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%

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

		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:

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

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

	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

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

Termo de Referência

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

1 OBJETO

1.1 Descrição do Objeto

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

2 FUNDAMENTAÇÃO DA CONTRATAÇÃO

2.1 Motivação da Contratação

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.

2.2 Objetivos

A contratação de serviço técnico especializado de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos, tem como objetivo o monitoramento contínuo e ininterrupto dos ativos computacionais a fim de prevenir tentativas de acesso não autorizados, bem como identificar eventos suspeitos ou incomuns relativos a ataques, violações de conformidade e comportamento suspeito que possam comprometer os serviços tecnológicos deste Regional e dos demais Tribunais coparticipantes da licitação. Com isso, espera-se também minimizar os impactos de uma possível ocorrência de grande magnitude.

[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/

2.3 Benefícios

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.

2.4 Alinhamento

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.

2.5 Referência aos Estudos Preliminares

Este Termo de Referência baseia-se nos estudos preliminares constantes do processo PROAD nº 9.605/2021.

2.6 Impactos Diretos e Indiretos da Contratação

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.

2.7 Relação entre a Demanda Prevista e a Quantidade

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.

2.8 Análise de Mercado

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

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

		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
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

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

		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 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$ 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

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

		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 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$ 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

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

		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
		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

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

		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,	Ativo monitorado semestralmente	N/A	R$ 350.000,00

	considerando um parque de até 2000 ativos monitorados.			
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:

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

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
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

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

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
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,	Tipo 1	Até 1000 ativos	Ativo monitorado anualmente	994	R$ 477,32	R$ 474.456,08	R$ 948.912,16

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

	detecção, notificação, investigação e resposta a ataques cibernéticos	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
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	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

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

	resposta a ataques cibernéticos	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 nas propostas das empresas Petacorp, Service IT, Suporte Informática e Network Secure 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:

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

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%
		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%

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

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%
		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%

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

		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%
		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%

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

		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.

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%

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	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, 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

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$ 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. Por isso, caso sejam utilizados os valores desta licitação na composição da estimativa de custo, eles podem não ser exequíveis.

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:

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

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	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 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.

2.9 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 efetivar 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 se 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.

2.10 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.

2.11 Forma de Adjudicação

Para efeito de adjudicação do objeto, recomenda-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.

2.12 Modalidade, Tipo de Licitação e Critérios de Seleção

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.

2.13 Impacto Ambiental

A Secretaria de Processamento e Acompanhamento de Contratos e Licitações, em sua Notificação Ambiental, documento 19 do PROAD 9.605/2021, dos itens 4.5 e 4.6 do Manual para Contratação de Solução de TIC e de acordo com a análise do objeto constante no presente Processo Administrativo de Contratação, informou que a Secretaria de Processamento e Acompanhamento de Contratos e Licitações e a Seção de Gestão Socioambiental verificaram, s.m.j, não haver critério de sustentabilidade a ser observado quando da contratação, conforme determinações previstas no Plano de Logística Sustentável (PLS-TRT2), no Guia de Contratações Sustentáveis do Conselho Superior da Justiça do Trabalho, Resolução nº 310/2021 ou no Guia Prático de Contratações Sustentáveis do TRT2.

Informou também que não há necessidade de participação da Seção de Gestão Socioambiental, com a indicação de integrante, no presente processo de contratação, em cumprimento ao item 4.6 do referido Manual.

2.14 Aderência da Contratação ao plano anual de compras

A contratação deverá estar prevista nas programações orçamentárias da Secretaria de Tecnologia da Informação e Comunicação para os anos de 2024 e 2025.

2.15 Conformidade com normas Técnicas e Legais

As especificações técnicas descritas no Anexo A deste Termo de Referência vislumbram a

aplicação de normas técnicas e legais específicas.

2.16 Prazo e Condições de Garantia

A CONTRATADA deve realizar a implantação, configuração e ativação da solução no prazo de até 45 (quarenta e cinco) dias corridos, contados a partir da assinatura do contrato, conforme objetivos, escopo, requisitos, premissas e demais condições detalhadas que constam das Especificações Técnicas em anexo.

O período de vigência deverá ser de 24 (vinte e quatro) meses a partir do Termo de Recebimento Definitivo do Serviço de implantação da solução, podendo ser prorrogado por mais 24 (vinte e quatro) meses ou até o limite legal.

2.17 Condições e Prazos de Pagamento

O pagamento relativo às subscrições de licenças do software de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos será realizado anualmente, devendo ser fornecidas conforme a quantidade de ativos definida pela CONTRATANTE e deverão ser nomeadas (para cada CONTRATANTE). A comprovação do fornecimento se dará através da Nota Fiscal e o pagamento somente será autorizado depois de efetuado o “atesto” pelo servidor competente, condicionado este ato à verificação da conformidade da Nota Fiscal/Fatura apresentada em relação às subscrições efetivamente fornecidas em nome da CONTRATANTE, conforme volumetria mínima prevista.

O pagamento relativo aos serviços de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos será realizado mensalmente, sendo realizado somente após a emissão do termo de recebimento definitivo, descontadas eventuais glosas do período avaliado, conforme Fator de Desconto (FD) calculado no período e das multas aplicadas, quando houver.

O pagamento do serviço de implantação deve ser realizado em parcela única, após a emissão do termo de recebimento definitivo.

O pagamento do treinamento deve ser realizado em parcela única após a emissão do termo de recebimento definitivo.

Além das retenções legais, serão automaticamente descontados dos valores faturados os percentuais decorrentes da aplicação dos critérios de níveis de serviço.

2.18 Previsão de Custo

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

Serão necessários recursos orçamentários para os próximos exercícios, conforme segue:

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

3 Equipe de Gestão e Fiscalização da Contratação

Papel	Servidor	Matrícula	Telefone	E-mail
Gestor 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	2726	riscos-ti@trt2.jus.br
Fiscal Técnico	Ramon Chiara – Assistente Administrativo Chefe da Seção de Gestão de Incidentes em Segurança da Informação	133167	2737	incidentesseg-ti@trt2.jus.br

Fiscal Técnico - Substituto	Lucas Ihara Alves - Seção de Gestão de Incidentes em Segurança da Informação	161020	2737	lucas.alves@trt2.jus.br

3.1 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	2737	incidentesseg-ti@trt2.jus.br
Lucas Ihara Alves	2737	lucas.alves@trt2.jus.br
Cláudia Sant'Anna Pinheiro	2073	seguranca-ti@trt2.jus.br

O prazo para o recebimento definitivo, após a conclusão do serviço de implantação, configuração e ativação da solução, será de até 45 (quarenta e cinco) dias corridos, contados a partir da assinatura do contrato. O prazo para sanar irregularidades, no caso de entrega/disponibilização de serviço em desacordo com o solicitado, será de até 15 (quinze) dias corridos da data de comunicação.

3.2 Obrigações Contratuais

As obrigações contratuais pormenorizadas constam da especificação técnica que acompanha este termo de referência.

Destaca-se o cumprimento das obrigações e requisitos detalhados no Anexo A – Especificações Técnicas, bem como a eventual aplicação das penalidades a eles vinculadas, descritas no mesmo anexo.

4 OUTRAS INFORMAÇÕES RELEVANTES

Os produtos deverão ser registrados em Ata de Registro de Preços conforme a tabela abaixo:

Item	Descrição	Tipo de Faixa	Faixa de Subscrição	Quant. Registrada	Pedido Inicial	Pedido Mínimo	Valor Unitário Máximo	Valor Total Máximo (24 meses)
01	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos monitorados anualmente	994	0	1	R$ 398,53 p/ ano	R$ 792.277,64
		Tipo 2	De 1001 a 2000 ativos monitorados anualmente	15.182	0	1	R$ 350,24 p/ ano	R$ 10.634.687,36
		Tipo 3	De 2001 a 5000 ativos monitorados anualmente	28.292	0	1	R$ 320,96 p/ ano	R$ 18.161.200,64
		Tipo 4	De 5001 a 8000 ativos monitorados anualmente	30.960	0	1	R$ 330,34 p/ ano	R$ 20.454.652,80
		Tipo 5	De 8001 a 12000 ativos monitorados anualmente	10.846	10.846	1	R$ 315,21 p/ ano	R$ 6.837.535,32

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

Item	Descrição	Tipo de Faixa	Faixa de Subscrição	Quant. Registrada	Pedido Inicial	Pedido Mínimo	Valor Unitário Máximo	Valor Total Máximo (24 meses)
		Rede	10Gbps (Gigabits por segundo) de tráfego diário monitorado anualmente	33	2	1	R$ 202.208,68 p/ ano	R$ 13.345.772,88
02	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes (Valor por turma)	40	1	1	R$ 47.052,12 p/ turma	R$ 1.882.084,80
03	Serviço de implantação da solução proposta	-	Serviço de implantação e ativação da solução e seus componentes	25	1	1	R$ 149.744,31 p/ serviço	R$ 3.743.607,75
04	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos monitorados mensalmente	1	0	1	R$ 37.343,77 p/ mês	R$ 896.250,48
		Tipo 2	De 1001 a 2000 ativos monitorados mensalmente	10	0	1	R$ 51.430,40 p/ mês	R$ 12.343.296,00
		Tipo 3	De 2001 a 5000 ativos monitorados mensalmente	8	0	1	R$ 69.998,20 p/ mês	R$ 13.439.654,40
		Tipo 4	De 5001 a 8000 ativos monitorados mensalmente	5	0	1	R$ 95.216,10 p/ mês	R$ 11.425.932,00
		Tipo 5	De 8001 a 12000 ativos monitorados mensalmente	1	1	1	R$ 104.948,67 p/ mês	R$ 2.518.768,08
							TOTAL	**R$ 116.475.720,15**

Cumpre informar também que a equipe de planejamento desta contratação não identificou impedimentos em relação à aplicação do decreto nº 7.174/2010. Porém, por se tratar de um mercado restrito de soluções que atendam plenamente a demanda, não se recomenda, s.m.j, que seja restringida a licitação a apenas empresas que atendam ao disposto no artigo 5º, sob o risco de fracasso do certame.

As empresas participantes deverão apresentar, no momento da sua habilitação no processo licitatório, Atestado(s) de Capacidade Técnica (ACT) em nome da licitante e emitido(s) por pessoa(s) jurídica(s) de direito público ou privado, onde comprove ter prestado ou estar prestando:

- Fornecimento de solução de Monitoramento, Detecção, Notificação, Investigação e Resposta a Ataques Cibernéticos similar à proposta, em ambiente computacional contendo no mínimo 4.000 (quatro mil) ativos monitorados;

- Fornecimento de serviço de Monitoramento, Detecção, Notificação, Investigação e Resposta a Ataques Cibernéticos, em regime 24x7x365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias ao ano), em ambiente computacional contendo no mínimo 4.000 (quatro mil) ativos monitorados;

- Para cada subitem acima, serão considerados somatórios de atestados para atingir as quantidades solicitadas.

Na fase da habilitação deverá ser apresentado: balanço patrimonial e demonstrações do resultado do exercício – DRE relativos ao último exercício social exigível, comprovando índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um),

em conformidade com os normativos pertinentes, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrado há mais de 3 (três) meses da data de apresentação da proposta, devendo apresentar as seguintes características:

- Estarem devidamente assinados pelo administrador da empresa e pelo profissional de Contabilidade;

- Estarem devidamente registrados na Junta Comercial do Estado correspondente ou disponibilizado pelo SPED;

- Constando Patrimônio Líquido igual ou superior a 10% (dez por cento) do valor estimado da contratação;

- Constando Capital circulante Líquido ou Capital de Giro (Ativo Circulante - Passivo Circulante) de, no mínimo, 16,66% (dezesseis inteiros e sessenta e seis centésimos por cento) do valor estimado da contratação.

A comprovação dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC) serão resultantes da aplicação das fórmulas:

$$LG = \frac{\text{Ativo Circulante + Realizável a Longo Prazo}}{\text{Passivo Circulante + Passivo Não Circulante}}$$

$$SG = \frac{\text{Ativo Total}}{\text{Passivo Circulante + Passivo Não Circulante}}$$

$$LC = \frac{\text{Ativo Circulante}}{\text{Passivo Circulante}}$$

No caso de empresa constituída no exercício social vigente, admite-se a apresentação de balanço patrimonial e demonstrações contábeis referentes ao período de existência da sociedade.

Com o objetivo de se 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.

A licitante vencedora deverá apresentar, junto com os demais documentos de habilitação, a planilha de comprovação de atendimento aos itens da especificação técnica devidamente preenchida, conforme Anexo B – Comprovação de atendimento aos itens da Especificação

Técnica, onde deverá constar a forma de atendimento a cada um dos itens mencionados no documento.

5 ESPECIFICAÇÃO TÉCNICAS

Conforme Anexo A – Especificações Técnicas.

Análises realizadas pela Equipe de Planejamento.

São Paulo, data da assinatura eletrônica.

Anexo A - Especificação Técnica

1. Objeto

Ata de registros de preços visando a contratação de solução de Monitoramento, Detecção, Notificação, Investigação e Resposta a Ataques Cibernéticos, bem como serviços de treinamento, implantação e sustentação da solução proposta, pelo período de 24 meses, conforme a tabela seguinte:

Item	Descrição	Tipo de Faixa	Faixa de Subscrição	Unidade de Medida
01	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos	Ativo monitorado anualmente
		Tipo 2	De 1001 a 2000 ativos	Ativo monitorado anualmente
		Tipo 3	De 2001 a 5000 ativos	Ativo monitorado anualmente
		Tipo 4	De 5001 a 8000 ativos	Ativo monitorado anualmente
		Tipo 5	De 8001 a 12000 ativos	Ativo monitorado anualmente
		Rede	1Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente
			10Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente
02	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes	Serviço pontual, por turma de treinamento
03	Serviço de implantação da solução proposta	-	Serviço de implantação e ativação da solução e seus componentes	Serviço pontual
04	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos monitorados	Serviço mensal
		Tipo 2	De 1001 a 2000 ativos monitorados	Serviço mensal
		Tipo 3	De 2001 a 5000 ativos monitorados	Serviço mensal
		Tipo 4	De 5001 a 8000 ativos monitorados	Serviço mensal
		Tipo 5	De 8001 a 12000 ativos monitorados	Serviço mensal

1.1 Definições para fins desta especificação:

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

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

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

1.1.2 Define-se “Tráfego diário monitorado” como sendo volume médio diário do tráfego da rede interna (em Gbps - Gigabits por segundo) que deverá ser monitorado pela solução proposta.

1.1.3 Para os dados do ambiente da CONTRATANTE que serão coletados pela solução proposta, compreende-se as seguintes definições:

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

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

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

1.2 Para soluções cuja subscrição seja baseada em EPS (Eventos Por Segundo), a CONTRATADA deve licenciar a solução para uma quantidade mínima de EPS suficiente para atender 100% dos ativos da CONTRATANTE e garantir a escalabilidade da solução, independentemente da quantidade de EPS gerados pelos ativos monitorados, observando-se o limite de licenciamento mínimo de EPS igual a 8 vezes a referida quantidade de ativos monitorados.

1.2.1 A CONTRATADA deverá aferir mensalmente o consumo de EPS e provar que a quantidade ofertada está comportando a quantidade de eventos ingerida pela solução, realizando correções no quantitativo se necessário, sem custo para a CONTRATANTE.

1.3 Para soluções cuja subscrição seja baseada em volumetria de logs, a CONTRATADA deve licenciar a solução para uma quantidade mínima de Área de Armazenamento em modalidade SaaS, suficiente para atender 100% dos ativos da CONTRATANTE e garantir a escalabilidade da solução, independentemente do volume de logs, dados de telemetria e de rede gerados pelos ativos monitorados, observando-se o limite de licenciamento mínimo de GB (gigabytes) igual a 2 vezes a referida quantidade de ativos monitorados e a retenção dos logs estipulada no item 2.8.

1.3.1 A CONTRATADA deverá aferir mensalmente a volumetria e provar que a quantidade ofertada está comportando a quantidade de eventos ingerida pela solução, realizando correções no quantitativo se necessário, sem custo para a CONTRATANTE.

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

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

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

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

2.3. A CONTRATADA deve prover, ao ambiente, soluções de segurança cibernética que permitam a visibilidade de logs, dados de telemetria, tráfego de rede e de informações correlatas, capazes de identificar eventos suspeitos ou incomuns que possam comprometer os serviços tecnológicos 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.

2.4. Para a prestação desse serviço, deve ser utilizada uma solução de Monitoramento, Detecção, Notificação, Investigação e Resposta a Ataques Cibernéticos, com capacidades de Coleta e Correlacionamento de Logs e Mecanismos de Detecção de Comportamento Anômalo de Usuários e Aplicações (UEBA – User and Entity

Behavior Analytics). Neste caso, entende-se por "Aplicações" como sendo os softwares instalados nos ativos monitorados.

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

2.5.1. Analisar, classificar, categorizar, correlacionar e notificar os eventos e incidentes classificados como ameaças à segurança cibernética, ou que sejam considerados relevantes de acordo com diretrizes estabelecidas pela CONTRATANTE;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.5.4.1.1.3. Gerar relatórios mensais do acordo de nível de serviço (SLA – Service Level Agreement) dos alertas, incidentes e chamados.

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

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

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

2.6.1. O fabricante da solução proposta para monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos deve ser atestado SOC 2 Type II;

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

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

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

2.6.5. Coletores de tráfego de rede: o software dos coletores de tráfego de rede, bem como os respectivos sistemas operacionais, sistemas gerenciadores de banco de dados, entre outros componentes (de software ou hardware) eventualmente necessários para a coleta e centralização de dados de tráfego de rede deverão ser fornecidos pela CONTRATADA, podendo ser de fabricantes distintos da solução, devendo ser compatíveis com a infraestrutura da CONTRATANTE (interfaces de rede de 1Gbps e 10Gbps).

2.6.5.1. O tráfego de rede deverá ser mensurado de acordo com o ambiente da CONTRATANTE.

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

2.6.6.1. 12 vCPUs;

2.6.6.2. 32Gb vRAM;

2.6.6.3. 200GB de espaço em disco.

2.6.7. Caso os recursos em ambiente virtual necessários para o pleno funcionamento da solução extrapolem os recursos disponibilizados pela CONTRATANTE, a CONTRATADA deve demonstrar, por meio de documento técnico do fabricante e/ou de boas práticas, a necessidade de aumento dos recursos, que serão disponibilizados pela CONTRATANTE conforme comprovação apresentada. Caso não haja comprovação, a critério da CONTRATANTE, a CONTRATADA deverá providenciar, sem custos adicionais para a CONTRATANTE, a entrega da infraestrutura (total ou remanescente) e em conformidade com a estrutura computacional da CONTRATANTE.

2.6.8. Agentes: software de baixo consumo de processamento que é instalado nos ativos suportados para centralizar e monitorar os dados de segurança cibernética. O agente oferece visibilidade e detecção de

ataques nos endpoints, coletando informações on-line do sistema, incluindo informações básicas de identificação de ativos, processos em execução, logs e outros dados de telemetria e as enviando de volta à solução para análise.

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

2.6.9.1. Google Chrome;

2.6.9.2. Mozilla Firefox.

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

2.6.10.1. Caso a solução seja composta por diversas ferramentas, a console de gerência principal deve permitir a visibilidade integrada e total do monitoramento, detecção, notificação, investigação e resposta aos ataques cibernéticos detectados e sendo tratados em todo o ambiente computacional.

2.6.10.2. As demais ferramentas podem estar hospedadas em ambiente provisionado pela CONTRATADA, sem custos adicionais para a CONTRATANTE.

2.6.10.3. Os ambientes utilizados pela solução (incluindo do fabricante) devem possuir, ao menos, uma cópia das informações localizadas no Brasil.

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

2.7. A solução deve ser fornecida dimensionada para a quantidade de ativos a serem monitorados ou para a quantidade de eventos por segundo (conforme item 1.2) ou para o volume de armazenamento de logs em ambiente SaaS (conforme item 1.3) de forma a abranger o escopo completo de ativos da CONTRATANTE, conforme conceito apresentado nesta especificação técnica. Assim, é obrigatório que a solução cubra 100% do ambiente da CONTRATANTE, incluindo estações de trabalho, notebooks, dispositivos móveis, servidores físicos e virtuais, containers, firewalls, ativos de rede ou qualquer equipamento similar ao listado, e não somente parcialmente, de forma a prover uma visibilidade plena da segurança cibernética do ambiente.

2.7.1. A solução deve suportar picos de EPS (Eventos Por Segundo) ou GB (gigabytes) acima do licenciado em até 30%.

2.7.1.1. Caso os picos de EPS ou GB ultrapassem o limite de 30%, a solução não deve descartar os eventos de forma que sejam processados posteriormente.

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.

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

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

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

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

2.9.4. Adicionalmente, para ambientes com Microsoft Active Directory:

2.9.4.1. Movimentação lateral com uso de credenciais de domínio;

2.9.4.2. Ataques de força bruta em contas de domínio;

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

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

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

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

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

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

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

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

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

2.13.1. Firewalls;

2.13.2. Web Application Firewalls;

2.13.3. IPS (Intrusion Prevention System) / IDS (Intrusion Detection System);

2.13.4. Web filtering;

2.13.5. Antivírus;

2.13.6. Microsoft Active Directory;

2.13.7. Open LDAP;

2.13.8. IAM (Identity and Access Management) / PAM (Privileged Access Management);

2.13.9. Servidores HTTP (HTTP Servers);

2.13.10. Balanceadores de Carga (Load Balancers);

2.13.11. DNS;

2.13.12. DHCP;

2.13.13. ELK Stack;

2.13.14. Sistemas Operacionais.

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

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

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

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

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

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

2.16. Para detectar incidentes, a solução também deverá suportar o recebimento e processamento de eventos de tráfego de rede e, opcionalmente, flow de rede, provendo as seguintes informações, no mínimo:

2.16.1. Sistemas com maior atividade baseada em volume de tráfego;

2.16.2. Principais aplicações e protocolos trafegados, baseado em volume de dados enviados e recebidos entre endpoints da rede;

2.16.3. Atividades de rede baseada em porta de destino e endereços de origem e destino;

2.16.4. Relação dos usuários ou ativos que mais consomem banda de rede, baseado em volume de tráfego.

2.16.5. Servidores DNS em uso;

2.16.6. Relação das principais aplicações em uso na rede;

2.16.7. Identificação de picos de consumo de banda de acesso à rede;

2.16.8. Relação de dispositivos, servidores e serviços que operam na rede.

2.17. A solução deve implementar a coleta e análise de diferentes fontes de eventos. A coleta deve ser realizada para logs, dados de telemetria e/ou de rede, devendo ser possível coletar e analisar eventos das seguintes soluções presentes atualmente de forma predominante no ambiente da CONTRATANTE:

2.17.1. De forma nativa (sem a necessidade de customização de parsers):

2.17.1.1. Checkpoint para proteção de perímetro (Firewall);

2.17.1.2. Fortinet FortiGate para proteção de perímetro (Firewall);

2.17.1.3. Forcepoint para proteção de perímetro (Firewall);

2.17.1.4. Microsoft Active Directory para serviços de diretório.

2.17.2. De forma nativa (sem a necessidade de customização de parsers) ou não:

2.17.2.1. Open LDAP para serviços de diretório;

2.17.2.2. OpenVPN;

2.17.2.3. Citrix;

2.17.2.4. RDP e RDPWeb;

2.17.2.5. Senha Segura para serviços de gerenciamento de acesso privilegiado;

2.17.2.6. Cyberark para serviços de gerenciamento de acesso privilegiado

2.17.2.7. Hashicorp Vault e Hashicorp Boundary para serviços de gerenciamento de acesso privilegiado;

2.17.2.8. Keycloak para gerenciamento de identidade e acesso;

2.17.2.9. midPoint para segurança de identidades (identity security);

2.17.2.10. ForeScout CounterACT (eyeSight e eyeControl) para serviços de NAC (Network Access Control);

2.17.2.11. Loqed;

2.17.2.12. Varonis;

2.17.2.13. IBM Spectrum Protect Plus para proteção de dados;

2.17.2.14. Kaspersky para proteção de endpoint;

2.17.2.15. Blackberry Cylance para proteção de endpoint.

2.17.2.16. Check Point Harmony para proteção de endpoint;

2.17.2.17. Tenable One para gerenciamento de exposição (exposure management platform);

2.17.2.18. Tenable.ep / Nessus para gerenciamento de vulnerabilidades;

2.17.2.19. Tenable.ad para proteção do Active Directory;

2.17.2.20. Trivy para varredura de vulnerabilidades;

2.17.2.21. VMware/vCenter para virtualização de máquinas;
2.17.2.22. VMware/Horizon para virtualização de estações de trabalho;
2.17.2.23. Hyper-V para virtualização de máquinas;
2.17.2.24. Ovirt para virtualização de máquinas;
2.17.2.25. Docker e Kubernetes;
2.17.2.26. Apache HTTP Server;
2.17.2.27. HAProxy;
2.17.2.28. Ingress;
2.17.2.29. Nginx;
2.17.2.30. Switches Cisco MDS;
2.17.2.31. Switches H3C;
2.17.2.32. Switches HP;
2.17.2.33. Switches Huawei;
2.17.2.34. Roteadores Cisco;
2.17.2.35. Roteadores Juniper;
2.17.2.36. Roteadores MikroTik;
2.17.2.37. Access Points Aruba;
2.17.2.38. Access Points Ruckus;
2.17.2.39. Controladoras Virtuais Aruba;
2.17.2.40. Bacula para serviços de backup;
2.17.2.41. Commvault (software de backup);
2.17.2.42. Veeam (software de backup);
2.17.2.43. Storage Huawei;
2.17.2.44. Storage IBM;
2.17.2.45. TSM Server IBM Spectrum Protect para serviços de backup;
2.17.2.46. Dell EMC Data Domain;
2.17.2.47. Dell EMC Isilon.

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

2.18.1. De forma nativa (sem a necessidade de customização de parsers):

2.18.1.1. AWS CloudTrail, via SQS ou API;
2.18.1.2. Google Cloud Platform, via API;
2.18.1.3. Google Workspace/Google Apps, via API;
2.18.1.4. Microsoft Office 365, via API.

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

2.19.1. De forma nativa (sem a necessidade de customização de parsers):

2.19.1.1. Windows 7;
2.19.1.2. Windows 8.1;
2.19.1.3. Windows 10;

2.19.1.4. Windows 11;
2.19.1.5. Windows Server 2008 R2;
2.19.1.6. Windows Server 2012;
2.19.1.7. Windows Server 2012 R2;
2.19.1.8. Windows Server 2016;
2.19.1.9. Windows Server 2019;
2.19.1.10. Windows Server 2022;
2.19.1.11. Red Hat Enterprise Linux / Oracle Enterprise Linux / Rocky Linux 8.4;
2.19.1.12. Red Hat Enterprise Linux / Oracle Enterprise Linux / Rocky Linux 8.5;
2.19.1.13. Red Hat Enterprise Linux / Oracle Enterprise Linux / Rocky Linux 9.0;
2.19.1.14. Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 7;
2.19.1.15. Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 8.0;
2.19.1.16. Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 8.1;
2.19.1.17. Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 8.2;
2.19.1.18. Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 8.3;
2.19.1.19. Amazon Linux;
2.19.1.20. Debian Linux;
2.19.1.21. Ubuntu Linux.

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

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

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

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

2.24. A solução deve possuir de maneira nativa detecções de, no mínimo, os seguintes vetores de ataque:
2.24.1. Requisição a domínio suspeito;
2.24.2. Execução de processos suspeitos;
2.24.3. Requisição de dados de registro do sistema de nome de domínio (DNS);
2.24.4. Comunicação com servidores Command & Control;
2.24.5. Tentativa de desabilitar recursos de Sysmon;
2.24.6. Execução de processos LSASS (Local Security Authority Subsystem Service) com objetivo de detectar dump de memória para acessar possíveis credenciais armazenadas;
2.24.7. Detecção do uso de msrsc.exe - Microsoft Terminal Services Client;
2.24.8. Detecção do uso de comandos estruturados consistentes pela ferramenta Impacket e Impacket-Obfuscation;
2.24.9. Detecção de atividade de linha de comando da execução da função GetSystem, usada pelo Meterpreter ou Cobalt Strike;
2.24.10. Detecção de execução do Mimikatz e variações;

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

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

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

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

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

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

2.29. A solução deve permitir o enriquecimento de dados relacionados a endereços IPs, buscando informações adicionais em fontes de OSINT (Open Source Intelligence).

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

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

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

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

2.31. 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.

2.31.1. Honeypot: máquina projetada para capturar informações sobre tentativas de acesso e exploração. Deve permitir a instalação de, ao menos, 05 (cinco) máquinas no ambiente;

2.31.1.1. Os honeypots devem ser fornecidos em formato OVA – virtual appliance.

2.31.2. Honey Credential: configuração de um conjunto de credenciais falsas na memória de um ativo;

2.31.3. Honey User: usuário falso que não está associado a uma pessoa real dentro da organização e, portanto, nunca deve ser acessado – monitoramento do Microsoft Active Directory;

2.31.4. Honey File: arquivo falso localizado em um compartilhamento de arquivos de rede.

2.31.5. A solução deve ser capaz de detectar o vetor de entrada da ameaça na rede, identificar o caminho utilizado pelo invasor até o ativo, credencial, usuário ou arquivo específico e apresentar as vulnerabilidades exploradas no ativo (quando for o caso).

2.32. Quando a solução não possuir capacidade de "deception", a capacidade de "Breach and Attack Simulation" (BAS) pode ser apresentada, com os seguintes critérios mínimos:

2.32.1. Caso a funcionalidade seja oferecida como um serviço, as licenças necessárias para a sua execução devem ser baseadas em vetores ou agentes, sendo um para cada tipologia: infraestrutura, network e e-mail; os 03 (três) tipos de licenças devem estar incluídas sem custos adicionais para a CONTRATANTE;

2.32.2. Deve ser executado, pelo menos, mensalmente;

2.32.3. Deve ser executado de forma automatizada, simulando ataques reais, mas que não coloquem em risco o ambiente computacional da CONTRATANTE;

2.32.4. As simulações devem utilizar diferentes vetores de ataque;

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

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

2.34. A solução deve possuir as funcionalidades de:

2.34.1. Monitoramento de comportamento (behavior monitor);

2.34.2. Controle de aplicação;

2.34.3. Monitoramento de eventos;

2.34.4. Auditoria de alterações no sistema;

2.34.5. Resposta automatizada a ameaças com a possibilidade de, mas não se limitando a, executar as ações propostas no item 2.62.

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

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

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

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

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

2.39.1. Segura e criptografada;

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

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

2.41. A solução deve monitorar, no mínimo:

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

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

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

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

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

2.41.6. Exploração mitigada (exploit mitigated);

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

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

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

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

2.41.11. Movimentação lateral com credenciais locais (lateral movement – local credentials);

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

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

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

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

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

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

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

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

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

2.45.2. Identificar quais eventos devem gerar alertas;

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

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

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

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

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

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

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

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

2.51.1. Crítico;

2.51.2. Alto;

2.51.3. Médio;

2.51.4. Baixo.

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

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

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

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

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

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

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

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

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

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

2.58.1.1. .bat

2.58.1.2. .cfg

2.58.1.3. .conf

2.58.1.4. .config

2.58.1.5. .dll

2.58.1.6. .exe

2.58.1.7. .ini

2.58.1.8. .sys

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

2.59. Para realizar o monitoramento do tráfego de rede, a solução deve ser do tipo passiva e ser instalada em modo off-line na rede, ou seja, não ser um ativo em linha ou permitir o envio de logs e/ou dados de telemetria/de rede através de integração.

2.60. A solução deve ser capaz de inspecionar o tráfego de rede baseado no volume de tráfego em Gbps da CONTRATANTE e realizar a análise dos dados coletados.

2.61. A solução deve, junto com o monitoramento do tráfego de rede (ou por meio de agentes), implementar regras de detecção de intrusão para correlacionar e trazer as informações sobre possíveis anomalias e ataques no nível de rede.

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

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

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

2.62.1. Envio de e-mails.

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

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

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

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

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

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

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

2.62.4.1. Ser totalmente automática;

2.62.4.2. Aguardar uma interação humana para ser realizada.

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

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

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

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

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

2.67.1. As notificações podem ser nativas ou, caso necessário, serem desenvolvidas pela CONTRATADA, sem custo para a CONTRATANTE, para viabilizar sua integração.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.88.4.1. Alertas e incidentes mais frequentes;

2.88.4.2. Nível de risco do ambiente;

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

2.88.4.4. Top 10 (dez) ativos com incidentes;

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

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

2.88.4.7. Ativos e contas descobertas;

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

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

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

2.88.6.1. Planilha: CSV e/ou Excel;

2.88.6.2. Texto: HTML e/ou PDF.

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

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

2.91. A solução deve permitir habilitar ou desabilitar um determinado usuário sem excluí-lo do console.

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

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

MONITORAMENTO DEEP/DARK WEB (MONITORAMENTO DE MARCA E AMEAÇAS GLOBAIS)

2.94. A CONTRATADA deverá realizar serviços de monitoramento de Deep/Dark Web por meio da solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos ofertada (nativamente ou por meio de solução complementar). Os serviços e a respectiva solução utilizada para a realização do monitoramento de Deep/Dark Web devem atender às seguintes especificações mínimas:

2.94.1. A solução de monitoramento de Deep/Dark Web deve ter como objetivo principal o rastreamento de salas, blogs, fóruns e sites na Deep/Dark Web para identificar informações relativas à CONTRATANTE e seus colaboradores como: credenciais roubadas e outros vazamentos de informações pessoais identificáveis.

2.94.2. A solução de monitoramento de Deep/Dark Web deve estar licenciada para monitorar até 06 (seis) domínios DNS da CONTRATANTE e uma quantidade de no mínimo 500 (quinhentos) termos por domínio.

2.94.3. O serviço de monitoramento de Deep/Dark Web deve ser prestado no regime 24x7 (vinte e quatro horas por dia, sete dias por semana).

2.94.4. A solução de monitoramento de Deep/Dark Web deve realizar buscas, no mínimo:

2.94.4.1. Na Darknet;

2.94.4.2. Em plataformas de compartilhamento de documentos;

2.94.4.3. Pelas seguintes categorias:

2.94.4.3.1. Por Bucket: Darknet TOR, Whois, Usenet, Leaks, Bot Logs, Wikileaks, Public Leaks, Dumpster, Sci-Hub;

2.94.4.3.2. Por Site Público: .com, .org, .net, .info, .eu.

2.94.4.3.3. Por Geolocalização.

2.94.5. A solução de monitoramento de Deep/Dark Web deve permitir a busca de termos considerando, no mínimo, as seguintes categorias:

2.94.5.1. Domínio DNS;

2.94.5.2. Endereço de e-mail;

2.94.5.3. Endereço Bitcoin;

2.94.5.4. Endereço Ethereum;

2.94.5.5. Endereço MAC;

2.94.5.6. Hash IPFS;

2.94.5.7. IBAN (Número de Conta Bancária Internacional);

2.94.5.8. IP e CIDR;

2.94.5.9. Número de telefone;

2.94.5.10. Número do cartão de crédito;

2.94.5.11. URL.

2.94.6. Deve detectar resultados de itens pesquisa duplicados, apresentando-os de forma consolidada, otimizando a busca por informações relevantes.

2.94.7. A solução de monitoramento de Deep/Dark Web deve ter a capacidade de buscar dados pelo período mínimo de 1 ano.

2.94.8. A solução de monitoramento de Deep/Dark Web deve ter a capacidade de filtrar e classificar os resultados das buscas:

2.94.8.1. Com base na data ou no tempo de publicação das informações encontradas (antigas e novas);

2.94.8.2. Com base nos domínios, e-mails e URLs encontrados;

2.94.8.3. Com base nos resultados mais relevante, menos relevante, mais recente e mais antigo;

2.94.8.4. Com capacidade de combinar ou excluir termos de pesquisa a fim de encontrar com eficiência informações relevantes no banco de dados.

2.94.9. A solução de monitoramento de Deep/Dark Web deve ter a capacidade de manter históricos de resultados de busca.

2.94.10. A solução de monitoramento de Deep/Dark Web deve contemplar os seguintes itens:

2.94.10.1. Monitoramento de atividades na Deep/Dark Web relacionadas às informações sobre domínios, URLs, IPs, hashes, credenciais, e-mails e informações sensíveis da CONTRATANTE.

2.94.10.2. Amplitude de rastreamento contemplando dados e informações disponibilizadas na Deep/Dark Web como:

2.94.10.2.1. Monitoramento das credenciais de funcionários em listas e bases de dados de credenciais vazadas na Deep/Dark Web, marketplaces, entre outros;

2.94.10.2.2. Monitoramento do Pastebin, incluindo posts deletados e outros sites, buscando por referências sobre a empresa, domínios ou endereços IP;

2.94.10.2.3. Monitoramento de documentos vazados ou roubados da empresa em páginas da Deep/Dark Web e fóruns hackers;

2.94.10.2.4. Monitoramento de referências aos sistemas em páginas da Deep/Dark Web e fóruns hackers, além de Threat Intelligence e listas de IoC's;

2.94.10.2.5. Busca de informações sobre redes sociais e plataformas de divulgação de vulnerabilidades vazadas na Deep/Dark Web.

2.94.10.3. Deve ser possível encontrar marketplaces, fóruns e agentes de ameaças;

2.94.10.4. Deve ser capaz de realizar avaliação da exposição da marca e vazamentos de informações na Deep/Dark Web;

2.94.10.5. Investigação de origens de vazamentos de, no mínimo:

2.94.10.5.1. Grupos de hackers;

2.94.10.5.2. Ameaças em fóruns;

2.94.10.5.3. Salas de chats reservadas;

2.94.10.5.4. Carteira de bitcoins e endereços;

2.94.10.5.5. Registros históricos.

2.94.10.6. As investigações deverão ser realizadas por uma equipe especializada à medida que informações monitoradas forem identificadas na Deep/Dark Web.

2.94.10.7. Geração e notificação de alertas acompanhados da enumeração das ameaças e riscos relacionados e ações de mitigação sugeridas.

2.95. A solução como um todo, bem como os seus componentes devem contar com garantia e suporte integrais conforme especificado neste documento.

PAGAMENTO

2.96. A emissão do termo de recebimento provisório será feita após a instalação e configuração do console de gerência, dos coletores de logs, dos coletores de tráfego de rede e de agentes em estações de trabalho e em servidores.

2.97. As subscrições deverão ser fornecidas conforme a quantidade de ativos definida pela CONTRATANTE e deverão ser nomeadas (para cada CONTRATANTE). A comprovação do fornecimento se dará através da Nota Fiscal e o pagamento somente será autorizado depois de efetuado o "atesto" pelo servidor competente, condicionado este ato à verificação da conformidade da Nota Fiscal/Fatura apresentada em relação às subscrições efetivamente fornecidas em nome da CONTRATANTE, conforme volumetria mínima prevista.

2.98. A emissão do termo de recebimento definitivo será feita após a verificação do perfeito funcionamento do console de gerência, dos coletores de logs, dos coletores de tráfego de rede, de agentes em estações de trabalho, de agentes em servidores e da integração de todos os componentes.

2.99. A quantidade de agentes a serem considerados em cada tipo de ativo nos termos de recebimento provisório e definitivo deve ser acordada na fase de Planejamento e Projeto (item 4.4.1), não sendo superior a 10% do parque computacional da CONTRATANTE.

2.100. A distribuição dos agentes (no restante do parque computacional) para os outros ativos a serem monitorados será de responsabilidade da CONTRATANTE, sem prejuízo do suporte que a CONTRATADA deve fornecer para a realização dessa etapa.

2.101. O pagamento da subscrição deve ser anual, em parcela única, sendo realizado somente após a emissão do termo de recebimento definitivo.

3. ITEM 2 – Requisitos mínimos de treinamento na solução

3.1. A CONTRATADA deve oferecer treinamento contemplando a perfeita instalação, configuração, operação e utilização da solução contratada.

3.2. O treinamento deverá proporcionar aos participantes condições de:

3.2.1. Compreender a arquitetura da solução;

3.2.2. Identificar e configurar os recursos disponibilizados no produto;

3.2.3. Configurar fontes de eventos;

3.2.4. Instalar e configurar agentes, coletores e outros módulos necessários para o perfeito funcionamento da solução;

3.2.5. Configurar honeypots, quando a solução tiver essa capacidade;

3.2.6. Configurar serviço de Breach and Attack Simulation (item 2.32), quando a solução tiver essa capacidade;

3.2.7. Configurar regras;

3.2.8. Configurar alertas;

3.2.9. Configurar playbooks;

3.2.10. Investigar incidentes;

3.2.11. Pesquisar em logs;

3.2.12. Criar dashboards;

3.2.13. Criar relatórios e agendamento de relatórios;

3.2.14. Gerenciar usuários, funções e permissões;

3.2.15. Identificar as possíveis causas de problemas e atuar na sua resolução;

3.2.16. Monitorar o funcionamento da solução (analisar mensagens de log, efetuar acesso remoto, atualizar os componentes que fazem parte da solução, administração e utilização dos recursos disponibilizados);

3.2.17. Conhecer os procedimentos para abertura de chamados técnicos;

3.2.18. Conhecer os procedimentos para obtenção de atualizações de software.

3.3. Devem ser fornecidos todos os recursos necessários para a realização do treinamento (material didático, equipamentos, instrutor, etc.). Os treinamentos serão realizados nas dependências da CONTRATANTE ou na modalidade EAD, a critério da CONTRATANTE.

3.4. O treinamento deve ser ministrado por pessoa certificada na solução.

3.5. O treinamento deve ser o treinamento oficial do fabricante ou com material oficial do fabricante.

3.6. O material didático e demais documentações deverão ser fornecidos, preferencialmente, em Português (Brasil). Em caso de não disponibilidade dessa versão, a mesma deverá ser disponibilizada em Inglês.

3.7. A CONTRATADA deverá apresentar, juntamente à documentação técnica, a programação, conteúdo programático e carga horária do curso, a fim de serem ajustados às necessidades da CONTRATANTE.

3.8. O treinamento deverá ser ministrado com carga horária mínima de 40 (quarenta) horas, com fornecimento de certificados a todos os participantes, em papel timbrado da empresa, constando: nome do treinando, identificação do treinamento, carga horária, período de ocorrência e conteúdo programático.

3.9. A critério da CONTRATANTE, o treinamento poderá ser dividido em turmas de, no mínimo, 02 (dois) alunos e, no máximo, 08 (oito) alunos.

3.10. O treinamento deverá ser ministrado em horário definido pela CONTRATANTE, em dias úteis.

3.11. O cronograma do treinamento será definido em conjunto com a CONTRATANTE, na fase de Planejamento e Projeto (item 4.4.1).

PAGAMENTO

3.12. A emissão do termo de recebimento provisório do treinamento será feita após a conclusão do treinamento.

3.13. A emissão do termo de recebimento definitivo do treinamento será feita após a avaliação dos participantes, com o preenchimento da Planilha de Avaliação de Treinamento, devendo ser obtida média superior a 70%, caso contrário a CONTRATANTE poderá solicitar a realização de novo treinamento com a reformulação que achar necessária.

3.14. O pagamento do treinamento deve ser realizado em parcela única após a emissão do termo de recebimento definitivo.

4. ITEM 3 – Requisitos mínimos de implantação da solução

4.1. A fase de ativação dos serviços deverá ser conduzida e concluída 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).

4.1.1. A CONTRATADA deve realizar o planejamento, a implantação, configuração e ativação dos serviços e soluções propostas no prazo de até 45 (quarenta e cinco) dias corridos, contados a partir da assinatura do contrato, conforme objetivos, escopo, requisitos, premissas e demais condições elencadas nesta especificação.

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

4.3. Os papéis e responsabilidades das partes nos processos de gestão de segurança cibernética, bem como indicadores necessários para medir e melhorá-los continuamente, serão definidos também com base nos referidos parâmetros (baseline).

4.4. As atividades de implantação e ativação do contrato poderão ocorrer de forma remota e deverão contemplar, no mínimo, as seguintes fases:

4.4.1. Planejamento e Projeto:

4.4.1.1. Reunião de kick-off;

4.4.1.2. Coleta de dados e requisitos complementares;

4.4.1.3. Detalhamento de cronograma;

4.4.1.4. Apresentação de parâmetros (baseline) e adequação de processos de gestão de segurança cibernética.

4.4.2. Implantação, Configuração e Ativação da solução:

4.4.2.1. Instalação e ativação da solução on-line e console de gerência;

4.4.2.2. Instalação e ativação dos agentes, coletores, console de gerência e demais componentes da solução (pertinentes aos ativos monitorados) no ambiente computacional da CONTRATANTE: servidores, estações de trabalho, firewalls, servidores de diretório e cloud;

4.4.2.3. Instalação e ativação dos coletores de logs e dos coletores de tráfego de rede;

4.4.2.4. Configuração e o correto funcionamento da coleta, processamento e correlação de logs de eventos em que a solução possua conectores nativos, ou seja, que não necessitem de customização de parsers para tal funcionamento (os conectores nativos devem contemplar a coleta, processamento e correlação de logs para os ambientes que constam nos itens 2.17.1, 2.18.1 e 2.19.1);

4.4.2.5. Testes e homologação.

4.4.3. Definição de Processos e Outras Configurações:

4.4.3.1. Implementação dos processos e recursos propostos;

4.4.3.2. Desenvolvimento de playbooks de resposta a ataques cibernéticos;

4.4.3.3. Configuração e correto funcionamento da coleta, processamento e correlação de logs de eventos em que haja a necessidade de customização de parsers para tal funcionamento (item 2.17.2).

4.4.3.4. Testes e homologação;

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

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

4.4.3.5.2. Playbooks implementados.

4.4.4. Treinamento de equipes.

4.4.5. Operação, Sustentação e Melhoria Contínua:

4.4.5.1. Sustentação/On-Going;

4.4.5.2. Reunião mensal;

4.4.5.2.1. Relatórios periódicos;

4.4.5.2.2. Acompanhamento de indicadores;

4.4.5.2.3. Melhoria contínua.

4.5. A lista de soluções constantes nos itens 2.13, 2.17, 2.18 e 2.19 não é exaustiva, de forma que, conforme houver evolução do parque tecnológico ao longo do contrato, a CONTRATADA deve, como parte da operação, sustentação e melhoria contínua da solução (item 4.4.5), realizar a configuração para o correto

funcionamento de parsing (quando houver), coleta, processamento e correlação de logs de eventos gerados pela novas soluções incluídas/alteradas no ambiente computacional.

RESPONSABILIDADES DA CONTRATADA

4.6. São responsabilidades da CONTRATADA:

4.6.1. Prestar os serviços conforme previsto e delimitados por esta especificação, dentro das normas e especificações técnicas aplicáveis à espécie;

4.6.2. Respeitar as normas e regulamentos da CONTRATANTE, inclusive aqueles relativos ao acesso, permanência e trânsito de pessoas e materiais, no estabelecimento desta, as quais deverão lhe ser fornecidas previamente e por escrito;

4.6.3. Observar integralmente a legislação e normas infralegais aplicáveis aos serviços, inclusive aqueles referentes à segurança cibernética e medicina do trabalho;

4.6.4. Zelar pela disponibilidade da infraestrutura de TI da CONTRATADA durante a realização dos serviços propostos;

4.6.5. Realizar a manutenção de software e hardware de sua propriedade e utilizados para a prestação dos serviços propostos.

4.7. A implantação, configuração, ativação e atualização da solução será de responsabilidade da CONTRATADA, bem como as despesas diretas ou indiretas para a execução das atividades pela sua equipe técnica.

4.8. A instalação e atualização dos softwares nos ativos monitorados (item 1.1.1) poderá ser realizada remotamente, sem causar indisponibilidade do ambiente, devendo ser realizada em horários a serem definidos pela CONTRATANTE.

4.9. O processo de implantação, configuração, ativação e atualização da solução deverá ser realizado por técnicos capacitados da CONTRATADA, acompanhados por servidores da CONTRATANTE.

PAGAMENTO

4.10. A emissão do termo de recebimento provisório será feita após a conclusão da fase de Implantação, Configuração e Ativação da solução (item 4.4.2);

4.11. A emissão do termo de recebimento definitivo será feita após a conclusão da fase de Definição de Processos e Outras Configurações (item 4.4.3);

4.12. O pagamento do serviço de implantação deve ser realizado em parcela única após a emissão do termo de recebimento definitivo.

5. ITEM 4 – Requisitos mínimos do serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos

5.1. Os serviços deverão ser prestados por meio do Centro de Operações de Segurança Cibernética (SOC) da CONTRATADA, em regime 24x7x365, que deverá atender os seguintes requisitos mínimos:

5.1.1. A prestação dos serviços deverá ser feita a partir de Centro de Operações de Segurança Cibernética especializado, sendo remoto às instalações da CONTRATANTE.

5.1.2. A equipe do SOC poderá, a critério da CONTRATADA, ser compartilhada com outros clientes, incluindo outros Órgãos da Justiça do Trabalho, de modo a otimizar os esforços, respeitando a confidencialidade das informações relativas ao objeto deste edital.

5.1.3. A solução contratada deve ter instância própria para a CONTRATANTE, exclusiva e dedicada para cada Tribunal e sem compartilhamento com outros clientes da CONTRATADA.

5.1.4. A CONTRATADA deve indicar, formalmente, quando da assinatura do contrato, PREPOSTO TITULAR e substituto que tenham capacidade gerencial para tratar de todos os assuntos previstos no instrumento contratual e coordenação da equipe para a execução dos serviços contratados.

5.1.5. O PREPOSTO deve, entre outras atividades, promover os contatos com o gestor do contrato bem como deve prestar atendimento aos profissionais em serviço, tais como:

5.1.5.1. Assegurar de que as determinações da CONTRATANTE sejam disseminadas junto aos profissionais alocados com vistas à execução dos serviços contratados;

5.1.5.2. Informar ao gestor do contrato sobre problemas de qualquer natureza que possam impedir o bom andamento dos serviços contratados;

5.1.5.3. Desenvolver atividades administrativas de responsabilidade da CONTRATADA, principalmente quanto ao controle de informações relativas ao seu faturamento mensal e apresentação de documentos quando solicitado;

5.1.5.4. O PREPOSTO não pode ser contabilizado como profissional para execução dos serviços contratados.

5.2. A CONTRATADA deve possuir um "Computer Security Incident Response Team (CSIRT)", ou Grupo de Resposta a Incidentes de Segurança – grupo de pessoas com a responsabilidade de identificar, receber, analisar e investigar as notificações e atividades relacionadas a incidentes de segurança cibernética nos ativos monitorados e orientar a CONTRATANTE quanto ao que deve ser feito para resolver o incidente de segurança cibernética.

5.3. 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.

5.4. Um incidente de segurança é definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação da CONTRATANTE, levando à perda de um ou mais princípios básicos de segurança cibernética: confidencialidade, integridade, disponibilidade ou privacidade.

5.5. O processo de notificação de incidentes de segurança se inicia sempre que um evento adverso for submetido por qualquer ferramenta de segurança, podendo o corpo técnico de segurança desta CONTRATANTE a qualquer momento, abrir um incidente de segurança junto à CONTRATADA.

5.6. A CONTRATANTE deverá ser informada sobre os incidentes detectados através do Portal de Atendimento, e-mail e/ou por telefone, conforme previamente acordado com a CONTRATADA na fase de Planejamento e Projeto (item 4.4.1).

5.7. As solicitações de serviços e as notificações de incidentes de segurança cibernética reportadas pela solução proposta ou pela CONTRATANTE deverão ser registradas no módulo de gestão de incidentes de segurança da solução ofertada (item 2.5.4).

5.8. Todo tipo de comunicação e documentação relacionados aos tratamentos de incidentes devem ser em Português.

OPERAÇÃO E SUSTENTAÇÃO

5.9. Os serviços de operação e sustentação da solução contemplam todas as atividades de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos identificados pela solução ofertada, bem como a sustentação da mesma, mediante a sua operação por parte da CONTRATADA.

5.10. Os seguintes serviços deverão ser realizados pela equipe da CONTRATADA para a operação da solução proposta:

5.10.1. Ativação e configuração dos módulos contratados;

5.10.2. Integração dos componentes contratados com o ambiente da CONTRATANTE;

5.10.3. Gestão do ciclo de vida da solução, contemplando a sua implantação e operação, além da inclusão, alteração e exclusão de ativos monitorados;

5.10.4. Abrir e fazer a triagem de chamados de segurança cibernética;

5.10.5. Fazer primeiro atendimento de reportes de incidentes de segurança cibernética;

5.10.6. Atender incidentes simples, os quais possuem instruções indicadas em playbooks (knowledge Base do ITSM);

5.10.7. Elaborar consultas(queries)/scripts de rastreamento quando necessário e/ou solicitados pela CONTRATANTE;

5.10.8. Elaborar manual de usuário das atividades que se fizerem necessários e/ou solicitados pela CONTRATANTE;

5.10.9. IPs externos deverão ser analisados e contextualizados conforme sua criticidade;

5.10.10. Fazer passagem de turno, acompanhar os incidentes e realizar “follow-ups”, de modo que haja acompanhamento integral dos tickets abertos;

5.10.11. Prestar suporte/apoio ao processo de automação das atividades relacionadas à resposta e tratamento de incidentes cibernéticos;

5.10.12. Desenvolvimento de playbooks de resposta a ataques cibernéticos;

5.10.13. Configuração de fontes de eventos;

5.10.14. Configuração de usuários VIP e usuários de serviço;

5.10.15. Criação de alertas customizados;

5.10.16. Configuração de coletores de eventos;

5.10.17. Configuração de monitoramento de arquivos e diretórios;

5.10.18. Liberação de acesso à solução para usuários autorizados pela CONTRATANTE;

5.10.19. Geração de indicadores de performance (KPI) definidos neste documento e acordados na fase de Planejamento e Projeto (item 4.4.1);

5.10.20. Zelar e empregar todos os esforços necessários para garantir o atendimento ao SLA estabelecido neste termo de referência, tanto que se refere aos serviços quanto às soluções contratadas;

5.10.21. Atualização da solução, quando necessário/aplicável e/ou solicitados pela CONTRATANTE;

5.10.22. Resolução de chamados de suporte junto ao(s) fabricante(s) da solução.

5.11. A equipe da CONTRATADA deve ter, no mínimo, uma pessoa responsável pelos assuntos técnicos (líder técnico) e que será o ponto de contato com a equipe de segurança cibernética da CONTRATANTE. O líder técnico tem, entre outras responsabilidades:

5.11.1. Após a assinatura do contrato, conhecer o parque tecnológico e as atividades em andamento, visando à preparação da equipe que prestará os serviços, conhecer os modelos de serviços realizados, as normas internas, procedimentos de segurança e a definição dos requisitos necessários;

5.11.2. Fazer uma reunião semanal com a equipe da CONTRATANTE para acompanhamento dos resultados (a frequência da reunião poderá ser revista oportunamente, a critério da CONTRATANTE).

5.11.3. Fazer a entrega e apresentação dos relatórios mensais, conforme especificação técnica contida neste documento (item 5.17);

5.11.4. Esclarecer dúvidas em relação às requisições, alertas, incidentes, relatórios, prazos de atendimento e outras atividades de responsabilidade da equipe da CONTRATADA;

5.11.5. Estar disponível por telefone e e-mail, de segunda a sexta-feira, das 09 (nove) às 18 (dezoito) horas e acessível por contato telefônico em qualquer outro horário (incluindo sábados, domingos e feriados).

INTELIGÊNCIA DE AMEAÇAS

5.12. A equipe da CONTRATADA deve prover serviços de pesquisa e desenvolvimento de inteligência (threat intelligence) para proteção contra ataques cibernéticos, sendo responsável por:

5.12.1. Pesquisar novos tipos de ataques, vírus, malwares, botnets, vulnerabilidades e afins com intuito de melhoria contínua de detecção e mitigação destes males dentro dos serviços e ativos de segurança fornecidos pela CONTRATADA;

5.12.2. Criar, em colaboração com a equipe de segurança cibernética da CONTRATANTE, casos de uso (regras) que devem ser implementados na solução fornecida;

5.12.3. Revisar, sempre que necessário e/ou solicitados pela CONTRATANTE, as regras da solução fornecida, realizando as adaptações e evoluções necessárias;

5.12.4. Produzir e entregar informação de inteligência acionável, na forma de procedimentos para triagem de alertas e procedimentos para notificação de incidentes correspondentes às regras da solução ofertada;

5.13. A equipe da CONTRATADA deve fornecer serviço de Password e Credential Assessment (avaliação de credenciais em serviços de diretório e banco de dados):

5.13.1. A solução deve avaliar o nível de dificuldade de quebra de senhas.

5.13.2. A solução deve avaliar possíveis vazamentos de credenciais na Dark/Deep Web.

5.13.3. O serviço deve poder ser executado sob demanda.

5.13.4. O serviço deve ser executado sem que senhas sejam fornecidas.

MONITORAMENTO E DETECÇÃO DE AMEAÇAS E ATAQUES

5.14. A equipe da CONTRATADA deve atuar no monitoramento dos incidentes detectados pela solução e serviços propostos, sendo responsável por:

5.14.1. Monitorar equipamentos e softwares componentes das soluções de segurança da CONTRATANTE, envolvendo identificação, classificação e análise de eventos que possam comprometer a disponibilidade, integridade e confidencialidade dos serviços.

5.14.2. Focar suas ações nos eventos significativos, classificando-os corretamente conforme as categorias abaixo:

5.14.2.1. Informativos: são eventos que não requerem ação, utilizados para verificação de funcionalidades dos ativos monitorados, ou seja, tem por objetivo identificar se as ferramentas e soluções estão tendo o comportamento esperado. São úteis para gerar informações acerca do ambiente monitorado como, por exemplo, quantidade de eventos gerados nas últimas 24 horas.

5.14.2.2. Avisos: são eventos utilizados para classificar comportamentos anômalos comparados à linha de base de operação do ambiente, porém que ainda não gerou impacto ao ambiente da CONTRATANTE como, por exemplo, espera-se que ocorram 10 bloqueios de um determinado hash diariamente e, entretanto, nos últimos 2 dias ocorreram 100 bloqueios, sendo que a ferramenta de antivírus continua bloqueando sem que haja qualquer impacto ou degradação no ambiente.

5.14.2.3. Exceções: são eventos que podem indicar que houve impacto em um ou mais dos pilares da segurança da informação (confidencialidade, integridade e confidencialidade) como, por exemplo, a ferramenta de antivírus não bloqueou a ação de um ransomware e dados da CONTRATANTE foram criptografados. Caso um evento seja classificado como "Exceção", o processo de resposta a incidentes de segurança deve ser iniciado imediatamente.

5.14.3. Comunicar, à equipe de segurança cibernética da CONTRATANTE, as informações iniciais sobre o incidente de segurança e quais serão as linhas de atuação para sua resolução.

5.14.4. Informar à CONTRATANTE, através do Portal de Atendimento, e-mail e/ou por telefone, conforme previamente acordado com a CONTRATADA na fase de Planejamento e Projeto (item 4.4.1), sobre os incidentes detectados.

5.14.5. Emitir relatórios mensais, provendo, no mínimo, as seguintes informações à CONTRATANTE:

5.14.5.1. Alertas e notificações;

5.14.5.2. Quantidade de incidentes por categoria;

5.14.5.3. Quantidade de incidentes por criticidade (severidade);

5.14.5.4. Quantidade de incidentes que geraram crise;

5.14.5.5. Porcentagem dos incidentes originários do monitoramento;

5.14.5.6. Quantidade de incidentes tratados/fechados;

5.14.5.7. Quantidade de incidentes registrados.

5.14.6. Relativo ao monitoramento de Deep/Dark Web, a CONTRATADA deverá prover, no mínimo, os seguintes serviços:

5.14.6.1. Monitoramento e envio de notificações para a equipe técnica da CONTRATANTE contendo os alertas identificados no regime 24x7 (vinte e quatro horas por dia, sete dias por semana);

5.14.6.2. Serviço de investigação pela equipe técnica da CONTRATADA, contendo os alertas identificados e sugestões de mitigação, em regime 8x5 (oito horas por dia, cinco dias por semana);

5.14.6.3. Envio de um relatório ao fim do mês à CONTRATANTE contendo, no mínimo, as informações a seguir:

5.14.6.3.1. Vazamento de dados da CONTRATANTE que foram encontrados na Deep/Dark Web, através do monitoramento de domínios, IPs, e e-mails.

5.14.6.3.2. Descrição do ambiente avaliado;

5.14.6.3.3. Tabela resumo de serviços descobertos, detecções e alertas;

5.14.6.3.4. Descrição detalhada dos alertas;

5.14.6.3.5. Descrição, evidências, screenshots relevantes e recomendações para mitigação dos riscos;

5.14.6.3.6. Testes executados e relatórios técnicos das ferramentas;

5.14.6.3.7. Apresentação técnica dos resultados, incluindo o detalhamento dos eventos identificados.

RESPOSTA E INVESTIGAÇÃO A INCIDENTES CIBERNÉTICOS

5.15. A equipe da CONTRATADA deve atuar no processo de resposta a incidentes detectados pela solução proposta, sendo responsável por:

5.15.1. Analisar, recomendar ações de remediação e contenção e documentar os eventos de segurança que, após analisados, demonstraram ser um ataque ao ambiente da CONTRATANTE,

tendo sido categorizados como "Eventos de Exceção" e, portanto, acionado o processo de resposta a incidentes cibernéticos.

5.15.2. Analisar, após um incidente de segurança ser aberto, os logs e artefatos enviados/coletados a fim de, no primeiro instante, identificar as fontes geradoras de tais eventos.

5.15.3. Identificar, uma vez realizadas as análises iniciais do incidente, quais foram os principais vetores de ataque ao ambiente da CONTRATANTE.

5.15.4. Definir, junto à equipe de segurança cibernética da CONTRATANTE, a severidade do incidente de segurança, que será obtida por meio de uma matriz GUT (Gravidade, Urgência e Tendência).

5.15.4.1. A matriz GUT será definida na fase de Planejamento e Projeto (item 4.4.1) pela CONTRATADA em conjunto à equipe de segurança cibernética da CONTRATANTE.

5.15.5. Apoiar a equipe técnica da CONTRATANTE nos processos de mitigação, contenção de ataques e restauração do seu ambiente tecnológico.

5.15.6. Realizar, após análises iniciais do incidente e a definição de severidade, uma análise aprofundada do incidente baseando-se no comportamento do ataque e/ou artefato (malware).

5.15.7. Documentar todo o processo de análise e resultado no módulo de gestão de incidentes de segurança da solução ofertada (item 2.5.4) para que a equipe de segurança cibernética da CONTRATANTE acompanhe os passos para a solução do incidente de segurança.

5.15.8. Definir e documentar, uma vez identificado o comportamento e os principais vetores de ataque, uma estratégia para a mitigação e contenção do ataque em questão e notificá-la à CONTRATANTE.

5.15.8.1. Qualquer tipo de alteração no parque computacional da CONTRATANTE para contenção e mitigação de incidentes de severidade alta ou crítica, deverá ser executada pela própria CONTRATANTE com o suporte da CONTRATADA, que deverá sugerir a melhor maneira de implantar a estratégia definida por ela para a resposta ao ataque, até a efetiva resolução do incidente.

5.15.9. Iniciar, mitigado o incidente de segurança, o processo de compilação de todas e quaisquer evidências e identificação dos serviços afetados. Tais evidências serão utilizadas até a finalização do processo para execução de eventual análise forense do incidente de segurança.

5.15.9.1. A necessidade de análise forense será indicada pela CONTRATANTE, seguindo os seus processos internos de gestão de incidentes de segurança, a serem apresentados na fase de Planejamento e Projeto (item 4.4.1).

5.15.9.2. Os dados coletados devem ser reunidos durante o processo de tratamento de incidente para subsidiar futura e eventual análise forense, seguindo as etapas de preservação, extração, análise e laudo. Tal análise deve ser realizada com o objetivo de identificar pessoas, locais ou eventos, correlacionando todas as informações reunidas e gerando como produto final um laudo sobre o incidente de segurança em questão.

5.15.10. Reconstruir o ataque, caso seja necessário e/ou solicitado pela CONTRATANTE. Esta ação deve ser realizada pela CONTRATADA em ambiente controlado (como um sandbox), utilizando mecanismos de segurança para separar programas em execução, geralmente utilizado em um esforço para mitigar falhas de sistema ou vulnerabilidades de segurança cibernética.

5.15.11. Documentar, no módulo de gestão de incidentes de segurança da solução ofertada (item 2.5.4), as lições aprendidas do incidente de segurança em questão, formando, durante todo o período de vigência do contrato, uma grande base de conhecimento sobre ataques adversos.

5.15.11.1. A solução deve permitir a exportação da base de conhecimentos para formato Word ou PDF.

5.16. O regime de execução dos serviços deve ser 24x7x365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias ao ano).

PAGAMENTO

5.17. A emissão do termo de recebimento provisório será feita após a entrega e apresentação dos relatórios indicados nesta especificação:

5.17.1. Incidentes de segurança cibernética (item 5.14.5);

5.17.2. Deep/Dark Web (item 5.14.6.3);

5.17.3. Breach and Attack Simulation (item 2.32.5), quando a solução tiver essa capacidade;

5.17.4. SLA (itens 5.22.2 e 5.23.8).

5.18. A emissão do termo de recebimento definitivo será feita após a verificação dos serviços prestados e sua aderência às condições estabelecidas nesta especificação.

5.19. O pagamento do serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos deve ser mensal, sendo realizado somente após a emissão do termo de recebimento definitivo, descontadas eventuais glosas do período avaliado, conforme Fator de Desconto (FD) calculado no período (item 5.25 e subitens) e das multas aplicadas, quando houver.

CONFIDENCIALIDADE E DESCARTE DE INFORMAÇÕES

5.20. Confidencialidade:

5.20.1. A CONTRATADA deve ser responsável pelo ciclo de vida das informações coletadas pela solução proposta, atendendo aos critérios definidos pela CONTRATANTE, devendo processar, armazenar e, após o término da sua finalidade, descartar os dados de maneira segura.

5.20.1.1. A CONTRATADA obriga-se a tratar como “segredos comerciais e confidenciais” quaisquer informações, dados, processos, fórmulas, códigos, obtidos em consequência ou por necessidade desta contratação, utilizando-os apenas para as finalidades previstas no contrato, não podendo revelá-los ou facilitar a revelação a terceiros, mediante assinatura dos Termos de Confidencialidade conforme anexos A1 e A2;

5.20.2. Ao final do contrato, o descarte das informações deve ser realizado com o emprego de medidas que impossibilitem a sua reconstrução, de acordo com as necessidades do suporte físico ou digital.

GARANTIA E ACORDO DE NÍVEL DE SERVIÇO

5.21. Da garantia:

5.21.1. A solução como um todo, bem como os seus componentes devem contar com garantia e suporte integrais conforme especificado.

5.21.2. A solução deve contar com garantia integral do fabricante (Garantia Compreensiva) durante toda a vigência do contrato e deve comportar a garantia comumente utilizada pelo comércio e prevista no Código de Defesa do Consumidor acrescida de suporte técnico nos moldes desta especificação.

5.22. Um acordo de nível de serviço (SLA – Service Level Agreement) define os índices a serem atingidos para o cumprimento do conjunto de compromissos acordados entre CONTRATANTE e CONTRATADA.

5.22.1. Tais índices serão medidos e aplicados aos serviços contratados e prestados pela CONTRATADA.

5.22.2. Mensalmente, os dados de nível de serviço devem ser apresentados à CONTRATANTE, incluindo informações sobre ações e necessidades para a correção de desvios, visando atingir, manter e melhorar os níveis desejados.

5.22.3. A abrangência e o nível de detalhamento serão definidos conforme as necessidades identificadas pela CONTRATANTE, podendo sofrer alterações ao longo do tempo, as quais serão encaminhadas à CONTRATADA.

5.22.4. Para a medição dos índices de nível de serviços, serão considerados os seguintes conceitos:

5.22.4.1. Requisição: solicitação da CONTRATANTE para intervenção preventiva ou corretiva no ambiente gerenciado e nos ativos monitorados (item 1.1.1) e previsto no escopo desta proposta. Cada requisição será identificada unicamente por meio de um código e será classificada conforme seu nível de severidade no momento da sua comunicação à CONTRATADA;

5.22.4.2. Incidentes de segurança: conforme definido nos itens 5.3, 5.4 e 5.5.

5.22.4.3. Severidade: nível de prioridade/emergência atribuído ou solicitado para a realização de um atendimento a uma requisição da CONTRATANTE ou dos alertas gerados para o ambiente gerenciado, conforme critérios descritos a seguir. Solicitações de alteração do nível de severidade poderão ser submetidas à CONTRATADA e, em comum acordo, serão prontamente atendidas.

5.22.4.3.1. Severidade crítica: o serviço está totalmente parado ou inoperante;

5.22.4.3.2. Severidade alta: o serviço está ativo mas com inoperância da maioria de suas funcionalidades, causando um impacto negativo no ambiente de produção;

5.22.4.3.3. Severidade média: o serviço está operativo, mas suas funcionalidades são executadas com restrições;

5.22.4.3.4. Severidade baixa: o serviço está operativo e a falha não compromete suas funcionalidades ou questões não tratadas pela documentação;

5.22.4.3.5. Severidade agendado: o atendimento está relacionado apenas a esclarecimentos de dúvidas ou necessidade de informações;

5.22.4.4. Triagem: notificação, da CONTRATADA para a CONTRATANTE, de que está ciente da requisição ou do incidente, conforme itens 5.14.3 e 5.14.4.

5.22.4.5. Resolução: comunicação, da CONTRATADA para a CONTRATANTE, das ações INICIAIS (podendo incluir soluções paliativas enquanto a CONTRATADA busca a solução definitiva para o incidente ou chamado) a serem executadas para resolução da requisição ou do incidente de segurança, conforme item 5.15.8 e subitens.

5.22.4.5.1. A CONTRATADA deve fornecer, em até 48h, o restante das ações (contendo a resolução paliativa ou definitiva) a serem executadas para a resolução do incidente ou chamado.

5.22.4.5.2. Caso seja fornecida uma solução paliativa, a CONTRATADA deve atuar proativamente na busca de uma solução definitiva, fornecendo o acompanhamento e suporte necessários para a CONTRATANTE, inclusive sugerindo a melhor maneira de implantar a estratégia definida por ela para a resposta ao ataque, até a efetiva resolução do incidente ou chamado.

5.22.4.5.3. Devido à natureza dos incidentes de segurança cibernética, a sua efetiva contenção e remediação não contarão para contagem dos tempos de SLA, não eximindo a CONTRATADA de registrar esses tempos no módulo de gestão de incidentes de segurança da solução e ITSM integrado.

5.22.5. Os seguintes SLAs devem ser cumpridos:

Atividade	SLA de atendimento
Triagem da requisição/incidente de segurança[1]	Em até 30 (trinta) minutos
Requisição/Incidentes de severidade crítica	Atuação em até 15 (quinze) minutos e resolução[2] em até 01 (uma) hora.
Requisição/Incidentes de severidade alta	Atuação em até 01 (uma) hora e resolução em até 02 (duas) horas.
Requisição/Incidentes de severidade média	Atuação em até 02 (duas) horas e resolução em até 04 (quatro) horas.
Requisição/Incidentes de severidade baixa	Atuação em até 04 (quatro) horas e resolução em até 12 (doze) horas.
Requisição de severidade agendado	Atuação em até 12 (doze) horas e resolução em até 24 (vinte e quatro) horas.

SUPORTE TÉCNICO

5.23. Suporte Técnico:

5.23.1. A abertura de chamados pela CONTRATANTE deve poder ser efetuada:

5.23.1.1. Pela plataforma web, em sistema de atendimento da CONTRATADA;

5.23.1.2. Pelo envio de mensagem de correio eletrônico;

5.23.1.3. Por meio do módulo de gestão de incidentes de segurança da solução ofertada (item 2.5.4);

5.23.1.4. Por telefone.

5.23.2. O atendimento aos chamados deve estar disponível em regime 24x7x365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias ao ano), conforme SLA apresentado (item 5.22.5).

5.23.3. Todo tipo de comunicação e documentação relacionados aos atendimento de chamados devem ser em Português.

5.23.4. A assistência técnica em garantia deve assegurar o fornecimento de acesso irrestrito (24 horas por dia, 07 dias da semana) da CONTRATANTE à área de suporte do fabricante, especialmente ao endereço eletrônico (web site) e a toda a documentação técnica pertinente (guias de instalação e configuração atualizados, FAQ's, bases de conhecimento e bases de soluções, com pesquisa efetuada através de ferramentas de busca).

5.23.5. O suporte técnico do fabricante deverá ser prestado em caso de falhas, dúvidas e/ou esclarecimentos de qualquer um dos produtos, módulos e programas referentes às soluções de software e hardware (inclusive virtual) dos produtos.

5.23.6. Os serviços de suporte 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, entre outros.

5.23.7. A CONTRATADA deve fornecer, mensalmente, relatório oriundo da ferramenta de ITSM (conforme item 2.5.4.1) indicando os SLAs de cada chamado e incidente registrado na solução.

[1] Pode ser considerado como o Tempo Médio de Detecção (Mean Time To Detect - MTTD)

[2] Para as atividades de Requisição/Incidentes: pode ser considerado como o Tempo Médio de Resposta (Mean Time To Respond - MTTR)

5.23.8. Para a aferição e a avaliação dos níveis de serviço, a CONTRATADA deve fornecer, mensalmente, relatório gerencial de serviços, apresentando-o à CONTRATANTE até o quinto dia útil do mês subsequente ao da prestação do serviço, sendo que devem constar, entre outras informações, os indicadores/metas de níveis de serviço alcançados conforme item 5.22.5, recomendações técnicas, as solicitações de abonos com justificativa e demais informações relevantes para a gestão contratual, em conformidade aos acordos realizados na fase de Planejamento e Projeto (item 4.4.1).

PENALIDADES

5.24. A CONTRATADA está sujeita às seguintes penalidades, desde que não apresente justificativa fundamentada e aceita pela CONTRATANTE, isolada ou cumulativamente:

5.24.1. Advertência;

5.24.2. Multa de 1% (um por cento) do valor mensal contratado em casos de atraso, exceto para as ocorrências verificadas nos subitens, por dia, até o limite de 15 (quinze por cento). Ultrapassado esse limite, poderá ser caracterizada a inexecução total do objeto;

5.24.2.1. Multa de 0,5% (meio por cento) do valor mensal do contrato, quando a CONTRATADA entregar com atraso a documentação exigida nos itens 5.25.13.3 até 5.25.13.8, inclusive subitens, por dia de atraso;

5.24.2.2. Multa de 0,5% (meio por cento) do valor mensal do contrato, quando a CONTRATADA entregar de forma incompleta a documentação exigida nos itens 5.25.13.3 até 5.25.13.8, inclusive subitens, por dia de atraso, até que sejam entregues todos os documentos faltantes;

5.24.2.3. Multa de 0,5% (meio por cento) do valor mensal do contrato, quando a CONTRATADA entregar com atraso os esclarecimentos formais solicitados para sanar as inconsistências ou dúvidas suscitadas durante a análise da documentação exigida nos itens 5.25.13.3 até 5.25.13.8, inclusive subitens, por dia de atraso.

5.24.3. Multa de 0,1% (um décimo por cento) sobre o valor mensal do contrato, multiplicada pelo Fator de Impacto no Serviço (FIS) do indicador, para cada indicador de nível de serviço que apresente discrepância superior a 20% em relação à meta prevista, em determinado mês, limitado a 10% sobre o valor mensal do contrato, que poderá ensejar a inexecução parcial ou total do contrato;

5.24.4. Multa de 0,5% (cinco décimos por cento) sobre o valor mensal do contrato, multiplicada pelo Fator de Impacto no Serviço (FIS) do indicador, para cada indicador de nível de serviço que apresente discrepância superior a 10% em relação à meta prevista em 3 medições consecutivas, ou em 3 medições não consecutivas realizadas no intervalo de 6 meses, limitado a 20% sobre o valor mensal do contrato, que poderá ensejar a inexecução parcial ou total do contrato;

5.24.5. Multa de 5% (cinco por cento) sobre o valor mensal do contrato para cada ocorrência de descumprimento de obrigações contratuais que não sejam relacionadas ao atingimento das metas estabelecidas para os indicadores de nível de serviço;

5.24.6. Multa de 30% (trinta por cento) do valor contratado, em caso de inexecução total ou parcial do objeto, sem prejuízo da responsabilidade civil e criminal; e suspensão, pelo prazo de até 02 (dois) anos, do direito de licitar e contratar com a CONTRATANTE;

INDICADORES DE DESEMPENHO E GLOSAS

5.25. Glosa quando a CONTRATADA não produzir os resultados, ou não executar com a qualidade mínima exigida as atividades contratadas, conforme disposto nos indicadores de níveis de serviço.

5.25.1. Para fins de faturamento, o valor mensal da prestação do serviço será ponderado em função do desempenho mensal alcançado nele. Na medição, será apurado o afastamento dos

indicadores de nível de serviço em relação às metas estabelecidas em contrato, aplicando-se um Fator de Desconto (FD);

5.25.2. Nos casos em que o afastamento ensejar o desempenho abaixo da meta exigida, o valor do afastamento será utilizado para abater valores financeiros dos preços previstos em contrato;

5.25.3. Os Fatores de Desconto (FD) serão calculados com base nos resultados alcançados nos indicadores de nível de serviço, previstos nesta especificação técnica (item 5.25.11);

5.25.3.1. Haverá uma tolerância de 5% em relação à meta para a aplicabilidade do fator de desconto, ou seja, caso o índice mensurado ultrapasse a tolerância, o FD será calculado conforme o item 5.25.6.

5.25.4. No cálculo do FD está previsto uma ponderação para cada indicador de nível de serviço, denominada de Fator de Impacto no Serviço (FIS), com o objetivo de adequar os descontos ao grau de importância daquele indicador no contexto do serviço;

5.25.4.1. O FD de cada indicador será limitado à porcentagem representada pelo FIS aplicada ao valor mensal da prestação do serviço.

5.25.5. O FIS será utilizado nas situações em que a meta exigida para o indicador não for efetivamente atingida. Nos casos em que a meta exigida for atingida não haverá abatimento;

5.25.6. No valor mensal do serviço será abatido o FD calculado para cada resultado de indicador não alcançado:

$$FD_{indicador} = Valor\ Mensal \times \frac{FIS_{indicador}}{100} \times \frac{\left| Meta_{indicador} - Resultado_{indicador} \right|}{Meta_{indicador}}$$

$$FD_{total} = \sum_{i=1}^{max(indicadores)} FD_i$$

5.25.7. Não há previsão de bônus ou pagamentos adicionais para os casos em que a contratada superar as metas previstas, ou caso seja necessária a alocação de maior número de profissionais para o alcance das metas;

5.25.8. A superação de uma das metas não poderá ser utilizada para compensar o não atendimento de outras metas no mesmo período, nem o não atendimento da mesma meta em outro período;

5.25.9. Todos os indicadores que dependem de amostra para cálculo serão mensurados com método aleatório de escolha do espaço amostral definido pela CONTRATANTE e serão aferidos com nível de confiança de 90% e margem de erro de 5%.

5.25.10. A CONTRATANTE comunicará a CONTRATADA sobre o recebimento definitivo a fim de possibilitar a emissão da nota fiscal, informando os valores correspondentes às glosas.

5.25.11. Os seguintes Indicadores de Nível de Serviço serão considerados:

Item	Indicador de Nível de Serviço	Fórmula de Cálculo	Unidade de Medida	Meta exigida	Fator de Impacto no Serviço (FIS)
1	Tempo médio de triagem de requisições/incidentes	Somatório dos tempos de triagem de requisições e incidentes / Total	minutos	<= 30	10

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

		de requisições e incidentes			
2	Tempo médio de resolução de requisições/incidentes de severidade crítica	Somatório dos tempos de resolução de requisições e incidentes de severidade crítica / Total de requisições e incidentes	horas	<= 1	20
3	Tempo médio de resolução de requisições/incidentes de severidade alta	Somatório dos tempos de resolução de requisições e incidentes de severidade alta / Total de requisições e incidentes	horas	<=2	20
4	Tempo médio de resolução de requisições/incidentes de severidade média	Somatório dos tempos de resolução de requisições e incidentes de severidade média / Total de requisições e incidentes	horas	<= 4	15
5	Tempo médio de resolução de requisições/incidentes de severidade baixa	Somatório dos tempos de resolução de requisições e incidentes de severidade baixa / Total de requisições e incidentes	horas	<= 12	10
6	Tempo médio de resolução de requisições de severidade agendado	Somatório dos tempos de resolução de requisições e incidentes de severidade agendado / Total de requisições e incidentes	horas	<= 24	5
7	Índice de informações inconsistentes, incompletas ou com erros de procedimento, cuja responsabilidade seja da contratada, na documentação dos incidentes de segurança	Total de eventos da amostra registradas de modo inconsistente, incompleto ou com erros de procedimento na documentação dos incidentes de segurança / Tamanho da amostra x 100	%	<= 5%	10
8	Índice de informações inconsistentes, incompletas ou com erros de procedimento, cuja responsabilidade seja da contratada, na documentação das lições aprendidas nos incidentes de segurança	Total de eventos da amostra registradas de modo inconsistente, incompleto ou com erros de procedimento na documentação das lições aprendidas / Tamanho da amostra x 100	%	<= 5%	5
9	Índice de qualificação da equipe conforme itens 5.25.13.3, 5.25.13.4 e 5.25.13.5	Total de certificados da equipe / Quantidade de certificados exigidos, contabilizados depois de 90 dias do profissional entrar em operação	%	= 100%	5

QUALIFICAÇÃO TÉCNICA

5.25.12. Qualificação Técnica da CONTRATADA:

5.25.12.1. A CONTRATADA deve apresentar, no momento da sua habilitação no processo licitatório, Atestado(s) de Capacidade Técnica (ACT) em nome da licitante e emitido(s) por pessoa(s) jurídica(s) de direito público ou privado, onde comprove ter prestado ou estar prestando:

5.25.12.1.1. Fornecimento de solução de Monitoramento, Detecção, Notificação, Investigação e Resposta a Ataques Cibernéticos similar à proposta, em ambiente computacional contendo no mínimo 4.000 (quatro mil) ativos monitorados;

5.25.12.1.2. Fornecimento de serviço de Monitoramento, Detecção, Notificação, Investigação e Resposta a Ataques Cibernéticos, em regime 24x7x365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias ao ano), em ambiente computacional contendo no mínimo 4.000 (quatro mil) ativos monitorados;

5.25.12.2. Para cada subitem do item 5.25.12.1, serão considerados somatórios de atestados para atingir as quantidades solicitadas.

5.25.13. Qualificação Técnica do Quadro Profissional:

5.25.13.1. A CONTRATADA deve apresentar, no ato da assinatura do contrato, as certificações e documentos listados nos itens 5.20.7.3, 5.20.7.4 e 5.20.7.5 a fim de comprovar a qualificação técnica dos profissionais alocados para a prestação dos serviços.

5.25.13.1.1. A comprovação dos perfis exigidos para os profissionais se dará por meio de documentação das certificações (dentro do período de validade).

5.25.13.2. É de responsabilidade da CONTRATADA dimensionar a quantidade de profissionais para a adequada prestação dos serviços previstos e delimitados por esta especificação, principalmente no que se refere aos acordos de níveis de serviço (item 5.22.5) e metas estabelecidas.

5.25.13.3. Os profissionais da equipe técnica da CONTRATADA, responsáveis pela sustentação da solução, deverão ter certificação oficial do fabricante da solução proposta de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos (Item 01 da contratação).

5.25.13.3.1. O líder técnico (Item 5.11) deve, obrigatoriamente, ter a certificação oficial do fabricante da solução proposta de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos.

5.25.13.4. Os profissionais da equipe técnica da CONTRATADA, responsáveis pela detecção, notificação e investigação de ataques cibernéticos, deverão ter certificação em segurança ofensiva, detendo, individualmente ou em conjunto, pelo menos 03 (três) das seguintes certificações, contabilizando no máximo 02 (dois) certificados por profissional:

5.25.13.4.1. CompTIA PenTest+;

5.25.13.4.2. EC-Concil Licensed Penetration Tester (LPT);

5.25.13.4.3. IACRB Certified Expert Penetration Tester (CEPT);

5.25.13.4.4. GIAC Exploit Researcher and Advanced Penetration Tester (GXPN);

5.25.13.4.5. GIAC Reverse Engineering Malware (GREM);

5.25.13.4.6. Offensive Security Certified Professional (OSCP);

5.25.13.4.7. Ethical Hacking Post Exploitation (EHPX);

5.25.13.4.8. Offensive Security Experienced Penetration Tester (OSEP);

5.25.13.4.9. Offensive Security Web Expert (OSWE);

5.25.13.4.10. Certified Red Team Expert (CRTE);

5.25.13.4.11. Offensive Security Certified Expert (OSCE);

5.25.13.4.12. Certified Ethical Hacker (CEH).

5.25.13.5. Os profissionais da equipe técnica da CONTRATADA, responsáveis pela resposta a ataques cibernéticos, deverão ter certificação em segurança defensiva, detendo, individualmente ou em conjunto, pelo menos 03 (três) das seguintes certificações, contabilizando no máximo 02 (dois) certificado por profissional:

5.25.13.5.1. Certified Information Security Manager (CISM);

5.25.13.5.2. GIAC Experienced Cybersecurity Specialist (GX-CS);

5.25.13.5.3. GIAC Reverse Engineering Malware (GREM);

5.25.13.5.4. Ethical Hacking Post Exploitation (EHPX);

5.25.13.5.5. CompTIA Security+;

5.25.13.5.6. CompTIA Advanced Security Practitioner;

5.25.13.5.7. EC-Council Security Analyst (ECSA);

5.25.13.5.8. Certified Information Systems Security Professional (CISSP);

5.25.13.5.9. CompTIA CYSA+ - Cybersecurity Analyst.

5.25.13.6. Deverá ser comprovado vínculo entre os profissionais detentores dos certificados e a CONTRATADA, através de cópia do livro de registro de funcionários ou cópia da carteira de trabalho contendo as respectivas anotações de contrato de trabalho; ou como contratado, por meio de contrato de prestação de serviços.

5.25.13.7. A CONTRATADA deverá promover, no prazo máximo de 03 (três) meses, a atualização das certificações de seus profissionais caso haja atualização de versão ou migração para uma nova solução de TI devido a modernização do ambiente tecnológico do CONTRATANTE. Este prazo se iniciará a partir da comunicação formal do CONTRATANTE.

5.25.13.8. A CONTRATANTE se reserva ao direito de realizar auditorias a qualquer tempo para verificar se as competências mínimas solicitadas são atendidas pela CONTRATADA durante toda a vigência do contrato. Desta forma, quando solicitado, a CONTRATADA deverá apresentar os documentos comprobatórios da qualificação dos profissionais alocados na prestação dos serviços, além das certificações requeridas.

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

Anexo A-1 - Termo de Confidencialidade - Empresa CONTRATADA

TERMO DE CONFIDENCIALIDADE

CONTRATO <SIGLA DO TRIBUNAL> Nº ____/_____

A **<PESSOA JURÍDICA OU FÍSICA CONTRATADA>**, doravante referida simplesmente como CONTRATADA, inscrita no CNPJ/MF sob o número **<NÚMERO DO CNPJ>**, com endereço **<ENDEREÇO>**, neste ato representada pelo **<VÍNCULO DO SIGNATÁRIO COM A CONTRATADA>**, **<NOME DO SIGNATÁRIO>**, nos termos do **<CONTRATO OU TERMO ADITIVO EM QUE FOI PACTUADO O SIGILO>**, compromete-se a observar o presente TERMO DE CONFIDENCIALIDADE, firmado perante o <TRIBUNAL>, doravante referido simplesmente como CONTRATANTE, em conformidade com as cláusulas que seguem:

CLÁUSULA PRIMEIRA - DO OBJETO

O objeto deste TERMO DE CONFIDENCIALIDADE é a necessária e adequada proteção às informações confidenciais fornecidas à CONTRATADA para que possa desenvolver as atividades contempladas especificamente no Contrato nº ___/_____.

Subcláusula Primeira - As estipulações constantes neste TERMO DE CONFIDENCIALIDADE se aplicam a toda e qualquer informação revelada à CONTRATADA.

Subcláusula Segunda - A CONTRATADA reconhece que, em razão da prestação de serviços ao CONTRATANTE, tem acesso a informações que pertencem ao CONTRATANTE, que devem ser tratadas como sigilosas.

CLÁUSULA SEGUNDA - DAS INFORMAÇÕES CONFIDENCIAIS

Deve ser considerada confidencial toda e qualquer informação observada ou revelada, por qualquer meio, em decorrência da execução do contrato, contendo ela ou não a expressão “CONFIDENCIAL”.

Subcláusula Primeira - O termo “Informação” abrange toda informação, por qualquer modo apresentada ou observada, tangível ou intangível, podendo incluir, mas não se limitando a: diagramas de redes, fluxogramas, processos, projetos, ambiente físico e lógico, topologia de redes, configurações de equipamentos, senhas, fotografias, plantas, programas de computador, discos, disquetes, fitas, contratos, projetos, outras informações técnicas, jurídicas, financeiras ou comerciais, entre outras a que, diretamente ou através de seus empregados, prepostos ou prestadores de serviço, venha a CONTRATADA ter acesso durante ou em razão da execução do contrato celebrado.

Subcláusula Segunda - Em caso de dúvida acerca da natureza confidencial de determinada informação, a CONTRATADA deverá mantê-la sob sigilo até que seja autorizada expressamente pelo representante legal do CONTRATANTE, referido no Contrato, a tratá-la diferentemente. Em hipótese alguma, a ausência de manifestação expressa do CONTRATANTE poderá ser interpretada como liberação de qualquer dos compromissos ora assumidos.

CLÁUSULA TERCEIRA - DOS LIMITES DA CONFIDENCIALIDADE

As estipulações e obrigações constantes do presente instrumento não serão aplicadas a nenhuma informação que seja comprovadamente de conhecimento público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;

CLÁUSULA QUARTA - DAS OBRIGAÇÕES

A CONTRATADA se obriga a manter sigilo de toda e qualquer informação definida como confidencial neste TERMO DE CONFIDENCIALIDADE, utilizando-as exclusivamente para os propósitos do contrato.

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

Subcláusula Primeira - A CONTRATADA determinará a observância deste TERMO DE CONFIDENCIALIDADE, bem como a observância e a assinatura do TERMO DE CONFIDENCIALIDADE - COLABORADOR, a todos os seus empregados, prepostos e prestadores de serviço que estejam direta ou indiretamente envolvidos com a execução do contrato.

Subcláusula Segunda - A CONTRATADA obriga-se a informar imediatamente ao CONTRATANTE qualquer violação das regras de sigilo ora estabelecidas que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo, bem como de seus empregados, prepostos e prestadores de serviço.

Subcláusula Terceira - Compromete-se, ainda, a CONTRATADA a não revelar, reproduzir ou utilizar, bem como não permitir que seus empregados, prepostos ou prestadores de serviço revelem, reproduzam ou utilizem, em hipótese alguma, as informações referidas no presente TERMO DE CONFIDENCIALIDADE como confidenciais, ressalvadas situações previstas no contrato e neste TERMO DE CONFIDENCIALIDADE.

Subcláusula Quarta - A CONTRATADA deve cuidar para que as informações consideradas confidenciais nos termos do presente TERMO DE CONFIDENCIALIDADE fiquem restritas ao conhecimento dos empregados, prepostos ou prestadores de serviço que estejam diretamente envolvidos nas discussões, análises, reuniões e negócios, devendo cientificá-los da existência deste TERMO DE CONFIDENCIALIDADE e da natureza confidencial das informações.

CLÁUSULA QUINTA - DO RETORNO DAS INFORMAÇÕES

A CONTRATADA devolverá imediatamente ao CONTRATANTE, ao término do Contrato, todo e qualquer material de propriedade desta, inclusive registro de documentos de qualquer natureza que tenham sido criados, usados ou mantidos sob seu controle ou posse, bem como de seus empregados, prepostos ou prestadores de serviço, assumindo o compromisso de não utilizar qualquer informação considerada confidencial, nos termos do presente TERMO DE CONFIDENCIALIDADE, a que teve acesso em decorrência do vínculo contratual com o CONTRATANTE.

CLÁUSULA SEXTA - DO DESCUMPRIMENTO

O descumprimento de qualquer cláusula deste TERMO DE CONFIDENCIALIDADE acarretará as responsabilidades civil, criminal e administrativa, conforme previsto na legislação

CLÁUSULA SÉTIMA - DA VIGÊNCIA

Tendo em vista o princípio da boa-fé objetiva, permanece em vigor o dever de sigilo, tratado no presente TERMO DE CONFIDENCIALIDADE, após o término do Contrato.

CLÁUSULA OITAVA - DAS DISPOSIÇÕES FINAIS

Os casos omissos neste TERMO DE CONFIDENCIALIDADE, assim como as dúvidas surgidas em decorrência da sua execução, serão resolvidos pelo CONTRATANTE.

Por estarem de acordo, a CONTRATADA, por meio de seu representante, firma o presente TERMO DE CONFIDENCIALIDADE, lavrando em duas vias de igual teor e forma.

São Paulo, ____ de _____ de 20____.

<TRIBUNAL>

_____	_____
Nome:	Nome:
Cargo:	Cargo:

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

NOME DA EMPRESA FORNECEDORA

_____	_____
Nome:	Nome:
Cargo:	Cargo:

TESTEMUNHAS:

_____	_____
Nome:	Nome:
CPF/MF.:	CPF/MF.:

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

Anexo A-2 – Termo de Confidencialidade - Colaborador da CONTRATADA

TERMO DE CONFIDENCIALIDADE - COLABORADOR

A **<PESSOA FÍSICA OU JURÍDICA>**, doravante referida simplesmente como COLABORADOR, inscrita no CPF/CNPJ sob o número **<NÚMERO DO CPF/CNPJ>**, compromete-se a observar o presente TERMO DE CONFIDENCIALIDADE, em conformidade com as cláusulas que seguem:

CLÁUSULA PRIMEIRA - DO OBJETO

O objeto deste TERMO DE CONFIDENCIALIDADE é a necessária e adequada proteção às informações confidenciais fornecidas aos empregados, prepostos ou prestadores de serviço de empresas contratadas pelo <TRIBUNAL> (<SIGLA DO TRIBUNAL>), para que possam desenvolver suas atividades institucionais.

Subcláusula Primeira - As estipulações constantes neste TERMO DE CONFIDENCIALIDADE se aplicam a toda e qualquer informação.

Subcláusula Segunda – O COLABORADOR reconhece que tem acesso a informações que pertencem ao <SIGLA DO TRIBUNAL>, que devem ser tratadas como sigilosas.

CLÁUSULA SEGUNDA - DAS INFORMAÇÕES CONFIDENCIAIS

Deve ser considerada confidencial toda e qualquer informação observada ou revelada, por qualquer meio, contendo ela ou não a expressão “CONFIDENCIAL”.

Subcláusula Primeira - O termo “Informação” abrange toda informação, por qualquer modo apresentada ou observada, tangível ou intangível, podendo incluir, mas não se limitando a: diagramas de redes, fluxogramas, processos, projetos, ambiente físico e lógico, topologia de redes, configurações de equipamentos, senhas, fotografias, plantas, programas de computador, discos, pen drives, fitas, contratos, projetos, outras informações técnicas, jurídicas,

financeiras ou comerciais, entre outras a que venha o COLABORADOR ter acesso durante ou em razão da execução de suas atividades profissionais.

Subcláusula Segunda - Em caso de dúvida acerca da natureza confidencial de determinada informação, o COLABORADOR deverá mantê-la sob sigilo até que seja autorizada expressamente pelo representante legal do <SIGLA DO TRIBUNAL>, a tratá-la diferentemente. Em hipótese alguma, a ausência de manifestação expressa do <SIGLA DO TRIBUNAL>poderá ser interpretada como liberação de qualquer dos compromissos ora assumidos.

CLÁUSULA TERCEIRA - DOS LIMITES DA CONFIDENCIALIDADE

As estipulações e obrigações constantes do presente instrumento não serão aplicadas a nenhuma informação que:

I - sejam comprovadamente de conhecimento público no momento da revelação, exceto se tal fato decorrer de ato ou omissão do COLABORADOR;

II - já esteja em poder do COLABORADOR, como resultado de sua própria pesquisa, contanto que o COLABORADOR possa comprovar referido fato; ou

III - tenha sido comprovada e legitimamente recebida de terceiros, contanto que o COLABORADOR possa comprovar referido fato.

CLÁUSULA QUARTA - DAS OBRIGAÇÕES

O COLABORADOR se obriga a manter sigilo de toda e qualquer informação definida como confidencial neste TERMO DE CONFIDENCIALIDADE, utilizando-as exclusivamente no desempenho de suas atividades profissionais enquanto contratado.

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

Subcláusula Primeira - Compromete-se, ainda, o COLABORADOR a não revelar, reproduzir ou utilizar, em hipótese alguma, as informações referidas no presente TERMO DE CONFIDENCIALIDADE como confidenciais, ressalvadas situações previstas neste documento.

CLÁUSULA QUINTA - DO DESCUMPRIMENTO

O descumprimento de qualquer cláusula deste TERMO DE CONFIDENCIALIDADE acarretará as responsabilidades civil, criminal e administrativa, conforme previsto na legislação.

CLÁUSULA SEXTA - DA VIGÊNCIA

Tendo em vista o princípio da boa-fé objetiva, permanecem em vigor os deveres de sigilo e de não utilização das informações, tratados no presente TERMO DE CONFIDENCIALIDADE, após o término do vínculo contratual.

CLÁUSULA SÉTIMA - DAS DISPOSIÇÕES FINAIS

Os casos omissos neste TERMO DE CONFIDENCIALIDADE, assim como as dúvidas surgidas em decorrência da sua execução, serão resolvidos pelo <SIGLA DO TRIBUNAL>.

Por estar de acordo, o COLABORADOR firma o presente TERMO DE CONFIDENCIALIDADE, lavrando em duas vias de igual teor e forma.

São Paulo, ____ de _____ de 20____.

_____

Nome:

Cargo / Função:

Empresa:

Anexo B

Anexo B – Comprovação de atendimento aos itens da Especificação Técnica		
Item	**Especificação**	**Comprovação de atendimento ao item**
2	**ITEM 1 – Requisitos mínimos da solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos**	
2.3	A CONTRATADA deve prover, ao ambiente, soluções de segurança cibernética que permitam a visibilidade de logs, dados de telemetria, tráfego de rede e de informações correlatas, capazes de identificar eventos suspeitos ou incomuns que possam comprometer os serviços tecnológicos 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.	
2.5	A solução permitirá monitorar em regime 24x7 (vinte e quatro horas por dia, sete dias por semana) eventos de segurança cibernética, identificando incidentes relativos a ataques, violações de conformidade e comportamento suspeito nas aplicações, rede e ativos computacionais da CONTRATANTE, compreendendo:	
2.5.1	Analisar, classificar, categorizar, correlacionar e notificar os eventos e incidentes classificados como ameaças à segurança cibernética, ou que sejam considerados relevantes de acordo com diretrizes estabelecidas pela CONTRATANTE;	
2.5.4	Registrar os incidentes no módulo de gestão de incidentes da solução ofertada, cujo acesso deverá estar disponível para a CONTRATANTE.	
2.5.4.1	O módulo de gestão de incidentes deverá ser nativo da solução ofertada ou ser implementado por meio de ferramenta de ITSM (IT Service Management), complementar e integrado à solução ofertada. As funcionalidades do módulo ou da ferramenta devem conter os dados dos alertas, incidentes e chamados além de informações sobre SLA para acompanhamento do tratamento dos chamados.	
2.5.4.1.1	O módulo ou ferramenta deve ser capaz de, minimamente:	
2.5.4.1.1.1	Permitir a criação e acompanhamento de incidentes cibernéticos, de forma manual e automática, com no mínimo as seguintes características:	
2.5.4.1.1.1.1	Sumário do incidente, incluindo título, sumário, detalhes, e a fonte geradora do incidente. Também deverá incluir o status do incidente, incluindo data de criação, de modificação, de fechamento, tempo em que o chamado está aberto, número de alertas agregados e, opcionalmente, prioridade e analistas envolvidos;	
2.5.4.1.1.1.2	Classificação inicial da ameaça, incluindo categoria, origem (interna/externa), possibilidade de modificação manual da prioridade e justificativa, além de informações específicas para subsidiar o relatório de incidentes e possibilidade de inclusão de documentação adicional através da anexação de arquivos;	
2.5.4.1.1.1.3	Possibilidade de manter o histórico de atividades realizadas pelos analistas, tais como criação de registros, atualização de campos, etc;	
2.5.4.1.1.1.4	Permitir inserir comentários dos analistas no incidente, de tal forma a possibilitar o registro de todas as atividades de análise;	
2.5.4.1.1.1.5	Permitir inserir evidências coletadas de eventual análise forense de host e rede como um complemento da análise do incidente;	

Anexo B

2.5.4.1.1.1.6	Permitir registrar ações de remediação que incluam contenção, erradicação, educação de usuários e melhorias no programa do SOC;	
2.5.4.1.1.1.7	Permitir registrar os resultados de um Incidente incluindo sua confirmação, categoria de ataque, identificação de técnicas utilizadas, detalhes sobre o alvo dos ataques e eficácia dos controles de detecção, prevenção e investigação.	
2.5.4.1.1.2	Permitir o recebimento de alertas de segurança, de forma automática, com no mínimo as seguintes características:	
2.5.4.1.1.2.1	Nome do alerta, fonte geradora, prioridade, data de criação, data original do alerta, categoria, ação, tipo, nível de severidade, descrição, serviço afetado, e detalhes do alerta;	
2.5.4.1.1.2.2	Dados de origem e destino: IPs e portas; quando disponível, informações de contexto de negócio de cada dispositivo de origem e destino: domínios, endereços MAC, nomes dos dispositivos, tipos, unidades de negócio, geolocalização, índices de criticidade e conformidade e proprietários;	
2.5.4.1.1.2.3	Capacidade de incluir arquivos anexos, de acordo com a necessidade de aprofundamento de detalhes dos alertas.	
2.5.4.1.1.3	Gerar relatórios mensais do acordo de nível de serviço (SLA – Service Level Agreement) dos alertas, incidentes e chamados.	
2.5.4.1.2	O módulo ou ferramenta de ITSM deverá estar licenciado para a CONTRATANTE, devendo ser hospedado em regime SaaS (Software as a Service) pela CONTRATADA, bem como deve estar protegida por autenticação do tipo MFA - Multi-Factor Authentication e acesso criptografado ponto a ponto.	
2.6	A solução deve ser fornecida no modelo Software as a Service (SaaS) permitindo a instalação de múltiplos coletores e agentes on-premises e em nuvem, a fim de realizar a implantação distribuída da arquitetura.	
2.6.1	O fabricante da solução proposta para monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos deve ser atestado SOC 2 Type II;	
2.6.9	O console de gerência deve ser acessado via web, de forma segura (HTTPS) e deve possuir compatibilidade com, no mínimo, os seguintes navegadores:	
2.6.9.1	Google Chrome;	
2.6.9.2	Mozilla Firefox.	
2.6.10	O console de gerência deve estar disponível no ambiente do próprio fabricante, que é responsável pelas manutenções, atualizações e disponibilidade da solução.	
2.6.10.3	Os ambientes utilizados pela solução (incluindo do fabricante) devem possuir, ao menos, uma cópia das informações localizadas no Brasil.	
2.6.11	O console de gerência deve possuir a capacidade de autenticação multifator (MFA - Multi-Factor Authentication).	
2.7.1	A solução deve suportar picos de EPS (Eventos Por Segundo) ou GB (gigabytes) acima do licenciado em até 30%.	
2.7.1.1	Caso os picos de EPS ou GB ultrapassem o limite de 30%, a solução não deve descartar os eventos de forma que sejam processados posteriormente.	
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.	

Anexo B

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.	
2.9	A solução deve possuir capacidade de monitorar e identificar o comportamento de usuários que representar ameaça (UEBA - User and Entity Behavior Analytics), em nível de ativos monitorados ou em nível de logs de eventos, do Microsoft Active Directory e do Open LDAP, monitorando diferentes vetores de ataque, como:	
2.9.1	Movimentação lateral com uso de credenciais locais de máquina;	
2.9.2	Ataques de força bruta em contas locais de máquinas;	
2.9.3	Usuários locais que tentam apagar arquivos de evento dos registros da máquina.	
2.9.4	Adicionalmente, para ambientes com Microsoft Active Directory:	
2.9.4.1	Movimentação lateral com uso de credenciais de domínio;	
2.9.4.2	Ataques de força bruta em contas de domínio;	
2.9.4.3	Usuários de domínio que tentem apagar arquivos de evento dos registros da máquina;	
2.10	A solução deve permitir, para ambientes com Microsoft Active Directory, monitorar ações de todos os usuários, permitindo campanhas de caças a ameaças, auditoria e criação de alertas para usuários específicos.	
2.11	A solução deve monitorar qualquer tipo de acesso de usuário:	
2.11.1	Em máquinas com credenciais locais – monitoramento com uso de agente da própria solução ou de terceiros;	
2.11.2	Com credenciais do domínio – monitoramento do Microsoft Active Directory;	
2.11.3	Ingress Authentication – como VPN, Google Workspace/Google Apps e Office 365;	
2.11.3.1	Para autenticações vindas de fora do ambiente – Ingress Authentication – a solução deve identificar e correlacionar a informações da origem do acesso – minimamente data, hora e IP.	
2.12	A solução deve suportar IPv4 ou IPv4/IPv6.	
2.13	Para detectar incidentes, a solução deverá implementar o recebimento e análise de logs, dados de telemetria e/ou de rede de, no mínimo:	
2.13.1	Firewalls;	
2.13.2	Web Application Firewalls;	
2.13.3	IPS (Intrusion Prevention System) / IDS (Intrusion Detection System);	
2.13.4	Web filtering;	
2.13.5	Antivírus;	
2.13.6	Microsoft Active Directory;	
2.13.7	Open LDAP;	
2.13.8	IAM (Identity and Access Management) / PAM (Privileged Access Management);	
2.13.9	Servidores HTTP (HTTP Servers);	
2.13.10	Balanceadores de Carga (Load Balancers);	
2.13.11	DNS;	
2.13.12	DHCP;	
2.13.13	ELK Stack;	
2.13.14	Sistemas Operacionais.	
2.14	A solução que fizer uso de parsers para análise dos dados recebidos deve permitir a ingestão de fontes de eventos por meio de, no mínimo, o protocolo Syslog.	
2.14.1	A solução deve permitir a leitura de logs e arquivos nos formatos CSV, XML, JSON e texto puro, de forma a permitir a inclusão de outras fontes de evento que não tenham conectores nativos.	

Anexo B

2.14.2	A solução deve possuir módulo nativo (já incluso) para realização de parsers customizados.	
2.14.2.1	A solução deve permitir utilização de expressões regulares (regex) nos parsers.	
2.14.2.2	A solução deve prover identificação de eventos com erro de parsing e de eventos sem suporte de coleta.	
2.15	A solução deve ter funcionalidade de coleta de eventos de auditoria de bancos de dados por meio de conectores nativos, coleta de logs, dados de telemetria e/ou de rede.	
2.16	Para detectar incidentes, a solução também deverá suportar o recebimento e processamento de eventos de tráfego de rede e, opcionalmente, flow de rede, provendo as seguintes informações, no mínimo:	
2.16.1	Sistemas com maior atividade baseada em volume de tráfego;	
2.16.2	Principais aplicações e protocolos trafegados, baseado em volume de dados enviados e recebidos entre endpoints da rede;	
2.16.3	Atividades de rede baseada em porta de destino e endereços de origem e destino;	
2.16.4	Relação dos usuários ou ativos que mais consomem banda de rede, baseado em volume de tráfego.	
2.16.5	Servidores DNS em uso;	
2.16.6	Relação das principais aplicações em uso na rede;	
2.16.7	Identificação de picos de consumo de banda de acesso à rede;	
2.16.8	Relação de dispositivos, servidores e serviços que operam na rede.	
2.17	A solução deve implementar a coleta e análise de diferentes fontes de eventos. A coleta deve ser realizada para logs, dados de telemetria e/ou de rede, devendo ser possível coletar e analisar eventos das seguintes soluções presentes atualmente de forma predominante no ambiente da CONTRATANTE:	
2.17.1	De forma nativa (sem a necessidade de customização de parsers):	
2.17.1.1	Checkpoint para proteção de perímetro (Firewall);	
2.17.1.2	Fortinet FortiGate para proteção de perímetro (Firewall);	
2.17.1.3	Forcepoint para proteção de perímetro (Firewall);	
2.17.1.4	Microsoft Active Directory para serviços de diretório.	
2.17.2	De forma nativa (sem a necessidade de customização de parsers) ou não:	
2.17.2.1	Open LDAP para serviços de diretório;	
2.17.2.2	OpenVPN;	
2.17.2.3	Citrix;	
2.17.2.4	RDP e RDPWeb;	
2.17.2.5	Senha Segura para serviços de gerenciamento de acesso privilegiado;	
2.17.2.6	Cyberark para serviços de gerenciamento de acesso privilegiado	
2.17.2.7	Hashicorp Vault e Hashicorp Boundary para serviços de gerenciamento de acesso privilegiado;	
2.17.2.8	Keycloak para gerenciamento de identidade e acesso;	
2.17.2.9	midPoint para segurança de identidades (identity security);	
2.17.2.10	ForeScout CounterACT (eyeSight e eyeControl) para serviços de NAC (Network Access Control);	
2.17.2.11	Loqed;	
2.17.2.12	Varonis;	
2.17.2.13	IBM Spectrum Protect Plus para proteção de dados;	
2.17.2.14	Kaspersky para proteção de endpoint;	
2.17.2.15	Blackberry Cylance para proteção de endpoint.	

Anexo B

2.17.2.16	Check Point Harmony para proteção de endpoint;	
2.17.2.17	Tenable One para gerenciamento de exposição (exposure management platform);	
2.17.2.18	Tenable.ep / Nessus para gerenciamento de vulnerabilidades;	
2.17.2.19	Tenable.ad para proteção do Active Directory;	
2.17.2.20	Trivy para varredura de vulnerabilidades;	
2.17.2.21	VMware/vCenter para virtualização de máquinas;	
2.17.2.22	VMware/Horizon para virtualização de estações de trabalho;	
2.17.2.23	Hyper-V para virtualização de máquinas;	
2.17.2.24	Ovirt para virtualização de máquinas;	
2.17.2.25	Docker e Kubernetes;	
2.17.2.26	Apache HTTP Server;	
2.17.2.27	HAProxy;	
2.17.2.28	Ingress;	
2.17.2.29	Nginx;	
2.17.2.30	Switches Cisco MDS;	
2.17.2.31	Switches H3C;	
2.17.2.32	Switches HP;	
2.17.2.33	Switches Huawei;	
2.17.2.34	Roteadores Cisco;	
2.17.2.35	Roteadores Juniper;	
2.17.2.36	Roteadores MikroTik;	
2.17.2.37	Access Points Aruba;	
2.17.2.38	Access Points Ruckus;	
2.17.2.39	Controladoras Virtuais Aruba;	
2.17.2.40	Bacula para serviços de backup;	
2.17.2.41	Commvault (software de backup);	
2.17.2.42	Veeam (software de backup);	
2.17.2.43	Storage Huawei;	
2.17.2.44	Storage IBM;	
2.17.2.45	TSM Server IBM Spectrum Protect para serviços de backup;	
2.17.2.46	Dell EMC Data Domain;	
2.17.2.47	Dell EMC Isilon.	
2.18	A solução deve ser capaz de coletar e processar fontes de eventos oriundas dos seguintes serviços de Cloud:	
2.18.1	De forma nativa (sem a necessidade de customização de parsers):	
2.18.1.1	AWS CloudTrail, via SQS ou API;	
2.18.1.2	Google Cloud Platform, via API;	
2.18.1.3	Google Workspace/Google Apps, via API;	
2.18.1.4	Microsoft Office 365, via API.	

Anexo B

2.19	A solução deve suportar e implementar a coleta e o processamento de fontes de eventos oriundas, no mínimo, dos seguintes sistemas operacionais. Para as soluções que fazem uso de agentes ou outro software externo/nativo do sistema operacional, eles devem ser compatíveis com as versões 32 e 64 bits dos sistemas operacionais (quanto existirem). Caso a solução não faça uso de agentes, os dados devem ser obtidos por meio da coleta do tráfego de rede.	
2.19.1	De forma nativa (sem a necessidade de customização de parsers):	
2.19.1.1	Windows 7;	
2.19.1.2	Windows 8.1;	
2.19.1.3	Windows 10;	
2.19.1.4	Windows 11;	
2.19.1.5	Windows Server 2008 R2;	
2.19.1.6	Windows Server 2012;	
2.19.1.7	Windows Server 2012 R2;	
2.19.1.8	Windows Server 2016;	
2.19.1.9	Windows Server 2019;	
2.19.1.10	Windows Server 2022;	
2.19.1.11	Red Hat Enterprise Linux / Oracle Enterprise Linux / Rocky Linux 8.4;	
2.19.1.12	Red Hat Enterprise Linux / Oracle Enterprise Linux / Rocky Linux 8.5;	
2.19.1.13	Red Hat Enterprise Linux / Oracle Enterprise Linux / Rocky Linux 9.0;	
2.19.1.14	Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 7;	
2.19.1.15	Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 8.0;	
2.19.1.16	Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 8.1;	
2.19.1.17	Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 8.2;	
2.19.1.18	Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 8.3;	
2.19.1.19	Amazon Linux;	
2.19.1.20	Debian Linux;	
2.19.1.21	Ubuntu Linux.	
2.20	Para os itens 2.13, 2.17, 2.18 e 2.19, as listas de soluções são do tipo "não exaustivas", devendo ser considerada pela CONTRATADA, por meio de configuração da solução, a possibilidade de inclusão ou alteração de produtos em decorrência da evolução do parque tecnológico da CONTRATANTE.	
2.21	A solução deve ser capaz de detectar comportamentos caracterizados como maliciosos de acordo com o MITRE ATT&CK Framework levando-se em consideração os dados recebidos dos ativos monitorados e gerados pelo coletor de tráfego de rede.	
2.22	A solução deve cobrir detecções nativas de, ao menos, os grupos de atacantes categorizados pelo MITRE ATT&CK.	
2.23	A solução deverá informar com qual técnica e tática do MITRE ATT&CK Framework o ataque está relacionado, além de possuir link direto para o site da organização.	
2.24	A solução deve possuir de maneira nativa detecções de, no mínimo, os seguintes vetores de ataque:	
2.24.1	Requisição a domínio suspeito;	
2.24.2	Execução de processos suspeitos;	
2.24.3	Requisição de dados de registro do sistema de nome de domínio (DNS);	
2.24.4	Comunicação com servidores Command & Control;	
2.24.5	Tentativa de desabilitar recursos de Sysmon;	

Anexo B

2.24.6	Execução de processos LSASS (Local Security Authority Subsystem Service) com objetivo de detectar dump de memória para acessar possíveis credenciais armazenadas;	
2.24.7	Detecção do uso de msrsc.exe - Microsoft Terminal Services Client;	
2.24.8	Detecção do uso de comandos estruturados consistentes pela ferramenta Impacket e Impacket-Obfuscation;	
2.24.9	Detecção de atividade de linha de comando da execução da função GetSystem, usada pelo Meterpreter ou Cobalt Strike;	
2.24.10	Detecção de execução do Mimikatz e variações;	
2.24.11	Detecção de processos que utilizam resultados do comando wget via Bash, Perl e Python;	
2.24.12	Detecção de tentativas de criação de reverse shells para Command & Control.	
2.25	A solução deve possuir a capacidade de identificar e monitorar o comportamento de atacantes baseados em IoC's (Indicators of Compromise) do próprio fabricante e de terceiros (threat intelligence).	
2.26	A solução deve possuir listas de terceiros com informações de IoC's com, no mínimo, IPs, domínios, URLs e hashes da família SHA e, opcionalmente, MD5.	
2.27	A solução deve possuir a capacidade de integração e/ou ingestão de dados de outras ferramentas de threat intelligence, de maneira manual ou por API, importando arquivos com base CSV ou STIX (Structured Threat Information Expression), através de assinatura de feeds de inteligência de ameaças de terceiros, aceitando, no mínimo, os seguintes tipos: IPs, domínios, URLs e hashes da família SHA e, opcionalmente, MD5.	
2.28	A solução deve disponibilizar informações a respeito dos principais ataques que estão ocorrendo no mundo, quais plataformas e países são afetados, além de links para obter mais informações.	
2.29	A solução deve permitir o enriquecimento de dados relacionados a endereços IPs, buscando informações adicionais em fontes de OSINT (Open Source Intelligence).	
2.30	A solução deve prover relatórios de inteligência de ameaças avançadas mais recentes e indicadores de comprometimento para ajudar na defesa proativa contra ameaças.	
2.30.1	A solução deve integrar relatórios de inteligência criados por especialistas em ameaças do fabricante e de terceiros para ajudar na identificação de ameaças.	
2.30.2	Após análise dos relatórios de ameaças pela CONTRATADA, deverá ser feita uma investigação dentro do ambiente computacional da CONTRATANTE e registrado um incidente caso sejam identificadas atividades presentes nos relatórios.	
2.30.3	Cada relatório deve possuir, no mínimo, informações como: região/país alvo, plataforma alvo e campanhas de ataques relacionadas aos dados do relatório.	
2.31	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.	
2.31.1	Honeypot: máquina projetada para capturar informações sobre tentativas de acesso e exploração. Deve permitir a instalação de, ao menos, 05 (cinco) máquinas no ambiente;	
2.31.1.1	Os honeypots devem ser fornecidos em formato OVA – virtual appliance.	
2.31.2	Honey Credential: configuração de um conjunto de credenciais falsas na memória de um ativo;	
2.31.3	Honey User: usuário falso que não está associado a uma pessoa real dentro da organização e, portanto, nunca deve ser acessado – monitoramento do Microsoft Active Directory;	
2.31.4	Honey File: arquivo falso localizado em um compartilhamento de arquivos de rede.	
2.31.5	A solução deve ser capaz de detectar o vetor de entrada da ameaça na rede, identificar o caminho utilizado pelo invasor até o ativo, credencial, usuário ou arquivo específico e apresentar as vulnerabilidades exploradas no ativo (quando for o caso).	

Anexo B

2.32	Quando a solução não possuir capacidade de “deception”, a capacidade de “Breach and Attack Simulation” (BAS) pode ser apresentada, com os seguintes critérios mínimos:	
2.32.1	Caso a funcionalidade seja oferecida como um serviço, as licenças necessárias para a sua execução devem ser baseadas em vetores ou agentes, sendo um para cada tipologia: infraestrutura, network e e-mail; os 03 (três) tipos de licenças devem estar incluídas sem custos adicionais para a CONTRATANTE;	
2.32.3	Deve ser executado de forma automatizada, simulando ataques reais, mas que não coloquem em risco o ambiente computacional da CONTRATANTE;	
2.32.4	As simulações devem utilizar diferentes vetores de ataque;	
2.32.5	O serviço deve gerar um relatório mensal que indique como corrigir os problemas que venham a ser encontrados.	
2.33	A solução que fizer uso de agentes deve permitir sua instalação de forma “silenciosa” nos ativos a serem monitorados.	
2.34	A solução deve possuir as funcionalidades de:	
2.34.1	Monitoramento de comportamento (behavior monitor);	
2.34.2	Controle de aplicação;	
2.34.3	Monitoramento de eventos;	
2.34.4	Auditoria de alterações no sistema;	
2.34.5	Resposta automatizada a ameaças com a possibilidade de, mas não se limitando a, executar as ações propostas no item 2.62.	
2.35	A solução deve monitorar os ativos em tempo real, estando eles dentro ou fora do domínio.	
2.36	Os agentes devem poder coexistir com outras soluções de proteção, como antivírus, instaladas nos ativos monitorados sem que gerem conflito nem incompatibilidade entre os softwares.	
2.37	Os agentes devem executar de maneira que não haja impacto na performance ou disponibilidade dos ativos monitorados.	
2.38	Os agentes e os coletores devem, em caso de desconexão com o console, manter as informações sendo coletadas a fim de serem enviadas quando a conexão for restabelecida.	
2.39	Os agentes e coletores devem enviar os dados para o console de maneira:	
2.39.1	Segura e criptografada;	
2.39.2	Que não haja impacto na performance ou disponibilidade da rede da CONTRATANTE.	
2.40	Os agentes e coletores, ao enviarem os dados para o console, não devem degradar o tráfego de saída da rede da CONTRATANTE.	
2.41	A solução deve monitorar, no mínimo:	
2.41.1	Força bruta no ativo (brute force – asset);	
2.41.2	Força bruta em conta local (brute force – local account);	
2.41.3	Detecção de evasão - Deleção de log de evento (detection evasion – event log deletion);	
2.41.4	Detecção de evasão - Deleção de log de evento local (detection evasion – local event log deletion);	
2.41.5	Correspondência de Threat Intel (endpoint threat intelligence match);	
2.41.6	Exploração mitigada (exploit mitigated);	
2.41.7	Hash sinalizado no ativo (flagged hash on asset) - a solução deve permitir cadastrar um hash qualquer para gerar um alerta quando for acessado no ativo;	
2.41.8	Processo sinalizado no ativo (flagged process on asset);	
2.41.9	Exploração de elevação de privilégio Kerberos (kerberos privilege elevation exploit);	

Anexo B

2.41.10	Movimentação lateral com personificação de administrador local (lateral movement – local administrator impersonation);	
2.41.11	Movimentação lateral com credenciais locais (lateral movement – local credentials);	
2.41.12	Tentativa de escalação de privilégio em honey credential local (local honey credential privilege escalation attempt);	
2.41.13	Hash malicioso no ativo (malicious hash on asset) - a solução deve gerar um alerta quando um hash já conhecido como malicioso é acessado no ativo;	
2.41.14	Criação de nova conta de usuário local (new local user account created);	
2.42	A solução deve ser capaz de fornecer uma listagem dos ativos sendo monitorados.	
2.43	A solução deve ser capaz de fornecer uma listagem dos ativos que estejam se comunicando no ambiente computacional da CONTRATANTE e que não estejam sendo monitorados.	
2.44	A solução deve ser capaz de identificar acessos a URLs maliciosas além das portas padrão 80 e 443.	
2.44.1	A solução deverá permitir classificar alertas relacionados a URLs em exceção para redução de falsos-positivos.	
2.45	A solução deve correlacionar logs e/ou dados de telemetria/de rede dos ativos monitorados para:	
2.45.1	Identificar comportamentos anômalos que aconteçam localmente no ativo monitorado;	
2.45.2	Identificar quais eventos devem gerar alertas;	
2.45.3	A solução deverá permitir classificar alertas relacionados a usuários e ativos em exceção para redução de falsos-positivos.	
2.46	O console de correlacionamento deve estar disponível no ambiente do próprio fabricante, que é responsável pelas manutenções, atualizações e disponibilidade da solução.	
2.47	A solução deve fazer uso de inteligência de ameaças do fabricante para analisar e correlacionar os dados recebidos.	
2.48	A solução deve detectar ameaças conhecidas usando casos de uso de detecção constantemente atualizados, e desconhecidas por meio de conjuntos de dados aprendidos.	
2.49	A solução deve prover funcionalidade de detecção de padrões em eventos coletados:	
2.49.1	A solução deve prover detecção de padrões de ataque em todas as suas fases, com base no modelo Cyber Kill Chain, MITRE ou NIST;	
2.50	A solução deve permitir a criação de alertas customizados baseados em um comportamento específico ou em um contexto de combinação de eventos.	
2.51	Os modelos de detecção deverão possuir níveis de severidade (score) individuais para cada modelo em pelo menos os seguintes níveis:	
2.51.1	Crítico;	
2.51.2	Alto;	
2.51.3	Médio;	
2.51.4	Baixo.	
2.52	A solução deve consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento.	
2.53	A solução deve informar qual o escopo de impacto ou dimensionar o impacto em servidores, estações de trabalho e usuários, indicando a quantidade de componentes afetados no ataque.	
2.54	A solução deve permitir a visualização da correlação entre usuários, servidores, processos/comandos, arquivos e demais componentes correlacionados em determinado ataque.	

Anexo B

2.55	A solução deve permitir o encerramento remoto de processos ativos executados nas estações de trabalho e servidores sob sua gestão.	
2.56	A solução deve ser capaz de isolar uma estação de trabalho, desconectando-a da rede e permitindo se comunicar exclusivamente com a central da solução.	
2.56.1	A solução deve ser capaz de restaurar a conectividade da estação de trabalho com a rede.	
2.57	A solução deve ser capaz de realizar as ações dos itens 2.55. e 2.56. sem a necessidade de fornecimento de credenciais de usuário administrativo, o que não significa que o agente (caso a solução faça uso) não possa ser instalado com direitos administrativos.	
2.58	A solução deve possuir a capacidade de monitorar a integridade de arquivos (FIM – File Integrity Monitoring) nos servidores monitorados.	
2.58.1	Nativamente, para os seguintes formatos de arquivos, no mínimo:	
2.58.1.1	.bat	
2.58.1.2	.cfg	
2.58.1.3	.conf	
2.58.1.4	.config	
2.58.1.5	.dll	
2.58.1.6	.exe	
2.58.1.7	.ini	
2.58.1.8	.sys	
2.58.2	A solução deve permitir a inclusão de novos formatos de arquivos diferentes dos nativos.	
2.59	Para realizar o monitoramento do tráfego de rede, a solução deve ser do tipo passiva e ser instalada em modo off-line na rede, ou seja, não ser um ativo em linha ou permitir o envio de logs e/ou dados de telemetria/de rede através de integração.	
2.60	A solução deve ser capaz de inspecionar o tráfego de rede baseado no volume de tráfego em Gbps da CONTRATANTE e realizar a análise dos dados coletados.	
2.61	A solução deve, junto com o monitoramento do tráfego de rede (ou por meio de agentes), implementar regras de detecção de intrusão para correlacionar e trazer as informações sobre possíveis anomalias e ataques no nível de rede.	
2.61.1	A solução deve permitir a criação de regras e/ou fornecer um conjunto de regras pré-definidas.	
2.61.1.1	No caso da solução possuir regras pré-definidas, deve haver sua atualização periódica cobrindo as informações de novas ameaças.	
2.62	A solução deve possuir funcionalidade de automação na resposta de incidentes com playbooks de resposta já funcionais, devendo suportar, no mínimo, a automação das seguintes tarefas:	
2.62.1	Envio de e-mails.	
2.62.2	Com a utilização de agentes (não deve haver a necessidade de fornecimento de credenciais de usuário administrativo, o que não significa que o agente não possa ser instalado com direitos administrativos) ou outro mecanismo que a solução utilize para a automação:	
2.62.2.1	Isolamento de uma máquina – caso seja detectado uma ameaça ou comportamento anômalo em uma máquina, deve ser possível isolá-la da rede;	
2.62.2.2	Encerrar um processo malicioso – caso o agente detecte algum processo malicioso na máquina, a solução deve ter a capacidade de finalizar esse processo;	
2.62.3	Com integrações para as soluções nativas indicadas no item 2.17.1:	
2.62.3.1	Alertas relacionados a usuários do Microsoft Active Directory – se um alerta for gerado associado a uma credencial de domínio, a solução deve desabilitar o usuário para conter a ameaça de maneira rápida;	

Anexo B

2.62.3.2	Sugerir e/ou criar regras no firewall – se um alerta for gerado associado a uma consulta DNS a um domínio considerado malicioso, a solução deve possibilitar a criação de regras de bloqueio no firewall ou sugerir qual regra deve ser criada para tal.	
2.62.4	A solução deve permitir que cada tarefa nos playbooks de resposta de incidentes possa ser configurada de forma a:	
2.62.4.1	Ser totalmente automática;	
2.62.4.2	Aguardar uma interação humana para ser realizada.	
2.63	Em casos de identificação de uma ameaça, a solução deve ter a capacidade de bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do sistema operacional ou demais aplicações instaladas no ativo.	
2.64	A solução deve conter regras pré-definidas para detecção de ransomware e as principais famílias deste tipo de malware.	
2.65	A solução deve possuir módulo de investigação e detecção integrados.	
2.66	A solução deve apresentar os alertas de ameaças consolidados e correlacionados para melhor investigação e resposta aos incidentes.	
2.67	A solução deve permitir configuração de notificações por e-mail (SMTP) e Webhooks (do Google Workspaces, no mínimo) para envio de alertas e notificações.	
2.67.1	As notificações podem ser nativas ou, caso necessário, serem desenvolvidas pela CONTRATADA, sem custo para a CONTRATANTE, para viabilizar sua integração.	
2.68	A solução deve permitir que as detecções sejam correlacionadas com dados recebidos dos ativos monitorados.	
2.69	A solução deve, através dos dados do alerta, permitir a criação de um incidente e vinculá-lo ao alerta, possibilitando a definição da gravidade do incidente com dados de gravidade da fonte do alerta.	
2.70	A solução deve permitir visualizar uma lista de incidentes e suas descrições, solicitar enriquecimentos e executar ações sobre os incidentes.	
2.71	A solução deve criar uma linha do tempo (timeline) do ataque detectado, incluindo as evidências sobre cada alerta gerado e informando qual ativo gerou aquela evidência.	
2.71.1	A solução deve prover visualização em linha do tempo com informações dos eventos monitorados em cada estação de trabalho.	
2.72	A solução deve ser capaz de classificar a relevância dos eventos, minimamente, em “crítico”, “alto”, “médio” e “baixo”.	
2.73	A solução deve permitir a alteração do status dos incidentes de acordo com seu tratamento e indicar falsos positivos para a plataforma.	
2.74	A solução deve permitir visualizar as atividades suspeitas de forma a sinalizar a causa raiz, seguindo as categorias do MITRE ATT&CK.	
2.75	A solução deve permitir investigar os alertas gerados pelos modelos de detecção por meio de análise de impacto e análise de causa raiz.	
2.75.1	Deve ser possível ativar ou desativar qualquer modelo de detecção.	
2.75.2	A solução deverá possuir todos os módulos de detecção completamente licenciados, sem custo para a CONTRATANTE, independentemente da quantidade de modelos de detecção que venham a ser disponibilizados futuramente.	
2.76	A solução deve permitir a criação de listas de exceção de objetos para redução de falsos-positivos.	
2.77	A solução deve adicionar os logs, dados de telemetria e/ou de rede coletados/correlacionados aos incidentes/alertas detectados.	
2.78	A solução deve permitir o registro de incidentes por demanda, sem a necessidade de a própria solução ter gerado um alerta.	
2.79	A solução deve possibilitar que, para cada incidente gerado, um analista seja vinculado ao incidente e que ele possa criar anotações sobre como está a evolução da resposta deste incidente;	

Anexo B

2.80	A solução deve permitir que incidentes possam ser fechados após atividades serem encerradas, permitir marcação como falsos positivos e, também, que possam ser reabertos.	
2.81	A solução deve exibir os eventos de forma a priorizar os alertas mais críticos para que o analista realize a investigação, indicando criticidade e níveis de prioridade.	
2.81.1	A classificação quanto ao nível de criticidade deve ser baseada nas regras do MITRE.	
2.82	A solução deve ter a capacidade de realizar buscas avançadas para localizar dados ou objetos no ambiente para análise avançada de atividades ou detecções.	
2.83	A solução deve permitir realizar buscas e filtros de objetos para possibilitar pesquisas e análises avançadas.	
2.84	A solução deve possibilitar a interação com cada um dos objetos relacionados ao evento para análise avançada e resposta.	
2.84.1	Ao clicar em quaisquer dos objetos, a solução deve permitir a realização de buscas específicas pelo objeto ou ainda executar ações como executar investigações mais aprofundadas.	
2.85	A solução deve prover diferentes métodos de pesquisa, filtros e uma linguagem de consulta para identificar, categorizar e recuperar os resultados da pesquisa.	
2.86	A solução deve permitir a realização de buscas através de strings parciais, exatas, valores nulos, coringas (wildcards) e caracteres especiais.	
2.87	A solução deve permitir salvar pesquisas com os critérios de busca e operadores lógicos utilizados para futuras consultas.	
2.88	A solução deve permitir a criação de dashboards e relatórios baseados em bibliotecas prontas ou, também, criar do zero.	
2.88.1	Deve possuir dashboards pré-configurados e permitir sua customização ou mesmo a criação de novos para refletir necessidades específicas da CONTRATANTE.	
2.88.2	Deve fornecer a possibilidade de criação de relatórios e dashboards para dados de todas as fontes de dados ingeridas (endpoints, rede, e-mail, nuvem, etc.), seja por meio de criação de consultas (queries) ou a partir de cliques com o mouse.	
2.88.3	Deve possuir dashboards pré-configurados que permitam a visualização executiva dos principais incidentes e atividades no ambiente com base em usuários, aplicações acessadas e estações de trabalho/servidores.	
2.88.4	Deve possuir, ao menos, 15 (quinze) dashboards em sua biblioteca, incluindo dashboards de fácil visualização de:	
2.88.4.1	Alertas e incidentes mais frequentes;	
2.88.4.2	Nível de risco do ambiente;	
2.88.4.3	Relatório dos últimos 30 (trinta) dias da detecção de incidentes;	
2.88.4.4	Top 10 (dez) ativos com incidentes;	
2.88.4.5	Os ativos que mais sofreram incidentes em um determinado período;	
2.88.4.6	Os usuários que mais sofreram incidentes em um determinado período;	
2.88.4.7	Ativos e contas descobertas;	
2.88.4.8	Ameaças descobertas e classificadas conforme a cadeia de ataque.	
2.88.5	Deve permitir configuração de atualização do tempo de cada dashboard.	
2.88.6	Deve permitir exportação dos relatórios para os seguintes formatos:	
2.88.6.1	Planilha: CSV e/ou Excel;	
2.88.6.2	Texto: HTML e/ou PDF.	
2.89	A solução deve permitir o gerenciamento de usuários, funções e permissões.	
2.90	A solução deve permitir a criação de usuários com permissões distintas, contendo no mínimo, permissão total e permissão para realizar investigações.	

Anexo B

2.91	A solução deve permitir habilitar ou desabilitar um determinado usuário sem excluí-lo do console.	
2.92	A solução deve registrar todas as atividades efetuadas pelos seus usuários, permitindo auditoria das ações realizadas.	
2.93	A solução deve disponibilizar APIs, com documentação e sem custo adicional, para integração com outras soluções.	
	MONITORAMENTO DEEP/DARK WEB (MONITORAMENTO DE MARCA E AMEAÇAS GLOBAIS)	
2.94	A CONTRATADA deverá realizar serviços de monitoramento de Deep/Dark Web por meio da solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos ofertada (nativamente ou por meio de solução complementar). Os serviços e a respectiva solução utilizada para a realização do monitoramento de Deep/Dark Web devem atender às seguintes especificações mínimas:	
2.94.1	A solução de monitoramento de Deep/Dark Web deve ter como objetivo principal o rastreamento de salas, blogs, fóruns e sites na Deep/Dark Web para identificar informações relativas à CONTRATANTE e seus colaboradores como: credenciais roubadas e outros vazamentos de informações pessoais identificáveis.	
2.94.2	A solução de monitoramento de Deep/Dark Web deve estar licenciada para monitorar até 06 (seis) domínios DNS da CONTRATANTE e uma quantidade de no mínimo 500 (quinhentos) termos por domínio.	
2.94.3	O serviço de monitoramento de Deep/Dark Web deve ser prestado no regime 24x7 (vinte e quatro horas por dia, sete dias por semana).	
2.94.4	A solução de monitoramento de Deep/Dark Web deve realizar buscas, no mínimo:	
2.94.4.1	Na Darknet;	
2.94.4.2	Em plataformas de compartilhamento de documentos;	
2.94.4.3	Pelas seguintes categorias:	
2.94.4.3.1	Por Bucket: Darknet TOR, Whois, Usenet, Leaks, Bot Logs, Wikileaks, Public Leaks, Dumpster, Sci-Hub;	
2.94.4.3.2	Por Site Público: .com, .org, .net, .info, .eu.	
2.94.4.3.3	Por Geolocalização.	
2.94.5	A solução de monitoramento de Deep/Dark Web deve permitir a busca de termos considerando, no mínimo, as seguintes categorias:	
2.94.5.1	Domínio DNS;	
2.94.5.2	Endereço de e-mail;	
2.94.5.3	Endereço Bitcoin;	
2.94.5.4	Endereço Ethereum;	
2.94.5.5	Endereço MAC;	
2.94.5.6	Hash IPFS;	
2.94.5.7	IBAN (Número de Conta Bancária Internacional);	
2.94.5.8	IP e CIDR;	
2.94.5.9	Número de telefone;	
2.94.5.10	Número do cartão de crédito;	
2.94.5.11	URL.	
2.94.6	Deve detectar resultados de itens pesquisa duplicados, apresentando-os de forma consolidada, otimizando a busca por informações relevantes.	
2.94.7	A solução de monitoramento de Deep/Dark Web deve ter a capacidade de buscar dados pelo período mínimo de 1 ano.	
2.94.8	A solução de monitoramento de Deep/Dark Web deve ter a capacidade de filtrar e classificar os resultados das buscas:	

Anexo B

2.94.8.1	Com base na data ou no tempo de publicação das informações encontradas (antigas e novas);	
2.94.8.2	Com base nos domínios, e-mails e URLs encontrados;	
2.94.8.3	Com base nos resultados mais relevante, menos relevante, mais recente e mais antigo;	
2.94.8.4	Com capacidade de combinar ou excluir termos de pesquisa a fim de encontrar com eficiência informações relevantes no banco de dados.	
2.94.9	A solução de monitoramento de Deep/Dark Web deve ter a capacidade de manter históricos de resultados de busca.	
2.94.10	A solução de monitoramento de Deep/Dark Web deve contemplar os seguintes itens:	
2.94.10.1	Monitoramento de atividades na Deep/Dark Web relacionadas às informações sobre domínios, URLs, IPs, hashes, credenciais, e-mails e informações sensíveis da CONTRATANTE.	
2.94.10.2	Amplitude de rastreamento contemplando dados e informações disponibilizadas na Deep/Dark Web como:	
2.94.10.2.1	Monitoramento das credenciais de funcionários em listas e bases de dados de credenciais vazadas na Deep/Dark Web, marketplaces, entre outros;	
2.94.10.2.2	Monitoramento do Pastebin, incluindo posts deletados e outros sites, buscando por referências sobre a empresa, domínios ou endereços IP;	
2.94.10.2.3	Monitoramento de documentos vazados ou roubados da empresa em páginas da Deep/Dark Web e fóruns hackers;	
2.94.10.2.4	Monitoramento de referências aos sistemas em páginas da Deep/Dark Web e fóruns hackers, além de Threat Intelligence e listas de IoC's;	
2.94.10.2.5	Busca de informações sobre redes sociais e plataformas de divulgação de vulnerabilidades vazadas na Deep/Dark Web.	
2.94.10.3	Deve ser possível encontrar marketplaces, fóruns e agentes de ameaças;	
2.94.10.4	Deve ser capaz de realizar avaliação da exposição da marca e vazamentos de informações na Deep/Dark Web;	
2.94.10.5	Investigação de origens de vazamentos de, no mínimo:	
2.94.10.5.1	Grupos de hackers;	
2.94.10.5.2	Ameaças em fóruns;	
2.94.10.5.3	Salas de chats reservadas;	
2.94.10.5.4	Carteira de bitcoins e endereços;	
2.94.10.5.5	Registros históricos.	
2.94.10.7	Geração e notificação de alertas acompanhados da enumeração das ameaças e riscos relacionados e ações de mitigação sugeridas.	
2.95	A solução como um todo, bem como os seus componentes devem contar com garantia e suporte integrais conforme especificado neste documento.	

JUSTIÇA DO TRABALHO

LUCIANO DE SOUZA PAIVA <l113247@trt2.jus.br>

RES: [9605/2021] Contratação XDR/SIEM - Solicitação de proposta comercial com dimensionamento - Intelliway
1 mensagem

Felipe Moyses <felipe.moyses@intelliway.com.br> 24 de agosto de 2023 às 20:43
Para: "luciano.paiva@trt2.jus.br" <luciano.paiva@trt2.jus.br>
Cc: "leonardo.toledo@trt2.jus.br" <leonardo.toledo@trt2.jus.br>, Carlos Eduardo Brandão <brandao@intelliway.com.br>, SEÇÃO DE APOIO À AQUISIÇÃO E CONTRATAÇÃO DE SOLUÇÕES DE TIC <aquisicoes-ti@trt2.jus.br>, SEÇÃO DE GESTÃO DE INCIDENTES EM SEGURANÇA DA INFORMAÇÃO <incidentesseg-ti@trt2.jus.br>

Luciano, boa tarde! Identifiquei um erro na planilha enviada. Segue novamente, já corrigida.

Att:

Felipe

Item	Descrição	Faixa	Faixa de Subscrição por Ativo	Unidade de Medida	Qtde.	Valor Unitário	Valor Total – 24 meses
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Subscrição de até 1000 ativos	Ativo monitorado anualmente	994	R$ 249,14	R$ 495.281,08
		Tipo 2	Subscrição de 1001 a 2000 ativos monitorados	Ativo monitorado anualmente	15182	R$ 242,10	R$ 7.351.066,04
		Tipo 3	Subscrição de 2001 a 5000 ativos monitorados	Ativo monitorado anualmente	28292	R$ 227,01	R$ 12.844.876,44
		Tipo 4	Subscrição de 5001 a 8000 ativos monitorados	Ativo monitorado anualmente	30960	R$ 222,39	R$ 13.770.566,37
		Tipo 5	Subscrição de 8001 a 12000 ativos monitorados	Ativo monitorado anualmente	10846	R$ 216,22	R$ 4.690.265,77
		Rede	1 Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	0	R$ -	R$ -
			10 Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	0	R$ -	R$ -
2	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes para 209 alunos	Serviço pontual, por turma de treinamento	40	R$ 31.156,36	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
4	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Serviços de SOC para até 1000 ativos monitorados	Serviço mensal	1	R$ 53.431,30	R$ 1.282.351,20
		Tipo 2	Serviços de SOC para 1001 a 2000 ativos monitorados	Serviço mensal	10	R$ 74.051,19	R$ 17.772.284,57
		Tipo 3	Serviços de SOC para 2001 a 5000 ativos monitorados	Serviço mensal	8	R$ 109.809,60	R$ 21.083.443,20
		Tipo 4	Serviços de SOC para 5001 a 8000 ativos monitorados	Serviço mensal	5	R$ 157.758,30	R$ 18.930.996,00
		Tipo 5	Serviços de SOC para 8001 a 12000 ativos monitorados	Serviço mensal	1	R$ 172.566,00	R$ 4.141.584,00
				Valor Total			R$ 105.641.042,07

INTELLIWAY
Felipe Moyses
Comercial
+55 27 3376-0163 | +55 27 99630-2682
www.intelliway.com.br
Rua Roberto da Silva, 20, Sala 310, Vitória-ES - CEP 29066-290

De: luciano.paiva@trt2.jus.br <luciano.paiva@trt2.jus.br>
Enviada em: sexta-feira, 18 de agosto de 2023 16:15
Para: Felipe Moyses <felipe.moyses@intelliway.com.br>
Cc: leonardo.toledo@trt2.jus.br; Carlos Eduardo Brandão <brandao@intelliway.com.br>; SEÇÃO DE APOIO À AQUISIÇÃO E CONTRATAÇÃO DE SOLUÇÕES DE TIC <aquisicoes-ti@trt2.jus.br>; SEÇÃO DE GESTÃO DE INCIDENTES EM SEGURANÇA DA INFORMAÇÃO <incidentesseg-ti@trt2.jus.br>
Assunto: Re: [9605/2021] Contratação XDR/SIEM - Solicitação de proposta comercial com dimensionamento - Intelliway

[EXTERNAL]

Prezado Felipe, boa tarde,

Conforme conversamos, gostaria de saber por gentileza se é possível alterar na proposta enviada, a quantidade de turmas para treinamento da solução, considerando que de acordo com a planilha de dimensionamento da solução, poderão ser até 40 turmas a serem treinadas.

Obrigado e qualquer dúvida, estou à disposição para os esclarecimentos necessários.

Atenciosamente,

Luciano de Souza Paiva
Secretaria de Tecnologia da Informação e Comunicação
Coordenadoria de Apoio ao Planejamento e à Governança de TIC
Seção de Apoio à Aquisição e Contratação de Soluções de TIC
Tel: (11) 3150-2070 / e-mail: luciano.paiva@trt2.jus.br

Tribunal Regional do Trabalho da 2ª Região
Av. Marquês de São Vicente, 121, Bloco A - 14º andar
Barra Funda - São Paulo/SP - CEP 01139-001
CNPJ: 03.241.738/0001-39

Em ter., 8 de ago. de 2023 às 19:14, Felipe Moyses <felipe.moyses@intelliway.com.br> escreveu:

> Prezado Luciano, boa noite!
>
> Seguem as respostas abaixo:
>
> 1) Eles não consideraram servidores em nuvem no quantitativo de ativos?
>
> Sim, no nosso caso, servidores em nuvem (máquinas virtuais) são considerados para efeito de licenciamento. Segue tabela abaixo com o quantitativo ajustado.
>
> 2) Sobre tráfego de rede, a solução deles é precificada nesse quesito também? (eu achava que não)
>
> Nossa solução não considera tráfego de rede para efeitos de licenciamento, porém é possível que tenhamos custos com hardware, eventualmente. Na tabela abaixo, nós absorveremos esse custo dentro dos valores de implantação.
>
> 2a) No valor de tráfego de rede de 1 Gbps, eles consideraram "1" no quantitativo? É isso mesmo?
>
> Corrigido.
>
> 2b) No valor de tráfego de rede de 10 Gbps, além da mesma dúvida de terem considerado "1" no quantitativo, o valor unitário e o de 24 meses é igual. É isso mesmo?
>
> Corrigido.

Item	Descrição	Faixa	Faixa de Subscrição por Ativo	Unidade de Medida	Qtde.	Valor Unitário	Valor Total – 24 meses
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Subscrição de até 1000 ativos	Ativo monitorado anualmente	994	R$ 249,14	R$ 495.281,08
		Tipo 2	Subscrição de 1001 a 2000 ativos monitorados	Ativo monitorado anualmente	15182	R$ 242,10	R$ 7.351.066,04
		Tipo 3	Subscrição de 2001 a 5000 ativos monitorados	Ativo monitorado anualmente	28292	R$ 227,01	R$ 12.844.876,44
		Tipo 4	Subscrição de 5001 a 8000 ativos monitorados	Ativo monitorado anualmente	30960	R$ 222,39	R$ 13.770.566,37
		Tipo 5	Subscrição de 8001 a 12000 ativos monitorados	Ativo monitorado anualmente	10846	R$ 216,22	R$ 4.690.265,77

		Rede	1 Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	0	R$ -	R$ -
			10 Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	0	R$ -	R$ -
2	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes para 209 alunos	Serviço pontual, por turma de treinamento	32	R$ 31.156,36	R$ 997.003,52
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
4	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Serviços de SOC para até 1000 ativos monitorados	Serviço mensal	1	R$ 53.431,30	R$ 1.282.351,20
		Tipo 2	Serviços de SOC para 1001 a 2000 ativos monitorados	Serviço mensal	10	R$ 74.051,19	R$ 17.772.284,57
		Tipo 3	Serviços de SOC para 2001 a 5000 ativos monitorados	Serviço mensal	8	R$ 109.809,60	R$ 21.083.443,20
		Tipo 4	Serviços de SOC para 5001 a 8000 ativos monitorados	Serviço mensal	5	R$ 157.758,30	R$ 18.930.996,00
		Tipo 5	Serviços de SOC para 8001 a 12000 ativos monitorados	Serviço mensal	1	R$ 172.566,00	R$ 4.141.584,00
				Valor Total			**R$ 105.391.791,19**

Fico à disposição caso tenham mais alguma dúvida.

Att:

INTELLIWAY

Felipe Moyses

Comercial

+55 27 3376-0163 | +55 27 99630-2682

www.intelliway.com.br

Rua Roberto da Silva, 20, Sala 310, Vitória-ES - CEP 29066-290

De: luciano.paiva@trt2.jus.br <luciano.paiva@trt2.jus.br>
Enviada em: terça-feira, 8 de agosto de 2023 11:19
Para: Felipe Moyses <felipe.moyses@intelliway.com.br>
Cc: leonardo.toledo@trt2.jus.br; Carlos Eduardo Brandão <brandao@intelliway.com.br>; SEÇÃO DE APOIO À AQUISIÇÃO E CONTRATAÇÃO DE SOLUÇÕES DE TIC <aquisicoes-ti@trt2.jus.br>; SEÇÃO DE GESTÃO DE INCIDENTES EM SEGURANÇA DA INFORMAÇÃO <incidentesseg-ti@trt2.jus.br>
Assunto: Re: [9605/2021] Contratação XDR/SIEM - Solicitação de proposta comercial com dimensionamento - Intelliway

[EXTERNAL]

Prezado Felipe, bom dia,

A nossa equipe técnica ficou com algumas dúvidas a respeito da proposta comercial enviada. Seguem abaixo os questionamentos:

1) Eles não consideraram servidores em nuvem no quantitativo de ativos?

2) Sobre tráfego de rede, a solução deles é precificada nesse quesito também? (eu achava que não)
2a) No valor de tráfego de rede de 1 Gbps, eles consideraram "1" no quantitativo? É isso mesmo?
2b) No valor de tráfego de rede de 10 Gbps, além da mesma dúvida de terem considerado "1" no quantitativo, o valor unitário e o de 24 meses é igual. É isso mesmo?

Obrigado e aguardo retorno.

Luciano de Souza Paiva
Secretaria de Tecnologia da Informação e Comunicação
Coordenadoria de Apoio ao Planejamento e à Governança de TIC
Seção de Apoio à Aquisição e Contratação de Soluções de TIC
Tel: (11) 3150-2070 / e-mail: luciano.paiva@trt2.jus.br

Tribunal Regional do Trabalho da 2ª Região
Av. Marquês de São Vicente, 121, Bloco A - 14º andar
Barra Funda - São Paulo/SP - CEP 01139-001
CNPJ: 03.241.738/0001-39

Em seg., 7 de ago. de 2023 às 17:21, luciano.paiva@trt2.jus.br <luciano.paiva@trt2.jus.br> escreveu:

> Prezado Felipe, boa tarde,
>
> Obrigado pelo envio da proposta comercial. Eu encaminhei para análise da nossa equipe técnica e qualquer novidade a respeito, volto a entrar em contato.
>
> Atenciosamente,

Luciano de Souza Paiva
Secretaria de Tecnologia da Informação e Comunicação
Coordenadoria de Apoio ao Planejamento e à Governança de TIC
Seção de Apoio à Aquisição e Contratação de Soluções de TIC
Tel: (11) 3150-2070 / e-mail: luciano.paiva@trt2.jus.br

Tribunal Regional do Trabalho da 2ª Região
Av. Marquês de São Vicente, 121, Bloco A - 14º andar
Barra Funda - São Paulo/SP - CEP 01139-001
CNPJ: 03.241.738/0001-39

Em seg., 7 de ago. de 2023 às 16:56, Felipe Moyses <felipe.moyses@intelliway.com.br> escreveu:

> Prezado Leonardo, boa tarde!
>
> Segue nossa proposta em resposta ao escopo apresentado. Porém, não conseguimos atender ao item abaixo:
>
> *2.63.1. A solução deve impedir, de maneira preditiva, que essas vulnerabilidades sejam exploradas, mesmo para sistemas operacionais e aplicações cujas versões já não possuam suporte dos respectivos fabricantes.*

Item	Descrição	Faixa	Faixa de Subscrição por Ativo	Unidade de Medida	Qtde.	Valor Unitário	Valor Total – 24 meses
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Subscrição de até 1000 ativos	Ativo monitorado anualmente	994	R$ 249,14	R$ 495.281,08
		Tipo 2	Subscrição de 1001 a 2000 ativos monitorados	Ativo monitorado anualmente	15055	R$ 242,10	R$ 7.289.573,13
		Tipo 3	Subscrição de 2001 a 5000 ativos monitorados	Ativo monitorado anualmente	28252	R$ 227,01	R$ 12.826.716,01
		Tipo 4	Subscrição de 5001 a 8000 ativos monitorados	Ativo monitorado anualmente	30906	R$ 222,39	R$ 13.746.547,94
		Tipo 5	Subscrição de 8001 a 12000 ativos monitorados	Ativo monitorado anualmente	10846	R$ 216,22	R$ 4.690.265,77
		Rede	1 Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	1	R$ 62.500,00	R$ 125.000,00
			10 Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	1	R$ 107.142,86	R$ 107.142,86
2	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes para 209 alunos	Serviço pontual, por turma de treinamento	32	R$ 31.156,36	R$ 997.003,52

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
4	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Serviços de SOC para até 1000 ativos monitorados	Serviço mensal	1	R$ 53.431,30	R$ 1.282.351,20
		Tipo 2	Serviços de SOC para 1001 a 2000 ativos monitorados	Serviço mensal	10	R$ 74.051,19	R$ 17.772.284,57
		Tipo 3	Serviços de SOC para 2001 a 5000 ativos monitorados	Serviço mensal	8	R$ 109.809,60	R$ 21.083.443,20
		Tipo 4	Serviços de SOC para 5001 a 8000 ativos monitorados	Serviço mensal	5	R$ 157.758,30	R$ 18.930.996,00
		Tipo 5	Serviços de SOC para 8001 a 12000 ativos monitorados	Serviço mensal	1	R$ 172.566,00	R$ 4.141.584,00
				Valor Total			**R$ 105.520.262,27**

Atenciosamente.

Felipe Moyses

Comercial

+55 27 3376-0163 | +55 27 99630-2682

www.intelliway.com.br

Rua Roberto da Silva, 20, Sala 310, Vitória-ES - CEP 29066-290

De: leonardo.toledo@trt2.jus.br <leonardo.toledo@trt2.jus.br>
Enviada em: quinta-feira, 27 de julho de 2023 14:53
Para: Carlos Eduardo Brandão <brandao@intelliway.com.br>; Felipe Moyses <felipe.moyses@intelliway.com.br>
Cc: LUCIANO DE SOUZA PAIVA <luciano.paiva@trt2.jus.br>; SEÇÃO DE APOIO À AQUISIÇÃO E CONTRATAÇÃO DE SOLUÇÕES DE TIC <aquisicoes-ti@trt2.jus.br>
Assunto: [9605/2021] Contratação XDR/SIEM - Solicitação de proposta comercial com dimensionamento - Intelliway

[EXTERNAL]

Prezados,

Solicito, por gentileza, emissão de proposta comercial referente à contratação de solução de Monitoramento, Detecção, Notificação, Investigação e Resposta a Ataques Cibernéticos, bem como serviços de treinamento, implantação e sustentação da solução pelo período de 24 meses.

As especificações técnicas revisadas, bem como o dimensionamento de todos os órgãos participantes encontram-se em anexo.

Atenciosamente,

--

Leonardo Henrique Day de Toledo

Secretaria de Tecnologia da Informação e Comunicação

Coordenadoria de Apoio ao Planejamento e à Governança de TIC

Seção de Apoio à Aquisição e Contratação de Soluções de TIC

Tel: (11) 3150-2000 Ramal: 2070 e-mail: leonardo.toledo@trtsp.jus.br

Tribunal Regional do Trabalho da 2ª Região

Av. Marquês de São Vicente, 235 - Bloco A, 1º andar

Barra Funda - São Paulo/SP - CEP 01139-001

CNPJ: 03.241.738/0001-39

Petacorp

JUSTIÇA DO TRABALHO
Tribunal Regional do Trabalho da 2ª Região (SP)

Proposta Comercial

Contratação de solução de Monitoramento, Detecção, Notificação, Investigação e Resposta a Ataques Cibernéticos

TREND MICRO™

SCES TR 02 LT 08 SL 03 – LAGO SUL – BRASÍLIA/DF
CEP 70.200-002 Brasília DF
www.petacorp.com
contato@petacorp.com.br

Ao

TRT - 2 – Tribunal Regional do Trabalho da 2 Região

A/C: Claudia Pinheiro - seguranca-ti@trtsp.jus.br

Prezada,

Servimo-nos da presente para apresentar proposta comercial da Soluçao **Contratação de solução de Monitoramento, Detecção, Notificação, Investigação e Resposta aAtaques Cibernéticos.**

Caso haja alguma duvida estamos a disposição.

Cordialmente,

Zuleide Silva

Gerente de Contas

SCES TR 02 LT 08 SL 03 – LAGO SUL – BRASÍLIA/DF
CEP 70.200-002 Brasília DF
www.petacorp.com
contato@petacorp.com.br

1.1. Confidencialidade

As informações contidas neste documento são de propriedade da **PETACORP**, sendo sua duplicação permitida apenas para uso interno do **CLIENTE**, não podendo ser utilizada como fonte de informações a terceiros, bem como todas as informações fornecidas à **PETACORP** não deverão ser divulgadas, salvo em caso de autorização por escrito de ambas as partes.

1.2. Validade da Proposta:

Esta proposta tem validade de 90 dias, contados a partir da data.

1.3. Objeto:

Contratação de solução de Monitoramento, Detecção, Notificação, Investigação e Resposta aAtaques Cibernéticos.

2. **Investimento:**

Item	Descrição	Faixa	Faixa de Subscrição por Ativo	Unidade de Medida	Quantidades a considerar	Valor Unitário Empresa X	Valor Total (em 12 meses) Empresa X	Valor Total (em 24 meses) Empresa X
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Subscrição de até 1000 ativos monitorados	Ativos monitorados anualmente	994	R$ 469,12	R$ 466.309,91	R$ 932.619,82
		Tipo 2	Subscrição de 1001 a 2000 ativos monitorados	Ativos monitorados anualmente	15182	R$ 399,41	R$ 6.063.784,71	R$ 12.127.569,43
		Tipo 3	Subscrição de 2001 a 5000 ativos monitorados	Ativos monitorados anualmente	28292	R$ 364,32	R$ 10.307.447,41	R$ 20.614.894,82
		Tipo 4	Subscrição de 5001 a 8000 ativos monitorados	Ativos monitorados anualmente	30960	R$ 382,61	R$ 11.845.544,82	R$ 23.691.089,63
		Tipo 5	Subscrição de 8001 a 12000 ativos monitorados	Ativos monitorados anualmente	10846	R$ 359,65	R$ 3.900.710,84	R$ 7.801.421,68
		Rede	1 Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	109	R$ 190.638,93	R$ 20.779.643,18	R$ 41.559.286,35
			10 Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	6	R$ 300.638,93	R$ 1.803.833,57	R$ 3.607.667,14
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	Serviços de SOC para até 1000 ativos monitorados	Serviço mensal	1	R$ 28.500,00	R$ 342.000,00	R$ 684.000,00
		Tipo 2	Serviços de SOC para 1001 a 2000 ativos monitorados	Serviço mensal	10	R$ 39.000,00	R$ 4.680.000,00	R$ 9.360.000,00
		Tipo 3	Serviços de SOC para 2001 a 5000 ativos monitorados	Serviço mensal	8	R$ 48.000,00	R$ 4.608.000,00	R$ 9.216.000,00
		Tipo 4	Serviços de SOC para 5001 a 8000 ativos monitorados	Serviço mensal	5	R$ 63.000,00	R$ 3.780.000,00	R$ 7.560.000,00
		Tipo 5	Serviços de SOC para 8001 a 12000 ativos monitorados	Serviço mensal	1	R$ 70.000,00	R$ 840.000,00	R$ 1.680.000,00
							R$ 75.917.274,43	**R$ 145.334.548,87**

SCES TR 02 LT 08 SL 03 – LAGO SUL – BRASÍLIA/DF
CEP 70.200-002 Brasília DF
www.petacorp.com
contato@petacorp.com.br

a. Tributos, Impostos e Taxas de Incidência

Todos os impostos, tributos e taxas de qualquer natureza, referente à prestação do serviço, fazem parte do preço ora avençado.

De responsabilidade do Cliente, como fonte pagadora, descontar, reter, e recolher, nos prazos da lei, dos pagamentos que efetuar, os tributos que estiver obrigada a fazê-lo pela legislação em vigor e contribuições cuja retenção lhe for imposta por lei, tais como II, CIDE, PIS, COFINS, CSLL, INSS, IRRF e ISS. Para todos os fins e efeitos, as partes reconhecem que o objeto do presente contrato não compreende cessão de mão de obra. Em caso de majoração de alíquotas ou de instituição de novos tributos, o preço (ou qualquer de suas parcelas) será reajustado na proporção equivalente.

b. Faturamento:

O faturamento será através de Nota Fiscal

c. Pagamento:

Conforme TR.

Dados da Empresa:

JAMC Consultoria e Representação de Software LTDA

CNPJ: 24.425.034/0001-96

I.E:07.760.481/001-40

ENDEREÇO:

Brasília, 28 de Agosto de 2023.

Zuleide Silva

Zuleide Silva

Gerente de Contas

SERVICE IT

PROPOSTA TÉCNICA/COMERCIAL

1. Controle de versão

Versão	Data	Responsável	Descrição
1.0	29/08/2023	Leandro Ferreira Wienen	Criação da Proposta

2. Termo de Confidencialidade e Proteção de Dados

As partes envolvidas obrigam-se a respeitar estritamente em caráter confidencial e sigiloso todas as informações relativas aos equipamentos, softwares e serviços, que contenham neste documento.

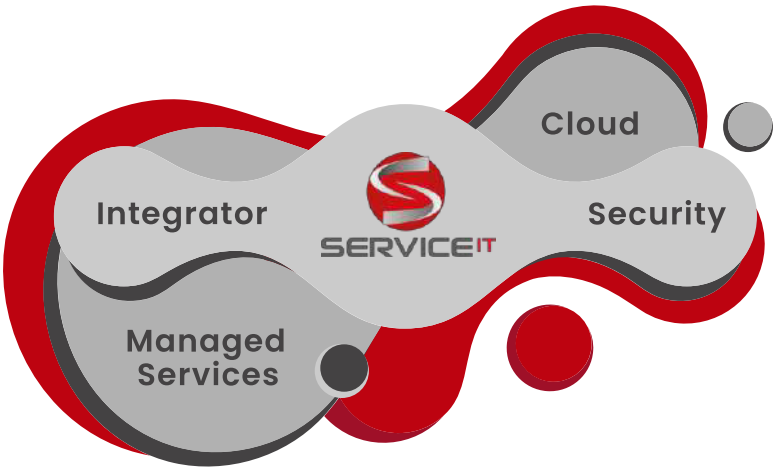
O conteúdo da presente proposta, bem como os dados pessoais obtidos na execução dos serviços ou fornecimento de produtos, fica protegido pela Lei nº 13.709/18 (Lei Geral de Proteção de Dados), conforme termo anexo devidamente assinado pelas partes.

3. Conhecendo a Service IT

A Service IT está no mercado desde 1995 como uma das maiores integradoras de soluções e serviços de TI da América Latina.

Com uma equipe de profissionais dedicados e altamente treinados, monitoramos e gerenciamos os ambientes de TI de nossos clientes através de nossos Centros de Operações próprios, NOC e SOC, para que eles possam se concentrar em seus negócios.

Mantemos unidades de negócios especializadas em infraestrutura, gerenciamento de serviços, cloud computing e segurança da informação, para oferecer um portfólio amplo de serviços que atendam às mais diversas necessidades de nossos clientes.



Além disso, investimos continuamente na certificação de nossos profissionais para fornecer serviços que superem as expectativas de nossos clientes. E nossas parcerias estratégicas com fabricantes de tecnologia e segurança mundiais visam oferecer o melhor da tecnologia em cada projeto.

Conheça algumas delas:

4. PROPOSTA DE PREÇOS

Ao
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO
Av. Marquês de São Vicente, 235 - Bloco A, 1º andar
Barra Funda - São Paulo/SP - CEP 01139-001
CNPJ: 03.241.738/0001-39

Pelo presente instrumento, vimos apresentar nossa proposta de preços relativa à **"ATA DE REGISTROS DE PREÇOS VISANDO A CONTRATAÇÃO DE SOLUÇÃO DE MONITORAMENTO, DETECÇÃO, NOTIFICAÇÃO, INVESTIGAÇÃO E RESPOSTA A ATAQUES CIBERNÉTICOS, BEM COMO SERVIÇOS DE TREINAMENTO, IMPLANTAÇÃO E SUSTENTAÇÃO DA SOLUÇÃO PROPOSTA, PELO PERÍODO DE 24 MESES"** conforme condições contidas no Termo de Referência e Anexos, integrantes deste edital.

Item	Descrição	Faixa	Faixa de Subscrição por Ativo	Unidade de Medida	Quant a considerar	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	Subscrição de até 1000 ativos monitorados	Ativos monitorados anualmente	994	R$477,32	R$ 474.456,08	R$ 948.912,16
		Tipo 2	Subscrição de 1001 a 2000 ativos monitorados	Ativos monitorados anualmente	15182	R$409,21	R$ 6.212.626,22	R$ 12.425.252,44
		Tipo 3	Subscrição de 2001 a 5000 ativos monitorados	Ativos monitorados anualmente	28292	R$371,54	R$ 10.511.609,68	R$ 21.023.219,36
		Tipo 4	Subscrição de 5001 a 8000 ativos monitorados	Ativos monitorados anualmente	30960	R$386,01	R$ 11.950.869,60	R$ 23.901.739,20
		Tipo 5	Subscrição de 8001 a 12000 ativos monitorados	Ativos monitorados anualmente	10846	R$369,76	R$ 4.010.416,96	R$ 8.020.833,92
		Rede	1 Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	109	R$192.456,97	R$ 20.977.809,73	R$ 41.955.619,46
			10 Gbps (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 resposta a ataques cibernéticos	Tipo 1	Serviços de SOC para até 1000 ativos monitorados	Serviço mensal	1	R$30.100,00	R$ 361.200,00	R$ 722.400,00
		Tipo 2	Serviços de SOC para 1001 a 2000 ativos monitorados	Serviço mensal	10	R$41.240,00	R$ 4.948.800,00	R$ 9.897.600,00
		Tipo 3	Serviços de SOC para 2001 a 5000 ativos monitorados	Serviço mensal	8	R$52.185,00	R$ 5.009.760,00	R$ 10.019.520,00
		Tipo 4	Serviços de SOC para 5001 a 8000 ativos monitorados	Serviço mensal	5	R$64.890,00	R$ 3.893.400,00	R$ 7.786.800,00
		Tipo 5	Serviços de SOC para 8001 a 12000 ativos monitorados	Serviço mensal	1	R$72.280,00	R$ 867.360,00	R$ 1.734.720,00
VALOR TOTAL DA PROPOSTA							**R$ 78.152.980,93**	**R$ 149.207.211,86**

- ✓ A proposta tem validade de 90 (noventa) dias, a contar da data da licitação.
- ✓ No preço proposto contempla todas as despesas, diretas ou indiretas, necessárias ao pleno fornecimento, tais como os encargos (obrigações sociais, impostos, taxas, frete etc.) incidentes sobre o fornecimento.

DADOS DA PROPONENTE

RAZÃO SOCIAL: SERVICE IT SECURITY CONSULTORIA DE SEGURANÇA EM TECNOLOGIA DA INFORMAÇÃO LTDA.
CNPJ: 12.373.559/0001-46 - Não optante pelo Simples Nacional
INSCRIÇÃO ESTADUAL: 124/0297650

END. e TEL.: Endereço: Av Unisinos, 950 - ED Padre Rick - Sala 308 CEP: 93022-000 - São Leopoldo - RS
AGÊNCIA e Nº DA CONTA BANCÁRIA: Banco: Itaú 341 - Agência: 0604 - Conta: 07542-4
REPRESENTANTE E CARGO: Laisa Maria Toebe Capssa (Diretora Comercial)
CARTEIRA DE IDENTIDADE E CPF: RG: 1054154347 SSP/RS / CPF: 939191820-49

DADOS PARA CORRESPONDÊNCIA (ENVIO DE CONTRATO, ATAS, OFÍCIO, EMPENHO):

SERVICE INFORMÁTICA LTDA.
Rua Lauro Muller, 116 – Sala 907 – Torre do Rio Sul – Botafogo - CEP:22290-160 – Rio de Janeiro/RJ
Tel.: (21) 2246-5815
E-mail: comercialrj@service.com.br

REPRESENTANTE LEGAL:

NOME: Laisa Maria Toebe Capssa
NACIONALIDADE: Brasileira
ESTADO CIVIL: Solteira
PROFISSÃO: Administradora de Empresas
FUNÇÃO NA SOCIEDADE: Diretora Comercial
RG: 1054154347 SSP/RS
CPF: 939191820-49

Rio de Janeiro, 29 de agosto de 2023.

_____

Laisa Maria Toebe Capssa

RG 1054154347 SSP/RS

CPF: 939.191.820-49

Diretora Comercial

SERVICE IT SECURITY CONSULTORIA DE SEGURANÇA EM TECNOLOGIA DA INFORMAÇÃO LTDA.

CNPJ: 12.373.559/0001-46

NETWORK SECURE

AO
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO - TRT2

COTAÇÃO DE PREÇO

Item	Descrição	Faixa	Faixa de Subscrição por Ativo	Unidade de Medida	Quantidades a considerar	Quantidades Tribunais	Valor Unitário Empresa X	Valor Total (em 12 meses) Empresa X	Valor Total (em 24 meses) Empresa X
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Subscrição de até 1000 ativos monitorados	Ativos monitorados anualmente	994	1	R$ 3.359,42	R$ 3.339.262,30	R$ 6.678.524,60
		Tipo 2	Subscrição de 1001 a 2000 ativos monitorados	Ativos monitorados anualmente	15182	10	R$ 3.110,06	R$ 47.216.983,00	R$ 94.433.966,00
		Tipo 3	Subscrição de 2001 a 5000 ativos monitorados	Ativos monitorados anualmente	28292	8	R$ 2.507,85	R$ 70.952.050,40	R$ 141.904.100,80
		Tipo 4	Subscrição de 5001 a 8000 ativos monitorados	Ativos monitorados anualmente	30960	5	R$ 2.102,12	R$ 65.081.571,50	R$ 130.163.143,00
		Tipo 5	Subscrição de 8001 a 12000 ativos monitorados	Ativos monitorados anualmente	10846	1	R$ 1.709,94	R$ 18.546.058,30	R$ 37.092.116,60
		Rede	1 Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	25 NDR(VM) 1 por unidade	25	R$ 850.000,00	R$ 21.250.000,00	R$ 42.500.000,00
			10 Gbps (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	Tipo 1	Serviços de SOC para até 1000 ativos monitorados	Serviço mensal	1		R$ 78.975,00	R$ 947.700,00	R$ 1.895.400,00
		Tipo 2	Serviços de SOC para	Serviço mensal	10		R$ 131.625,00	R$ 15.795.000,00	R$ 31.590.000,00

	cibernéticos		1001 a 2000 ativos monitorados						
		Tipo 3	Serviços de SOC para 2001 a 5000 ativos monitorados	Serviço mensal	8		R$ 210.600,00	R$ 20.217.600,00	R$ 40.435.200,00
		Tipo 4	Serviços de SOC para 5001 a 8000 ativos monitorados	Serviço mensal	5		R$ 263.250,00	R$ 15.795.000,00	R$ 31.590.000,00
		Tipo 5	Serviços de SOC para 8001 a 12000 ativos monitorados	Serviço mensal	1		R$ 315.900,00	R$ 3.790.800,00	R$ 7.581.600,00
								R$ 341.382.025,50	**R$ 624.314.051,00**

Valor Total: R$ 624.314.051,00 (seiscentos e vinte e quatro milhões trezentos e quatorze mil e cinquenta e um reais)

Validade da proposta é de **60 (sessenta) dias.**

DADOS DA EMPRESA

Razão Social - NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA
CNPJ - 05.250.796/0001-54
Endereço - Av. Pontes Vieira, 2340 - Dionísio Torres, UNO - Medical & Office - Sala 510 - 514 - 5º andar, Fortaleza/CE - CEP: 60135-238
Telefone - (85) 3195-2200 / 2231 / 2212
E-mail - licitacoes@networksecure.com.br

DADOS DO REPRESENTANTE LEGAL

Nome completo: Yure Leopoldo Sabino De Freitas
Cargo/Funçao: Diretor Comercial
E-mail: yure.sabino@networksecure.com.br
Telefone: (85) 3195-2200
Domicílio: Rua General Tertuliano Potiguara, 158, Apto 701, Aldeota, Fortaleza/CE, CEP: 60135-280

Fortaleza/CE, 18 de outubro de 2023

YURE LEOPOLDO SABINO DE FREITAS
Assinado de forma digital por YURE LEOPOLDO SABINO DE FREITAS
Dados: 2023.10.18 12:00:06 -03'00'

NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA
CNPJ Nº 05.250.796/0001-54
Yure Leopoldo Sabino De Freitas
Diretor Comercial
CPF Nº 525.285.023-20

AO
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO - TRT2

TABELA DE PART NUMBER

ITEM 1 - Faixa 1 - Até 1000 Ativos			
PRODUTO	**Quant.**	**HW/SW**	**SKU / PARTNUMBER**
FortiSIEM	50	**SW**	FC1-10-FSM98-180-02-12: FortiSIEM All-In-One Subscription License Per Device Subscription License that manages minimum 50 devices, 10 EPS/Device. Does not include Maintenance & Support
	950	**SW**	FC4-10-FSM98-184-02-12: FortiSIEM End-Point Device Subscription License Per End-Point Subscription License for minimum 500 End-Points, 2 EPS/End-Point . Does not include Maintenance & Support
	1000	**SW**	FC5-10-FSM98-182-02-12: FortiSIEM Subscription License for Advanced Agents Per Agent Subscription License - Log & FIM - minimum 1000 Advanced Agents.Does not include Maintenance & Support.
	1000	**SW**	FC4-10-FSM98-334-02-12: FortiSIEM-UEBA Subscription License Per Advanced Agent - UEBA Telemetry Subscription License, a minimum of 500 Agents. Does not include Maintenance & Support. See Datasheet for support on F Series hardware. Powered by FortiInsight AI
	5600	**SW**	FC1-10-FSM98-183-02-12: Add EPS - subscription Add 1 EPS subscription
	1	**SW**	FC8-10-FSM97-248-02-12: FortiCare Support for Software based FortiSIEM deployments FortiCare Premium Support (1 - 1000 points) for FortiSIEM Software deployments. 1 "Device" or 2 "End points" or 3 "Advanced Agents - Log & FIM" or 10 "Advanced Agents - UEBA Telemetry" equals 1 point.
	1	**SW**	FC8-10-FSM98-149-02-12: IOC Service for FortiSIEM deployments (1 - 1000 Points) FortiSIEM Indicators of Compromise (IOC) Service
FortiEDR	2	**SW**	FC2-10-FEDR1-394-01-12: FortiEDR Discover, Protect & Respond and XDR (500 seats MOQ) FortiEDR Discover, Protect & Respond and XDR Cloud Subscription and FortiCare Premium for 500 endpoints
	1	**SW**	FC1-10-EDBPS-310-02-12: FortiCare BPS Subscription for FortiEDR FortiEDR Best Practice Service for up to 1,000 Endpoints/users
FortiDeceptor	5	**SW**	FC1-10-DCVMS-496-02-12: FortiDeceptor-VM Subscription License VM model FortiCare Premium, Deceptor Bundle Contract included license for Deception Decoys, Deception Lures plus FortiGuard Services Subscriptions (ARAE, AV, IPS, and Web Filtering). 1 network VLAN unit price, minimum order of 2 VLANs. Support up to 20 Deception VMs and up to 128 network VLANS
	5	**SW**	LIC-FDC-WIN: FortiDeceptor Windows License
FortiRecon	1	**SW**	FC2-10-RNSVC-535-02-12: FortiRecon External Attack Surface Monitoring Brand Protect & Adversary Centric Intelligence FortiRecon External Attack Surface Monitoring, Brand Protect & Adversary Centric Intelligence - up to 500 monitored assets

ITEM 1 - Faixa 2 - De 1001 a 2000 ativos			
PRODUTO	**Quant.**	**HW/SW**	**SKU / PARTNUMBER**
FortiSIEM	100	**SW**	FC1-10-FSM98-180-02-12: FortiSIEM All-In-One Subscription License Per Device Subscription License that manages minimum 50 devices, 10 EPS/Device. Does not include Maintenance & Support

	1900	**SW**	FC4-10-FSM98-184-02-12: FortiSIEM End-Point Device Subscription License Per End-Point Subscription License for minimum 500 End-Points, 2 EPS/End-Point . Does not include Maintenance & Support
	2000	**SW**	FC5-10-FSM98-182-02-12: FortiSIEM Subscription License for Advanced Agents Per Agent Subscription License - Log & FIM - minimum 1000 Advanced Agents.Does not include Maintenance & Support.
	2000	**SW**	FC4-10-FSM98-334-02-12: FortiSIEM-UEBA Subscription License Per Advanced Agent - UEBA Telemetry Subscription License, a minimum of 500 Agents. Does not include Maintenance & Support. See Datasheet for support on F Series hardware. Powered by FortiInsight AI
	11200	**SW**	FC1-10-FSM98-183-02-12: Add EPS - subscription Add 1 EPS subscription
	1	**SW**	FC8-10-FSM97-248-02-12: FortiCare Support for Software based FortiSIEM deployments FortiCare Premium Support (1 - 1000 points) for FortiSIEM Software deployments. 1 "Device" or 2 "End points" or 3 "Advanced Agents - Log & FIM" or 10 "Advanced Agents - UEBA Telemetry" equals 1 point.
	1	**SW**	FC8-10-FSM98-149-02-12: IOC Service for FortiSIEM deployments (1 - 1000 Points) FortiSIEM Indicators of Compromise (IOC) Service
FortiEDR	2	**SW**	FC2-10-FEDR1-394-01-12: FortiEDR Discover, Protect & Respond and XDR (500 seats MOQ) FortiEDR Discover, Protect & Respond and XDR Cloud Subscription and FortiCare Premium for 500 endpoints
	1	**SW**	FC1-10-EDBPS-310-02-12: FortiCare BPS Subscription for FortiEDR FortiEDR Best Practice Service for up to 1,000 Endpoints/users
FortiDeceptor	5	**SW**	FC1-10-DCVMS-496-02-12: FortiDeceptor-VM Subscription License VM model FortiCare Premium, Deceptor Bundle Contract included license for Deception Decoys, Deception Lures plus FortiGuard Services Subscriptions (ARAE, AV, IPS, and Web Filtering). 1 network VLAN unit price, minimum order of 2 VLANs. Support up to 20 Deception VMs and up to 128 network VLANS
	5	**SW**	LIC-FDC-WIN: FortiDeceptor Windows License
FortiRecon	1	**SW**	FC2-10-RNSVC-535-02-12: FortiRecon External Attack Surface Monitoring Brand Protect & Adversary Centric Intelligence FortiRecon External Attack Surface Monitoring, Brand Protect & Adversary Centric Intelligence - up to 500 monitored assets

ITEM 1 - Faixa 3 - De 2001 a 5000 ativos

PRODUTO	Quant.	HW/SW	SKU / PARTNUMBER
FortiSIEM	250	**SW**	FC1-10-FSM98-180-02-12: FortiSIEM All-In-One Subscription License Per Device Subscription License that manages minimum 50 devices, 10 EPS/Device. Does not include Maintenance & Support
	4750	**SW**	FC4-10-FSM98-184-02-12: FortiSIEM End-Point Device Subscription License Per End-Point Subscription License for minimum 500 End-Points, 2 EPS/End-Point . Does not include Maintenance & Support
	5000	**SW**	FC5-10-FSM98-182-02-12: FortiSIEM Subscription License for Advanced Agents Per Agent Subscription License - Log & FIM - minimum 1000 Advanced Agents.Does not include Maintenance & Support.
	5000	**SW**	FC4-10-FSM98-334-02-12: FortiSIEM-UEBA Subscription License Per Advanced Agent - UEBA Telemetry Subscription License, a minimum of 500 Agents. Does not include Maintenance & Support. See Datasheet for support on F Series hardware. Powered by FortiInsight AI
	28000	**SW**	FC1-10-FSM98-183-02-12: Add EPS - subscription Add 1 EPS subscription

	1	SW	FC8-10-FSM97-248-02-12: FortiCare Support for Software based FortiSIEM deployments FortiCare Premium Support (1 - 1000 points) for FortiSIEM Software deployments. 1 "Device" or 2 "End points" or 3 "Advanced Agents - Log & FIM" or 10 "Advanced Agents - UEBA Telemetry" equals 1 point.
	1	SW	FC8-10-FSM98-149-02-12: IOC Service for FortiSIEM deployments (1 - 1000 Points) FortiSIEM Indicators of Compromise (IOC) Service
FortiEDR	2	SW	FC2-10-FEDR1-394-01-12: FortiEDR Discover, Protect & Respond and XDR (500 seats MOQ) FortiEDR Discover, Protect & Respond and XDR Cloud Subscription and FortiCare Premium for 500 endpoints
	1	SW	FC1-10-EDBPS-310-02-12: FortiCare BPS Subscription for FortiEDR FortiEDR Best Practice Service for up to 1,000 Endpoints/users
FortiDeceptor	5	SW	FC1-10-DCVMS-496-02-12: FortiDeceptor-VM Subscription License VM model FortiCare Premium, Deceptor Bundle Contract included license for Deception Decoys, Deception Lures plus FortiGuard Services Subscriptions (ARAE, AV, IPS, and Web Filtering). 1 network VLAN unit price, minimum order of 2 VLANs. Support up to 20 Deception VMs and up to 128 network VLANS
	5	SW	LIC-FDC-WIN: FortiDeceptor Windows License
FortiRecon	1	SW	FC2-10-RNSVC-535-02-12: FortiRecon External Attack Surface Monitoring Brand Protect & Adversary Centric Intelligence FortiRecon External Attack Surface Monitoring, Brand Protect & Adversary Centric Intelligence - up to 500 monitored assets

ITEM 1 - Faixa 4 - De 5001 a 8000 ativos

PRODUTO	Quant.	HW/SW	SKU / PARTNUMBER
FortiSIEM	400	SW	FC1-10-FSM98-180-02-12: FortiSIEM All-In-One Subscription License Per Device Subscription License that manages minimum 50 devices, 10 EPS/Device. Does not include Maintenance & Support
	7600	SW	FC4-10-FSM98-184-02-12: FortiSIEM End-Point Device Subscription License Per End-Point Subscription License for minimum 500 End-Points, 2 EPS/End-Point . Does not include Maintenance & Support
	8000	SW	FC5-10-FSM98-182-02-12: FortiSIEM Subscription License for Advanced Agents Per Agent Subscription License - Log & FIM - minimum 1000 Advanced Agents.Does not include Maintenance & Support.
	8000	SW	FC4-10-FSM98-334-02-12: FortiSIEM-UEBA Subscription License Per Advanced Agent - UEBA Telemetry Subscription License, a minimum of 500 Agents. Does not include Maintenance & Support. See Datasheet for support on F Series hardware. Powered by FortiInsight AI
	44800	SW	FC1-10-FSM98-183-02-12: Add EPS - subscription Add 1 EPS subscription
	1	SW	FC8-10-FSM97-248-02-12: FortiCare Support for Software based FortiSIEM deployments FortiCare Premium Support (1 - 1000 points) for FortiSIEM Software deployments. 1 "Device" or 2 "End points" or 3 "Advanced Agents - Log & FIM" or 10 "Advanced Agents - UEBA Telemetry" equals 1 point.
	1	SW	FC8-10-FSM98-149-02-12: IOC Service for FortiSIEM deployments (1 - 1000 Points) FortiSIEM Indicators of Compromise (IOC) Service
FortiEDR	2	SW	FC2-10-FEDR1-394-01-12: FortiEDR Discover, Protect & Respond and XDR (500 seats MOQ) FortiEDR Discover, Protect & Respond and XDR Cloud Subscription and FortiCare Premium for 500 endpoints
	1	SW	FC1-10-EDBPS-310-02-12: FortiCare BPS Subscription for FortiEDR FortiEDR Best Practice Service for up to 1,000 Endpoints/users

FortiDeceptor	5	**SW**	FC1-10-DCVMS-496-02-12: FortiDeceptor-VM Subscription License VM model FortiCare Premium, Deceptor Bundle Contract included license for Deception Decoys, Deception Lures plus FortiGuard Services Subscriptions (ARAE, AV, IPS, and Web Filtering). 1 network VLAN unit price, minimum order of 2 VLANs. Support up to 20 Deception VMs and up to 128 network VLANS
	5	**SW**	LIC-FDC-WIN: FortiDeceptor Windows License
FortiRecon	1	**SW**	FC2-10-RNSVC-535-02-12: FortiRecon External Attack Surface Monitoring Brand Protect & Adversary Centric Intelligence FortiRecon External Attack Surface Monitoring, Brand Protect & Adversary Centric Intelligence - up to 500 monitored assets

ITEM 1 - Faixa 5 - De 8001 a 12000 ativos

PRODUTO	Quant.	HW/SW	SKU / PARTNUMBER
FortiSIEM	600	**SW**	FC1-10-FSM98-180-02-12: FortiSIEM All-In-One Subscription License Per Device Subscription License that manages minimum 50 devices, 10 EPS/Device. Does not include Maintenance & Support
	11400	**SW**	FC4-10-FSM98-184-02-12: FortiSIEM End-Point Device Subscription License Per End-Point Subscription License for minimum 500 End-Points, 2 EPS/End-Point . Does not include Maintenance & Support
	12000	**SW**	FC5-10-FSM98-182-02-12: FortiSIEM Subscription License for Advanced Agents Per Agent Subscription License - Log & FIM - minimum 1000 Advanced Agents.Does not include Maintenance & Support.
	12000	**SW**	FC4-10-FSM98-334-02-12: FortiSIEM-UEBA Subscription License Per Advanced Agent - UEBA Telemetry Subscription License, a minimum of 500 Agents. Does not include Maintenance & Support. See Datasheet for support on F Series hardware. Powered by FortiInsight AI
	67200	**SW**	FC1-10-FSM98-183-02-12: Add EPS - subscription Add 1 EPS subscription
	1	**SW**	FC8-10-FSM97-248-02-12: FortiCare Support for Software based FortiSIEM deployments FortiCare Premium Support (1 - 1000 points) for FortiSIEM Software deployments. 1 "Device" or 2 "End points" or 3 "Advanced Agents - Log & FIM" or 10 "Advanced Agents - UEBA Telemetry" equals 1 point.
	1	**SW**	FC8-10-FSM98-149-02-12: IOC Service for FortiSIEM deployments (1 - 1000 Points) FortiSIEM Indicators of Compromise (IOC) Service
FortiEDR	2	**SW**	FC2-10-FEDR1-394-01-12: FortiEDR Discover, Protect & Respond and XDR (500 seats MOQ) FortiEDR Discover, Protect & Respond and XDR Cloud Subscription and FortiCare Premium for 500 endpoints
	1	**SW**	FC1-10-EDBPS-310-02-12: FortiCare BPS Subscription for FortiEDR FortiEDR Best Practice Service for up to 1,000 Endpoints/users
FortiDeceptor	5	**SW**	FC1-10-DCVMS-496-02-12: FortiDeceptor-VM Subscription License VM model FortiCare Premium, Deceptor Bundle Contract included license for Deception Decoys, Deception Lures plus FortiGuard Services Subscriptions (ARAE, AV, IPS, and Web Filtering). 1 network VLAN unit price, minimum order of 2 VLANs. Support up to 20 Deception VMs and up to 128 network VLANS
	5	**SW**	LIC-FDC-WIN: FortiDeceptor Windows License
FortiRecon	1	**SW**	FC2-10-RNSVC-535-02-12: FortiRecon External Attack Surface Monitoring Brand Protect & Adversary Centric Intelligence FortiRecon External Attack Surface Monitoring, Brand Protect & Adversary Centric Intelligence - up to 500 monitored assets

ITEM 1 - REDE - 1 Gbps (Gigabits por segundo)

PRODUTO	Quant.	HW/SW	SKU / PARTNUMBER
NDR - 1Gbps	1	HW	FNR-1000F: FortiNDR-1000F
	1	SW	FC-10-AI1KF-331-02-12: FortiNDR-1000F FortiCare Premium with NDR and ANN engine updates & baseline
	1	SW	FC-10-AI1KF-588-02-12: FortiNDR-1000F Netflow Support for FortiNDR-1000F

ITEM 1 - REDE - 10 Gbps (Gigabits por segundo)

PRODUTO	Quant.	HW/SW	SKU / PARTNUMBER
NDR - 10Gbps	1	HW	FNR-1000F: FortiNDR-1000F
	1	SW	FC-10-AI1KF-331-02-12: FortiNDR-1000F FortiCare Premium with NDR and ANN engine updates & baseline
	1	SW	FC-10-AI1KF-588-02-12: FortiNDR-1000F Netflow Support for FortiNDR-1000F

ITEM 1 - REDE - 1 Gbps (Gigabits por segundo) VIRTUAL

PRODUTO	Quant.	HW/SW	SKU / PARTNUMBER
	1	SW	FC3-10-AIVMS-461-02-12: FortiNDR-VM Subscription License with Bundle Subscriptions license for FortiNDR-VM (16 CPU) with FortiCare Premium with NDR and ANN engine updates & baseline.Netflow order separately
	1	SW	FC3-10-AIVMS-588-02-12: FortiNDR-VM Subscription License with Bundle Netflow Support for FortiNDR-VM16

ITEM 1 - REDE - 10 Gbps (Gigabits por segundo) VIRTUAL

PRODUTO	Quant.	HW/SW	SKU / PARTNUMBER
	1	SW	FC4-10-AIVMS-461-02-12: FortiNDR-VM Subscription License with Bundle Subscriptions license for FortiNDR-VM (32 CPU) with FortiCare Premium with NDR and ANN engine updates & baseline.Netflow order separately.
	1	SW	FC4-10-AIVMS-588-02-12: FortiNDR-VM Subscription License with Bundle Netflow Support for FortiNDR-VM32

Fortaleza/CE, 18 de outubro de 2023

YURE LEOPOLDO SABINO DE FREITAS

Assinado de forma digital por YURE LEOPOLDO SABINO DE FREITAS
Dados: 2023.10.18 12:00:42 -03'00'

NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA
CNPJ Nº 05.250.796/0001-54
Yure Leopoldo Sabino De Freitas
Diretor Comercial
CPF Nº 525.285.023-20

SUPORTE Informática

Av. João de Barros, 1261
Espinheiro – Recife – PE
CEP.52.021-180
Fone 81.3202.9100
Fax 81.3244.9697
Proposta Nº 18.000-01

Recife, 24 de agosto de 2023.

A(o),
Tribunal Regional do Trabalho da 2° Região - TRT2
CNPJ 03.241.738/0001-39
Att.: Sr(a). Luciano Paiva

Proposta Nº 18.000-01

Prezado Senhor,

A Suporte Informática atua nos segmentos de software e hardware, agregando um alto valor através da sua equipe profissional altamente especializada e certificada. Provendo soluções tecnológicas alinhadas às necessidades do mercado, buscando aperfeiçoar o desempenho organizacional, reduzindo os custos totais e otimizando o retorno sobre o investimento das empresas em todo território nacional, quaisquer que sejam seus tamanhos e segmentos.

Antecipadamente agradecemos a oportunidade, encaminhando a seguir nossa proposta, ficando inteiramente à disposição para o esclarecimento de eventuais dúvidas.

Atenciosamente,

Camilo Lima
camilo.lima@suporteinformatica.com

SUPORTE Informática

Av. João de Barros, 1261
Espinheiro – Recife – PE
CEP.52.021-180
Fone 81.3202.9100
Fax 81.3244.9697
Proposta Nº 18.000-01

Proposta 18.000-01

1. Objetivo

Fornecimento de solução de Monitoramento, Detecção, Notificação, Investigação e Resposta a Ataques Cibernéticos, bem como serviços de treinamento, implantação e sustentação da solução pelo período de 24 meses.

2. Proposta Comercial

Item	Descrição	Faixa	Faixa de Subscrição por Ativo	Unidade de Medida	Quantidades a considerar	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	Subscrição de até 1000 ativos monitorados	Ativos monitorados anualmente	994	R$ 843,32	R$ 838.260,08	R$ 1.676.520,16
		Tipo 2	Subscrição de 1001 a 2000 ativos monitorados	Ativos monitorados anualmente	15182	R$ 843,32	R$ 12.803.284,24	R$ 25.606.568,48
		Tipo 3	Subscrição de 2001 a 5000 ativos monitorados	Ativos monitorados anualmente	28292	R$ 843,32	R$ 23.859.209,44	R$ 47.718.418,88
		Tipo 4	Subscrição de 5001 a 8000 ativos monitorados	Ativos monitorados anualmente	30960	R$ 843,32	R$ 26.109.187,20	R$ 52.218.374,40
		Tipo 5	Subscrição de 8001 a 12000 ativos monitorados	Ativos monitorados anualmente	10846	R$ 843,32	R$ 9.146.648,72	R$ 18.293.297,44
		Rede	1 Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	109	R$ 23.308,74	R$ 2.540.652,66	R$ 5.081.305,32
			10 Gbps (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

SUPORTE Informática

Av. João de Barros, 1261
Espinheiro – Recife – PE
CEP.52.021-180
Fone 81.3202.9100
Fax 81.3244.9697
Proposta Nº 18.000-01

4	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Serviços de SOC para até 1000 ativos monitorados	Serviço mensal	1	R$ 15.950,00	R$ 191.400,00	R$ 382.800,00
		Tipo 2	Serviços de SOC para 1001 a 2000 ativos monitorados	Serviço mensal	10	R$ 31.900,00	R$ 3.828.000,00	R$ 7.656.000,00
		Tipo 3	Serviços de SOC para 2001 a 5000 ativos monitorados	Serviço mensal	8	R$ 79.950,00	R$ 7.675.200,00	R$ 15.350.400,00
		Tipo 4	Serviços de SOC para 5001 a 8000 ativos monitorados	Serviço mensal	5	R$ 127.600,00	R$ 7.656.000,00	R$ 15.312.000,00
		Tipo 5	Serviços de SOC para 8001 a 12000 ativos monitorados	Serviço mensal	1	R$ 191.400,00	R$ 2.296.800,00	R$ 4.593.600,00
							R$ 102.981.625,34	**R$ 200.003.250,68**

- Forma de pagamento: 30 dias para cada faturamento.
- Validade da proposta: 90 dias corridos.

3. Observações finais

- Os valores expressos em dólares americanos (US$) serão convertidos em Reais na data efetiva do faturamento, com base na taxa PTAX;
- Uma vez colocado o pedido, o mesmo não poderá ser objeto de desistência por parte do cliente final. Para os pedidos de software, as licenças são intransferíveis e emitidas para uso exclusivo do cliente final.
- Essa proposta não contempla qualquer tipo de serviço (instalação, configuração, e etc.) além dos expressamente descritos;
- O prazo de entrega dos produtos é de, aproximadamente, 45 dias;
- Esta proposta contempla suporte e garantias prestadas pelo próprio fabricante aos produtos ofertados pelo período e modalidades descritas acima;
- O(s) produto(s) será(ão) faturado(s) pela Suporte Informática Soluções LTDA;
- O(s) serviço(s) será(ão) faturado(s) pela Suporte Informática Soluções LTDA.
- Os valores descritos na proposta já incluem as tarifas referentes a impostos e frete.

Recife, 24 de agosto de 2023.
Ref. Proposta: 18.000-01

Suporte Informática Soluções LTDA.
CNPJ 07.880.897/0001-34

Tribunal Regional do Trabalho da 2° Região - TRT2
CNPJ 03.241.738/0001-39

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

Anexo A - Especificação Técnica

1. Objeto

Ata de registros de preços visando a contratação de solução de Monitoramento, Detecção, Notificação, Investigação e Resposta a Ataques Cibernéticos, bem como serviços de treinamento, implantação e sustentação da solução proposta, pelo período de 24 meses, conforme a tabela seguinte:

Item	Descrição	Tipo de Faixa	Faixa de Subscrição	Unidade de Medida
01	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos	Ativo monitorado anualmente
		Tipo 2	De 1001 a 2000 ativos	Ativo monitorado anualmente
		Tipo 3	De 2001 a 5000 ativos	Ativo monitorado anualmente
		Tipo 4	De 5001 a 8000 ativos	Ativo monitorado anualmente
		Tipo 5	De 8001 a 12000 ativos	Ativo monitorado anualmente
		Rede	1Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente
			10Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente
02	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes	Serviço pontual, por turma de treinamento
03	Serviço de implantação da solução proposta	-	Serviço de implantação e ativação da solução e seus componentes	Serviço pontual
04	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos monitorados	Serviço mensal
		Tipo 2	De 1001 a 2000 ativos monitorados	Serviço mensal
		Tipo 3	De 2001 a 5000 ativos monitorados	Serviço mensal
		Tipo 4	De 5001 a 8000 ativos monitorados	Serviço mensal
		Tipo 5	De 8001 a 12000 ativos monitorados	Serviço mensal

1.1 Definições para fins desta especificação:

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

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

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

1.1.2 Define-se “Tráfego diário monitorado” como sendo volume médio diário do tráfego da rede interna (em Gbps - Gigabits por segundo) que deverá ser monitorado pela solução proposta.

1.1.3 Para os dados do ambiente da CONTRATANTE que serão coletados pela solução proposta, compreende-se as seguintes definições:

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

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

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

1.2 Para soluções cuja subscrição seja baseada em EPS (Eventos Por Segundo), a CONTRATADA deve licenciar a solução para uma quantidade mínima de EPS suficiente para atender 100% dos ativos da CONTRATANTE e garantir a escalabilidade da solução, independentemente da quantidade de EPS gerados pelos ativos monitorados, observando-se o limite de licenciamento mínimo de EPS igual a 8 vezes a referida quantidade de ativos monitorados.

1.2.1 A CONTRATADA deverá aferir mensalmente o consumo de EPS e provar que a quantidade ofertada está comportando a quantidade de eventos ingerida pela solução, realizando correções no quantitativo se necessário, sem custo para a CONTRATANTE.

1.3 Para soluções cuja subscrição seja baseada em volumetria de logs, a CONTRATADA deve licenciar a solução para uma quantidade mínima de Área de Armazenamento em modalidade SaaS, suficiente para atender 100% dos ativos da CONTRATANTE e garantir a escalabilidade da solução, independentemente do volume de logs, dados de telemetria e de rede gerados pelos ativos monitorados, observando-se o limite de licenciamento mínimo de GB (gigabytes) igual a 2 vezes a referida quantidade de ativos monitorados e a retenção dos logs estipulada no item 2.8.

1.3.1 A CONTRATADA deverá aferir mensalmente a volumetria e provar que a quantidade ofertada está comportando a quantidade de eventos ingerida pela solução, realizando correções no quantitativo se necessário, sem custo para a CONTRATANTE.

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

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

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

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

2.3. A CONTRATADA deve prover, ao ambiente, soluções de segurança cibernética que permitam a visibilidade de logs, dados de telemetria, tráfego de rede e de informações correlatas, capazes de identificar eventos suspeitos ou incomuns que possam comprometer os serviços tecnológicos 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.

2.4. Para a prestação desse serviço, deve ser utilizada uma solução de Monitoramento, Detecção, Notificação, Investigação e Resposta a Ataques Cibernéticos, com capacidades de Coleta e Correlacionamento de Logs e Mecanismos de Detecção de Comportamento Anômalo de Usuários e Aplicações (UEBA – User and Entity

Behavior Analytics). Neste caso, entende-se por "Aplicações" como sendo os softwares instalados nos ativos monitorados.

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

2.5.1. Analisar, classificar, categorizar, correlacionar e notificar os eventos e incidentes classificados como ameaças à segurança cibernética, ou que sejam considerados relevantes de acordo com diretrizes estabelecidas pela CONTRATANTE;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.5.4.1.1.3. Gerar relatórios mensais do acordo de nível de serviço (SLA – Service Level Agreement) dos alertas, incidentes e chamados.

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

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

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

2.6.1. O fabricante da solução proposta para monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos deve ser atestado SOC 2 Type II;

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

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

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

2.6.5. Coletores de tráfego de rede: o software dos coletores de tráfego de rede, bem como os respectivos sistemas operacionais, sistemas gerenciadores de banco de dados, entre outros componentes (de software ou hardware) eventualmente necessários para a coleta e centralização de dados de tráfego de rede deverão ser fornecidos pela CONTRATADA, podendo ser de fabricantes distintos da solução, devendo ser compatíveis com a infraestrutura da CONTRATANTE (interfaces de rede de 1Gbps e 10Gbps).

2.6.5.1. O tráfego de rede deverá ser mensurado de acordo com o ambiente da CONTRATANTE.

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

2.6.6.1. 12 vCPUs;

2.6.6.2. 32Gb vRAM;

2.6.6.3. 200GB de espaço em disco.

2.6.7. Caso os recursos em ambiente virtual necessários para o pleno funcionamento da solução extrapolem os recursos disponibilizados pela CONTRATANTE, a CONTRATADA deve demonstrar, por meio de documento técnico do fabricante e/ou de boas práticas, a necessidade de aumento dos recursos, que serão disponibilizados pela CONTRATANTE conforme comprovação apresentada. Caso não haja comprovação, a critério da CONTRATANTE, a CONTRATADA deverá providenciar, sem custos adicionais para a CONTRATANTE, a entrega da infraestrutura (total ou remanescente) e em conformidade com a estrutura computacional da CONTRATANTE.

2.6.8. Agentes: software de baixo consumo de processamento que é instalado nos ativos suportados para centralizar e monitorar os dados de segurança cibernética. O agente oferece visibilidade e detecção de ataques nos endpoints, coletando informações on-line do sistema, incluindo informações básicas de

identificação de ativos, processos em execução, logs e outros dados de telemetria e as enviando de volta à solução para análise.

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

2.6.9.1. Google Chrome;

2.6.9.2. Mozilla Firefox.

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

2.6.10.1. Caso a solução seja composta por diversas ferramentas, a console de gerência principal deve permitir a visibilidade integrada e total do monitoramento, detecção, notificação, investigação e resposta aos ataques cibernéticos detectados e sendo tratados em todo o ambiente computacional.

2.6.10.2. As demais ferramentas podem estar hospedadas em ambiente provisionado pela CONTRATADA, sem custos adicionais para a CONTRATANTE.

2.6.10.3. Os ambientes utilizados pela solução (incluindo do fabricante) devem possuir, ao menos, uma cópia das informações localizadas no Brasil.

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

2.7. A solução deve ser fornecida dimensionada para a quantidade de ativos a serem monitorados ou para a quantidade de eventos por segundo (conforme item 1.2) ou para o volume de armazenamento de logs em ambiente SaaS (conforme item 1.3) de forma a abranger o escopo completo de ativos da CONTRATANTE, conforme conceito apresentado nesta especificação técnica. Assim, é obrigatório que a solução cubra 100% do ambiente da CONTRATANTE, incluindo estações de trabalho, notebooks, dispositivos móveis, servidores físicos e virtuais, containers, firewalls, ativos de rede ou qualquer equipamento similar ao listado, e não somente parcialmente, de forma a prover uma visibilidade plena da segurança cibernética do ambiente.

2.7.1. A solução deve suportar picos de EPS (Eventos Por Segundo) ou GB (gigabytes) acima do licenciado em até 30%.

2.7.1.1. Caso os picos de EPS ou GB ultrapassem o limite de 30%, a solução não deve descartar os eventos de forma que sejam processados posteriormente.

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.

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

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

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

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

2.9.4. Adicionalmente, para ambientes com Microsoft Active Directory:

2.9.4.1. Movimentação lateral com uso de credenciais de domínio;

2.9.4.2. Ataques de força bruta em contas de domínio;

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

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

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

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

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

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

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

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

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

2.13.1. Firewalls;

2.13.2. Web Application Firewalls;

2.13.3. IPS (Intrusion Prevention System) / IDS (Intrusion Detection System);

2.13.4. Web filtering;

2.13.5. Antivírus;

2.13.6. Microsoft Active Directory;

2.13.7. Open LDAP;

2.13.8. IAM (Identity and Access Management) / PAM (Privileged Access Management);

2.13.9. Servidores HTTP (HTTP Servers);

2.13.10. Balanceadores de Carga (Load Balancers);

2.13.11. DNS;

2.13.12. DHCP;

2.13.13. ELK Stack;

2.13.14. Sistemas Operacionais.

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

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

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

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

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

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

2.16. Para detectar incidentes, a solução também deverá suportar o recebimento e processamento de eventos de tráfego de rede e, opcionalmente, flow de rede, provendo as seguintes informações, no mínimo:

2.16.1. Sistemas com maior atividade baseada em volume de tráfego;

2.16.2. Principais aplicações e protocolos trafegados, baseado em volume de dados enviados e recebidos entre endpoints da rede;

2.16.3. Atividades de rede baseada em porta de destino e endereços de origem e destino;

2.16.4. Relação dos usuários ou ativos que mais consomem banda de rede, baseado em volume de tráfego.

2.16.5. Servidores DNS em uso;

2.16.6. Relação das principais aplicações em uso na rede;

2.16.7. Identificação de picos de consumo de banda de acesso à rede;

2.16.8. Relação de dispositivos, servidores e serviços que operam na rede.

2.17. A solução deve implementar a coleta e análise de diferentes fontes de eventos. A coleta deve ser realizada para logs, dados de telemetria e/ou de rede, devendo ser possível coletar e analisar eventos das seguintes soluções presentes atualmente de forma predominante no ambiente da CONTRATANTE:

2.17.1. De forma nativa (sem a necessidade de customização de parsers):

2.17.1.1. Checkpoint para proteção de perímetro (Firewall);

2.17.1.2. Fortinet FortiGate para proteção de perímetro (Firewall);

2.17.1.3. Forcepoint para proteção de perímetro (Firewall);

2.17.1.4. Microsoft Active Directory para serviços de diretório.

2.17.2. De forma nativa (sem a necessidade de customização de parsers) ou não:

2.17.2.1. Open LDAP para serviços de diretório;

2.17.2.2. OpenVPN;

2.17.2.3. Citrix;

2.17.2.4. RDP e RDPWeb;

2.17.2.5. Senha Segura para serviços de gerenciamento de acesso privilegiado;

2.17.2.6. Cyberark para serviços de gerenciamento de acesso privilegiado

2.17.2.7. Hashicorp Vault e Hashicorp Boundary para serviços de gerenciamento de acesso privilegiado;

2.17.2.8. Keycloak para gerenciamento de identidade e acesso;

2.17.2.9. midPoint para segurança de identidades (identity security);

2.17.2.10. ForeScout CounterACT (eyeSight e eyeControl) para serviços de NAC (Network Access Control);

2.17.2.11. Loqed;

2.17.2.12. Varonis;

2.17.2.13. IBM Spectrum Protect Plus para proteção de dados;

2.17.2.14. Kaspersky para proteção de endpoint;

2.17.2.15. Blackberry Cylance para proteção de endpoint.

2.17.2.16. Check Point Harmony para proteção de endpoint;

2.17.2.17. Tenable One para gerenciamento de exposição (exposure management platform);

2.17.2.18. Tenable.ep / Nessus para gerenciamento de vulnerabilidades;

2.17.2.19. Tenable.ad para proteção do Active Directory;

2.17.2.20. Trivy para varredura de vulnerabilidades;

2.17.2.21. VMware/vCenter para virtualização de máquinas;

2.17.2.22. VMware/Horizon para virtualização de estações de trabalho;

2.17.2.23. Hyper-V para virtualização de máquinas;

2.17.2.24. Ovirt para virtualização de máquinas;

2.17.2.25. Docker e Kubernetes;
2.17.2.26. Apache HTTP Server;
2.17.2.27. HAProxy;
2.17.2.28. Ingress;
2.17.2.29. Nginx;
2.17.2.30. Switches Cisco MDS;
2.17.2.31. Switches H3C;
2.17.2.32. Switches HP;
2.17.2.33. Switches Huawei;
2.17.2.34. Roteadores Cisco;
2.17.2.35. Roteadores Juniper;
2.17.2.36. Roteadores MikroTik;
2.17.2.37. Access Points Aruba;
2.17.2.38. Access Points Ruckus;
2.17.2.39. Controladoras Virtuais Aruba;
2.17.2.40. Bacula para serviços de backup;
2.17.2.41. Commvault (software de backup);
2.17.2.42. Veeam (software de backup);
2.17.2.43. Storage Huawei;
2.17.2.44. Storage IBM;
2.17.2.45. TSM Server IBM Spectrum Protect para serviços de backup;
2.17.2.46. Dell EMC Data Domain;
2.17.2.47. Dell EMC Isilon.

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

2.18.1. De forma nativa (sem a necessidade de customização de parsers):

2.18.1.1. AWS CloudTrail, via SQS ou API;
2.18.1.2. Google Cloud Platform, via API;
2.18.1.3. Google Workspace/Google Apps, via API;
2.18.1.4. Microsoft Office 365, via API.

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

2.19.1. De forma nativa (sem a necessidade de customização de parsers):

2.19.1.1. Windows 7;
2.19.1.2. Windows 8.1;
2.19.1.3. Windows 10;
2.19.1.4. Windows 11;
2.19.1.5. Windows Server 2008 R2;
2.19.1.6. Windows Server 2012;
2.19.1.7. Windows Server 2012 R2;

2.19.1.8. Windows Server 2016;
2.19.1.9. Windows Server 2019;
2.19.1.10. Windows Server 2022;
2.19.1.11. Red Hat Enterprise Linux / Oracle Enterprise Linux / Rocky Linux 8.4;
2.19.1.12. Red Hat Enterprise Linux / Oracle Enterprise Linux / Rocky Linux 8.5;
2.19.1.13. Red Hat Enterprise Linux / Oracle Enterprise Linux / Rocky Linux 9.0;
2.19.1.14. Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 7;
2.19.1.15. Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 8.0;
2.19.1.16. Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 8.1;
2.19.1.17. Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 8.2;
2.19.1.18. Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 8.3;
2.19.1.19. Amazon Linux;
2.19.1.20. Debian Linux;
2.19.1.21. Ubuntu Linux.

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

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

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

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

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

2.24.1. Requisição a domínio suspeito;
2.24.2. Execução de processos suspeitos;
2.24.3. Requisição de dados de registro do sistema de nome de domínio (DNS);
2.24.4. Comunicação com servidores Command & Control;
2.24.5. Tentativa de desabilitar recursos de Sysmon;
2.24.6. Execução de processos LSASS (Local Security Authority Subsystem Service) com objetivo de detectar dump de memória para acessar possíveis credenciais armazenadas;
2.24.7. Detecção do uso de msrsc.exe - Microsoft Terminal Services Client;
2.24.8. Detecção do uso de comandos estruturados consistentes pela ferramenta Impacket e Impacket-Obfuscation;
2.24.9. Detecção de atividade de linha de comando da execução da função GetSystem, usada pelo Meterpreter ou Cobalt Strike;
2.24.10. Detecção de execução do Mimikatz e variações;
2.24.11. Detecção de processos que utilizam resultados do comando wget via Bash, Perl e Python;
2.24.12. Detecção de tentativas de criação de reverse shells para Command & Control.

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

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

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

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

2.29. A solução deve permitir o enriquecimento de dados relacionados a endereços IPs, buscando informações adicionais em fontes de OSINT (Open Source Intelligence).

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

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

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

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

2.31. 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.

2.31.1. Honeypot: máquina projetada para capturar informações sobre tentativas de acesso e exploração. Deve permitir a instalação de, ao menos, 05 (cinco) máquinas no ambiente;

2.31.1.1. Os honeypots devem ser fornecidos em formato OVA – virtual appliance.

2.31.2. Honey Credential: configuração de um conjunto de credenciais falsas na memória de um ativo;

2.31.3. Honey User: usuário falso que não está associado a uma pessoa real dentro da organização e, portanto, nunca deve ser acessado – monitoramento do Microsoft Active Directory;

2.31.4. Honey File: arquivo falso localizado em um compartilhamento de arquivos de rede.

2.31.5. A solução deve ser capaz de detectar o vetor de entrada da ameaça na rede, identificar o caminho utilizado pelo invasor até o ativo, credencial, usuário ou arquivo específico e apresentar as vulnerabilidades exploradas no ativo (quando for o caso).

2.32. Quando a solução não possuir capacidade de "deception", a capacidade de "Breach and Attack Simulation" (BAS) pode ser apresentada, com os seguintes critérios mínimos:

2.32.1. Caso a funcionalidade seja oferecida como um serviço, as licenças necessárias para a sua execução devem ser baseadas em vetores ou agentes, sendo um para cada tipologia: infraestrutura, network e e-mail; os 03 (três) tipos de licenças devem estar incluídas sem custos adicionais para a CONTRATANTE;

2.32.2. Deve ser executado, pelo menos, mensalmente;

2.32.3. Deve ser executado de forma automatizada, simulando ataques reais, mas que não coloquem em risco o ambiente computacional da CONTRATANTE;

2.32.4. As simulações devem utilizar diferentes vetores de ataque;

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

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

2.34. A solução deve possuir as funcionalidades de:

2.34.1. Monitoramento de comportamento (behavior monitor);

2.34.2. Controle de aplicação;

2.34.3. Monitoramento de eventos;

2.34.4. Auditoria de alterações no sistema;

2.34.5. Resposta automatizada a ameaças com a possibilidade de, mas não se limitando a, executar as ações propostas no item 2.62.

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

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

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

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

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

2.39.1. Segura e criptografada;

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

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

2.41. A solução deve monitorar, no mínimo:

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

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

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

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

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

2.41.6. Exploração mitigada (exploit mitigated);

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

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

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

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

2.41.11. Movimentação lateral com credenciais locais (lateral movement – local credentials);

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

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

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

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

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

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

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

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

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

2.45.2. Identificar quais eventos devem gerar alertas;

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

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

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

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

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

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

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

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

2.51.1. Crítico;

2.51.2. Alto;

2.51.3. Médio;

2.51.4. Baixo.

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

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

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

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

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

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

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

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

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

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

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

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

2.59. Para realizar o monitoramento do tráfego de rede, a solução deve ser do tipo passiva e ser instalada em modo off-line na rede, ou seja, não ser um ativo em linha ou permitir o envio de logs e/ou dados de telemetria/de rede através de integração.

2.60. A solução deve ser capaz de inspecionar o tráfego de rede baseado no volume de tráfego em Gbps da CONTRATANTE e realizar a análise dos dados coletados.

2.61. A solução deve, junto com o monitoramento do tráfego de rede (ou por meio de agentes), implementar regras de detecção de intrusão para correlacionar e trazer as informações sobre possíveis anomalias e ataques no nível de rede.

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

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

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

2.62.1. Envio de e-mails.

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

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

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

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

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

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

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

2.62.4.1. Ser totalmente automática;

2.62.4.2. Aguardar uma interação humana para ser realizada.

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

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

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

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

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

2.67.1. As notificações podem ser nativas ou, caso necessário, serem desenvolvidas pela CONTRATADA, sem custo para a CONTRATANTE, para viabilizar sua integração.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.88.4.1. Alertas e incidentes mais frequentes;

2.88.4.2. Nível de risco do ambiente;

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

2.88.4.4. Top 10 (dez) ativos com incidentes;

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

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

2.88.4.7. Ativos e contas descobertas;

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

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

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

2.88.6.1. Planilha: CSV e/ou Excel;

2.88.6.2. Texto: HTML e/ou PDF.

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

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

2.91. A solução deve permitir habilitar ou desabilitar um determinado usuário sem excluí-lo do console.

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

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

MONITORAMENTO DEEP/DARK WEB (MONITORAMENTO DE MARCA E AMEAÇAS GLOBAIS)

2.94. A CONTRATADA deverá realizar serviços de monitoramento de Deep/Dark Web por meio da solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos ofertada (nativamente ou por meio de solução complementar). Os serviços e a respectiva solução utilizada para a realização do monitoramento de Deep/Dark Web devem atender às seguintes especificações mínimas:

2.94.1. A solução de monitoramento de Deep/Dark Web deve ter como objetivo principal o rastreamento de salas, blogs, fóruns e sites na Deep/Dark Web para identificar informações relativas à CONTRATANTE e seus colaboradores como: credenciais roubadas e outros vazamentos de informações pessoais identificáveis.

2.94.2. A solução de monitoramento de Deep/Dark Web deve estar licenciada para monitorar até 06 (seis) domínios DNS da CONTRATANTE e uma quantidade de no mínimo 500 (quinhentos) termos por domínio.

2.94.3. O serviço de monitoramento de Deep/Dark Web deve ser prestado no regime 24x7 (vinte e quatro horas por dia, sete dias por semana).

2.94.4. A solução de monitoramento de Deep/Dark Web deve realizar buscas, no mínimo:

2.94.4.1. Na Darknet;

2.94.4.2. Em plataformas de compartilhamento de documentos;

2.94.4.3. Pelas seguintes categorias:

2.94.4.3.1. Por Bucket: Darknet TOR, Whois, Usenet, Leaks, Bot Logs, Wikileaks, Public Leaks, Dumpster, Sci-Hub;

2.94.4.3.2. Por Site Público: .com, .org, .net, .info, .eu.

2.94.4.3.3. Por Geolocalização.

2.94.5. A solução de monitoramento de Deep/Dark Web deve permitir a busca de termos considerando, no mínimo, as seguintes categorias:

2.94.5.1. Domínio DNS;

2.94.5.2. Endereço de e-mail;

2.94.5.3. Endereço Bitcoin;

2.94.5.4. Endereço Ethereum;

2.94.5.5. Endereço MAC;

2.94.5.6. Hash IPFS;

2.94.5.7. IBAN (Número de Conta Bancária Internacional);

2.94.5.8. IP e CIDR;

2.94.5.9. Número de telefone;

2.94.5.10. Número do cartão de crédito;

2.94.5.11. URL.

2.94.6. Deve detectar resultados de itens pesquisa duplicados, apresentando-os de forma consolidada, otimizando a busca por informações relevantes.

2.94.7. A solução de monitoramento de Deep/Dark Web deve ter a capacidade de buscar dados pelo período mínimo de 1 ano.

2.94.8. A solução de monitoramento de Deep/Dark Web deve ter a capacidade de filtrar e classificar os resultados das buscas:

2.94.8.1. Com base na data ou no tempo de publicação das informações encontradas (antigas e novas);

2.94.8.2. Com base nos domínios, e-mails e URLs encontrados;

2.94.8.3. Com base nos resultados mais relevante, menos relevante, mais recente e mais antigo;

2.94.8.4. Com capacidade de combinar ou excluir termos de pesquisa a fim de encontrar com eficiência informações relevantes no banco de dados.

2.94.9. A solução de monitoramento de Deep/Dark Web deve ter a capacidade de manter históricos de resultados de busca.

2.94.10. A solução de monitoramento de Deep/Dark Web deve contemplar os seguintes itens:

2.94.10.1. Monitoramento de atividades na Deep/Dark Web relacionadas às informações sobre domínios, URLs, IPs, hashes, credenciais, e-mails e informações sensíveis da CONTRATANTE.

2.94.10.2. Amplitude de rastreamento contemplando dados e informações disponibilizadas na Deep/Dark Web como:

2.94.10.2.1. Monitoramento das credenciais de funcionários em listas e bases de dados de credenciais vazadas na Deep/Dark Web, marketplaces, entre outros;

2.94.10.2.2. Monitoramento do Pastebin, incluindo posts deletados e outros sites, buscando por referências sobre a empresa, domínios ou endereços IP;

2.94.10.2.3. Monitoramento de documentos vazados ou roubados da empresa em páginas da Deep/Dark Web e fóruns hackers;

2.94.10.2.4. Monitoramento de referências aos sistemas em páginas da Deep/Dark Web e fóruns hackers, além de Threat Intelligence e listas de IoC's;

2.94.10.2.5. Busca de informações sobre redes sociais e plataformas de divulgação de vulnerabilidades vazadas na Deep/Dark Web.

2.94.10.3. Deve ser possível encontrar marketplaces, fóruns e agentes de ameaças;

2.94.10.4. Deve ser capaz de realizar avaliação da exposição da marca e vazamentos de informações na Deep/Dark Web;

2.94.10.5. Investigação de origens de vazamentos de, no mínimo:

2.94.10.5.1. Grupos de hackers;

2.94.10.5.2. Ameaças em fóruns;

2.94.10.5.3. Salas de chats reservadas;

2.94.10.5.4. Carteira de bitcoins e endereços;

2.94.10.5.5. Registros históricos.

2.94.10.6. As investigações deverão ser realizadas por uma equipe especializada à medida que informações monitoradas forem identificadas na Deep/Dark Web.

2.94.10.7. Geração e notificação de alertas acompanhados da enumeração das ameaças e riscos relacionados e ações de mitigação sugeridas.

2.95. A solução como um todo, bem como os seus componentes devem contar com garantia e suporte integrais conforme especificado neste documento.

PAGAMENTO

2.96. A emissão do termo de recebimento provisório será feita após a instalação e configuração do console de gerência, dos coletores de logs, dos coletores de tráfego de rede e de agentes em estações de trabalho e em servidores.

2.97. As subscrições deverão ser fornecidas conforme a quantidade de ativos definida pela CONTRATANTE e deverão ser nomeadas (para cada CONTRATANTE). A comprovação do fornecimento se dará através da Nota Fiscal e o pagamento somente será autorizado depois de efetuado o "atesto" pelo servidor competente, condicionado este ato à verificação da conformidade da Nota Fiscal/Fatura apresentada em relação às subscrições efetivamente fornecidas em nome da CONTRATANTE, conforme volumetria mínima prevista.

2.98. A emissão do termo de recebimento definitivo será feita após a verificação do perfeito funcionamento do console de gerência, dos coletores de logs, dos coletores de tráfego de rede, de agentes em estações de trabalho, de agentes em servidores e da integração de todos os componentes.

2.99. A quantidade de agentes a serem considerados em cada tipo de ativo nos termos de recebimento provisório e definitivo deve ser acordada na fase de Planejamento e Projeto (item 4.4.1), não sendo superior a 10% do parque computacional da CONTRATANTE.

2.100. A distribuição dos agentes (no restante do parque computacional) para os outros ativos a serem monitorados será de responsabilidade da CONTRATANTE, sem prejuízo do suporte que a CONTRATADA deve fornecer para a realização dessa etapa.

2.101. O pagamento da subscrição deve ser anual, em parcela única, sendo realizado somente após a emissão do termo de recebimento definitivo.

3. ITEM 2 – Requisitos mínimos de treinamento na solução

3.1. A CONTRATADA deve oferecer treinamento contemplando a perfeita instalação, configuração, operação e utilização da solução contratada.

3.2. O treinamento deverá proporcionar aos participantes condições de:

3.2.1. Compreender a arquitetura da solução;

3.2.2. Identificar e configurar os recursos disponibilizados no produto;

3.2.3. Configurar fontes de eventos;

3.2.4. Instalar e configurar agentes, coletores e outros módulos necessários para o perfeito funcionamento da solução;

3.2.5. Configurar honeypots, quando a solução tiver essa capacidade;

3.2.6. Configurar serviço de Breach and Attack Simulation (item 2.32), quando a solução tiver essa capacidade;

3.2.7. Configurar regras;

3.2.8. Configurar alertas;

3.2.9. Configurar playbooks;

3.2.10. Investigar incidentes;

3.2.11. Pesquisar em logs;

3.2.12. Criar dashboards;

3.2.13. Criar relatórios e agendamento de relatórios;

3.2.14. Gerenciar usuários, funções e permissões;

3.2.15. Identificar as possíveis causas de problemas e atuar na sua resolução;

3.2.16. Monitorar o funcionamento da solução (analisar mensagens de log, efetuar acesso remoto, atualizar os componentes que fazem parte da solução, administração e utilização dos recursos disponibilizados);

3.2.17. Conhecer os procedimentos para abertura de chamados técnicos;

3.2.18. Conhecer os procedimentos para obtenção de atualizações de software.

3.3. Devem ser fornecidos todos os recursos necessários para a realização do treinamento (material didático, equipamentos, instrutor, etc.). Os treinamentos serão realizados nas dependências da CONTRATANTE ou na modalidade EAD, a critério da CONTRATANTE.

3.4. O treinamento deve ser ministrado por pessoa certificada na solução.

3.5. O treinamento deve ser o treinamento oficial do fabricante ou com material oficial do fabricante.

3.6. O material didático e demais documentações deverão ser fornecidos, preferencialmente, em Português (Brasil). Em caso de não disponibilidade dessa versão, a mesma deverá ser disponibilizada em Inglês.

3.7. A CONTRATADA deverá apresentar, juntamente à documentação técnica, a programação, conteúdo programático e carga horária do curso, a fim de serem ajustados às necessidades da CONTRATANTE.

3.8. O treinamento deverá ser ministrado com carga horária mínima de 40 (quarenta) horas, com fornecimento de certificados a todos os participantes, em papel timbrado da empresa, constando: nome do treinando, identificação do treinamento, carga horária, período de ocorrência e conteúdo programático.

3.9. A critério da CONTRATANTE, o treinamento poderá ser dividido em turmas de, no mínimo, 02 (dois) alunos e, no máximo, 08 (oito) alunos.

3.10. O treinamento deverá ser ministrado em horário definido pela CONTRATANTE, em dias úteis.

3.11. O cronograma do treinamento será definido em conjunto com a CONTRATANTE, na fase de Planejamento e Projeto (item 4.4.1).

PAGAMENTO

3.12. A emissão do termo de recebimento provisório do treinamento será feita após a conclusão do treinamento.

3.13. A emissão do termo de recebimento definitivo do treinamento será feita após a avaliação dos participantes, com o preenchimento da Planilha de Avaliação de Treinamento, devendo ser obtida média superior a 70%, caso contrário a CONTRATANTE poderá solicitar a realização de novo treinamento com a reformulação que achar necessária.

3.14. O pagamento do treinamento deve ser realizado em parcela única após a emissão do termo de recebimento definitivo.

4. ITEM 3 – Requisitos mínimos de implantação da solução

4.1. A fase de ativação dos serviços deverá ser conduzida e concluída 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).

4.1.1. A CONTRATADA deve realizar o planejamento, a implantação, configuração e ativação dos serviços e soluções propostas no prazo de até 45 (quarenta e cinco) dias corridos, contados a partir da assinatura do contrato, conforme objetivos, escopo, requisitos, premissas e demais condições elencadas nesta especificação.

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

4.3. Os papéis e responsabilidades das partes nos processos de gestão de segurança cibernética, bem como indicadores necessários para medir e melhorá-los continuamente, serão definidos também com base nos referidos parâmetros (baseline).

4.4. As atividades de implantação e ativação do contrato poderão ocorrer de forma remota e deverão contemplar, no mínimo, as seguintes fases:

4.4.1. Planejamento e Projeto:

4.4.1.1. Reunião de kick-off;

4.4.1.2. Coleta de dados e requisitos complementares;

4.4.1.3. Detalhamento de cronograma;

4.4.1.4. Apresentação de parâmetros (baseline) e adequação de processos de gestão de segurança cibernética.

4.4.2. Implantação, Configuração e Ativação da solução:

4.4.2.1. Instalação e ativação da solução on-line e console de gerência;

4.4.2.2. Instalação e ativação dos agentes, coletores, console de gerência e demais componentes da solução (pertinentes aos ativos monitorados) no ambiente computacional da CONTRATANTE: servidores, estações de trabalho, firewalls, servidores de diretório e cloud;

4.4.2.3. Instalação e ativação dos coletores de logs e dos coletores de tráfego de rede;

4.4.2.4. Configuração e o correto funcionamento da coleta, processamento e correlação de logs de eventos em que a solução possua conectores nativos, ou seja, que não necessitem de customização de parsers para tal funcionamento (os conectores nativos devem contemplar a coleta, processamento e correlação de logs para os ambientes que constam nos itens 2.17.1, 2.18.1 e 2.19.1);

4.4.2.5. Testes e homologação.

4.4.3. Definição de Processos e Outras Configurações:

4.4.3.1. Implementação dos processos e recursos propostos;

4.4.3.2. Desenvolvimento de playbooks de resposta a ataques cibernéticos;

4.4.3.3. Configuração e correto funcionamento da coleta, processamento e correlação de logs de eventos em que haja a necessidade de customização de parsers para tal funcionamento (item 2.17.2).

4.4.3.4. Testes e homologação;

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

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

4.4.3.5.2. Playbooks implementados.

4.4.4. Treinamento de equipes.

4.4.5. Operação, Sustentação e Melhoria Contínua:

4.4.5.1. Sustentação/On-Going;

4.4.5.2. Reunião mensal;

4.4.5.2.1. Relatórios periódicos;

4.4.5.2.2. Acompanhamento de indicadores;

4.4.5.2.3. Melhoria contínua.

4.5. A lista de soluções constantes nos itens 2.13, 2.17, 2.18 e 2.19 não é exaustiva, de forma que, conforme houver evolução do parque tecnológico ao longo do contrato, a CONTRATADA deve, como parte da operação, sustentação e melhoria contínua da solução (item 4.4.5), realizar a configuração para o correto funcionamento de parsing (quando houver), coleta, processamento e correlação de logs de eventos gerados pela novas soluções incluídas/alteradas no ambiente computacional.

RESPONSABILIDADES DA CONTRATADA

4.6. São responsabilidades da CONTRATADA:

4.6.1. Prestar os serviços conforme previsto e delimitados por esta especificação, dentro das normas e especificações técnicas aplicáveis à espécie;

4.6.2. Respeitar as normas e regulamentos da CONTRATANTE, inclusive aqueles relativos ao acesso, permanência e trânsito de pessoas e materiais, no estabelecimento desta, as quais deverão lhe ser fornecidas previamente e por escrito;

4.6.3. Observar integralmente a legislação e normas infralegais aplicáveis aos serviços, inclusive aqueles referentes à segurança cibernética e medicina do trabalho;

4.6.4. Zelar pela disponibilidade da infraestrutura de TI da CONTRATADA durante a realização dos serviços propostos;

4.6.5. Realizar a manutenção de software e hardware de sua propriedade e utilizados para a prestação dos serviços propostos.

4.7. A implantação, configuração, ativação e atualização da solução será de responsabilidade da CONTRATADA, bem como as despesas diretas ou indiretas para a execução das atividades pela sua equipe técnica.

4.8. A instalação e atualização dos softwares nos ativos monitorados (item 1.1.1) poderá ser realizada remotamente, sem causar indisponibilidade do ambiente, devendo ser realizada em horários a serem definidos pela CONTRATANTE.

4.9. O processo de implantação, configuração, ativação e atualização da solução deverá ser realizado por técnicos capacitados da CONTRATADA, acompanhados por servidores da CONTRATANTE.

PAGAMENTO

4.10. A emissão do termo de recebimento provisório será feita após a conclusão da fase de Implantação, Configuração e Ativação da solução (item 4.4.2);

4.11. A emissão do termo de recebimento definitivo será feita após a conclusão da fase de Definição de Processos e Outras Configurações (item 4.4.3);

4.12. O pagamento do serviço de implantação deve ser realizado em parcela única após a emissão do termo de recebimento definitivo.

5. ITEM 4 – Requisitos mínimos do serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos

5.1. Os serviços deverão ser prestados por meio do Centro de Operações de Segurança Cibernética (SOC) da CONTRATADA, em regime 24x7x365, que deverá atender os seguintes requisitos mínimos:

5.1.1. A prestação dos serviços deverá ser feita a partir de Centro de Operações de Segurança Cibernética especializado, sendo remoto às instalações da CONTRATANTE.

5.1.2. A equipe do SOC poderá, a critério da CONTRATADA, ser compartilhada com outros clientes, incluindo outros Órgãos da Justiça do Trabalho, de modo a otimizar os esforços, respeitando a confidencialidade das informações relativas ao objeto deste edital.

5.1.3. A solução contratada deve ter instância própria para a CONTRATANTE, exclusiva e dedicada para cada Tribunal e sem compartilhamento com outros clientes da CONTRATADA.

5.1.4. A CONTRATADA deve indicar, formalmente, quando da assinatura do contrato, PREPOSTO TITULAR e substituto que tenham capacidade gerencial para tratar de todos os assuntos previstos no instrumento contratual e coordenação da equipe para a execução dos serviços contratados.

5.1.5. O PREPOSTO deve, entre outras atividades, promover os contatos com o gestor do contrato bem como deve prestar atendimento aos profissionais em serviço, tais como:

5.1.5.1. Assegurar de que as determinações da CONTRATANTE sejam disseminadas junto aos profissionais alocados com vistas à execução dos serviços contratados;

5.1.5.2. Informar ao gestor do contrato sobre problemas de qualquer natureza que possam impedir o bom andamento dos serviços contratados;

5.1.5.3. Desenvolver atividades administrativas de responsabilidade da CONTRATADA, principalmente quanto ao controle de informações relativas ao seu faturamento mensal e apresentação de documentos quando solicitado;

5.1.5.4. O PREPOSTO não pode ser contabilizado como profissional para execução dos serviços contratados.

5.2. A CONTRATADA deve possuir um "Computer Security Incident Response Team (CSIRT)", ou Grupo de Resposta a Incidentes de Segurança – grupo de pessoas com a responsabilidade de identificar, receber, analisar e investigar as notificações e atividades relacionadas a incidentes de segurança cibernética nos ativos monitorados e orientar a CONTRATANTE quanto ao que deve ser feito para resolver o incidente de segurança cibernética.

5.3. 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.

5.4. Um incidente de segurança é definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação da CONTRATANTE, levando à perda de um ou mais princípios básicos de segurança cibernética: confidencialidade, integridade, disponibilidade ou privacidade.

5.5. O processo de notificação de incidentes de segurança se inicia sempre que um evento adverso for submetido por qualquer ferramenta de segurança, podendo o corpo técnico de segurança desta CONTRATANTE a qualquer momento, abrir um incidente de segurança junto à CONTRATADA.

5.6. A CONTRATANTE deverá ser informada sobre os incidentes detectados através do Portal de Atendimento, e-mail e/ou por telefone, conforme previamente acordado com a CONTRATADA na fase de Planejamento e Projeto (item 4.4.1).

5.7. As solicitações de serviços e as notificações de incidentes de segurança cibernética reportadas pela solução proposta ou pela CONTRATANTE deverão ser registradas no módulo de gestão de incidentes de segurança da solução ofertada (item 2.5.4).

5.8. Todo tipo de comunicação e documentação relacionados aos tratamentos de incidentes devem ser em Português.

OPERAÇÃO E SUSTENTAÇÃO

5.9. Os serviços de operação e sustentação da solução contemplam todas as atividades de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos identificados pela solução ofertada, bem como a sustentação da mesma, mediante a sua operação por parte da CONTRATADA.

5.10. Os seguintes serviços deverão ser realizados pela equipe da CONTRATADA para a operação da solução proposta:

5.10.1. Ativação e configuração dos módulos contratados;

5.10.2. Integração dos componentes contratados com o ambiente da CONTRATANTE;

5.10.3. Gestão do ciclo de vida da solução, contemplando a sua implantação e operação, além da inclusão, alteração e exclusão de ativos monitorados;

5.10.4. Abrir e fazer a triagem de chamados de segurança cibernética;

5.10.5. Fazer primeiro atendimento de reportes de incidentes de segurança cibernética;

5.10.6. Atender incidentes simples, os quais possuem instruções indicadas em playbooks (knowledge Base do ITSM);

5.10.7. Elaborar consultas(queries)/scripts de rastreamento quando necessário e/ou solicitados pela CONTRATANTE;

5.10.8. Elaborar manual de usuário das atividades que se fizerem necessários e/ou solicitados pela CONTRATANTE;

5.10.9. IPs externos deverão ser analisados e contextualizados conforme sua criticidade;

5.10.10. Fazer passagem de turno, acompanhar os incidentes e realizar “follow-ups”, de modo que haja acompanhamento integral dos tickets abertos;

5.10.11. Prestar suporte/apoio ao processo de automação das atividades relacionadas à resposta e tratamento de incidentes cibernéticos;

5.10.12. Desenvolvimento de playbooks de resposta a ataques cibernéticos;

5.10.13. Configuração de fontes de eventos;

5.10.14. Configuração de usuários VIP e usuários de serviço;

5.10.15. Criação de alertas customizados;

5.10.16. Configuração de coletores de eventos;

5.10.17. Configuração de monitoramento de arquivos e diretórios;

5.10.18. Liberação de acesso à solução para usuários autorizados pela CONTRATANTE;

5.10.19. Geração de indicadores de performance (KPI) definidos neste documento e acordados na fase de Planejamento e Projeto (item 4.4.1);

5.10.20. Zelar e empregar todos os esforços necessários para garantir o atendimento ao SLA estabelecido neste termo de referência, tanto que se refere aos serviços quanto às soluções contratadas;

5.10.21. Atualização da solução, quando necessário/aplicável e/ou solicitados pela CONTRATANTE;

5.10.22. Resolução de chamados de suporte junto ao(s) fabricante(s) da solução.

5.11. A equipe da CONTRATADA deve ter, no mínimo, uma pessoa responsável pelos assuntos técnicos (líder técnico) e que será o ponto de contato com a equipe de segurança cibernética da CONTRATANTE. O líder técnico tem, entre outras responsabilidades:

5.11.1. Após a assinatura do contrato, conhecer o parque tecnológico e as atividades em andamento, visando à preparação da equipe que prestará os serviços, conhecer os modelos de serviços realizados, as normas internas, procedimentos de segurança e a definição dos requisitos necessários;

5.11.2. Fazer uma reunião semanal com a equipe da CONTRATANTE para acompanhamento dos resultados (a frequência da reunião poderá ser revista oportunamente, a critério da CONTRATANTE).

5.11.3. Fazer a entrega e apresentação dos relatórios mensais, conforme especificação técnica contida neste documento (item 5.17);

5.11.4. Esclarecer dúvidas em relação às requisições, alertas, incidentes, relatórios, prazos de atendimento e outras atividades de responsabilidade da equipe da CONTRATADA;

5.11.5. Estar disponível por telefone e e-mail, de segunda a sexta-feira, das 09 (nove) às 18 (dezoito) horas e acessível por contato telefônico em qualquer outro horário (incluindo sábados, domingos e feriados).

INTELIGÊNCIA DE AMEAÇAS

5.12. A equipe da CONTRATADA deve prover serviços de pesquisa e desenvolvimento de inteligência (threat intelligence) para proteção contra ataques cibernéticos, sendo responsável por:

5.12.1. Pesquisar novos tipos de ataques, vírus, malwares, botnets, vulnerabilidades e afins com intuito de melhoria contínua de detecção e mitigação destes males dentro dos serviços e ativos de segurança fornecidos pela CONTRATADA;

5.12.2. Criar, em colaboração com a equipe de segurança cibernética da CONTRATANTE, casos de uso (regras) que devem ser implementados na solução fornecida;

5.12.3. Revisar, sempre que necessário e/ou solicitados pela CONTRATANTE, as regras da solução fornecida, realizando as adaptações e evoluções necessárias;

5.12.4. Produzir e entregar informação de inteligência acionável, na forma de procedimentos para triagem de alertas e procedimentos para notificação de incidentes correspondentes às regras da solução ofertada;

5.13. A equipe da CONTRATADA deve fornecer serviço de Password e Credential Assessment (avaliação de credenciais em serviços de diretório e banco de dados):

5.13.1. A solução deve avaliar o nível de dificuldade de quebra de senhas.

5.13.2. A solução deve avaliar possíveis vazamentos de credenciais na Dark/Deep Web.

5.13.3. O serviço deve poder ser executado sob demanda.

5.13.4. O serviço deve ser executado sem que senhas sejam fornecidas.

MONITORAMENTO E DETECÇÃO DE AMEAÇAS E ATAQUES

5.14. A equipe da CONTRATADA deve atuar no monitoramento dos incidentes detectados pela solução e serviços propostos, sendo responsável por:

5.14.1. Monitorar equipamentos e softwares componentes das soluções de segurança da CONTRATANTE, envolvendo identificação, classificação e análise de eventos que possam comprometer a disponibilidade, integridade e confidencialidade dos serviços.

5.14.2. Focar suas ações nos eventos significativos, classificando-os corretamente conforme as categorias abaixo:

5.14.2.1. Informativos: são eventos que não requerem ação, utilizados para verificação de funcionalidades dos ativos monitorados, ou seja, tem por objetivo identificar se as ferramentas e soluções estão tendo o comportamento esperado. São úteis para gerar informações acerca do ambiente monitorado como, por exemplo, quantidade de eventos gerados nas últimas 24 horas.

5.14.2.2. Avisos: são eventos utilizados para classificar comportamentos anômalos comparados à linha de base de operação do ambiente, porém que ainda não gerou impacto ao ambiente da CONTRATANTE como, por exemplo, espera-se que ocorram 10 bloqueios de um determinado hash diariamente e, entretanto, nos últimos 2 dias ocorreram 100 bloqueios, sendo que a ferramenta de antivírus continua bloqueando sem que haja qualquer impacto ou degradação no ambiente.

5.14.2.3. Exceções: são eventos que podem indicar que houve impacto em um ou mais dos pilares da segurança da informação (confidencialidade, integridade e confidencialidade) como, por exemplo, a ferramenta de antivírus não bloqueou a ação de um ransomware e dados da CONTRATANTE foram criptografados. Caso um evento seja classificado como "Exceção", o processo de resposta a incidentes de segurança deve ser iniciado imediatamente.

5.14.3. Comunicar, à equipe de segurança cibernética da CONTRATANTE, as informações iniciais sobre o incidente de segurança e quais serão as linhas de atuação para sua resolução.

5.14.4. Informar à CONTRATANTE, através do Portal de Atendimento, e-mail e/ou por telefone, conforme previamente acordado com a CONTRATADA na fase de Planejamento e Projeto (item 4.4.1), sobre os incidentes detectados.

5.14.5. Emitir relatórios mensais, provendo, no mínimo, as seguintes informações à CONTRATANTE:

5.14.5.1. Alertas e notificações;

5.14.5.2. Quantidade de incidentes por categoria;

5.14.5.3. Quantidade de incidentes por criticidade (severidade);

5.14.5.4. Quantidade de incidentes que geraram crise;

5.14.5.5. Porcentagem dos incidentes originários do monitoramento;

5.14.5.6. Quantidade de incidentes tratados/fechados;

5.14.5.7. Quantidade de incidentes registrados.

5.14.6. Relativo ao monitoramento de Deep/Dark Web, a CONTRATADA deverá prover, no mínimo, os seguintes serviços:

5.14.6.1. Monitoramento e envio de notificações para a equipe técnica da CONTRATANTE contendo os alertas identificados no regime 24x7 (vinte e quatro horas por dia, sete dias por semana);

5.14.6.2. Serviço de investigação pela equipe técnica da CONTRATADA, contendo os alertas identificados e sugestões de mitigação, em regime 8x5 (oito horas por dia, cinco dias por semana);

5.14.6.3. Envio de um relatório ao fim do mês à CONTRATANTE contendo, no mínimo, as informações a seguir:

5.14.6.3.1. Vazamento de dados da CONTRATANTE que foram encontrados na Deep/Dark Web, através do monitoramento de domínios, IPs, e e-mails.

5.14.6.3.2. Descrição do ambiente avaliado;

5.14.6.3.3. Tabela resumo de serviços descobertos, detecções e alertas;

5.14.6.3.4. Descrição detalhada dos alertas;

5.14.6.3.5. Descrição, evidências, screenshots relevantes e recomendações para mitigação dos riscos;

5.14.6.3.6. Testes executados e relatórios técnicos das ferramentas;

5.14.6.3.7. Apresentação técnica dos resultados, incluindo o detalhamento dos eventos identificados.

RESPOSTA E INVESTIGAÇÃO A INCIDENTES CIBERNÉTICOS

5.15. A equipe da CONTRATADA deve atuar no processo de resposta a incidentes detectados pela solução proposta, sendo responsável por:

5.15.1. Analisar, recomendar ações de remediação e contenção e documentar os eventos de segurança que, após analisados, demonstraram ser um ataque ao ambiente da CONTRATANTE, tendo sido categorizados como "Eventos de Exceção" e, portanto, acionado o processo de resposta a incidentes cibernéticos.

5.15.2. Analisar, após um incidente de segurança ser aberto, os logs e artefatos enviados/coletados a fim de, no primeiro instante, identificar as fontes geradoras de tais eventos.

5.15.3. Identificar, uma vez realizadas as análises iniciais do incidente, quais foram os principais vetores de ataque ao ambiente da CONTRATANTE.

5.15.4. Definir, junto à equipe de segurança cibernética da CONTRATANTE, a severidade do incidente de segurança, que será obtida por meio de uma matriz GUT (Gravidade, Urgência e Tendência).

5.15.4.1. A matriz GUT será definida na fase de Planejamento e Projeto (item 4.4.1) pela CONTRATADA em conjunto à equipe de segurança cibernética da CONTRATANTE.

5.15.5. Apoiar a equipe técnica da CONTRATANTE nos processos de mitigação, contenção de ataques e restauração do seu ambiente tecnológico.

5.15.6. Realizar, após análises iniciais do incidente e a definição de severidade, uma análise aprofundada do incidente baseando-se no comportamento do ataque e/ou artefato (malware).

5.15.7. Documentar todo o processo de análise e resultado no módulo de gestão de incidentes de segurança da solução ofertada (item 2.5.4) para que a equipe de segurança cibernética da CONTRATANTE acompanhe os passos para a solução do incidente de segurança.

5.15.8. Definir e documentar, uma vez identificado o comportamento e os principais vetores de ataque, uma estratégia para a mitigação e contenção do ataque em questão e notificá-la à CONTRATANTE.

5.15.8.1. Qualquer tipo de alteração no parque computacional da CONTRATANTE para contenção e mitigação de incidentes de severidade alta ou crítica, deverá ser executada pela própria CONTRATANTE com o suporte da CONTRATADA, que deverá sugerir a melhor maneira de implantar a estratégia definida por ela para a resposta ao ataque, até a efetiva resolução do incidente.

5.15.9. Iniciar, mitigado o incidente de segurança, o processo de compilação de todas e quaisquer evidências e identificação dos serviços afetados. Tais evidências serão utilizadas até a finalização do processo para execução de eventual análise forense do incidente de segurança.

5.15.9.1. A necessidade de análise forense será indicada pela CONTRATANTE, seguindo os seus processos internos de gestão de incidentes de segurança, a serem apresentados na fase de Planejamento e Projeto (item 4.4.1).

5.15.9.2. Os dados coletados devem ser reunidos durante o processo de tratamento de incidente para subsidiar futura e eventual análise forense, seguindo as etapas de preservação, extração, análise e laudo. Tal análise deve ser realizada com o objetivo de identificar pessoas, locais ou eventos, correlacionando todas as informações reunidas e gerando como produto final um laudo sobre o incidente de segurança em questão.

5.15.10. Reconstruir o ataque, caso seja necessário e/ou solicitado pela CONTRATANTE. Esta ação deve ser realizada pela CONTRATADA em ambiente controlado (como um sandbox), utilizando mecanismos de segurança para separar programas em execução, geralmente utilizado em um esforço para mitigar falhas de sistema ou vulnerabilidades de segurança cibernética.

5.15.11. Documentar, no módulo de gestão de incidentes de segurança da solução ofertada (item 2.5.4), as lições aprendidas do incidente de segurança em questão, formando, durante todo o período de vigência do contrato, uma grande base de conhecimento sobre ataques adversos.

5.15.11.1. A solução deve permitir a exportação da base de conhecimentos para formato Word ou PDF.

5.16. O regime de execução dos serviços deve ser 24x7x365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias ao ano).

PAGAMENTO

5.17. A emissão do termo de recebimento provisório será feita após a entrega e apresentação dos relatórios indicados nesta especificação:

5.17.1. Incidentes de segurança cibernética (item 5.14.5);

5.17.2. Deep/Dark Web (item 5.14.6.3);

5.17.3. Breach and Attack Simulation (item 2.32.5), quando a solução tiver essa capacidade;

5.17.4. SLA (itens 5.22.2 e 5.23.8).

5.18. A emissão do termo de recebimento definitivo será feita após a verificação dos serviços prestados e sua aderência às condições estabelecidas nesta especificação.

5.19. O pagamento do serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos deve ser mensal, sendo realizado somente após a emissão do termo de recebimento definitivo, descontadas eventuais glosas do período avaliado, conforme Fator de Desconto (FD) calculado no período (item 5.25 e subitens) e das multas aplicadas, quando houver.

CONFIDENCIALIDADE E DESCARTE DE INFORMAÇÕES

5.20. Confidencialidade:

5.20.1. A CONTRATADA deve ser responsável pelo ciclo de vida das informações coletadas pela solução proposta, atendendo aos critérios definidos pela CONTRATANTE, devendo processar, armazenar e, após o término da sua finalidade, descartar os dados de maneira segura.

5.20.1.1. A CONTRATADA obriga-se a tratar como "segredos comerciais e confidenciais" quaisquer informações, dados, processos, fórmulas, códigos, obtidos em consequência ou por necessidade desta contratação, utilizando-os apenas para as finalidades previstas no contrato, não podendo revelá-los ou facilitar a revelação a terceiros, mediante assinatura dos Termos de Confidencialidade conforme anexos A1 e A2;

5.20.2. Ao final do contrato, o descarte das informações deve ser realizado com o emprego de medidas que impossibilitem a sua reconstrução, de acordo com as necessidades do suporte físico ou digital.

GARANTIA E ACORDO DE NÍVEL DE SERVIÇO

5.21. Da garantia:

5.21.1. A solução como um todo, bem como os seus componentes devem contar com garantia e suporte integrais conforme especificado.

5.21.2. A solução deve contar com garantia integral do fabricante (Garantia Compreensiva) durante toda a vigência do contrato e deve comportar a garantia comumente utilizada pelo comércio e prevista no Código de Defesa do Consumidor acrescida de suporte técnico nos moldes desta especificação.

5.22. Um acordo de nível de serviço (SLA – Service Level Agreement) define os índices a serem atingidos para o cumprimento do conjunto de compromissos acordados entre CONTRATANTE e CONTRATADA.

5.22.1. Tais índices serão medidos e aplicados aos serviços contratados e prestados pela CONTRATADA.

5.22.2. Mensalmente, os dados de nível de serviço devem ser apresentados à CONTRATANTE, incluindo informações sobre ações e necessidades para a correção de desvios, visando atingir, manter e melhorar os níveis desejados.

5.22.3. A abrangência e o nível de detalhamento serão definidos conforme as necessidades identificadas pela CONTRATANTE, podendo sofrer alterações ao longo do tempo, as quais serão encaminhadas à CONTRATADA.

5.22.4. Para a medição dos índices de nível de serviços, serão considerados os seguintes conceitos:

5.22.4.1. Requisição: solicitação da CONTRATANTE para intervenção preventiva ou corretiva no ambiente gerenciado e nos ativos monitorados (item 1.1.1) e previsto no escopo desta proposta. Cada requisição será identificada unicamente por meio de um código e será classificada conforme seu nível de severidade no momento da sua comunicação à CONTRATADA;

5.22.4.2. Incidentes de segurança: conforme definido nos itens 5.3, 5.4 e 5.5.

5.22.4.3. Severidade: nível de prioridade/emergência atribuído ou solicitado para a realização de um atendimento a uma requisição da CONTRATANTE ou dos alertas gerados para o ambiente gerenciado, conforme critérios descritos a seguir. Solicitações de alteração do nível de severidade poderão ser submetidas à CONTRATADA e, em comum acordo, serão prontamente atendidas.

5.22.4.3.1. Severidade crítica: o serviço está totalmente parado ou inoperante;

5.22.4.3.2. Severidade alta: o serviço está ativo mas com inoperância da maioria de suas funcionalidades, causando um impacto negativo no ambiente de produção;

5.22.4.3.3. Severidade média: o serviço está operativo, mas suas funcionalidades são executadas com restrições;

5.22.4.3.4. Severidade baixa: o serviço está operativo e a falha não compromete suas funcionalidades ou questões não tratadas pela documentação;

5.22.4.3.5. Severidade agendado: o atendimento está relacionado apenas a esclarecimentos de dúvidas ou necessidade de informações;

5.22.4.4. Triagem: notificação, da CONTRATADA para a CONTRATANTE, de que está ciente da requisição ou do incidente, conforme itens 5.14.3 e 5.14.4.

5.22.4.5. Resolução: comunicação, da CONTRATADA para a CONTRATANTE, das ações INICIAIS (podendo incluir soluções paliativas enquanto a CONTRATADA busca a solução definitiva para o incidente ou chamado) a serem executadas para resolução da requisição ou do incidente de segurança, conforme item 5.15.8 e subitens.

5.22.4.5.1. A CONTRATADA deve fornecer, em até 48h, o restante das ações (contendo a resolução paliativa ou definitiva) a serem executadas para a resolução do incidente ou chamado.

5.22.4.5.2. Caso seja fornecida uma solução paliativa, a CONTRATADA deve atuar proativamente na busca de uma solução definitiva, fornecendo o acompanhamento e suporte necessários para a CONTRATANTE, inclusive sugerindo a melhor maneira de implantar a estratégia definida por ela para a resposta ao ataque, até a efetiva resolução do incidente ou chamado.

5.22.4.5.3. Devido à natureza dos incidentes de segurança cibernética, a sua efetiva contenção e remediação não contarão para contagem dos tempos de SLA, não eximindo a CONTRATADA de registrar esses tempos no módulo de gestão de incidentes de segurança da solução e ITSM integrado.

5.22.5. Os seguintes SLAs devem ser cumpridos:

Atividade	SLA de atendimento
Triagem da requisição/incidente de segurança[1]	Em até 30 (trinta) minutos
Requisição/Incidentes de severidade crítica	Atuação em até 15 (quinze) minutos e resolução[2] em até 01 (uma) hora.
Requisição/Incidentes de severidade alta	Atuação em até 01 (uma) hora e resolução em até 02 (duas) horas.
Requisição/Incidentes de severidade	Atuação em até 02 (duas) horas e resolução em até 04 (quatro) horas.

[1] Pode ser considerado como o Tempo Médio de Detecção (Mean Time To Detect - MTTD)

[2] Para as atividades de Requisição/Incidentes: pode ser considerado como o Tempo Médio de Resposta (Mean Time To Respond - MTTR)

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

média	
Requisição/Incidentes de severidade baixa	Atuação em até 04 (quatro) horas e resolução em até 12 (doze) horas.
Requisição de severidade agendado	Atuação em até 12 (doze) horas e resolução em até 24 (vinte e quatro) horas.

SUPORTE TÉCNICO

5.23. Suporte Técnico:

5.23.1. A abertura de chamados pela CONTRATANTE deve poder ser efetuada:

5.23.1.1. Pela plataforma web, em sistema de atendimento da CONTRATADA;

5.23.1.2. Pelo envio de mensagem de correio eletrônico;

5.23.1.3. Por meio do módulo de gestão de incidentes de segurança da solução ofertada (item 2.5.4);

5.23.1.4. Por telefone.

5.23.2. O atendimento aos chamados deve estar disponível em regime 24x7x365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias ao ano), conforme SLA apresentado (item 5.22.5).

5.23.3. Todo tipo de comunicação e documentação relacionados aos atendimento de chamados devem ser em Português.

5.23.4. A assistência técnica em garantia deve assegurar o fornecimento de acesso irrestrito (24 horas por dia, 07 dias da semana) da CONTRATANTE à área de suporte do fabricante, especialmente ao endereço eletrônico (web site) e a toda a documentação técnica pertinente (guias de instalação e configuração atualizados, FAQ's, bases de conhecimento e bases de soluções, com pesquisa efetuada através de ferramentas de busca).

5.23.5. O suporte técnico do fabricante deverá ser prestado em caso de falhas, dúvidas e/ou esclarecimentos de qualquer um dos produtos, módulos e programas referentes às soluções de software e hardware (inclusive virtual) dos produtos.

5.23.6. Os serviços de suporte 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, entre outros.

5.23.7. A CONTRATADA deve fornecer, mensalmente, relatório oriundo da ferramenta de ITSM (conforme item 2.5.4.1) indicando os SLAs de cada chamado e incidente registrado na solução.

5.23.8. Para a aferição e a avaliação dos níveis de serviço, a CONTRATADA deve fornecer, mensalmente, relatório gerencial de serviços, apresentando-o à CONTRATANTE até o quinto dia útil do mês subsequente ao da prestação do serviço, sendo que devem constar, entre outras informações, os indicadores/metas de níveis de serviço alcançados conforme item 5.22.5, recomendações técnicas, as solicitações de abonos com justificativa e demais informações relevantes para a gestão contratual, em conformidade aos acordos realizados na fase de Planejamento e Projeto (item 4.4.1).

PENALIDADES

5.1. A CONTRATADA está sujeita às seguintes penalidades, desde que não apresente justificativa fundamentada e aceita pela CONTRATANTE, isolada ou cumulativamente:

5.1.1. Advertência;

5.1.2. Multa de 0,5% (cinco décimos por cento) do valor do contrato caso a CONTRATADA apresente os documentos comprobatórios da qualificação dos profissionais alocados na prestação dos serviços, além das certificações requeridas (item 5.31 e subitens) em prazo superior a 20 dias úteis até o limite de 30 dias úteis. Ultrapassado esse limite, além da multa, ensejará a inexecução parcial ou total do objeto;

5.1.3. Multa de 1% (um por cento) do valor do contrato caso a disponibilidade de toda a infraestrutura necessária à prestação dos serviços tenha valor apurado de 99% (noventa e nove por cento) por mês até o limite de 95% (noventa e cinco por cento) de disponibilidade. Ultrapassado esse limite, além da multa, ensejará a inexecução parcial ou total do objeto. A medição da disponibilidade deve considerar o período compreendido entre o primeiro e o último dia de cada mês.

5.1.4. Multa de 0,5% (cinco décimos por cento) do valor do contrato, para cada indicador de nível de serviço (item 5.25.9) que apresente discrepância superior a 50% (cinquenta por cento) até o limite de 100% (cem por cento). Ultrapassado esse limite, além da multa, ensejará a inexecução parcial ou total do objeto.

5.1.5. Multa de 0,5% (cinco décimos por cento) do valor do contrato, caso a CONTRATADA apresente discrepância superior a 20% (vinte por cento) em relação à meta prevista para mais de 03 (três) indicadores de nível de serviço (item 5.25.9), até o limite de 05 (cinco indicadores). Ultrapassado esse limite, além da multa, ensejará a inexecução parcial ou total do objeto.

5.1.6. Multa de 1% (um por cento) do valor do contrato, caso haja execução de procedimentos, intencionais ou não, que burlem ou prejudiquem o atingimento de metas de nível de serviço. Em caso de reincidência, ensejará a inexecução parcial ou total do contrato;

5.1.7. Multa de 1% (um por cento) do valor do contrato, para cada indicador/meta de níveis de serviço que tenha sido objeto de tentativa de manipulação ou descaracterização pela CONTRATADA. Em caso de reincidência, ensejará a inexecução parcial ou total do contrato;

5.1.8. Multa de 0,5% (cinco décimos por cento) do valor do contrato para cada ocorrência de descumprimento de obrigações contratuais que não sejam relacionadas ao atingimento das metas estabelecidas para os indicadores de nível de serviço (item 5.25.9);

5.1.9. Multa de 30% (trinta por cento) do valor contratado, em caso de inexecução total ou parcial do objeto, sem prejuízo da responsabilidade civil e criminal; e suspensão, pelo prazo de até 02 (dois) anos, do direito de licitar e contratar com a CONTRATANTE;

INDICADORES DE DESEMPENHO E GLOSAS

5.2. Glosa quando a CONTRATADA não produzir os resultados, ou não executar com a qualidade mínima exigida as atividades contratadas, conforme disposto nos indicadores de níveis de serviço.

5.2.1. Para fins de faturamento, o valor mensal da prestação do serviço será ponderado em função do desempenho mensal alcançado nele. Na medição, será apurado o afastamento dos indicadores de nível de serviço em relação às metas estabelecidas em contrato, aplicando-se um Fator de Desconto (FD);

5.2.2. Nos casos em que o afastamento ensejar o desempenho abaixo da meta exigida, o valor do afastamento será utilizado para abater valores financeiros dos preços previstos em contrato;

5.2.3. Os Fatores de Desconto (FD) serão calculados com base nos resultados alcançados nos indicadores de nível de serviço, previstos nesta especificação técnica (item 5.25.9);

5.2.3.1. Haverá uma tolerância de 5% em relação à meta para a aplicabilidade do fator de desconto, ou seja, caso o índice mensurado ultrapasse a tolerância, o FD será calculado conforme o item 5.25.6.

5.2.4. No cálculo do FD está previsto uma ponderação para cada indicador de nível de serviço, denominada de Fator de Impacto no Serviço (FIS), com o objetivo de adequar os descontos ao grau de importância daquele indicador no contexto do serviço;

5.2.4.1. O FD de cada indicador será limitado à porcentagem representada pelo FIS aplicada ao valor mensal da prestação do serviço.

5.2.5. O FIS será utilizado nas situações em que a meta exigida para o indicador não for efetivamente atingida. Nos casos em que a meta exigida for atingida não haverá abatimento;

5.2.6. No valor mensal do serviço será abatido o FD calculado para cada resultado de indicador não alcançado:

$$FD_{indicador} = Valor\ Mensal \times \frac{FIS_{indicador}}{100} \times \frac{\left|Meta_{indicador} - Resultado_{indicador}\right|}{Meta_{indicador}}$$

$$FD_{total} = \sum_{i=1}^{max(indicadores)} FD_i$$

5.2.7. Além da aplicação do FD, haverá glosa adicional de 0,2% (dois décimos por cento) sobre o valor mensal do contrato, multiplicada pelo Fator de Impacto no Serviço (FIS) do indicador, para cada indicador de nível de serviço que apresente discrepância superior a 20% (vinte por cento) em relação à meta prevista, até o limite de 50% (cinquenta por cento). Ultrapassado esse limite, além da glosa adicional, haverá cobrança de multa (item 5.24.4);

5.2.8. Além da aplicação do FD, haverá glosa adicional de 0,5% (cinco décimos por cento) sobre o valor mensal do contrato, multiplicada pelo Fator de Impacto no Serviço (FIS) do indicador, para cada indicador de nível de serviço que apresente discrepância superior a 10% em relação à meta prevista em 3 medições consecutivas e poderá ensejar a inexecução parcial ou total do contrato;

5.2.9. Os seguintes Indicadores de Nível de Serviço serão considerados:

Item	Indicador de Nível de Serviço	Fórmula de Cálculo	Unidade de Medida	Meta exigida	Fator de Impacto no Serviço (FIS)
1	Tempo médio de triagem de requisições/incidentes	Somatório dos tempos de triagem de requisições e incidentes / Total de requisições e incidentes	minutos	<= 30	10
2	Tempo médio de resolução de requisições/incidentes de severidade crítica	Somatório dos tempos de resolução de requisições e incidentes de severidade crítica / Total de requisições e incidentes	horas	<= 1	20

3	Tempo médio de resolução de requisições/incidentes de severidade alta	Somatório dos tempos de resolução de requisições e incidentes de severidade alta / Total de requisições e incidentes	horas	<=2	20
4	Tempo médio de resolução de requisições/incidentes de severidade média	Somatório dos tempos de resolução de requisições e incidentes de severidade média / Total de requisições e incidentes	horas	<= 4	15
5	Tempo médio de resolução de requisições/incidentes de severidade baixa	Somatório dos tempos de resolução de requisições e incidentes de severidade baixa / Total de requisições e incidentes	horas	<= 12	10
6	Tempo médio de resolução de requisições de severidade agendado	Somatório dos tempos de resolução de requisições e incidentes de severidade agendado / Total de requisições e incidentes	horas	<= 24	5
7	Índice de informações inconsistentes, incompletas ou com erros de procedimento, cuja responsabilidade seja da contratada, na documentação dos incidentes de segurança	Total de eventos da amostra registradas de modo inconsistente, incompleto ou com erros de procedimento na documentação dos incidentes de segurança / Tamanho da amostra x 100	%	<= 5%	10
8	Índice de informações inconsistentes, incompletas ou com erros de procedimento, cuja responsabilidade seja da contratada, na documentação das lições aprendidas nos incidentes de segurança	Total de eventos da amostra registradas de modo inconsistente, incompleto ou com erros de procedimento na documentação das lições aprendidas / Tamanho da amostra x 100	%	<= 5%	5
9	Índice de qualificação da equipe conforme itens 5.31.3, 5.31.4 e 5.31.5	Total de certificados da equipe / Quantidade de certificados exigidos, contabilizados depois de 90 dias do profissional entrar em operação	%	= 100%	5
10	Índice de disponibilidade da infraestrutura necessária à prestação dos serviços	A medição da disponibilidade deve considerar o período compreendido entre o primeiro e o último dia de cada mês	%	>= 99,9%	–

5.2.10. Glosa adicional de 0,5% (cinco décimos por cento) sobre o valor mensal do contrato, por dia de atraso, caso a CONTRATADA apresente os documentos comprobatórios da qualificação dos profissionais alocados na prestação dos serviços, além das certificações requeridas (item 5.31 e

subitens), em prazo superior a 05 (cinco) dias úteis até o limite de 20 (vinte) dias úteis, quando haverá, além da glosa, cobrança de multa (item 5.24.2);

5.2.11. Glosa adicional de 5% (cinco por cento) sobre o valor mensal do contrato caso a disponibilidade de toda infraestrutura necessária à prestação dos serviços seja inferior a 99,90% (noventa e nove vírgula nove por cento) até o limite de 99% (noventa e nove por cento), quando haverá, além da glosa, cobrança de multa (item 5.24.3). A medição da disponibilidade deve considerar o período compreendido entre o primeiro e o último dia de cada mês.

5.3. Não há previsão de bônus ou pagamentos adicionais para os casos em que a contratada superar as metas previstas, ou caso seja necessária a alocação de maior número de profissionais para o alcance das metas;

5.4. A superação de uma das metas não poderá ser utilizada para compensar o não atendimento de outras metas no mesmo período, nem o não atendimento da mesma meta em outro período;

5.5. Todos os indicadores que dependem de amostra para cálculo serão mensurados com método aleatório de escolha do espaço amostral definido pela CONTRATANTE e serão aferidos com nível de confiança de 90% e margem de erro de 5%.

5.6. A CONTRATANTE comunicará a CONTRATADA sobre o recebimento definitivo a fim de possibilitar a emissão da nota fiscal, informando os valores correspondentes às glosas.

QUALIFICAÇÃO TÉCNICA

5.7. Qualificação Técnica da CONTRATADA:

5.7.1. A CONTRATADA deve apresentar, no momento da sua habilitação no processo licitatório, Atestado(s) de Capacidade Técnica (ACT) em nome da licitante e emitido(s) por pessoa(s) jurídica(s) de direito público ou privado, onde comprove ter prestado ou estar prestando:

5.7.1.1. Fornecimento de solução de Monitoramento, Detecção, Notificação, Investigação e Resposta a Ataques Cibernéticos similar à proposta, em ambiente compatível ao da CONTRATANTE, contendo no mínimo 4.000 (quatro mil) ativos monitorados;

5.7.1.2. Fornecimento de serviço de Monitoramento, Detecção, Notificação, Investigação e Resposta a Ataques Cibernéticos, em regime 24x7x365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias ao ano), em ambiente compatível ao da CONTRATANTE, contendo no mínimo 4.000 (quatro mil) ativos monitorados;

5.7.2. Para cada subitem do item 5.30.1, serão considerados somatórios de atestados para atingir as quantidades solicitadas.

5.8. Qualificação Técnica do Quadro Profissional:

5.8.1. A CONTRATADA deve apresentar, no ato da assinatura do contrato, as certificações e documentos listados nos itens 5.31.3, 5.31.4 e 5.31.5 a fim de comprovar a qualificação técnica dos profissionais alocados para a prestação dos serviços.

5.8.1.1. A comprovação dos perfis exigidos para os profissionais se dará por meio de documentação das certificações (dentro do período de validade).

5.8.2. É de responsabilidade da CONTRATADA dimensionar a quantidade de profissionais para a adequada prestação dos serviços previstos e delimitados por esta especificação, principalmente no que se refere aos acordos de níveis de serviço (item 5.25.9) e metas estabelecidas.

5.8.3. Os profissionais da equipe técnica da CONTRATADA, responsáveis pela sustentação da solução, deverão ter certificação oficial do fabricante da solução proposta de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos (Item 01 da contratação).

5.8.3.1. O líder técnico (Item 5.11) deve, obrigatoriamente, ter a certificação oficial do fabricante da solução proposta de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos.

5.8.4. Os profissionais da equipe técnica da CONTRATADA, responsáveis pela detecção, notificação e investigação de ataques cibernéticos, deverão ter certificação em segurança ofensiva, detendo, individualmente ou em conjunto, pelo menos 03 (três) das seguintes certificações, contabilizando no máximo 02 (dois) certificados por profissional:

5.8.4.1. CompTIA PenTest+;

5.8.4.2. EC-Concil Licensed Penetration Tester (LPT);

5.8.4.3. IACRB Certified Expert Penetration Tester (CEPT);

5.8.4.4. GIAC Exploit Researcher and Advanced Penetration Tester (GXPN);

5.8.4.5. GIAC Reverse Engineering Malware (GREM);

5.8.4.6. Offensive Security Certified Professional (OSCP);

5.8.4.7. Ethical Hacking Post Exploitation (EHPX);

5.8.4.8. Offensive Security Experienced Penetration Tester (OSEP);

5.8.4.9. Offensive Security Web Expert (OSWE);

5.8.4.10. Certified Red Team Expert (CRTE);

5.8.4.11. Offensive Security Certified Expert (OSCE);

5.8.4.12. Certified Ethical Hacker (CEH).

5.8.5. Os profissionais da equipe técnica da CONTRATADA, responsáveis pela resposta a ataques cibernéticos, deverão ter certificação em segurança defensiva, detendo, individualmente ou em conjunto, pelo menos 03 (três) das seguintes certificações, contabilizando no máximo 02 (dois) certificado por profissional:

5.8.5.1. Certified Information Security Manager (CISM);

5.8.5.2. GIAC Experienced Cybersecurity Specialist (GX-CS);

5.8.5.3. GIAC Reverse Engineering Malware (GREM);

5.8.5.4. Ethical Hacking Post Exploitation (EHPX);

5.8.5.5. CompTIA Security+;

5.8.5.6. CompTIA Advanced Security Practitioner;

5.8.5.7. EC-Council Security Analyst (ECSA);

5.8.5.8. Certified Information Systems Security Professional (CISSP);

5.8.5.9. CompTIA CYSA+ - Cybersecurity Analyst.

5.8.6. Deverá ser comprovado vínculo entre os profissionais detentores dos certificados e a CONTRATADA, através de cópia do livro de registro de funcionários ou cópia da carteira de trabalho contendo as respectivas anotações de contrato de trabalho; ou como contratado, por meio de contrato de prestação de serviços.

5.8.7. A CONTRATADA deverá promover, no prazo máximo de 03 (três) meses, a atualização das certificações de seus profissionais caso haja atualização de versão ou migração para uma nova solução de TI devido a modernização do ambiente tecnológico do CONTRATANTE. Este prazo se iniciará a partir da comunicação formal do CONTRATANTE.

5.8.8. A CONTRATANTE se reserva ao direito de realizar auditorias a qualquer tempo para verificar se as competências mínimas solicitadas são atendidas pela CONTRATADA durante toda a vigência do contrato. Desta forma, quando solicitado, a CONTRATADA deverá apresentar os documentos comprobatórios da qualificação dos profissionais alocados na prestação dos serviços, além das certificações requeridas.

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

Anexo A-1 - Termo de Confidencialidade - Empresa CONTRATADA

TERMO DE CONFIDENCIALIDADE

CONTRATO <SIGLA DO TRIBUNAL> Nº ____/_____

A **<PESSOA JURÍDICA OU FÍSICA CONTRATADA>**, doravante referida simplesmente como CONTRATADA, inscrita no CNPJ/MF sob o número **<NÚMERO DO CNPJ>**, com endereço **<ENDEREÇO>**, neste ato representada pelo **<VÍNCULO DO SIGNATÁRIO COM A CONTRATADA>**, **<NOME DO SIGNATÁRIO>**, nos termos do **<CONTRATO OU TERMO ADITIVO EM QUE FOI PACTUADO O SIGILO>**, compromete-se a observar o presente TERMO DE CONFIDENCIALIDADE, firmado perante o <TRIBUNAL>, doravante referido simplesmente como CONTRATANTE, em conformidade com as cláusulas que seguem:

CLÁUSULA PRIMEIRA - DO OBJETO

O objeto deste TERMO DE CONFIDENCIALIDADE é a necessária e adequada proteção às informações confidenciais fornecidas à CONTRATADA para que possa desenvolver as atividades contempladas especificamente no Contrato nº ___/_____.

Subcláusula Primeira - As estipulações constantes neste TERMO DE CONFIDENCIALIDADE se aplicam a toda e qualquer informação revelada à CONTRATADA.

Subcláusula Segunda - A CONTRATADA reconhece que, em razão da prestação de serviços ao CONTRATANTE, tem acesso a informações que pertencem ao CONTRATANTE, que devem ser tratadas como sigilosas.

CLÁUSULA SEGUNDA - DAS INFORMAÇÕES CONFIDENCIAIS

Deve ser considerada confidencial toda e qualquer informação observada ou revelada, por qualquer meio, em decorrência da execução do contrato, contendo ela ou não a expressão “CONFIDENCIAL”.

Subcláusula Primeira - O termo “Informação” abrange toda informação, por qualquer modo apresentada ou observada, tangível ou intangível, podendo incluir, mas não se limitando a: diagramas de redes, fluxogramas, processos, projetos, ambiente físico e lógico, topologia de redes, configurações de equipamentos, senhas, fotografias, plantas, programas de computador, discos, disquetes, fitas, contratos, projetos, outras informações técnicas, jurídicas, financeiras ou comerciais, entre outras a que, diretamente ou através de seus empregados, prepostos ou prestadores de serviço, venha a CONTRATADA ter acesso durante ou em razão da execução do contrato celebrado.

Subcláusula Segunda - Em caso de dúvida acerca da natureza confidencial de determinada informação, a CONTRATADA deverá mantê-la sob sigilo até que seja autorizada expressamente pelo representante legal do CONTRATANTE, referido no Contrato, a tratá-la diferentemente. Em hipótese alguma, a ausência de manifestação expressa do CONTRATANTE poderá ser interpretada como liberação de qualquer dos compromissos ora assumidos.

CLÁUSULA TERCEIRA - DOS LIMITES DA CONFIDENCIALIDADE

As estipulações e obrigações constantes do presente instrumento não serão aplicadas a nenhuma informação que seja comprovadamente de conhecimento público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;

CLÁUSULA QUARTA - DAS OBRIGAÇÕES

A CONTRATADA se obriga a manter sigilo de toda e qualquer informação definida como confidencial neste TERMO DE CONFIDENCIALIDADE, utilizando-as exclusivamente para os propósitos do contrato.

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

Subcláusula Primeira - A CONTRATADA determinará a observância deste TERMO DE CONFIDENCIALIDADE, bem como a observância e a assinatura do TERMO DE CONFIDENCIALIDADE - COLABORADOR, a todos os seus empregados, prepostos e prestadores de serviço que estejam direta ou indiretamente envolvidos com a execução do contrato.

Subcláusula Segunda - A CONTRATADA obriga-se a informar imediatamente ao CONTRATANTE qualquer violação das regras de sigilo ora estabelecidas que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo, bem como de seus empregados, prepostos e prestadores de serviço.

Subcláusula Terceira - Compromete-se, ainda, a CONTRATADA a não revelar, reproduzir ou utilizar, bem como não permitir que seus empregados, prepostos ou prestadores de serviço revelem, reproduzam ou utilizem, em hipótese alguma, as informações referidas no presente TERMO DE CONFIDENCIALIDADE como confidenciais, ressalvadas situações previstas no contrato e neste TERMO DE CONFIDENCIALIDADE.

Subcláusula Quarta - A CONTRATADA deve cuidar para que as informações consideradas confidenciais nos termos do presente TERMO DE CONFIDENCIALIDADE fiquem restritas ao conhecimento dos empregados, prepostos ou prestadores de serviço que estejam diretamente envolvidos nas discussões, análises, reuniões e negócios, devendo cientificá-los da existência deste TERMO DE CONFIDENCIALIDADE e da natureza confidencial das informações.

CLÁUSULA QUINTA - DO RETORNO DAS INFORMAÇÕES

A CONTRATADA devolverá imediatamente ao CONTRATANTE, ao término do Contrato, todo e qualquer material de propriedade desta, inclusive registro de documentos de qualquer natureza que tenham sido criados, usados ou mantidos sob seu controle ou posse, bem como de seus empregados, prepostos ou prestadores de serviço, assumindo o compromisso de não utilizar qualquer informação considerada confidencial, nos termos do presente TERMO DE CONFIDENCIALIDADE, a que teve acesso em decorrência do vínculo contratual com o CONTRATANTE.

CLÁUSULA SEXTA - DO DESCUMPRIMENTO

O descumprimento de qualquer cláusula deste TERMO DE CONFIDENCIALIDADE acarretará as responsabilidades civil, criminal e administrativa, conforme previsto na legislação

CLÁUSULA SÉTIMA - DA VIGÊNCIA

Tendo em vista o princípio da boa-fé objetiva, permanece em vigor o dever de sigilo, tratado no presente TERMO DE CONFIDENCIALIDADE, após o término do Contrato.

CLÁUSULA OITAVA - DAS DISPOSIÇÕES FINAIS

Os casos omissos neste TERMO DE CONFIDENCIALIDADE, assim como as dúvidas surgidas em decorrência da sua execução, serão resolvidos pelo CONTRATANTE.

Por estarem de acordo, a CONTRATADA, por meio de seu representante, firma o presente TERMO DE CONFIDENCIALIDADE, lavrando em duas vias de igual teor e forma.

São Paulo, ____ de _____ de 20____.

<TRIBUNAL>

_____	_____
Nome:	Nome:
Cargo:	Cargo:

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

NOME DA EMPRESA FORNECEDORA

_____	_____
Nome:	Nome:
Cargo:	Cargo:

TESTEMUNHAS:

_____	_____
Nome:	Nome:
CPF/MF.:	CPF/MF.:

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

Anexo A-2 – Termo de Confidencialidade - Colaborador da CONTRATADA

TERMO DE CONFIDENCIALIDADE - COLABORADOR

A **<PESSOA FÍSICA OU JURÍDICA>**, doravante referida simplesmente como COLABORADOR, inscrita no CPF/CNPJ sob o número **<NÚMERO DO CPF/CNPJ>**, compromete-se a observar o presente TERMO DE CONFIDENCIALIDADE, em conformidade com as cláusulas que seguem:

CLÁUSULA PRIMEIRA - DO OBJETO

O objeto deste TERMO DE CONFIDENCIALIDADE é a necessária e adequada proteção às informações confidenciais fornecidas aos empregados, prepostos ou prestadores de serviço de empresas contratadas pelo <TRIBUNAL> (<SIGLA DO TRIBUNAL>), para que possam desenvolver suas atividades institucionais.

Subcláusula Primeira - As estipulações constantes neste TERMO DE CONFIDENCIALIDADE se aplicam a toda e qualquer informação.

Subcláusula Segunda – O COLABORADOR reconhece que tem acesso a informações que pertencem ao <SIGLA DO TRIBUNAL>, que devem ser tratadas como sigilosas.

CLÁUSULA SEGUNDA - DAS INFORMAÇÕES CONFIDENCIAIS

Deve ser considerada confidencial toda e qualquer informação observada ou revelada, por qualquer meio, contendo ela ou não a expressão “CONFIDENCIAL”.

Subcláusula Primeira - O termo “Informação” abrange toda informação, por qualquer modo apresentada ou observada, tangível ou intangível, podendo incluir, mas não se limitando a: diagramas de redes, fluxogramas, processos, projetos, ambiente físico e lógico, topologia de redes, configurações de equipamentos, senhas, fotografias, plantas, programas de computador, discos, pen drives, fitas, contratos, projetos, outras informações técnicas, jurídicas,

financeiras ou comerciais, entre outras a que venha o COLABORADOR ter acesso durante ou em razão da execução de suas atividades profissionais.

Subcláusula Segunda - Em caso de dúvida acerca da natureza confidencial de determinada informação, o COLABORADOR deverá mantê-la sob sigilo até que seja autorizada expressamente pelo representante legal do <SIGLA DO TRIBUNAL>, a tratá-la diferentemente. Em hipótese alguma, a ausência de manifestação expressa do <SIGLA DO TRIBUNAL>poderá ser interpretada como liberação de qualquer dos compromissos ora assumidos.

CLÁUSULA TERCEIRA - DOS LIMITES DA CONFIDENCIALIDADE

As estipulações e obrigações constantes do presente instrumento não serão aplicadas a nenhuma informação que:

I - sejam comprovadamente de conhecimento público no momento da revelação, exceto se tal fato decorrer de ato ou omissão do COLABORADOR;

II - já esteja em poder do COLABORADOR, como resultado de sua própria pesquisa, contanto que o COLABORADOR possa comprovar referido fato; ou

III - tenha sido comprovada e legitimamente recebida de terceiros, contanto que o COLABORADOR possa comprovar referido fato.

CLÁUSULA QUARTA - DAS OBRIGAÇÕES

O COLABORADOR se obriga a manter sigilo de toda e qualquer informação definida como confidencial neste TERMO DE CONFIDENCIALIDADE, utilizando-as exclusivamente no desempenho de suas atividades profissionais enquanto contratado.

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

Subcláusula Primeira - Compromete-se, ainda, o COLABORADOR a não revelar, reproduzir ou utilizar, em hipótese alguma, as informações referidas no presente TERMO DE CONFIDENCIALIDADE como confidenciais, ressalvadas situações previstas neste documento.

CLÁUSULA QUINTA - DO DESCUMPRIMENTO

O descumprimento de qualquer cláusula deste TERMO DE CONFIDENCIALIDADE acarretará as responsabilidades civil, criminal e administrativa, conforme previsto na legislação.

CLÁUSULA SEXTA - DA VIGÊNCIA

Tendo em vista o princípio da boa-fé objetiva, permanecem em vigor os deveres de sigilo e de não utilização das informações, tratados no presente TERMO DE CONFIDENCIALIDADE, após o término do vínculo contratual.

CLÁUSULA SÉTIMA - DAS DISPOSIÇÕES FINAIS

Os casos omissos neste TERMO DE CONFIDENCIALIDADE, assim como as dúvidas surgidas em decorrência da sua execução, serão resolvidos pelo <SIGLA DO TRIBUNAL>.

Por estar de acordo, o COLABORADOR firma o presente TERMO DE CONFIDENCIALIDADE, lavrando em duas vias de igual teor e forma.

São Paulo, ____ de _____ de 20____.

_____

Nome:

Cargo / Função:

Empresa: