Estudos Preliminares 38/2024

Informações Básicas

Número do artefato	UASG	Editado por	Atualizado em
38/2024	70008-TRIBUNAL REGIONAL ELEITORAL DO RIO G. DO NORTE	ERNESTO LECA PINTO	08/04/2024 16:30 (v 2.1)

Status

RASCUNHO

Outras informações

Categoria	Número da Contratação	Processo Administrativo
II - compra, inclusive por encomenda/Bens permanentes		PAE 9656/2023

1. Objetivo

1. Objetivo

1.1 O presente Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação, à luz do disposto no art. 18, I e §1º, da Lei nº 14.133/2021, no art. 14 da Res. 468/2022 do CNJ e no Guia de Contratações de TIC do Poder Judiciário.

2. Definição especificação das necessidades

2. Definição e especificação das necessidades e requisitos

2.1 Identificação das necessidades de negócio

2.1.1 A solução deverá permitir o fornecimento de bens e serviços de inteligência cibernética, no formato de prestação de serviço, voltados para monitoramento, coleta e análise de dados, internos e externos, sobre ameaças cibernéticas do ambiente de rede do TRE-RN, com adoção de tecnologias de análise de comportamento, uso de inteligência artificial e machine learning não supervisionado.

2.2 Identificação das necessidades tecnológicas

2.2.1 Descrição da solução e quantidades:

Item	Descrição	Unidade	Quant.
1	Solução de inteligência cibernética, contendo licenças de uso de software, hardware, prestação de serviços e entregáveis, no formato de prestação de serviços, com monitoração e ação 24x7x365, suporte técnico, garantia e manutenção pelo período de 24 (vinte e quatro) meses, e pagamento em parcela	meses	01
2	Serviço de Ativação da Solução	unidade	01
3	Serviço de Operação Assistida	blocos de 04 horas	24
4	Treinamento (por pessoa)	servidores	06

2.2.2 Descrição do tipo de perfil:

Tipo de Perfil		Quant.
Throughput	de 01 Gbps até 02 Gbps	1.1 Gbps
Ativos Monitorados	de 2.001 até 2.500 ativos monitorados	2.100
Conexões por Minuto	de 50.001 até 75.000 conexões por minuto	74.844
E-mail VIP	de 101 a 150 caixas de e-mail	120

2.3 Demais requisitos necessários e suficientes à escolha da solução de TIC

2.3.1 Características Gerais

2.3.1.1 A solução deve ser dotada de tecnologia baseada em Inteligência Artificial a fim de identificar anomalias de comportamento e ataques não identificados pelas tecnologias tradicionais de segurança da informação.

2.3.1.2 A solução, composta de hardware, software e serviços, deverá ser fornecida através de aquisição por meio de subscrição de direito de uso durante o período contratual, na versão mais recente publicada pelo desenvolvedor e com prazo de garantia (atualização, manutenção

e suporte técnico) mínimo de 24 (vinte e quatro) meses, com possibilidade de renovação até 60 meses.
2.3.1.3 A solução poderá ser formada por vários fabricantes ou serviços integrados por meio de API's (Application Programming Interface) ou única, sem a necessidade de desenvolvimento, desde que atenda todas as especificações técnicas.
2.3.1.4 A solução terá prazo de garantia de **24 (vinte e quatro) meses**, com o seu pagamento sendo realizado em parcela única, após a homologação da entrega, com devidos aceites, exceto para os treinamentos e os serviços sob demanda, que serão liquidados e pagos a medida de sua execução.

2.3.2 De Capacitação/Treinamento
2.3.2.1 Deverá ser fornecido treinamento oficial a solução que será alocada no ambiente do Tribunal, com carga horária **mínima de 40 horas**, abarcando a solução, no conteúdo necessário para a perfeita compreensão e operação de todos os seus requisitos.
2.3.2.1.1 Ações complementares como workshops internos e treinamentos no formato hands-on podem ser também considerados no escopo do treinamento.
2.3.2.1.2 O treinamento deverá ser realizado de forma remota, via videoconferência, objetivando agilizar a capacitação das equipes envolvidas.
2.3.2.2 O treinamento deverá ser fornecido, por aluno, para servidores detentores de cargos efetivos do TRE-RN, com emissão de certificados e pesquisa de satisfação ao final do treinamento, estando sujeita a CONTRATADA a atingir uma qualidade mínima, sob pena de sanção aplicável, a ser definida no Termo de Referência.
2.3.2.3 Poderão ser indicados mais participantes na categoria de ouvintes, sem a exigência de certificado de participação e material (limitando-se a 04 participantes adicionais do tipo “ouvintes”).
2.3.2.4 Todas as despesas referentes à realização do treinamento ou ao custeio de insumos deverão estar inclusas no valor contratado.

2.3.3 De Garantia e Manutenção
2.3.3.1 A solução deverá ser ofertada com garantia e manutenção do fabricante e deverá ser prestado na modalidade **24 (vinte e quatro) horas por dia e 07 (setes) dias por semana (24x7), pelo prazo de 24 (vinte e quatro) meses**, sem custos adicionais ao TRE-RN, contados a partir da emissão do Termo de Recebimento Definitivo da Solução.
2.3.3.2 A garantia deverá cobrir falhas no serviço de instalação e configuração da solução, fornecimento de correções de software, substituição de hardware defeituoso e fornecimento de atualizações corretivas e evolutivas de software.
2.3.3.3 O acionamento da garantia ocorrerá por meio de abertura dos chamados técnicos via número de telefone de discagem gratuita (0800), envio de e-mail ou acesso ao site oficial de suporte da CONTRATADA.

2.3.4 Temporais
2.3.4.1 Na contagem dos prazos estabelecidos nestes estudos preliminares, quando não expressados de forma contrária, excluir-se-á o dia do início e incluir-se-á o do vencimento.
2.3.4.2 Todos os prazos citados, quando não expresso de forma contrária, serão considerados em dias úteis (ou horas úteis, quando definido em horas).
2.3.4.3 Todos os eventos de trabalho que envolvam a participação de integrantes do TRE-RN, serão realizados durante os horários de expediente adotados, de segunda-feira a sexta-feira, exceto feriados, salvo casos de urgência e/ou acordo entre as partes, desde que tempestivamente informados e solicitados.
2.3.4.4 Todos os eventos de trabalho que envolva participação de integrantes da CONTRATADA em ambiente da CONTRATANTE serão realizados durante os horários de expediente adotados, de segunda-feira a sexta-feira, exceto feriados, salvo casos de urgência e

/ou acordo entre as partes, desde que tempestivamente informados e solicitados.
2.3.4.5 Não será computado o tempo de atraso quando este estiver sido ocasionado pela CONTRATANTE ou por fatos supervenientes que impeçam ações da CONTRATADA, desde que devidamente justificado e aceito pela CONTRATANTE.
2.3.4.6 Não serão considerados casos ou fatos supervenientes as situações externas que possam ser contornadas ou mitigadas por ações de logísticas preventivas ou reativas da CONTRATADA.

2.3.5 De Segurança da Informação
2.3.5.1 A fornecedora da solução deverá obedecer aos critérios, padrões, normas e procedimentos operacionais adotados pela JUSTIÇA ELEITORAL e, em especial:
2.3.5.2 O fornecimento dos equipamentos e a prestação da garantia.
2.3.5.3 Manter sigilo, sob pena de responsabilidades civis, penais e administrativas, sobre todo e qualquer assunto de interesse da JUSTIÇA ELEITORAL ou de terceiros de que tomar conhecimento em razão da execução do objeto desta contratação devendo orientar seus funcionários nesse sentido.
2.3.5.4 Submeter seus recursos técnicos aos regulamentos de segurança e disciplina instituídos pela JUSTIÇA ELEITORAL, durante o tempo de permanência nas suas dependências, observando a Portaria 226/2018-GP-TRE/RN, que dispõe sobre as medidas de controle de acesso, circulação e permanência de pessoas nos prédios do Edifício-Sede do TRE /RN, do Centro de Operações da Justiça Eleitoral (COJE), Fórum Eleitoral de Natal e, no que couber, aos prédios das Zonas Eleitorais do Interior do Estado.

3. Análise das soluções possíveis

3. Análise das soluções possíveis

3.1 Levantamento das soluções:

3.1.1 Para o presente objeto foi realizada pesquisa no mercado de tecnologia voltado para segurança da informação, onde se buscou por contratações na Administração Pública Federal - APF, e análise para o atendimento do objeto que consta no Documento de Oficialização da Demanda:

3.1.1.1 **Solução 01** – Serviço continuado de inteligência cibernética, incluindo serviços gerenciados de ferramentas de segurança da informação, análise de incidentes cibernéticos e prevenção de eventos, com forte destaque na alocação de mão de obra.

3.1.1.2 **Solução 02** – Contratação de solução de serviço de monitoramento de segurança da informação, incluindo licenças de software, equipamentos, garantia e manutenção, suporte técnico especializado, instalação e treinamento.

3.1.1.3 **Solução 03** - Contratação envolvendo tanto segurança cibernética para rede interna e externa, com uso de inteligência artificial, respostas autônomas e machine learning não supervisionado, integrados com recursos de inteligência cibernética, fornecida como serviço e pagamento em parcela única.

3.1.2 Para as contratações na Administração Pública Federal - APF observou-se que ele tem se direcionado basicamente para duas vertentes, conforme descrito nas soluções 01 e 02.

3.1.3 É habitual em ambos os cenários, a adoção de 02 (dois) ou mais fabricantes e/ou ferramentas na definição da solução para pleno atendimento ao objeto que a APF contratou.

3.1.4 Algumas contratações existentes, já licitadas pela APF podem atender parcialmente aos requisitos desejados, contudo, pela complexidade da solução entende-se que será necessária a composição de ferramentas, que se devidamente integradas, poderão atender a solução que está desenhada.

3.1.5 Foram identificados alguns órgãos que realizaram contratações cujo objeto apresenta similaridade com o que foi apresentado aqui e no **item 2.1.1**, sendo importante ressaltar que não foi encontrada nenhuma contratação que pudesse ser utilizada completamente para comparação e estimativa de custos.

3.1.6 Reforça-se que apenas alguns itens dessas contratações poderão ser aproveitados para fins de estimativa de custos para solução que se pretende contratar, devido às diferenças em relação às especificidades e quantitativos por item, além da dificuldade ou impossibilidade de validar quesitos relacionados à segurança cibernética, inteligência artificial, respostas autônomas, machine learning não supervisionado e análise comportamental, integrada com solução de inteligência cibernética, prestado como serviço, em função da ausência dessas informações diretamente nos documentos analisados.

3.1.7 O levantamento foi realizado dentro dos parâmetros previstos e em atendimento às práticas adotadas pela Estratégia Nacional de Cibersegurança da Justiça Eleitoral, quanto às contratações conjuntas, junto a empresas do mercado e análise de contratos realizados pela Administração Pública Federal.

3.1.8 Com base nas informações recebidas dos fabricantes CISCO, TRENDMICRO, DARKTRACE e FORTINET, foi realizada a consulta das seguintes empresas:

3.1.8.1 Parceiras TRENDMICRO:

3.1.8.1.1 ServiceIT.

3.1.8.1.2 AllTech.

3.1.8.2 Parceiras CISCO:

3.1.8.2.1 Logicalis.

3.1.8.2.2 Teletex.

3.1.8.2.3 Global.

3.1.8.2.4 WiseIT.

3.1.8.2.5 Atelecom.

3.1.8.2.6 Yssy.

3.1.8.2.7 Netsafecorp.

3.1.8.2.8 Teltecsolutions.

3.1.8.3 Parceiras DARKTRACE:

3.1.8.3.1 RC2.

3.1.8.3.2 Grg Tech.

3.1.8.3.3 INN Tecnologia.

3.1.8.4 Parceiras FORTINET:

3.1.8.4.1 Global Sectecnologia.

3.1.9 Seguem abaixo algumas contratações identificadas na APF com seus respectivos itens que foram analisados quanto à possibilidade ou não de utilização como referência para apoiar na comparação de custos unitários e totais desta contratação:

Administração Pública Federal	Descrição
Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira – INEP (Pregão nº 009/2017)	Solução Integrada de Serviços Gerenciados de Segurança
	Serviços Técnicos Evolutivos
Tribunal de Contas da União - TCU (Pregão nº 034/2017)	Solução Integrada de Serviços Gerenciados de Segurança
Conselho da Justiça Federal – CJF (Pregão nº 001/2020)	Solução Integrada de Serviços Gerenciados de Segurança
Supremo Tribunal Federal - STF (Pregão nº 008/2023)	Serviço de Gestão de Vulnerabilidades
	Serviço de Gestão de Incidentes de Segurança (CSIRT - Blue Team)
	Serviço de Testes de Invasão (Red Team)
	Serviço de Operação, Controle e Suporte à Infraestrutura
	Serviço de Análise de Inteligência em Ameaças Cibernéticas (CIT)
Tribunal de Justiça do Estado do Rio de Janeiro - TJRJ (Pregão nº 050/2022)	Serviço de Gestão de Incidentes de Segurança, Vulnerabilidades e Ameaças
Banco da Amazônia - BASA (Pregão nº 043/2021)	Serviço de monitoramento de incidentes
	Serviço de resposta a incidentes

Instituto Brasileiro de Geografia e Estatística - IBGE (Pregão nº 011/2021)	Gestão de Riscos - Processo integrado envolvendo a Gestão de Vulnerabilidades, Gestão de Riscos, Compliance e Monitoração de Marca
	Gestão de Incidentes - Processo integrado envolvendo a Análise de Incidentes Globais e o Monitoramento de Incidentes
	Resposta aos Incidentes - Processo integrado envolvendo a prevenção, bloqueio e resposta aos incidentes, bem como a análise de sua causa raiz
TCE-RR (Pregão nº 011/2021)	Serviço de Operação Assistida e consultoria especializada com bloco de 4 horas
Tribunal Superior Eleitoral - TSE (Pregão nº 058/2021)	Operação Assistida 10 dias úteis de 8h diárias
TCE-MT (Pregão nº 006/2020)	Serviço de Operação Assistida
TELEBRAS (Pregão nº 007/2021)	Operação Assistida por blocos de 8 dias corridos
CNJ 036/2019	Treinamentos

3.2 A alternativa descrita no item 3.1, refere-se à aquisição de serviço e encontram-se implantadas:

3.2.1 No Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira – INEP (Pregão nº 009/2017) - Solução Integrada de Serviços Gerenciados de Segurança; Serviços Técnicos Evolutivos.

3.2.2 No Tribunal de Contas da União - TCU (Pregão nº 034/2017) - Solução Integrada de Serviços Gerenciados de Segurança; Serviços Técnicos Evolutivos; Treinamentos.

3.2.3 No CNJ (036/2019) - Treinamentos.

3.2.4 No Conselho da Justiça Federal – CJF (Pregão nº 001/2020) - Solução Integrada de Serviços Gerenciados de Segurança.

3.2.5 No TCE-MT (06/2020) - Serviço de Operação Assistida.

3.2.6 No TCE-RR (017/2021) - Serviço de Operação Assistida e consultoria especializada com bloco de 04 horas.

3.2.7 No TSE (058/2021) - Operação Assistida 10 dias úteis de 8h diárias.

3.2.8 Na TELEBRAS (007/2021) - Operação Assistida por blocos de 08 (oito) dias corridos.

3.2.9 No Banco da Amazônia - BASA (Pregão nº 043/2021) - Serviço de monitoramento de incidentes; Serviço de resposta a incidentes; Serviço de gestão de vulnerabilidades; Serviço de feeds de inteligência, detecção e proteção de ameaças direcionadas; Serviços técnicos especializados em segurança da informação - UST (sob demanda); Serviço de capacitação nos produtos e softwares utilizados para atender aos requisitos desta contratação (sob demanda) com carga horária de 24 horas; Serviço de capacitação em Security Analytics (sob demanda) com carga horária de 40 horas.

3.2.10 No Instituto Brasileiro de Geografia e Estatística - IBGE (Pregão nº 011/2021) - Gestão de Riscos - Processo integrado envolvendo a Gestão de Vulnerabilidades, Gestão de Riscos, Compliance e Monitoração de Marca; Gestão de Incidentes - Processo integrado envolvendo a Análise de Incidentes Globais e o Monitoramento de Incidentes; Resposta aos Incidentes - Processo integrado envolvendo a prevenção, bloqueio e resposta aos incidentes, bem como a análise de sua causa raiz.

3.2.11 No Tribunal de Justiça do Estado do Rio de Janeiro - TJRJ (Pregão nº 050/2022) - Serviço de Privacidade e Proteção de Dados; Serviço de Gestão de Segurança de Ativos; Serviço de Gestão de Incidentes de Segurança, Vulnerabilidades e Ameaças; Serviço de Gestão de Problemas; Serviço de Auditoria e Investigação; Serviço de Melhorias.

3.2.12 No Supremo Tribunal Federal - STF (Pregão nº 008/2023) - Serviço de Operação e Atendimento a Requisições; Serviço de Gestão de Vulnerabilidades; Serviço de Gestão de Incidentes de Segurança (CSIRT - Blue Team); Serviço de Testes de Invasão (Red Team); Serviço de Operação, Controle e Suporte à Infraestrutura; Serviço de Análise de Inteligência em Ameaças Cibernéticas (CIT).

3.3 Capacidade e alternativas no mercado de TIC, inclusive a existência de software livre ou software público.

3.3.1 Não foram identificadas a existência de software livre ou de soluções no Portal do Software Público Brasileiro capazes de atender plenamente as necessidades e requisitos desta contratação.

3.4 Observância às políticas, premissas e especificações técnicas definidas pelos modelo nacional de interoperabilidade do Poder Judiciário (MNI) e modelo de acessibilidade de governo eletrônico (E-MAG).

3.4.1 Não se aplica por tratar de uma solução que não possui o requisito para intercâmbio de informações de processos judiciais e assemelhados entre os diversos órgãos de administração de justiça, nem tampouco servir de base para implementação das funcionalidades pertinentes no âmbito do sistema processual, nos termos tratados pela Resolução Conjunta CNJ/CNMP nº 3 de 16/04/2013.

3.5 Aderência às regulamentações da Infraestrutura de chaves Públicas Brasileiras (ICP-Brasil), quando houver necessidade de utilização de certificado digital, observada a legislação sobre o assunto.

3.5.1 As alternativas de solução levantadas são capazes de fazer uso dos recursos tecnológicos disponíveis em certificados digitais, estando alinhadas à Infraestrutura de Chaves Públicas – ICP Brasil e em conformidade com a MP nº 2.200-2 – de 24 de agosto de 2001 - e demais

arcabouços normativos aplicáveis a solução, instituídos pelo Instituto Nacional de Tecnologia da Informação (ITI).

3.6 Observância às orientações, premissas e especificações técnicas e funcionais definidas pelo Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário (Moreq-Jus), do Conselho Nacional de Justiça – CNJ e pelo E-ARQ (normas e padrões de arquivologia).

3.6.1 Não se aplica por tratar de uma solução que não possui o requisito de gestão de processos e documentos, nos termos tratados pela Resolução CNJ nº 91 de 29/09/2009.

3.7 Modelos de prestação do serviço:

3.7.1 Por se tratar de licenças de uso de software, hardware, prestação de serviços e entregáveis há necessidade de treinamento, porém não há necessidade de modelo de prestação de serviços associado.

3.8 Orçamento estimado que expresse a composição de todos os custos unitários resultantes dos itens a serem contratados, elaborado com base em pesquisa fundamentada de preços, como os praticados no mercado de Tecnologia da Informação e Comunicação em contratações similares realizadas por órgãos ou entidades da Administração Pública, entre outros pertinentes.

3.8.1 Em consulta realizada em âmbito nacional para uma prévia estimativa de custos, se obteve o seguinte:

Item	Descrição	Valor Estimado
1	Solução de inteligência cibernética, contendo licenças de uso de software, hardware, prestação de serviços e entregáveis, no formato de prestação de serviços, com monitoração e ação 24x7x365, suporte técnico, garantia e manutenção pelo período de 24 (vinte e quatro) meses, e pagamento em parcela (unidade)	R$ 3.590.000,00
2	Serviço de Ativação da Solução (unidade)	R$ 74.000,00
3	Serviço de Operação Assistida (bloco de 4h)	R$ 590,00
4	Treinamento (por pessoa)	R$ 22.520,00

3.9 Análise comparativa das soluções

3.9.1 Ao compararmos as possíveis soluções se observa que a solução indicada no **item 3.1.3** é a única alternativa que atende todas as necessidades desta contratação.

3.10 Análise comparativa de custos

3.10.1 Seguem abaixo algumas contratações identificadas na **Administração Pública Federal (**APF) com seus respectivos itens que foram analisados quanto à possibilidade ou não de utilização como referência para apoiar na comparação de custos unitários e totais desta contratação:

Administração Pública Federal	Descrição	Valor Total
Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira – INEP (Pregão nº 009/2017)	Solução Integrada de Serviços Gerenciados de Segurança	R$4.090.800,00 (12 meses)
	Serviços Técnicos Evolutivos	R$ 434.000,00 (2.000 horas)
Tribunal de Contas da União - TCU (Pregão nº 034/2017)	Solução Integrada de Serviços Gerenciados de Segurança	R$ 9.719.237,40 (60 meses)
Conselho da Justiça Federal – CJF (Pregão nº 001/2020)	Solução Integrada de Serviços Gerenciados de Segurança	R$ 3.602.025,36 (24 meses)
Supremo Tribunal Federal - STF (Pregão nº 008/2023)	Serviço de Gestão de Vulnerabilidades	R$ 165.392,00 (04/serviço)
	Serviço de Gestão de Incidentes de Segurança (CSIRT - Blue Team)	R$ 285.852,00 (04/serviço)
	Serviço de Testes de Invasão (Red Team)	R$ 84.168,00 (04/serviço)
	Serviço de Operação, Controle e Suporte à Infraestrutura	R$ 1.479.999,96 (12 meses)
	Serviço de Análise de Inteligência em Ameaças Cibernéticas (CIT)	R$ 354.999,96 (12 meses)
Tribunal de Justiça do Estado do Rio de Janeiro - TJRJ (Pregão nº 050/2022)	Serviço de Gestão de Incidentes de Segurança, Vulnerabilidades e Ameaças	R$ 24.764.309,76 (24 meses)

Banco da Amazônia - BASA (Pregão nº 043/2021)	Serviço de monitoramento de incidentes	R$ 4.549.999,68 (36 meses)
	Serviço de resposta a incidentes	R$ 1.199.999,88 (36 meses)
Instituto Brasileiro de Geografia e Estatística - IBGE (Pregão nº 011/2021)	Gestão de Riscos - Processo integrado envolvendo a Gestão de Vulnerabilidades, Gestão de Riscos, Compliance e Monitoração de Marca	R$ 1.429.999,92 (24 meses)
	Gestão de Incidentes - Processo integrado envolvendo a Análise de Incidentes Globais e o Monitoramento de Incidentes	R$1.099.999,92 (24 meses)
	Resposta aos Incidentes - Processo integrado envolvendo a prevenção, bloqueio e resposta aos incidentes, bem como a análise de sua causa raiz	R$ 699.999,84 (24 meses)
TCE-RR (Pregão nº 011/2021)	Serviço de Operação Assistida e consultoria especializada com bloco de 4 horas	R$ 12.000,00 (40 horas)
Tribunal Superior Eleitoral - TSE (Pregão nº 058/2021)	Operação Assistida 10 dias úteis de 8h diárias	R$ 21.719,20 (80 horas)
TCE-MT (Pregão nº 006/2020)	Serviço de Operação Assistida	R$ 869.760,00 (2.112 horas)
TELEBRAS (Pregão nº 007/2021)	Operação Assistida por blocos de 8 dias corridos	R$ 938.892,15 (2.880 horas)
CNJ 036/2019	Treinamentos	R$ 20.050,00

		(03 servidores)

4. Cálculos dos custos totais

4. Cálculos dos custos totais

4.1 Serão necessárias a aquisição dos itens abaixo, totalizando o custo estimado de **R$3.813.280,00** para um período de **24 (vinte e quatro) meses,** conforme memória de cálculo abaixo:

Item	Descrição	Unidade	Quant.	Valor Estim
1	Solução de inteligência cibernética, contendo licenças de uso de software, hardware, prestação de serviços e entregáveis, no formato de prestação de serviços, com monitoração e ação 24x7x365, suporte técnico, garantia e manutenção pelo período de 24 (vinte e quatro) meses, e pagamento em parcela	meses	01	R$ 3.590.0
2	Serviço de Ativação da Solução	unidade	01	R$ 74.0
3	Serviço de Operação Assistida	blocos de 04 horas	24	R$ 14.1
4	Treinamento (por pessoa)	servidores	06	R$ 135.0
VALOR TOTAL				**R$ 3.813.2**

Item	Descrição	Unidade	Quant.	Valor Estimado
1	Solução de inteligência cibernética, contendo licenças de uso de software, hardware, prestação de serviços e entregáveis, no formato de prestação de serviços, com monitoração e ação 24x7x365, suporte técnico, garantia e manutenção pelo período de 24 (vinte e quatro) meses, e pagamento em parcela	meses	01	R$ 3.590.000,00
2	Serviço de Ativação da Solução	unidade	01	R$ 74.000,00
3	Serviço de Operação Assistida	blocos de 04 horas	24	R$ 14.160,00
4	Treinamento (por pessoa)	servidores	06	R$ 135.020,00
VALOR TOTAL				**R$ 3.813.280,00**

5. Descrição solução TIC a ser contratada

5. Descrição da solução de TIC a ser contratada

5.1. CARACTERÍSTICAS GERAIS DA SOLUÇÃO

5.1.1. A solução deve ser dotada de tecnologia baseada em Inteligência Artificial a fim de identificar anomalias de comportamento e ataques sutis não identificados pelas tecnologias tradicionais de segurança da informação.

5.1.2. A solução deve identificar de forma autônoma, sem intervenção humana, todas as redes ativas no ambiente (que tiveram tráfego inspecionado) e apresentar uma relação com todas as

redes, máscara de rede, primeira vez em que a rede foi observada e quantidade de dispositivos observados na rede correspondente.

5.1.3. A solução, composta de hardware, software e serviço, deve ser fornecida na forma de prestação de serviços, com fornecimento de todos os licenciamentos, softwares e hardwares necessários para entrega e atendimento das especificações aqui definidas, durante todo o período contratual, com direito de uso de toda a tecnologia envolvida na solução, na versão mais recente publicada pelo desenvolvedor/fabricante, e com prazo de garantia (atualização, manutenção e suporte técnico) mínimo de 24 (vinte e quatro) meses.

5.1.4. Deve utilizar no mínimo os seguintes métodos de inteligência artificial para criação de perfis de uso e identificação de desvios comportamentais na rede:

5.1.4.1. Machine learning não supervisionado.

5.1.4.2. Machine learning supervisionado.

5.1.4.3. Deep Learning.

5.1.4.4. Redes Neurais.

5.1.5. A solução poderá ser formada por vários fabricantes e/ou serviços integrados por meio de API's (Application Programming Interface) ou única, sem a necessidade de desenvolvimento, desde que atenda todas as especificações técnicas deste Termo de Referência. Se na oferta da licitante contiver software a licitante não poderá ofertar soluções em desenvolvimento, soluções de código aberto ou software livre, em função da natureza dos serviços prestados pelo TRE-RN.

5.1.6. A solução deve permitir Threat Hunting, análise comportamental da rede e seus componentes, detecção de anomalia(s) e visibilidade de rede.

5.1.7. A solução deve ser capaz de aprender o comportamento da rede e de seus componentes (dispositivos e usuários) de forma autônoma e contínua, se adaptando a variações de comportamento destes durante o tempo.

5.1.8. Não serão aceitos produtos ou serviços OpenSource.

5.1.9. Todos os componentes devem ser oficialmente suportados pelo(s) fabricante(s) da solução em acordo com as condições especificadas.

5.1.10. A solução não deve depender de pré-configurações baseadas na rede do TRE-RN para que identifique associações entre múltiplos elementos da rede para que consiga identificar anomalias de comportamento.

5.1.11. A solução deve realizar todas as inspeções, processamento, análise e detecção de anormalidades e gerenciamento localmente, ou seja, é vedada qualquer forma de envio de dados para fora da rede do TRE-RN para o funcionamento da solução.

5.1.12. Solução deve realizar o aprendizado do ambiente de rede e inspeção do tráfego de forma off-line através de tráfego espelhado de porta nos switches, ou seja, não dependendo de qualquer escaneamento ativo, alteração de roteamento e fluxo de dados da rede.

5.1.13. A solução deve ser capaz de tomar ações autônomas de resposta contra ameaças e/ou ataques cibernéticos baseadas em sua inteligência artificial.

5.1.14. A solução deve ser capaz de integrar-se a soluções de segurança terceiras a fim de permitir ações adicionais de bloqueio contra ataques cibernéticos.

5.1.15. A solução deve permitir a inspeção de plataformas como:

5.1.15.1. Amazon AWS.

5.1.15.2. Microsoft Azure.

5.1.15.3. Google G-Suite.

5.1.15.4. Office 365/Microsoft 365.

5.1.15.5. Dropbox enterprise.

5.1.15.6. Componentes virtuais (máquinas virtuais).

5.1.15.7. Endpoint para Sistemas Operacionais.

5.1.15.8. Docker e Kubernet.

5.1.16. Deve ser dotada de interfaces que permitam o gerenciamento centralizado dos componentes da solução.

5.1.17. Deve ter a capacidade de personalizar a sua busca por ameaças cibernéticas.

5.1.18. Deverá possuir integração através de feeds com a ferramenta de análise interna.

5.1.19. Deverá ter capacidade de direcionar as pesquisas por ameaças cibernéticas levando em consideração os ativos críticos do TRE-RN, outros segmentos do mercado, localização e ameaças direcionadas.

5.1.20. Deve possuir características para enfatizar as ameaças urgentes e priorizá-las automaticamente.

5.1.21. Deve permitir que os usuários criem alertas dedicados com base em parâmetros definidos.

5.1.22. Deve permitir e oferecer análise constante de fluxo de inteligência acionável, baseada em contexto e que possa alertar os usuários sobre atividades cibernéticas suspeitas.

5.1.23. A solução deve permitir que os usuários realizem consultas ad-hoc ilimitadas para uma ou mais de suas fontes de dados.

5.1.24. A solução deve disponibilizar, permitir o monitoramento e coleta 24 horas por dia e 07 dias por semana dos fóruns fechados da Deep e Dark Web.

5.1.25. A solução deve disponibilizar monitoramento e coletas 24 horas por dia e 7 dias por semana dos marketplaces fraudulentos e de sites que vendem os números de cartões de crédito.

5.1.26. Possuir acesso a pelo menos 20 plataformas de compartilhamento de dados, onde os agentes de ameaças vazam dados, publicam código-fonte de malware e distribuem listas de alvos. As plataformas de compartilhamento de dados são os ambientes onde os hackers costumam vazar dados e demais informações das organizações que foram objeto de vazamento. É de suma importância identificar possíveis registros vazados como forma de

mitigar comprometimentos em sua infraestrutura e respectiva base de dados, ou mesmo códigos-fonte. Quanto maior for o número de plataformas de compartilhamento de dados, mais assertivo será o trabalho realizado pela solução. Este requisito está plenamente aderente à Portaria CNJ nº162 que trata da aprovação dos Protocolos e Manuais criados pela Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ). Os protocolos abordam os seguintes temas:

5.1.26.1. Prevenção de Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ).

5.1.26.2. Gerenciamento de Crises Cibernéticas do Poder Judiciário (PGCRC-PJ).

5.1.26.3. Investigação de Ilícitos Cibernéticos do Poder Judiciário (PIILC-PJ).

5.1.27. Possuir acesso no mínimo às seguintes redes anônimas: Darknet e Zeronet.

5.1.28. A coleta de dados para análise de ameaças deverá ser realizada diariamente.

5.1.29. A solução deverá permitir habilitar sua integração com vários produtos de inteligência do (s) fabricante(s).

5.1.30. A solução deverá possuir resposta automática e autônoma em tempo real a qualquer comportamento potencialmente ameaçador que tenha sido detectado na infraestrutura de rede do Tribunal.

5.1.31. A solução não deve depender de assinaturas predefinidas para respostas.

5.1.32. A solução deverá possuir um modelo padrão para identificar os usuários e demais dispositivos que tramitam informações pela rede, podendo executar ações diferentes dependendo do incidente identificado.

5.1.33. A solução deverá possuir controles personalizáveis para que seu uso seja agendado para horários fora do expediente normal do Tribunal, evitando atividades maliciosas e permitindo que as equipes investiguem os incidentes durante o horário de trabalho.

5.1.34. A solução deverá oferecer features de respostas proativas contra ameaças, sem interromper as atividades do Tribunal.

5.1.35. Possuir funcionalidade de bloquear as ameaças de forma proativa.

5.1.36. A solução deverá possuir funcionalidade que identifique que o dispositivo utilize conexões e transferência de dados que a solução considere como normal para esse dispositivo.

5.1.37. A solução deverá possuir capacidade de bloquear downloads de arquivos maliciosos de fontes não confiáveis.

5.1.38. A solução deverá ter capacidade de colocar em quarentena todo o tráfego de entrada e saída de um dispositivo, e se o problema persistir, efetuar o bloqueio do tráfego.

5.1.39. A solução deverá possuir uma lista, na ferramenta de gestão, para escolha dos firewalls que poderão ser instruídos quanto aos ataques cibernéticos.

5.1.40. A solução deverá, de forma automática, bloquear apenas a porta daquele dispositivo que está comprometido.

5.1.41. A solução deverá ser habilitada no console de uso de todas as outras ferramentas do(s) fabricante(s).

5.1.42. A solução deverá funcionar 24h x 7d x 365 dias do ano.

5.1.43. A solução deverá possuir mecanismos de proteção para usuários Vips.

5.1.44. A solução não deve trabalhar com defesas pré-programadas.

5.1.45. A solução deverá reconhecer um ataque mesmo que não tenha sido identificado ou definido pelos padrões e frameworks em uso pelo mercado.

5.1.46. A solução deverá possuir capacidade de resposta autônoma em toda a força de trabalho do tribunal, fornecendo proteção sob medida para serviços implantados em qualquer lugar (nuvem, IoT e na rede corporativa).

5.1.47. A solução deverá, por meio de integrações ativas, se conectar e aprimorar o ecossistema de segurança existente, informando aos dispositivos (tais como firewalls por exemplo) e dispositivos de rede sobre ataques ocorridos.

5.1.48. A solução deverá possuir capacidade de uso em aplicativos móveis.

5.1.49. A solução deverá entender quais eventos merecem uma resposta autônoma.

5.1.50. Solução deve buscar no Shodan, fóruns russos e DarkWeb, informações sobre IPs e servidores relacionados com o Tribunal e criar um dashboard com vulnerabilidades e severidades associadas com cada ativo encontrado.

5.1.51. A solução deve trazer gráficos e quadros de informação que apresentem estatísticas e KPIs de segurança, que permitam ao Tribunal verificar o nível de riscos, nível de exposição na DarkWeb, registros vazados na DarkWeb, entre outros.

5.1.52. A solução deve lidar com grandes volumes de dados (Big Data), por exemplo:

5.1.52.1. A partir da definição do que se deseja monitorar nas camadas da Web (Web aberta, Web privada, Deep Web e DarkWeb), o sistema deve ser capaz de coletar, analisar e organizar volumes de dados que ultrapassam milhões de dados.

5.1.53. A solução deve permitir que se faça consultas ad-hoc e individuais a fontes específicas da DarkWeb. Por exemplo, além de ser possível configurar "traga tudo da DarkWeb sobre essa 'expressão'", o Tribunal pode executar uma consulta a uma fonte específica como fórum particular de hackers russos.

5.1.54. Logo após criar um Plano de Monitoramento com as expressões e informações para monitoramento da DarkWeb e demais camadas da Web, a solução deve iniciar o monitoramento e mantê-lo 24/7 (fluxo de procura e chegada de informações constantes). Informações novas devem aparecer destacadas nas buscas.

5.1.55. A solução deve fornecer em dashboard, um "Feed" de notícias de segurança cibernética atuais, com comentários e sugestões. Esse Feed permitirá ao Tribunal ficar sempre atualizado quanto aos últimos acontecimentos cibernéticos. Deve também ser possível fazer buscas e filtros no Feed diário de cyber.

5.1.56. A solução deve mostrar quando há registros vazados do Tribunal (ou de organizações monitoradas) na DarkWeb. Deve mostrar a data do vazamento, o nome do vazamento, informações do vazamento e senha (quando houver). A senha deverá ser apresentada em texto claro, HASH ou outra forma encontrada no vazamento. A solução deve mostrar também uma descrição para o nome da base de dados onde foi encontrado o vazamento de dados.

5.1.57. A solução deverá ser capaz de realizar efetivo acompanhamento e monitoramento detalhado de possíveis registros vazados possibilitando mitigar ataques cibernéticos, onde os agressores, de posse de registros de acesso válidos, podem comprometer a infraestrutura dos tribunais. Ao identificar detalhes dos registros vazados, o tribunal pode analisar com maior riqueza de detalhes as origens dos vazamentos.

5.1.58. A solução deve ser capaz de monitorar TTPs (Táticas, Técnicas e Procedimentos) de atores de ameaça cibernéticos, incluindo ciber criminosos, estados nações, hacktivistas e cyber terroristas. Deve ser possível inclusive pesquisar dados do Framework MITRE-ATTACK.

5.1.59. O parque computacional do TRE-RN é composto por 2.042 (dois mil e quarenta e dois) ativos e todos devem fazer parte da solução proposta.

5.1.60. O parque computacional do TRE-RN é composto por 150 (cento e cinquenta) caixas postais consideradas VIPs e todas devem fazer parte da solução proposta.

5.1.61. Todas as pesquisas mensais no ambiente externo em Dark e Deep Web a serem administradas e realizadas pela CONTRATADA, devem contemplar no mínimo 50 (cinquenta) termos (uma frase, um nome, domínio,...) e também, pelo menos 01 (um) usuário com permissão de visualização para o Tribunal. Toda e qualquer alteração que o Tribunal queira fazer nos termos pesquisados, será enviada à CONTRATADA para que nova pesquisa seja realizada.

5.1.61.1. A quantidade mínima para os termos pesquisados referenciados no item 1.61, se aplica aos Tribunais com os Perfis de 1 a 4, conforme definido no Anexo X.

5.1.61.2. Para os Tribunais com Perfis 5 e 6, conforme definido no Anexo X, a quantidade mínima de termos pesquisados deve ser de até 100 termos por pesquisa realizada, e também deverá ser fornecido pela CONTRATADA 01 (um) usuário com permissão de visualização para o Tribunal.

5.1.61.3. Para o Tribunal com Perfil 7, conforme definido no Anexo X, a quantidade mínima de termos pesquisados deve ser de até 150 termos por pesquisa realizada, e também deverá ser fornecido pela CONTRATADA 01 (um) usuário com permissão de visualização para o Tribunal.

5.1.62. A solução deve ser capaz de aprender o comportamento da rede e de seus componentes (dispositivos e usuários) de forma autônoma e contínua, se adaptando a variações de comportamento destes ao longo do tempo.

5.2. CARACTERÍSTICAS TÉCNICAS DA SOLUÇÃO

5.2.1. A solução deverá identificar de forma autônoma, sem intervenção humana, todos os endereços IPs que trafegaram nas redes inspecionadas apresentando uma relação com no mínimo os seguintes dados:

5.2.1.1. Classificação do tipo de dispositivo (desktop, servidor, Impressora, câmera, iot, etc).

5.2.1.2. IP do dispositivo.

5.2.1.3. Mac Address.

5.2.1.4. Nome DNS do dispositivo.

5.2.1.5. Primeira vez que o dispositivo/IP foi visto na rede .

5.2.1.6. Última vez que o dispositivo foi visto na rede.

5.2.1.7. Deve ser possível visualizar o histórico de IPs de um determinado dispositivo baseado no IP provido pelo servidor DHCP.

5.2.2. A solução deve inspecionar e analisar os dados brutos da rede através de espelhamento de porta (SPAN/Port Mirror) ou através do uso de TAP – Terminal Access Point.

5.2.3. A solução deve suportar a ingestão de dados através de mecanismos de tunelamento de tráfego na camada 2 (enlace) do modelo OSI como VXLAN e ERSPAN.

5.2.4. A solução deve possuir mecanismos de DPI (Deep Packet Inspection).

5.2.5. A solução deve criar métricas, de forma autônoma, de raridade de Ips, domínios DNS, dispositivos e outros (etc), baseado na frequência que estes são acessados através da rede.

5.2.6. A solução deve criar métricas, de forma autônoma, de anormalidades comparando a ação atual de um dispositivo, usuário, IP, domínio etc. contra as ações de mesmo escopo realizadas no passado.

5.2.7. A métrica de anormalidade deve apresentar o percentual de desvio do comportamento atual de um dispositivo comparado com o comportamento passado aprendido.

5.2.8. A solução deve ser comprovadamente baseada em análise de comportamento permitindo a detecção de, no mínimo, as seguintes anomalias:

5.2.8.1. Dispositivo realizando conexões para destinos raros na internet não frequentemente visitados por dispositivos da rede interna.

5.2.8.2. Dispositivo se comunicando com um servidor externo usando um certificado auto assinado.

5.2.8.3. Dispositivo se comunicando com um servidor usando um certificado expirado.

5.2.8.4. Dispositivo se comunicando com um dispositivo externo usando um certificado inválido.

5.2.8.5. Dispositivo iniciando várias conexões para um IP externo raro de maneira regular. (Beaconing)

5.2.8.6. Dispositivo gerando um grande número de solicitações para servidores Web internos o qual está retornando códigos de erro HTTP.

5.2.8.7. Novo dispositivo entrou na rede e começou a utilizar o software de teste de penetração ou escaneamento de rede.

5.2.8.8. Vários dispositivos internos começaram a desviar de suas atividades normais e escanearam a rede interna.

5.2.8.9. Dispositivo fazendo requisições de DNS repetidas recebendo respostas com registro TXT. (Tunelamento via DNS).

5.2.8.10. Dispositivo se comunicando externamente via DNS de maneira consistente com o tunelamento de DNS.

5.2.8.11. Dispositivo fazendo conexões criptografadas para um domínio relacionado a DNS Dinâmico.

5.2.8.12. Dispositivo gerando um volume anormalmente alto de solicitações DNS.

5.2.8.13. Dispositivo fazendo uma série de conexões utilizando Hostnames raros que parecem não ter uma resolução de DNS legítima.

5.2.8.14. Um servidor DNS interno está agindo como um resolvedor de DNS aberto (OpenDns).

5.2.8.15. Dispositivo se comunicando com o serviço de anonimização da rede TOR.

5.2.8.16. Dispositivo se comunicando com a rede Tor por meio de um Web Service intermediário.

5.2.8.17. Atividade anormal de PowerShell e o Windown Romote Mamagement, seguido por uma conexão a um destino externo raro seguido de download de arquivo suspeito.

5.2.8.18. Dispositivo executando comandos PsExec em uma máquina remota que nunca havia recebido tráfego similar anteriormente.

5.2.8.19. Dispositivo se conectando repetidamente a destinos externos que não possuem nomes legíveis para humanos.

5.2.8.20. Dispositivo detectado conectando-se a hostnames identificados como trojans financeiros.

5.2.8.21. Dispositivo fazendo conexões com hostnames raros associados a uma botnet.

5.2.8.22. Dispositivo solicitando um domínio conhecido por hospedar malwares.

5.2.8.23. Dispositivo gravando arquivos com nomes suspeitos, relacionado a ransomware, em Servidores de Arquivos da rede SMB.

5.2.8.24. Dispositivo transferindo um volume de moderado a grande de dados para fora da rede durante um período de 24 horas ou mais por meio de um grande volume de conexões.

5.2.8.25. Dispositivo fazendo download de dados de um sistema interno e fazendo upload de volumes de dados semelhantes para destino externo.

5.2.8.26. Dispositivo se comunicando com domínios suspeitos na internet e, ao mesmo tempo, realizando comportamentos incomuns de SMB na rede interna.

5.2.8.27. Dispositivo acessando uma grande quantidade de compartilhamentos SMB que não foram acessados anteriormente pelo mesmo dispositivo.

5.2.8.28. Dispositivo enviando um grande volume de dados para um IP externo que raramente é utilizado por qualquer dispositivo na rede interna.

5.2.8.29. Dispositivo fazendo conexões web externas sem usar um proxy web.

5.2.8.30. Dispositivo sendo bloqueado repetidamente por um proxy web durante um período de várias horas.

5.2.8.31. Dispositivo solicitando informações de configuração de proxy (WPAD) para um IP externo.

5.2.8.32. Dispositivo fazendo conexões HTTP suspeitas, de forma repetitiva, diretamente para um endereço IP sem utilizar um Hostname.

5.2.8.33. Dispositivo foi redirecionado para um Hostname HTTP raro e em seguida baixou um executável ou outro arquivo binário.

5.2.8.34. Dispositivo causando repetidos picos de conexões HTTP ou SSL na rede interna ou para a internet.

5.2.8.35. Dispositivo fazendo requisições HTTP suspeitas repetidamente em portas não padrão.

5.2.8.36. Dispositivo fazendo download de um arquivo que não corresponde ao seu 'File Type' de uma fonte externa que a rede normalmente não acessa.

5.2.8.37. Dispositivo fazendo download de arquivo executável vindo de uma fonte a qual não é comumente acessada por dispositivos da rede interna.

5.2.8.38. Dispositivo fazendo download de arquivo comprimido vindo de uma fonte a qual não é comumente acessada por dispositivos da rede interna.

5.2.8.39. Dispositivo fazendo download de um arquivo suspeito e em seguida fez uma conexão para um destino externo com o qual a rede normalmente não se comunica.

5.2.8.40. Dispositivo usando uma plataforma externa de armazenamento de arquivos de terceiros.

5.2.8.41. Dispositivo enviando dados para o Pastebin.

5.2.8.42. Dispositivo usando um sistema terceiro de mensageria (Whatsapp ou similares).

5.2.8.43. Dispositivo acessando rede social (Facebook ou similares).

5.2.8.44. Dispositivo se comunicando com um destino raro na internet usando portas normalmente usadas apenas na rede interna.

5.2.8.45. Dispositivo fazendo conexões peer-to-peer BitTorrent.

5.2.8.46. Dispositivo recebeu um número anormalmente grande de conexões de entrada de IP externos raros.

5.2.8.47.Dispositivo fazendo conexões SQL para IPs externos a rede.

5.2.8.48. Dispositivo enviando uma quantidade anormal alta de dados para destinos fora da rede.

5.2.8.49. Dispositivo trocando um volume de dados anormal com outro dispositivo na rede interna.

5.2.8.50. Dispositivo enviando uma quantidade anormalmente alta de dados externamente para um local para o qual a rede não enviou dados anteriormente.

5.2.8.51. Dispositivo explorando vulnerabilidade Heartbleed na rede interna.

5.2.8.52. Dispositivo se conectando a um DNS SinkHole conhecido.

5.2.8.53. Dispositivo realizando grandes volumes de pequenas conexões SSH e/ou RDP.

5.2.8.54. Dispositivo iniciando um grande número de conexões para um servidor RDP e/ou SSH.

5.2.8.55. Dispositivo recebendo um grande número de conexões RDP de entrada de IPs externos raros.

5.2.8.56. Alteração no comportamento de tráfego DHCP.

5.2.8.57. Novo servidor DNS na rede.

5.2.8.58. Novo servidor de proxy web na rede.

5.2.8.59. Uma senha de credencial de alto privilégio foi alterada no domínio Windows.

5.2.8.60. Uma credencial efetuando login de uma origem incomum.

5.2.8.61. Uma credencial foi usada em múltiplos dispositivos internos.

5.2.8.62. Um dispositivo gerou um grande número de falhas de sessão SMB.

5.2.8.63. Um dispositivo desviou de suas atividades normais criando várias falhas de login Kerberos.

5.2.9. Deve ser possível criar regras utilizando um ou mais dos componentes do item acima.

5.2.10. Todos os dados processados pela solução devem ser armazenados para posterior análise independentemente de terem gerado alertas ou não.

5.2.11. A solução deve possuir mecanismos para exportar os dados armazenados no padrão de extensão ‘.pcap’.

5.2.12. Deve ser capaz de agrupar de forma autônoma dispositivos em grupos baseado em sua similaridade de comportamento.

5.2.13. Deve ser capaz de tomar ações baseadas em desvio de comportamento.

5.2.14. Deve possuir a capacidade de quarentenar ou semi-quarentenar temporariamente dispositivos na rede.

5.2.15. Deve possuir a habilidade para responder e/ou parar ameaças autonomamente.

5.2.16. Deve ser capaz de marcar dispositivos automaticamente para decisões de resposta e ajuste fino.

5.2.17. Deve ser altamente configurável permitindo vários níveis de resposta a uma anomalia na rede.

5.2.18. Deve ser capaz de registrar todas as ações de resposta para propósitos de auditoria.

5.2.19. Deve ser configurável para supervisão e aprovação de analistas em ações de tomada de decisão / resposta.

5.2.20. Capacidade de personalizar a sua busca por ameaças cibernéticas.

5.2.21. Deverá possuir integração através de feeds com a ferramenta de análise interno.

5.2.22. Capacidade de direcionar as pesquisas por ameaças cibernéticas levando em consideração ativos críticos do TRE-RN, outros segmentos do mercado, localização e ameaças direcionadas.

5.2.23. Possuir funcionalidade de personalização dos usuários, para fácil acesso às ameaças ao TRE-RN.

5.2.24. Possuir uso de algoritmos de pontuação de ameaças baseados nos fluxos de trabalho e processo de análise de pesquisadores experientes em inteligência de ameaças cibernéticas.

5.2.25. Possuir características para enfatizar as ameaças urgentes e priorizá-las automaticamente.

5.2.26. Permitir que os usuários criem alertas dedicados com base em parâmetros definidos.

5.2.27. Oferecer análise constante de fluxo de inteligência acionável, baseada em contexto e que possa alertar os usuários sobre atividades cibernéticas suspeitas.

5.2.28. Oferecer cruzamento automático das descobertas de ameaças com um repositório de inteligência final e histórico para aumentar a consciência situacional da organização.

5.2.29. Permitir que os usuários possam gerenciar os incidentes.

5.2.30. A solução deverá disponibilizar um conjunto pré-configurado de filtros estatísticos dedicados ao campo de inteligência de ameaças.

5.2.31. A solução deve permitir consultas ad-hoc ilimitadas para uma ou mais de suas fontes de dados, mantendo correlação com as quantidades de termos descritas no item 1.61 e respectivos subitens.

5.2.32. A solução de inteligência cibernética, deverá possuir recursos necessários para compreensão de ameaças em mais de 20 idiomas, incluindo:

5.2.32.1. Russo.

5.2.32.2. Chinês.

5.2.32.3. Farsi.

5.2.32.4. Árabe.

5.2.32.5. Idiomas europeus.

5.2.32.6. Inglês.

5.2.32.7. Hebraico.

5.2.33. Disponibilizar monitoramento e coleta 24 horas por dia e 7 dias por semana dos fóruns fechados da Deep e Dark Web.

5.2.34. Disponibilizar monitoramento e coletas 24 horas por dia e 7 dias por semana dos marketplaces fraudulentos.

5.2.35. Permitir acesso a possíveis dados do TRE-RN vazados e postados em mais de 20 plataformas de compartilhamento de dados (isto é sites de colagem – ambiente onde possíveis invasores costumam divulgar dados vazados, além de também serem usados para publicar códigos-fonte de malwares e listas de possíveis alvos).

5.2.36 Possuir domínios de especialização, incluindo minimamente, crimes financeiros, hacktivismo e ciberterrorismo.

5.2.37. Possuir acesso a pelo menos 20 plataformas de compartilhamento de dados, onde os agentes de ameaças vazam dados, publicam código-fonte de malware e distribuem listas de alvos. As plataformas de compartilhamento de dados são os ambientes onde os hackers costumam vazar dados e demais informações das organizações que foram objeto de vazamento. É de suma importância identificar possíveis registros vazados como forma de mitigar comprometimentos em sua infraestrutura e respectiva base de dados, ou mesmo códigos-fonte. Quanto maior for o número de plataformas de compartilhamento de dados, mais assertivo será o trabalho realizado pela solução. Este requisito está plenamente aderente à Portaria CNJ nº162 que trata da aprovação dos Protocolos e Manuais criados pela Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ). Os protocolos abordam os seguintes temas:

5.2.37.1. Prevenção de Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ).

5.2.37.2. Gerenciamento de Crises Cibernéticas do Poder Judiciário (PGCRC-PJ).

5.2.37.3. Investigação de Ilícitos Cibernéticos do Poder Judiciário (PIILC-PJ).

5.2.38. Possuir acesso as seguintes redes anônimas: Darknet e Zeronet.

5.2.39. A coleta de dados para análise de ameaças deverá ser realizada diariamente.

5.2.40. Todos os requisitos mencionados entre os itens 2.20 a 2.39 neste Anexo I ao Termo de Referência, deverão ser suportados e monitorados pela CONTRATADA, podendo ser externo ao ambiente do Tribunal, em uma segunda console de visualização.

5.2.41. A solução, deverá possuir documentação que habilite a integração da solução com vários produtos de inteligência do fabricante.

5.2.42. Disponibilizar painel com KPIs de segurança que pode ser customizado pelo TRE-RN.

5.2.43. Obter informações de repositórios de códigos GitHub.

5.2.44. Obter informações da Zeronet.

5.2.45. Permitir ao TRE-RN organizar plano de mitigação de ameaça por dentro da solução, trazendo também recomendações pré configuradas.

5.2.46. Solução deve ter algoritmo de threat scoring para priorizar as ameaças identificadas.

5.2.47. A solução deverá suportar, no mínimo, os seguintes servidores/serviços de e-mail:

5.2.47.1. Google Gmail e Microsoft Exchange (Microsoft 365 ou Office 365).

5.2.47.2. A solução deverá considerar o quantitativo de 150 caixas postais prioritárias, estabelecidas pelo TRE-RN e que serão informadas oportunamente a CONTRATADA.

5.2.47.3. Dado a característica do serviço do Google Gmail e do Microsoft Exchange (Microsoft 365 ou Office 365) o qual são executados na nuvem, será aceito processamento do tráfego de e-mails em ambiente externo ao ambiente do órgão.

5.2.48. A solução deve realizar a inspeção de todos os e-mails recebidos e enviados de forma offline, ou seja, sem a necessidade da alteração do fluxo de emails entre clientes e MTA (Mail Tranfer Agent) do órgão.

5.2. 49. A solução deverá armazenar o histórico de e-mails enviados e recebidos independentemente se estes foram considerados anômalos ou não.

5.2.50. A solução deverá correlacionar de forma autônoma, sem intervenção humana, as caixas de correspondência (mailboxes) aos respectivos dispositivos internos na rede do órgão que acessam cada mailbox.

5.2.51. A solução deve identificar e proteger o ambiente de e-mail do órgão contra as seguintes anomalias:

5.2.51.1. Spoofing.

5.2.51.2. Links anômalos/suspeitos.

5.2.51.3. Anexos suspeitos.

5.2.51.4. SPAM.

5.2.51.5. Phising/Spearphishing.

5.2.51.6. Sequestro de conta de e-mail.

5.2.51.7. Envio de dados sensíveis para fora do órgão.

5.2.52. A solução deve realizar a inspeção e apresentar os dados de, no mínimo, os seguintes parâmetros para cada e-mail:

5.2.52.1. Sender Policy Framework (SPF).

5.2.52.2. Domain Keys Identified Mail (DKIM).

5.2.52.3. Forwarded-confirmed Reverse DNS (FCRDNS).

5.2.52.4. IP do servidor de e-mail de origem e seu ASN correspondente.

5.2.52.5. Todos os cabeçalhos do e-mail.

5.2.52.6. Anexos (se existentes), nome dos anexos, tamanho, mime type, quantidade de vezes em que o anexo foi observado em caixas postais.

5.2.53. A solução deve permitir a tomada de ações contra e-mails como:

5.2.53.1. Reter o e-mail no servidor de e-mail evitando que a correspondência anômala seja enviada para o destinatário.

5.2.53.2. Entregar o e-mail para o cliente direcionando-o para a pasta de lixo eletrônico do cliente.

5.2.53.3. Substituir um link considerado anômalo por um link gerado pela solução a fim de evitar que o usuário acesse o link original, mas ao mesmo tempo mantendo o registro da tentativa de acesso ao novo link (substituído pela solução).

5.2.53.4. Remover link do e-mail substituindo-o por uma mensagem informando o usuário que o link foi removido por questões de segurança.

5.2.53.5. Remover anexos do e-mail original antes do envio para o cliente.

5.2.53.6. Converter anexos anômalos para o padrão PDF. Quando a conversão não for possível o anexo deverá ser removido.

5.2.53.7. Remover o nome do remetente (unspoof) apresentando o endereço de e-mail completo do mesmo.

5.2.53.8. Adicionar banner (mensagem customizada) ao e-mail antes do envio para o cliente.

5.2.53.9. Enviar uma notificação para e-mail terceiro para posterior análise quando um e-mail original contiver algum dado de interesse ou apresentar alguma anomalia.

5.2.54. A solução deve apresentar, para cada e-mail identificado como anômalo:

5.2.54.1. Índice de anomalia do e-mail.

5.2.54.2. Categoria(s) que apresentam o motivo da anomalia.

5.2.54.3. Ações tomadas contra o e-mail, de acordo com item 2.53.

5.2.54.4. Dados sobre o remetente de acordo com item 2.52.

5.2.54.5. Se o e-mail contiver link, apresentar o link, seu índice de anomalia, motivos para ser classificado como anômalo e se o link foi acessado pelo cliente.

5.2.55. A solução deve apresentar uma listagem de todas as caixas postais ativas e inativas do ambiente. Para cada mailbox a solução deverá apresentar no mínimo as seguintes informações:

5.2.55.1. Nome do usuário baseado no atributo do Azure Active Directory (O365).

5.2.55.2. Grupos do Azure Active Directory (O365) a qual o usuário faz parte.

5.2.55.3. Mapa de interações freqüentes com usuários externos agrupados por domínio.

5.2.55.4. Lista de Alias da caixa postal.

5.2.55.5. Dispositivo dentro da rede do órgão o qual foi observado utilizando a caixa postal.

5.2.55.6. Índice de risco da caixa postal.

5.2.55.7. Índice de prevalência para spoofing da caixa postal.

5.2.55..8. Lista de ações tomadas a e-mails anômalos, de acordo com o item 2.54, e a respectiva quantidade de ações tomadas.

5.2.55.9. Quantidade de e-mails enviados e recebidos nos últimos 7 dias.

5.2.56. A solução deve permitir a procura de e-mails baseado em qualquer informação disponível no cabeçalho dos e-mails.

5.2.57. A solução deve possuir interface apresentando a quantidade de e-mails recebidos em um período de tempo, a quantidade de ações tomadas nas contas de e-mails e o percentual total de ações tomadas.

5.2.57.1 Deve apresentar as ações tomadas, quantidade de e-mails acionados por cada grupo de ações, motivo para a ação tomada, quantidade de e-mails lidos pelos usuários e link para acessar os e-mails acionados individualmente.

5.2.58. A solução deve apresentar tendências (aumento ou diminuição) sobre quantidade de e-mails recebidos e anomalias identificadas.

5.2.59. A solução deve identificar, de forma autônoma, o recebimento e/ou envio de e-mails para contas pessoais hospedadas em servidores de e-mail externo ao órgão.

5.2.60. A solução não deve depender de configurações específicas baseadas no ambiente de e-mail do órgão para funcionar, porém deve permitir a customização de regras se necessário for.

5.2.61. Solução deve permitir a busca por atores de ameaça cibernético, sendo necessário o seguinte:

5.2.61.1. Identificar blogs, fóruns, serviços de mensageria, mercados negros onde o ator de ameaça está presente.

5.2.61.2. Apresentar posts realizados pelo ator de ameaça em cada fonte.

5.2.61.3. Extrair de forma automática palavras do ator de ameaça em cada fonte de informação identificada.

5.2.61.4. Extrair entidades como IPs, e-mails dos posts realizados pelo ator de ameaça em cada fonte de informação identificada.

5.2.62. A solução deve permitir:

5.2.62.1. Descobrir IPs e servidores a partir de nomes associados com a organização.

5.2.62.2. Filtros por severidade, de forma a encontrar IPs e servidores com vulnerabilidades mais graves.

5.2.62.3. Mostrar a origem das informações e a data de atualização da informação apresentada.

5.2.63. A solução deve permitir aos analistas criar incidentes, vincularem informações aos incidentes e compartilhar informações entre analistas cibernéticos.

5.2.64. A solução deve fornecer workflows de mitigação para as atividades e riscos encontrados.

5.2.65. Deve ser possível à solução definir tarefas de mitigação para os itens encontrados /filtrados da pesquisa.

5.2.66. O sistema deve gerar relatórios de inteligência contendo os KPIs e informações coletadas de todas as camadas da Web.

5.2.67. A solução deve prover acesso a dados compartilhados em sistemas de compartilhamentos de textos (como Pastebin), tanto na Web aberta como DarkWeb.

5.2.68. A solução deve permitir monitoramento de repositórios de códigos, incluindo o GitHub, onde criminosos muitas vezes colocam e compartilham suas ferramentas.

5.2.69. A solução deve permitir o monitoramento de banco de dados de vulnerabilidades como NVD, CVEDetails e Exploit-DB.

5.2.70. A solução deve permitir a coleta de dados por Feeds RSS.

5.2.71. A solução deve permitir a coleta e análise de dados de plataformas de mensagens instantâneas, como o Telegram, onde vários criminosos montam seus planos de ataque.

5.2.72. A solução deve permitir pesquisas por IOCs – Indicadores de Comprometimento, relacionados a determinada ameaça ou incidente cibernético.

5.2.73. A solução deve trazer auditoria, a fim de monitorar as ações dos usuários dentro da solução.

5.2.74. A solução deve exportar dados (como IOCs) por API no formato STIX.

5.2.75. A solução deve permitir buscas e análise de resultados vindos do Shodan.

5.2.76. A solução deve permitir buscas por carteiras de criptomoedas, assim como buscar expressões ligadas às criptomoedas, como Bitcoin, Ethereum e outros.

5.2.77. A solução deve permitir filtrar por línguas o conteúdo extraído das fontes de coleta. Deve ser possível filtrar todo conteúdo que está escrito em português Brasil.

5.2.78. A solução deve trazer um Manual de instruções embutido na interface.

5.3. CARACTERÍSTICAS DE GERENCIAMENTO

5.3.1. O gerenciador deve possuir controle de interface gráfica (GUI: Graphical User Interface) e interface texto (CLI).

5.3.2. A interface de texto (CLI) deve possuir comandos para permitir a realização de troubleshooting.

5.3.3. A interface gráfica não deve ser desenvolvida ou conter componentes baseados em java por questões de compatibilidade com browsers modernos.

5.3.4. A interface gráfica deve possuir no mínimo:

5.3.4.1. Lista de alertas de anormalidade identificadas.

5.3.4.2. Critérios de filtro dos alertas de anormalidade por categoria de alerta, dispositivo ou usuários.

5.3.4.3. Critérios de filtro de período (data e horário) para os alertas de anormalidade.

5.3.4.4. Critérios de filtro de prioridade (risco) para os alertas de anormalidade.

5.3.4.5. Apresentar a posição geográfica das redes no ambiente de TI.

5.3.4.6. Opções de configuração do sistema.

5.3.4.7. Área de gerenciamento de usuários.

5.3.4.8. Área para gerenciamento de arquivos pcap, exportação e visualização na própria interface.

5.3.4.9. Área de busca de dados na base de dados da solução.

5.3.5. Os alertas de anomalia devem conter no mínimo os seguintes dados:

5.3.5.1. Identificador único (Unique ID).

5.3.5.2. Data e horário.

5.3.5.3. Dispositivo que originou a ação.

5.3.5.4. Apresentar o IP de origem do dispositivo.

5.3.5.5. Apresentar o MAC address do dispositivo.

5.3.5.6. Apresentar o Hostname (DNS) do dispositivo.

5.3.5.7. Apresentar o (s) usuário(s) que se eventualmente se logaram no dispositivo nas últimas horas.

5.3.5.8. Apresentar o a rede a qual o dispositivo estava conectado.

5.3.5.9. Descrição técnica do evento.

5.3.5.10. Gráfico apresentando a quantidade de eventos similares e evolução do nível de risco.

5.3.5.11. Atalho para acesso rápido às configurações da política que gerou o alerta.

5.3.5.12. Dados técnicos resumidos das ações que causaram a anomalia e subsequente alerta.

5.3.5.13. Atalho para acessar dados detalhados das ações que causaram a anomalia e subsequente alerta.

5.3.5.14. Durante a investigação de uma anomalia/alerta o administrador pode acessar os dados abaixo utilizando apenas o mouse:

5.3.5.14.1. Dados detalhados do dispositivo que originou a anomalia.

5.3.5.14.2. IP do dispositivo.

5.3.5.14.3. Mac Address.

5.3.5.14.4. Nome DNS do dispositivo.

5.3.5.14.5. Primeira vez que o dispositivo/IP foi visto na rede.

5.3.5.14.6. Última vez que o dispositivo foi visto na rede.

5.3.5.14.7. Apresentar o (s) usuário(s) que se eventualmente se logou(aram) no dispositivo.

5.3.5.14.8. Apresentar a rede a qual o dispositivo estava conectado.

5.3.5.14.9. Acesso a todas as comunicações realizadas pelo dispositivo na rede.

5.3.5.14.10. Acesso a todas as anomalias as quais o dispositivo gerou na rede.

5.3.6. Acesso a ferramenta para geração de gráficos que facilitem a investigação utilizando critérios como, mas não limitados a:

5.3.6.1. Dados relacionados a conexões.

5.3.6.2. Tráfego de dados.

5.3.6.3. Requisições DNS.

5.3.6.4. Erros de Login.

5.3.6.5. Ações utilizando SMB.

5.3.6.6. Apresentar gráfico representando os fluxos de comunicação entre os dispositivos que originaram e receberam tráfego anômalo.

5.3.7. A solução deve possuir mecanismo para automação de investigação de alertas permitindo a correlação entre múltiplos eventos apresentando em uma única tela as seguintes informações:

5.3.7.1. Linha do tempo apontando a correlação entre alertas emitidos para um determinado dispositivo, data e horário em que cada alerta foi emitido bem como o período em que cada ação anômala, que gerou o alerta, ocorreu.

5.3.7.2. Apresentação individual de cada alerta contendo:

5.3.7.2.1. Descrição do comportamento anômalo e riscos associados.

5.3.7.3. Dados técnicos relacionados ao alerta como:

5.3.7.3.1. Período em que a anomalia foi observada.

5.3.7.3.2. IP de origem.

5.3.7.3.3. IP(s) de destino.

5.3.7.3.4. Credencial de usuário observada no dispositivo.

5.3.7.3.5. Ação anômala identificada pela solução.

5.3.7.3.6. Acesso aos logs do tráfego anômalo.

5.3.7.3.7. Deverá classificar cada alerta baseado em fases de ataque.

5.3.7.4. Deve permitir ao administrador exportar todas as informações do item 3.7.3 em documento padrão .pdf.

5.3.8. A interface deve permitir a procura e navegação de qualquer dispositivo, usuário, Ips, etc que tenham sido inspecionados em qualquer data armazenada pela solução.

5.3.9. Ao navegar pelas comunicações do dispositivo o administrador pode utilizar filtros baseados em IP, Porta e Protocolo para facilitar a visualização.

5.3.10. Ao navegar pelas comunicações do dispositivo o administrador pode utilizar um IP de destino como filtro permitindo a investigação de ‘Origem > Destino’ ou ‘Destino > Origem’.

5.3.11. Ao navegar pelas comunicações de um usuário o administrador pode analisar todo o histórico de login do mesmo contendo a data, o ip de origem do dispositivo que utilizou a credencial do usuário e estado da autenticação.

5.3.12. O administrador pode gerar arquivos ‘.pcap’ para quaisquer comunicação inspecionada pela solução.

5.3.13. A solução deve se integrar com serviço LDAP a fim de possibilitar a autenticação e autorização de usuários na interface de administração e para consultas com objetivos de enriquecer os dados inspecionados.

5.3.14. A solução deve permitir a utilização de segundo fator de autenticação para logins na interface web.

5.3.15. A solução deve possuir mecanismo de gerenciamento de usuários da interface web permitindo:

5.3.15.1. Criação, modificação ou remoção de usuários.

5.3.15.2. Gerenciamento de permissionamento dos usuários.

5.3.15.3. Opção de gerar usuário com permissão de leitura apenas.

5.3.15.4. Deve possuir interface para visualização dos aspectos do sistema como:

5.3.15.4.1. A versão de software, espaço utilizado em disco, consumo de CPU e consumo de memória.

5.3.15.4.2. Informação de todas as interfaces ativas e respectivo tráfego recebido através de cada uma delas.

5.3.15.4.3. Total de banda processada no momento, a média de banda processada e o pico de banda registrado nas últimas semanas.

5.3.15.5. Uma análise detalhada de todo o tráfego recebido no dispositivo bem como a última vez em que os principais protocolos foram vistos dentre eles, HTTP, HTTPS, FTP, LDAP, SMTP, SSH, SMB, SSDP, POP3, NTLM, IMAP, Kerberos, dentre outros.

5.3.15.6. Listagem de todas as sub redes identificadas no ambiente bem como a quantidade de dispositivos em cada sub rede.

5.3.16. Deve permitir o envio de e-mails de alertas emitidos pela solução.

5.3.17. Deve permitir o envio de logs para sistemas externos utilizando os seguintes padrões:

5.3.17.1. CEF.

5.3.17.2. LEEF.

5.3.17.3. JSON.

5.3.17.4. Syslog.

5.3.18. Deve permitir a integração com plataformas de Threat Inteligence utilizando os protocolos STIX/TAXII.

5.3.19. A plataforma deve possuir OPEN API para suportar integração com sistemas terceiros.

5.3.20. Deve possuir Inteligência artificial para automatizar triagens, análises e investigações de ameaças.

5.3.21. Deve possuir um aplicativo mobile capaz de visualizar, responder a incidentes, notificar, reportar e aprovar remediações para Android e iOS.

5.3.22. Deve possuir painel incorporado para executar consultas em metadados no tráfego inspecionado.

5.4. CARACTERÍSTICAS DE GERENCIAMENTO DE RELATÓRIOS

5.4.1. Deve permitir a criação automática de relatórios executivos cobrindo no mínimo:

5.4.1.1. Indicação da quantidade total de dispositivos, quantidade total de sub redes e banda média processada.

5.4.1.2. Sumário das violações por fase do ataque.

5.4.1.3. Sumário dos dispositivos com maior nível de brechas não usuais.

5.4.1.4. Sumário dos top dispositivos que mais violaram comportamentos anômalos.

5.4.1.5. Violações mais frequentes a principais itens de compliance como: uso de USB no dispositivo, google drive, tráfego RDP saindo da rede, acesso a servidor SQL através da internet, e serviços similares oferecidos pela Microsoft, dentre outros.

5.4.1.6. Sumário dos dispositivos que mais violaram os itens de compliance gerando risco a organização.

5.4.2. Deve permitir que o relatório seja exportado para documento padrão .PDF e/ou .csv.

5.4.3. Deve possuir mecanismo para busca de dados diretamente na base de dados da solução.

5.4.4. O administrador pode gerar pesquisas e relatório dos seguintes critérios, mas não limitados a:

5.4.4.1. Data e Horário.

5.4.4.2. Endereços IPs de origem e destino.

5.4.4.3. Versão do protocolo IP.

5.4.4.4. Protocolo de comunicação.

5.4.4.5. Estado da conexão.

5.4.4.6. Dados trafegados de entrada e saída.

5.4.4.7. Método HTTP.

5.4.4.8. Cabeçalhos HTTP.

5.4.4.9. Versão do SSL.

5.4.4.10. Cifragem da Conexão SSL.

5.4.4.11. Logins Kerberos.

5.4.4.12. Comunicações DNS.

5.4.4.13. Comunicações FTP.

5.4.4.14. Comunicações LDAP.

5.4.4.15. Comunicações Kerberos.

5.4.4.16. Comunicações de mineração de criptomoedas.

5.4.4.17. Comunicações SMB.

5.4.4.18. Comunicações Radius.

5.4.4.19. Comunicações RDP.

5.4.4.20. Comunicações SIP.

5.4.5. A procura na base da solução deve apresentar resultados em menos de 5 minutos de execução independentemente do escopo da pesquisa.

5.5. CARACTERÍSTICAS GERAIS DO HARDWARE

5.5.1. Deverá ser fornecido para monitoramento do ambiente interno na modalidade física, equipamentos Appliances em comodato, (após o término da vigência do contrato, serão retirados pela CONTRATADA) capazes de processar o tráfego dos Tribunais. As informações contidas nesses equipamentos, não devem ser processadas fora do ambiente dos mesmos, somente internamente.

5.5.2. Deve ser fornecido em uma arquitetura MASTER-SLAVE (Appliances) aonde toda a análise e correlação dos dados será realizada localmente, e apenas metadados serão encaminhados para o MASTER (administração centralizada) de forma a não onerar a rede.

5.5.3. Deverá ser entregue equipamento único baseado em Appliance para maior segurança. Não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais podem instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris ou GNU/Linux.

5.5.4. Para atender às necessidades de todos os Tribunais quanto a solução que será fornecida, foram definidos alguns tipos e portes de equipamentos, conforme detalhamento abaixo:

5.5.4.1. Equipamento Tipo 1

5.5.4.1.1. Deverá suportar throughput de até 500Mbps.

5.5.4.1.2. Deverá ter capacidade de analisar e identificar 1.500 dispositivos.

5.5.4.1.3. Deverá suportar e analisar até 25.000 conexões por minuto.

5.5.4.1.4. Deverá considerar a inspeção de até 50 caixas postais prioritárias (VIP’s).

5.5.4.1.5. Deverá possuir 1 (uma) interface padrão 100/1000 BASE-T para atuar como interface de administração.

5.5.4.1.6. Deverá possuir pelo menos 2 (duas) interfaces padrão 100/1000 BASE-T para atuarem como interfaces de análise de tráfego.

5.5.4.1.7. Deverá possuir pelo menos 2 (duas) interfaces padrão 10 Gbe SFP+ para atuarem como interface de análise de tráfego.

5.5.4.1.8. O hardware fornecido deverá possuir fonte de alimentação redundante

5.5.4.2. Equipamento Tipo 2

5.5.4.2.1. Deverá suportar throughput de até 01Gbps.

5.5.4.2.2. Deverá ter capacidade de analisar e identificar 2.000 dispositivos.

5.5.4.2.3. Deverá suportar e analisar até 50.000 conexões por minuto.

5.5.4.2.4. Deverá considerar a inspeção de até 100 caixas postais prioritárias (VIP’s).

5.5.4.2.5. Deverá possuir 1 (uma) interface padrão 100/1000 BASE-T para atuar como interface de administração.

5.5.4.2.6. Deverá possuir pelo menos 2 (duas) interfaces padrão 100/1000 BASE-T para atuarem como interfaces de análise de tráfego.

5.5.4.2.7. Deverá possuir pelo menos 2 (duas) interfaces padrão 10 Gbe SFP+ para atuarem como interface de análise de tráfego.

5.5.4.2.8. O hardware fornecido deverá possuir fonte de alimentação redundante.

5.5.4.3. Equipamento Tipo 3

5.5.4.3.1. Deverá suportar throughput de até 02Gbps.

5.5.4.3.2. Deverá ter capacidade de analisar e identificar 2.500 dispositivos.

5.5.4.3.3. Deverá suportar e analisar até 75.000 conexões por minuto.

5.5.4.3.4. Deverá considerar a inspeção de até 150 caixas postais prioritárias (VIP’s).

5.5.4.3.5. Deverá possuir 1 (uma) interface padrão 100/1000 BASE-T para atuar como interface de administração.

5.5.4.3.6. Deverá possuir pelo menos 2 (duas) interfaces padrão 100/1000 BASE-T para atuarem como interfaces de análise de tráfego.

5.5.4.3.7. Deverá possuir pelo menos 2 (duas) interfaces padrão 10 Gbe SFP+ para atuarem como interface de análise de tráfego.

5.5.4.3.8. O hardware fornecido deverá possuir fonte de alimentação redundante.

5.5.4.4. Equipamento Tipo 4

5.5.4.4.1. Deverá suportar throughput de até 03Gbps.

5.5.4.4.2. Deverá ter capacidade de analisar e identificar 3.500 dispositivos.

5.5.4.4.3. Deverá suportar e analisar até 100.000 conexões por minuto.

5.5.4.4.4. Deverá considerar a inspeção de até 200 caixas postais prioritárias (VIP’s).

5.5.4.4.5. Deverá possuir 1 (uma) interface padrão 100/1000 BASE-T para atuar como interface de administração.

5.5.4.4.6. Deverá possuir pelo menos 2 (duas) interfaces padrão 100/1000 BASE-T para atuarem como interfaces de análise de tráfego.

5.5.4.4.7. Deverá possuir pelo menos 2 (duas) interfaces padrão 10 Gbe SFP+ para atuarem como interface de análise de tráfego.

5.5.4.4.8. O hardware fornecido deverá possuir fonte de alimentação redundante.

5.5.4.5. Equipamento Tipo 5

5.5.4.5.1. Deverá suportar throughput de até 05Gbps.

5.5.4.5.2. Deverá ter capacidade de analisar e identificar 5.000 dispositivos.

5.5.4.5.3. Deverá suportar e analisar até 150.000 conexões por minuto.

5.5.4.5.4. Deverá considerar a inspeção de até 250 caixas postais prioritárias (VIP’s).

5.5.4.5.5. Deverá possuir 1 (uma) interface padrão 100/1000 BASE-T para atuar como interface de administração.

5.5.4.5.6. Deverá possuir pelo menos 2 (duas) interfaces padrão 100/1000 BASE-T para atuarem como interfaces de análise de tráfego.

5.5.4.5.7. Deverá possuir pelo menos 2 (duas) interfaces padrão 10 Gbe SFP+ para atuarem como interface de análise de tráfego.

5.5.4.5.8. O hardware fornecido deverá possuir fonte de alimentação redundante.

5.5.4.6. Equipamento Tipo 6

5.5.4.6.1. Deverá suportar throughput de 10 a 15Gbps.

5.5.4.6.2. Deverá ter capacidade de analisar e identificar 9.000 dispositivos.

5.5.4.6.3. Deverá suportar e analisar até 450.000 conexões por minuto.

5.5.4.6.4. Deverá considerar a inspeção de até 300 caixas postais prioritárias (VIP’s).

5.5.4.6.5. Deverá possuir 1 (uma) interface padrão 100/1000 BASE-T para atuar como interface de administração.

5.5.4.6.6. Deverá possuir pelo menos 2 (duas) interfaces padrão 100/1000 BASE-T para atuarem como interfaces de análise de tráfego.

5.5.4.6.7. Deverá possuir pelo menos 2 (duas) interfaces padrão 10 Gbe SFP+ para atuarem como interface de análise de tráfego.

5.5.4.6.8. O hardware fornecido deverá possuir fonte de alimentação redundante.

5.5.4.7. Equipamento Tipo 7

5.5.4.7.1. Deverá suportar throughput de até 20Gbps.

5.5.4.7.2. Deverá ter capacidade de analisar e identificar 13.000 dispositivos.

5.5.4.7.3. Deverá suportar e analisar até 1,5 milhões de conexões por minuto.

5.5.4.7.4. Deverá considerar a inspeção de até 300 caixas postais prioritárias (VIP's).

5.5.4.7.5. Deverá possuir 1 (uma) interface padrão 100/1000 BASE-T para atuar como interface de administração.

5.5.4.7.6. Deverá possuir pelo menos 2 (duas) interfaces padrão 100/1000 BASE-T para atuarem como interfaces de análise de tráfego.

5.5.4.7.7. Deverá possuir pelo menos 02 (duas) interfaces padrão 10 Gbe SFP+ para atuarem como interface de análise de tráfego.

5.5.4.7.8. O hardware fornecido deverá possuir fonte de alimentação redundante.

6. Justificativa parcelamento da solução

6. Justificativa de parcelamento ou não da solução

6.1 Em função da heterogeneidade das infraestruturas de TIC e respectivas capacidades de processamento dos serviços oferecidos pelos mesmos, bem como visando ampliar a competitividade, possibilitando que mais fabricantes e empresas parceiras possam participar da licitação corroborando com o melhor uso do recurso público, constata-se que o parcelamento do objeto desta contratação é viável.

7. Realizar avaliação das necessidades

7. Realizar avaliação das necessidades de adequação do ambiente do órgão

7.1 Não existe necessidade de adequação do ambiente para a execução contratual.

8. Estimativa do custo total da contratação

8. Estimativa do custo total da contratação

8.1 O custo total da contratação está estimado em **R$ 3.813.280,00** (conforme detalhado no **item 4.1**).

8.2 O valor oficial será apurado pela Seção de Análise Técnica de Contratações (SETEC) após a finalização do Termo de Referência.

9. Justificativa p escolha da sol. de TIC

9. Justificativa para escolha da solução de TIC

9.1 Inicialmente a solução escolhida foi a do **item 3.1.3** que refere-se à **Solução 03** - “Contratação envolvendo tanto segurança cibernética para rede interna e externa, com uso de inteligência artificial, respostas autônomas e machine learning não supervisionado, integrados com recursos de inteligência cibernética, fornecida como serviço e pagamento em parcela única”.

9.1.1 Conforme análise no item 3, as soluções citadas tanto no **item 3.1.1** quanto no **item 3.1.2** apresentam contratações realizadas no âmbito da Administração Pública Federal identificadas durante a pesquisa nos portais de compras públicas, com características e condições comerciais diversas.

9.1.2 A **Solução 01** apresenta como característica marcante a alocação de mão de obra técnica por parte da CONTRATADA.

9.1.2.1 Isso vai de encontro à filosofia de busca de soluções que possam ser autônomas, e não criem nenhum tipo de dependência humana para a sua execução.

9.1.3 A **Solução 02** possui como particularidade o aglomerado de serviços de segurança da informação que não possui relação direta com os requisitos desta análise de viabilidade.

9.1.4 Em comum às soluções, às diferentes realidades de infraestrutura das contratações identificadas na pesquisa de mercado criam dificuldades para identificar similaridades para fins de referência de custos, porém, foram identificados alguns itens nestas contratações que poderão ser utilizados, resultando nas estimativas de custos apresentadas na tabela que se encontra no **item 2.4**, bem como as estimativas de custos coletadas junto a empresas de mercado.

9.1.5 Portanto a solução, inicialmente escolhida seria a **Solução 03**, uma contratação envolvendo tanto segurança cibernética para rede interna e externa, com uso de inteligência artificial, respostas autônomas e machine learning não supervisionado, integrados com recursos de inteligência cibernética, fornecida como serviço e pagamento em parcela única, pelos seguintes motivos:

9.1.5.1 Emprego de Inteligência Artificial, machine learning, análise preditiva e inteligência cibernética, reduzirá sobremaneira o esforço operacional das equipes envolvidas na análise e tratamento de incidentes quanto ocorrem ou ocorrerem.

9.1.5.2 Redução significativa de intervenções operacionais em caso de incidente.

9.1.5.3 Aumento da capacidade de análise de informações e eventos capturados durante a análise do tráfego interno e externo (Internet, Dark e Deepweb).

9.1.5.4 Melhora significativa no tempo e na eficiência das análises, identificações, tratamento e resposta a incidentes de segurança da informação e cibersegurança.

9.1.5.5 Melhora da visão e situação da rede interna e externa do Tribunal.

9.1.5.6 Proporcionará atuação mais específica nas áreas efetivamente críticas e mais atacadas.

9.2 Porém, em virtude da aprovação da Estratégia Nacional de Cibersegurança para o período de 2021 a 2024, com o objetivo de servir como direcionador para as diversas ações necessárias em segurança cibernética, foram instituídos diversos grupos de trabalho em Segurança da Informação, dentre eles um para a aquisição da solução, descrita no item anterior (**item 3.1.3**), para toda Justiça Eleitoral.

9.3 A alternativa que oferece mais vantajosidade para o Tribunal Regional Eleitoral do Rio Grande do Norte é a de atuar como partícipe da Ata de Registro de Preços (ARP), Pregão Eletrônico SRP nº 08/2023, atualmente em curso no Tribunal Regional Eleitoral do Distrito Federal (TRE-DF).

9.4 Justificativa da escolha:

9.4.1 A Ata de Registro de Preços (ARP) para a contratação de empresa especializada no fornecimento de bens e serviços de inteligência cibernética, no formato de prestação de serviço, voltados para monitoramento, coleta e análise de dados, internos e externos, sobre ameaças cibernéticas do ambiente de rede do TRE-DF e demais Tribunais partícipes, com adoção de tecnologias de análise de comportamento, uso de inteligência artificial e machine learning não supervisionado, consoante especificações, condições, quantidades e prazos constantes do Termo de Referência e anexos, do Tribunal Regional Eleitoral do Distrito Federal (TRE-DF), atende a todos os requisitos elencados neste estudo, onde o processo está finalizado e se configura a solução mais vantajosa, caso o Tribunal Regional Eleitoral do Rio Grande do Norte opte por participar do referido registro de preços.

9.4.2 O processo em curso contemplará, além das necessidades do Tribunal Regional Eleitoral do Distrito Federal (TRE-DF), as demandas dos demais Tribunais Eleitorais interessados, que integrarão a contratação como partícipes desde a origem.

9.4.3 Esta ata de registro de preços é composta por:

Item	Descrição	Unidade	Quant.	Valor Estimado
1	Solução de inteligência cibernética, contendo licenças de uso de software, hardware, prestação de serviços e entregáveis, no formato de prestação de serviços, com monitoração e ação 24x7x365, suporte técnico, garantia e manutenção pelo período de 24 (vinte e quatro) meses, e pagamento em parcela	meses	01	R$ 3.590.000,00
2	Serviço de Ativação da Solução	unidade	01	R$ 74.000,00
3	Serviço de Operação Assistida	blocos de 04 horas	24	R$ 14.160,00
4	Treinamento (por pessoa)	servidores	06	R$ 135.020,00
VALOR TOTAL				**R$ 3.813.280,00**

9.5 A solução escolhida permitirá:

9.5.1 Aprimorar a infraestrutura de cibersegurança.

9.6 A solução é composta por licenças de uso de software, hardware, prestação de serviços e entregáveis, relacionados no item 2.2.1.

9.7 Os valores estimados estão descritos no item 3.8.1.

9.8 Os benefícios gerados são:

9.8.1 Manter uma infraestrutura tecnológica de cibersegurança, priorizando as ferramentas elencadas no rol de soluções tecnológicas que foi elaborado para atender a Estratégia de Cibersegurança da Justiça Eleitoral, de acordo com os níveis de criticidade pré-definidos, alinhados com as necessidades do TRE/RN e de acordo com a sua capacidade operacional.

9.8.2 Permitir o monitoramento de anomalias e ataques cibernéticos no ambiente computacional da Justiça Eleitoral.

9.8.3 Aumentar a resiliência da Justiça Eleitoral.

9.9 A solução está alinhada:

9.9.1 Às necessidades de negócio e requisitos tecnológicos e está em consonância com os seguintes instrumentos:

9.9.1.1 **PLANO ESTRATÉGICO DA JUSTIÇA ELEITORAL DO RN 2021-2026 (PEJERN):**

9.9.1.1.1 Fortalecimento da segurança da informação – Objetivo Estratégico AC3.

9.9.1.1.1.1 Aprimorar a infraestrutura tecnológica e os serviços em nuvem – Iniciativa AC3.3.

9.9.1.1.2 Garantia dos direitos de cidadania – Objetivo Estratégico S.1.

9.9.1.1.2.1 Prover a acessibilidade física e digital das instalações e dos serviços às pessoas com deficiência ou mobilidade reduzida – Iniciativa S1.3.

9.9.1.1.3 Aprimoramento da governança institucional - Objetivo Estratégico PI.3.

9.9.1.1.3.1 Fortalecer o processo de gestão e comunicação da estratégia através de projetos, otimização de processos e análise estatística – Iniciativa PI3.2.

9.9.1.2 **PLANEJAMENTO ESTRATÉGICO DO PODER JUDICIÁRIO – ENTIC / JUD 2021 A 2026**, onde dentre os objetivos da Resolução 370/2021 CNJ, pode-se destacar:

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

9.9.1.2.2 Objetivo 8: Promover Serviços de Infraestrutura e Soluções Corporativas.

9.9.1.3 **RESOLUÇÃO Nº 396, DE 07 DE JUNHO DE 2021, DO CONSELHO NACIONAL DE JUSTIÇA – CNJ**, instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ) que estabelece, dentre outras coisas que:

9.9.1.3.1 Para elevar o nível de segurança das infraestruturas críticas, deve-se (Art.11): I – Estabelecer todas as ações que possibilitem maior eficiência, ou seja, capacidade de responder de forma satisfatória a incidentes de segurança, permitindo a contínua prestação dos serviços essenciais a cada órgão; ... 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.

9.9.1.4 **PORTARIA Nº 162, DE 10 DE JUNHO DE 2021, DO CONSELHO NACIONAL DE JUSTIÇA** aprovou o estabelecimento dos seguintes Protocolos e Manuais:

9.9.1.4.1 Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ), onde podemos destacar a aderência desta Análise de Viabilidade aos seguintes pontos: (3) - Princípios Críticos: … (3.2.6) - Automação – incentivo à busca de soluções automatizadas de segurança cibernética para que as organizações obtenham medições confiáveis, escaláveis e contínuas. (7) – Boas Práticas de Segurança Cibernéticas: … (7.5.2) – Identificação: capacidade de identificar que um ataque cibernético está em andamento, por meio da

percepção de sinais de anomalias ou de comportamentos inesperados. Trata-se da aptidão dos entes para diferenciar as irregularidades em redes de dados e identificar o mau funcionamento dos sistemas críticos, em razão de ataques cibernéticos em curso. (7.5.3) – Contenção: Visa a garantir que o incidente não cause mais danos. Nessa dimensão, a prioridade geral é isolar o que foi afetado, manter a produção e, acima de tudo, garantir que as ações não comprometam, ainda mais, a segurança ou as operações críticas.

9.9.1.4.2 Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário (PGCRC-PJ).

9.9.1.4.3 Protocolo de Investigação de Ilícitos Cibernéticos do Poder Judiciário (PIILC-PJ).

9.9.1.4.4 Manual de Proteção de Infraestruturas Críticas de TIC.

9.9.1.4.5 Manual de Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital.

9.9.1.5 **PLANEJAMENTO ESTRATÉGICO DO TRIBUNAL SUPERIOR ELEITORAL 2021-2026:**

9.9.1.5.1 Na perspectiva de Processos Internos é possível verificar que a demanda deste egrégio Tribunal Regional Eleitoral encontra aderência com o objetivo:

9.9.1.5.1.1 APERFEIÇOAR A SEGURANÇA DA INFORMAÇÃO - refere-se à implementação de políticas, métodos e práticas reconhecidas e relacionadas à segurança da informação. Abrange a gestão da continuidade de negócios ou serviços e a gestão de riscos de TIC.

9.9.1.5.2 Na perspectiva de Aprendizado e Crescimento é possível verificar que a demanda deste egrégio Tribunal Regional Eleitoral encontra aderência com o objetivo:

9.9.1.5.2.1 GARANTIR OS RECURSOS TECNOLÓGICOS PARA A AMPLIAÇÃO DE SERVIÇOS DIGITAIS, INOVAÇÃO E SEGURANÇA DE TIC - Trata-se de garantir os recursos tecnológicos (sistemas, serviços e infraestrutura) necessários à ampliação dos serviços digitais, às iniciativas inovadoras e à implementação de mecanismos e práticas de segurança.

9.9.1.5.3 Por fim cabem ser destacados os seguintes documentos que também subsidiaram a contratação em análise:

9.9.1.5.3.1 Estratégica Nacional de CiberSegurança – 2021 a 2024 (TSE e TREs).

9.9.1.5.3.2 Arquitetura de CiberSegurança – do GT-SI – Grupo de Trabalho de Segurança da Informação da Justiça Eleitoral.

9.9.1.5.4 A Estratégia Nacional de Cibersegurança consolida conceitos fundamentais sobre cibersegurança e descreve os eixos estruturantes da Estratégia Nacional de Cibersegurança da Justiça Eleitoral, englobando o Tribunal Superior Eleitoral, os Tribunais Regionais Eleitorais e as Zonas Eleitorais dispersas pelo país.

9.9.1.5.5 A Arquitetura de CiberSegurança integra a Estratégia Nacional de Cibersegurança e foi organizada pelo Grupo de Trabalho de Segurança da Informação da Justiça Eleitoral, com o apoio de diversos servidores do TSE e dos Tribunais Regionais Eleitorais.

9.9.1.5.6 De acordo com os eixos definidos na Arquitetura de CiberSegurança da JE, as necessidades previstas nesta contratação podem ser identificadas nos seguintes eixos:

9.9.1.5.6.1 Eixo 3 – Sistema Eletrônico de Votação. O requisito de Inteligência de Ameaças está aderente com as necessidades apresentadas na contratação (ID_F38).

9.9.1.5.6.2 Eixo 5 – Segurança de Aplicações. O requisito de Monitoramento de Rede está aderente com as necessidades apresentadas na contratação (ID_F36).

10. Declaração de viabilidade

10. Declaração de viabilidade

11.1 Em conformidade com o disposto no Manual de Contratações de Tecnologia da Informação e Comunicação, subitem 4.1.1.11, DECLARAMOS a viabilidade da contratação, com base no estudo realizado. Natal/RN, *(datação eletrônica)*

Equipe de Planejamento da Contratação		
Integrante Demandante	**Integrante Técnico**	**Integrante Administrativo**
(assinado eletronicamente) **Carlos Magno do Rozário Câmara** COINF/STIE	(assinado eletronicamente) **Denilson Bastos da Silva** SSI/COINF/STIE	(assinado eletronicamente) **Ernesto Leca Pinto** SETEC/COLIC/SAOF

11. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

ERNESTO LECA PINTO:02432252454

Assinado de forma digital por ERNESTO LECA PINTO:02432252454
Dados: 2024.04.08 16:35:50 -03'00'

ERNESTO LECA PINTO

Membro da comissão de contratação

DENILSON BASTOS DA SILVA:56533691449
Assinado de forma digital por DENILSON BASTOS DA SILVA:56533691449
Dados: 2024.04.08 17:04:16 -03'00'

DENILSON BASTOS DA SILVA

Membro da comissão de contratação

CARLOS MAGNO DO ROZARIO CAMARA:30024407
Assinado de forma digital por CARLOS MAGNO DO ROZARIO CAMARA:30024407
Dados: 2024.04.08 16:56:12 -03'00'

CARLOS MAGNO DO ROZARIO CAMARA

Membro da comissão de contratação