipo de Licitação

Verifica-se que o objeto pretendido é oferecido por alguns fornecedores no mercado de TIC e apresenta características padronizadas e usuais. Assim, se pode concluir que o objeto é comum e, portanto, sugere-se como melhor opção a utilização da licitação na modalidade pregão eletrônico do tipo menor preço.

Considerando que a demanda se enquadra nas hipóteses previstas no artigo 3º, incisos III e V do decreto nº 11.462/2023, sugere-se que seja adotado o Sistema de Registros de Preços (SRP). O Registro de Preços poderá ser adotado quando a Administração julgar pertinente, em especial quando for conveniente para atendimento a mais de um órgão ou a mais de uma entidade, inclusive nas compras centralizadas e quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela Administração.

Além disso, recomenda-se que seja aplicado o disposto no artigo 49 da lei complementar 123/2006, considerando se tratar de serviço especializado em solução complexa e não ter sido encontrado microempresas ou empresas de pequeno porte que possam atender à demanda. Por isso, com o objetivo de não frustrar o processo licitatório, sugere-se, s.m.j., que a licitação não seja exclusiva para empresas que se enquadrem nessas categorias.

3.5 Classificação e Indicação Orçamentária

O objeto da contratação constitui despesa corrente, classificação orçamentária 3390.40.07 e 3390.40.20, estimada em R$ 116.475.720,15 (cento e dezesseis milhões, quatrocentos e setenta e cinco mil, setecentos e vinte reais e quinze centavos) para todos os TRTs e o TST e em R$ 10.361.934,55 (dez milhões, trezentos e sessenta e um mil, novecentos e trinta e quatro reais e cinquenta e cinco centavos) para o TRT2 para um período de 24 meses de

contratação, e deverá constar nas programações orçamentárias de SETIC para os anos de 2024 e 2025, sendo distribuído da seguinte forma:

Todos os TRTs e TST:

Treinamento: 3390.40.20 – R$ 1.882.084,80

Manut. Corretiva/Adaptativa e Sustentação de Softwares: 3390.40.07 – R$ 114.593.635,35

Somente TRT 2ª Região:

Treinamento: 3390.40.20 – R$ 47.052,12

Manut. Corretiva/Adaptativa e Sustentação de Softwares: 3390.40.07 – R$ 10.314.882,43

3.6 Vigência da Prestação de Serviço

Os serviços serão prestados pelo período de 24 (vinte e quatro) meses, a partir da publicação do extrato do contrato, podendo ser prorrogado por mais 24 (vinte e quatro) meses ou até o limite legal.

3.7 Necessidade de Recursos para os Próximos Exercícios Orçamentários

As despesas deverão ocorrer nos exercícios de 2024 e 2025, conforme segue:

Ano	Valor - Serviços	Valor - Treinamento
2024	R$ 5.232.313,37	R$ 47.052,12
2025	R$ 5.082.569,06	---------

3.8 Equipe de Gestão e Fiscalização da Contratação

Papel	Nome	Matrícula	Ramal	E-Mail
Gestora do Contrato	Cláudia Sant'Anna Pinheiro – Diretora da Coordenadoria de Segurança de TIC	97500	2073	seguranca-ti@trt2.jus.br
Gestor do Contrato - Substituto	Leonardo Luis Soares - Assistente Administrativo Chefe da Seção de Gestão de Riscos e Continuidade	132870	2073	riscos-ti@trt2.jus.br

Fiscal Técnico	Ramon Chiara – Assistente Administrativo Chefe da Seção de Gestão de Incidentes em Segurança da Informação	133167	2073	incidentesseg-ti@trt2.jus.br
Fiscal Técnico - Substituto	Lucas Ihara Alves - Seção de Gestão de Incidentes em Segurança da Informação	161020	2073	lucas.alves@trt2.jus.br

3.9 Equipe de Apoio ao Pregoeiro

Nome	Ramal	E-Mail
Luciano de Souza Paiva	2070	luciano.paiva@trt2.jus.br
Leonardo Henrique Day de Toledo	2070	leonardo.toledo@trt2.jus.br
Ramon Chiara	2073	incidentesseg-ti@trt2.jus.br
Lucas Ihara Alves	2073	lucas.alves@trt2.jus.br

Conforme portaria GP nº 17/2022.

3.10 Equipe de Recebimento da Contratação

O recebimento, conforme determinado pelo Ato GP 37/2018, deverá ser feito pela seguinte equipe nomeada:

Nome	Ramal	E-Mail
Ramon Chiara	2073	incidentesseg-ti@trt2.jus.br
Lucas Ihara Alves	2073	lucas.alves@trt2.jus.br
Cláudia Sant'Anna Pinheiro	2073	seguranca-ti@trt2.jus.br

4 ANÁLISE DE RISCOS

Matriz de exposição do risco (Grau do Risco): Probabilidade x Impacto			
Probabilidade	**Impacto**		
	Baixo	**Médio**	**Alto**
Alta	**Médio**	**Alto**	**Extremo**
Média	**Baixo**	**Médio**	**Alto**
Baixa	**Mínimo**	**Baixo**	**Médio**

4.1 Riscos da contratação

Descrição do risco	Demora ou não efetivação da contratação.	
Consequência	Falta de recursos para aumentar a segurança do ambiente computacional do TRT.	
Probabilidade	**Impacto**	**Grau do risco**
Baixa	Médio	Baixo
Mitigação	Sensibilizar as partes envolvidas sobre a importância e necessidade de celeridade na efetivação da contratação.	
Contingência		
Responsável	Equipe de planejamento da contratação	
Prazo	Durante a Contratação	

Descrição do risco	Utilizar estimativa de custo muito abaixo do valor de mercado.	
Consequência	Inviabilização do processo licitatório.	
Probabilidade	**Impacto**	**Grau do risco**
Baixa	Médio	Baixo
Mitigação	Utilizar estimativas com valores mais próximos possíveis aos praticados no mercado e planejamento de contingência no caso de atraso para conclusão do processo por conta de fracasso da licitação, com a ciência por parte dos gestores de segurança de TIC sobre esse risco.	
Contingência		
Responsável	Equipe de planejamento da contratação	
Prazo	Durante a Contratação	

4.2 Riscos da Implantação

Descrição do risco	Atrasos na entrega da solução.	
Consequência	Atraso no monitoramento dos sistemas computacionais pela ferramenta objeto da contratação.	
Probabilidade	**Impacto**	**Grau do risco**
Baixa	Médio	Baixo
Mitigação	Prever prazos de entrega adequados.	
Contingência		
Responsável	Equipe de planejamento da contratação	
Prazo	Durante a Contratação	

4.3 Riscos da Solução

Descrição do risco	Má prestação do serviço ou inexecução contratual da empresa contratada.	
Consequência	Má qualidade no monitoramento, detecção e tratamento de incidentes cibernéticos e consequentemente, má prestação jurisdicional.	
Probabilidade	**Impacto**	**Grau do risco**
Média	Médio	Médio

Mitigação	Estabelecer claramente no Termo de Referência as obrigações da empresa contratada e multas contratuais.
Contingência	Revisão dos termos da contratação ou revisão de estratégia de contratação e iniciar outro processo de contratação.
Responsável	Equipe de planejamento da contratação
Prazo	Durante a Contratação

Descrição do risco	A empresa não possui qualificação adequada para executar os serviços.	
Consequência	Baixa qualidade na prestação dos serviços.	
Probabilidade	**Impacto**	**Grau do risco**
Média	Médio	Médio
Mitigação	Exigir o cumprimento das garantias contratuais cabíveis.	
Contingência	Revisão dos termos da contratação ou revisão de estratégia de contratação e iniciar outro processo de contratação.	
Responsável	Equipe de planejamento da contratação	
Prazo	Durante a Contratação	

Descrição do risco	Indisponibilidade ou lentidão no acesso a qualquer funcionalidade ou serviço integrantes da solução.	
Consequência	Prejuízo ou atraso na prestação jurisdicional devido ao atraso ou não detecção de uso abusivo ou malicioso dos recursos computacionais.	
Probabilidade	**Impacto**	**Grau do risco**
Baixa	Alto	Médio
Mitigação	Estabelecer claramente os tempos máximos de indisponibilidade ou lentidão da solução, toleráveis pelo TRT e respectivos prazos para restabelecimento ou normalização do acesso, com previsão de multas contratuais em caso de atrasos.	
Contingência	Revisão dos termos da contratação ou revisão de estratégia de contratação e iniciar outro processo de contratação.	
Responsável	Gestor e Fiscal do Contrato	
Prazo	Durante a Execução do Contrato	

Análises realizadas pela Equipe de Planejamento.

São Paulo, data da assinatura eletrônica

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

Anexo I - Parecer do SNSEC

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
CONSELHO SUPERIOR DA JUSTIÇA DO TRABALHO

Brasília, 12 de junho de 2023.

Assunto: **Parecer do SNSEC sobre contratação nacional sob gestão do Tribunal Regional do Trabalho da 2ª Região, para solução de Monitoramento, Detecção, Notificação, Investigação e Resposta a Ataques Cibernéticos, ou XDR, SOC/SIEM.**

Trata-se de parecer do SNSEC para recomendar a contratação de solução de Monitoramento, Detecção, Notificação, Investigação e Resposta a Ataques Cibernéticos, soluções também conhecidas XDR, SOC/SIEM, cujo processo de contratação está em andamento pelo TRT da 2ª Região, para todos os órgãos da Justiça do Trabalho, pelos seguintes motivos:

- A Especificação Técnica da contratação citada foi revisada pelo SNSEC e está alinhada com as recomendações de segurança dos normativos atuais, especialmente a Resolução CNJ n. 396/2021, que Institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ) e em especial a Portaria CNJ nº 162/2021, que aprova os Protocolos e Manuais criados pela ENSEC-PJ.

- Devido a solução XDR permitir identificar e tratar ameaças cibernéticas a partir de um único console, reunindo, resumidamente, os seguintes aspectos:

a) Coleta de dados: Etapa que reúne e normaliza grandes volumes de dados de ferramentas de segurança, como tráfego de rede, contêineres virtuais, entre outros.
b) Detecção: Trata-se da análise e correlação de dados para detectar ameaças de forma automática.
c) Resposta: Consiste em priorizar o tratamento de ameaças por gravidade, para apoiar a decisão de tratamento a partir de um único centro, com a disponibilização de ferramentas e apoio técnico de pessoal para a prevenção das ameaças.

- Pelo motivo da tecnologia XDR evidenciar as etapas de uma invasão, identificando a sequência de processos antes do ataque final, a solução permite a antecipação aos cibercriminosos, permitindo adoção de ações de contingência ou mitigação dos ataques.

- Por contemplar serviços de suporte que deverão ser corretivos, proativos e consultivos, envolvendo atividades como auxílio na configuração de políticas e administração da solução, garantir o fornecimento e instalação de novas versões, patches e hotfixes (tanto de componentes on-premises quanto em nuvem), análise de dúvidas sobre melhores práticas de

configuração, suprindo eventuais dificuldades técnicas dos Tribunais;

Diante do contexto apresentado e da exposição cada vez maior da Justiça do Trabalho a riscos de segurança da informação e sob à luz da Resolução 396/2021, o Subcomitê Nacional de Segurança Cibernética recomenda que todos os órgãos componentes da JT registrem participação no Pregão que resultará em futura Ata de Registro de Preços para Solução de Detecção e Resposta estendidas, ou XDR, que será gerenciada pelo TRT da 2ª Região, possibilitando estabelecer esse produto como um padrão nacional.

gov.br Documento assinado digitalmente
ANTONIO FRANCISCO MORAIS ROLLA
Data: 15/06/2023 15:41:09-0300
Verifique em https://validar.iti.gov.br

ANTONIO FRANCISCO MORAIS ROLLA
Coordenador do Subcomitê Nacional de
Segurança Cibernética (SNSEC)
Secretário da Tecnologia da Informação e Comunicação
Conselho Superior da Justiça do Trabalho

Anexo II – Dimensionamento

Anexo II – Dimensionamento																									
Dimensionamento	**TST**	**TRT1**	**TRT2**	**TRT3**	**TRT4**	**TRT5**	**TRT6**	**TRT7**	**TRT8**	**TRT9**	**TRT10**	**TRT11**	**TRT12**	**TRT13**	**TRT14**	**TRT15**	**TRT16**	**TRT17**	**TRT18**	**TRT19**	**TRT20**	**TRT21**	**TRT22**	**TRT23**	**TRT24**
Quantidade de pessoas a participar do treinamento (Item 02)	20	21	8	8	4	10	4	8	6	15	10	10	10	6	8	17	11	15	20	8	6	8	5	5	8
Quantidade de usuários do Tribunal	4500	4242	12888	7433	6331	3491	2200	1500	1800	4243	1503	1200	1850	1100	1050	6148	1130	1130	1969	1236	780	900	1257	1200	1000
Qual o regime de trabalho do Tribunal (8x5, 12x5, ...)?	12x5	8x5	12x5	12x5	12x5	8x5	8x5	8x5	8x5	8x5	12x5	8x5	8x5	10x5	7x5	8x5	7x5	12x5	12x5	8x5	8x5	7x5	7x5	7x5	8x5
Quantidade de domínios a serem monitorados (deep/dark web)	4	4	2	2	2	1	1	2	1	3	1	1	2	1	1	3	1	2	6	1	1	1	1	1	1
Quantidade de data centers	2	1	2	2	2	1	2	2	1	3	2	2	2	1	2	2	2	2	1	2	2	2	2	2	1
Quantidade de estações de trabalho/notebooks	4500	6279	10170	4500	5521	3800	3569	2000	3344	4641	2700	1600	2638	1300	1300	6000	760	1492	2731	1200	970	1300	863	1300	1350
Quantidade de servidores Linux	1043	646	615	220	517	214	360	200	274	530	385	250	298	150	150	526	183	92	337	140	133	279	120	194	250
Quantidade de servidores Windows	197	80	61	60	173	81	170	80	96	182	30	50	30	30	50	71	51	86	135	37	135	60	31	93	50
Quantidade de servidores em nuvem	50	4	0	0	0	0	0	0	40	0	0	0	0	0	0	0	0	77	0	0	0	0	4	0	46
Quais ambientes de nuvem (AWS, Azure, GCP, ...)?	AWS, Azure, Google	AWS, Google Workspace	AWS (Route 53/WAF/CDN), Google Workspace	Google Workspace	AWS (Route 53), Google Workspace	AWS, Google Workspace	Google Workspace	AWS (WAF/CDN), Google Workspace	AWS	AWS, Google Workspace	Office365	Google Workspace	AWS, Google Workspace	AWS (WAF/CDN), Google Workspace	AWS (Route 53/WAF/CDN), Google Workspace	AWS (WAF/CDN), Google Workspace	Google Workspace	AWS, Azure	Google Workspace, PowerBI	AWS (WAF/CDN), Google Workspace	AWS, Google Workspace	Google Wokspace	AWS	AWS (Route 53/WAF/CDN), Google Workspace, PowerBI	AWS, Google Wokspace
Quantidade de aplicações web	300	81	190	82	162	100	68	180	270	822	35	50	250	165	150	126	44	50	376	110	165	80	61	85	34
Quantidade de servidores de banco de dados	39	85	154	13	80	44	63	18	65	42	53	12	25	35	15	64	34	38	35	32	30	38	17	22	28
Quantidade de bancos de dados em DB2	0	0	0	0	1	0	0	0	0	0	0	0	0	1	1	0	0	0	1	1	0	0	0	0	0
Quantidade de bancos de dados em MariaDB	0	0	0	0	0	0	0	2	0	0	0	0	2	0	14	0	9	0	0	0	2	0	0	4	0
Quantidade de bancos de dados em MySQL	0	2	12	6	1	10	36	27	7	6	2	1	0	32	1	2	0	2	10	4	2	2	2	6	1
Quantidade de bancos de dados em Oracle	25	85	23	12	85	63	42	5	8	52	26	5	10	4	4	11	14	5	21	16	6	12	5	4	3
Quantidade de bancos de dados em PostgreSQL	9	175	63	32	3	427	60	49	47	88	13	2	13	140	34	49	220	14	269	20	18	170	6	14	17
Quantidade de bancos de dados em SQL Server	3	1	3	3	1	8	2	2	2	8	0	2	0	8	0	1	1	4	36	3	2	1	2	1	0
Quantidade de bancos de dados em Apache Solr	0	2	6	0	1	1	0	2	0	4	6	1	0	2	0	1	7	7	2	2	1	2	0	2	2
Quantidade de bancos de dados em ElasticSearch	2	3	12	0	18	1	4	7	0	22	4	1	0	5	0	5	4	6	26	12	6	2	2	6	5
Quantidade de bancos de dados em Redis	0	0	2	0	0	1	0	0	1	6	2	1	0	2	0	1	1	4	17	0	0	2	0	2	0
Quantidade de servidores DNS	5	3	6	6	4	5	31	10	24	4	6	8	4	4	1	6	7	17	8	12	6	14	4	25	28
Quantidade de servidores DHCP	2	43	4	2	2	1	31	16	1	3	2	6	32	2	1	105	2	34	2	2	3	8	2	24	23
Quandidade de ADs / OpenLDAPs	3	4	21	10	13	4	32	11	4	3	2	10	2	2	1	5	4	16	2	9	3	12	9	25	2
Quantidade de firewalls	2	3	4	2	68	31	2	2	2	2	10	2	2	2	2	2	2	16	27	2	2	2	10	2	2
Qual o fabricante dos firewalls?	Forcepoint	Checkpoint, PFSense	Checkpoint (nova licitação prevista)	Checkpoint	Checkpoint, Fortinet (SD-WAN)	Checkpoint	Checkpoint	Checkpoint	Fortinet	Checkpoint	Checkpoint, PFSense	Checkpoint	Checkpoint	Checkpoint	Checkpoint	Checkpoint	Checkpoint	Checkpoint, Fortinet (SD-WAN), AWS (WAF)	Checkpoint, Fortinet (SD-WAN)	Check Point	Check Point	Checkpoint	Checkpoint, PFSense	Checkpoint	Checkpoint (em nova licitação prevista)
Quantidade de soluções de backup	3	1	2	1	1	2	1	1	2	1	1	2	2	2	1	1	2	2	2	2	2	1	1	1	2
Ativos	5790	7009	10846	4780	6211	4095	4099	2280	3754	5353	3115	1900	2966	1480	1500	6597	994	1747	3203	1377	1238	1639	1018	1587	1696
Faixa	4	4	5	3	4	3	3	3	3	4	3	2	3	2	2	4	1	2	3	2	2	2	2	2	2
Rede 1 Gbps	8	6	5	5	8	0	7	2	2	9	8	7	7	1	4	1	5	4	5	1	4	2	2	4	2
Rede 10 Gbps	2	0	1	1	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
Rede 1 Gbps (com vantagem econômica)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Rede 10 Gbps (com vantagem econômica)	4	1	2	2	1	2	1	1	1	2	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1
Turmas	3	3	1	1	1	2	1	1	1	2	2	2	2	1	1	3	2	2	3	1	1	1	1	1	1