TERMO DE REFERÊNCIA
(CONFORME RESOLUÇÃO CNJ Nº 182/2013)

CONTRATAÇÃO DE SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO (STIC)

1. DEFINIÇÃO DO OBJETO:

Contratação de empresa especializada para 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 deste Termo de Referência e anexos.

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO:

2.1. MOTIVAÇÃO DA CONTRATAÇÃO:

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

A inteligência cibernética está entre os principais itens de discussão das organizações governamentais, motivados, essencialmente, pelo crescente número de diferentes ataques cibernéticos destinados a portais e serviços entregues pelo Poder Judiciário. Essas discussões, também, são frutos de análise em relatórios cibernéticos de diversos e grandes fabricantes. A empresa alemã Roland Berger, por exemplo, elaborou uma pesquisa onde o resultado foi gritante para o nosso país. O Brasil foi o 5º (quinto) país que mais recebeu ataques cibernéticos, apenas no primeiro trimestre de 2021 foram 9,1 milhões de ocorrências, número maior que o ano inteiro de 2020.

Atualmente os ataques cibernéticos são uma realidade latente e têm afetado diversos órgãos governamentais, ocasionando grandes prejuízos tais como: parada/interrupção na prestação de serviços ao cidadão e roubo/furto de informações protegidas por sigilo legal.

Em novembro de 2020 o Superior Tribunal de Justiça – STJ foi alvo do maior ataque cibernético já realizado a um órgão do Governo Brasileiro. Foram mais de sete dias com todos os sistemas indisponíveis. O foco do ataque foi a infraestrutura do Datacenter do STJ.

Ataque com consequência semelhante foi realizado no Tribunal de Justiça do Rio

Grande do Sul, TJ/RS, no final de abril de 2021, mas o foco, dessa vez, foram as mais de 12.000 estações de trabalho do TJ/RS, conhecidos como endpoints. Focos diferentes, estragos semelhantes, modo de operação similar: ataques do tipo ransomware que exploram vulnerabilidades existentes.

O relatório do Grupo de Trabalho em Segurança da Informação da Justiça Eleitoral (TSE, 2021) lista exemplos práticos da incidência de ataques cibernéticos sobre órgãos públicos em tempos recentes, especificamente a partir do mês de novembro de 2020:

- Acesso e exposição indevidos de dados administrativos do próprio TSE, na data do primeiro turno das eleições municipais de 2020 (15/11/20);
- Ataque de negação de serviço que inviabilizou o uso do sistema de justificativa e de consulta a local de votação no dia do primeiro turno da eleição de 2020;
- Ataque de ransomware ao STJ, em novembro de 2020, criptografou a totalidade dos servidores virtuais daquele órgão, tornando-os inutilizáveis, causando interrupção de todo o trabalho baseado em tecnologia da informação, bem como suspensão de todos os prazos processuais por, aproximadamente, uma semana;
- Ataque ao Tribunal Regional Federal da 1ª Região, em novembro de 2020, que também interrompeu seus serviços de TI e os prazos processuais por cerca de uma semana;
- Ataque ao Tribunal de Justiça do Pará, ocorrido em 07 de novembro de 2020, onde hackers utilizaram vulnerabilidades no Sistema de Acompanhamento de Processos Judiciais para suspender serviços;
- Ataque à Procuradoria do Município de Vitória, Espírito Santo, ocorrido em 10 de novembro de 2020, acarretando suspensão dos serviços informatizados;
- Ataque ao Tribunal Regional do Trabalho da 17ª Região, que atende ao estado do Espírito Santo, ocorrido em fevereiro de 2022, acarretando suspensão dos serviços informatizados por mais de 15 dias;
- Ataque ao Tribunal Regional Federal da 3ª Região – TRF3, que atende aos estados de São Paulo e Mato Grosso do Sul – evento ocorrido em março de 2022, que tornou indisponíveis os serviços prestados pelo tribunal por vários dias, ataque do qual aquele tribunal continua se recuperando até o momento da elaboração deste documento;
- Ataque à Biblioteca Nacional que, da mesma forma, teve seus serviços de TI interrompidos por 15 dias, até que fossem restaurados com segurança;
- Ataque de ransomware ao Tribunal de Justiça do Rio Grande do Sul, ocorrido no último dia 28 de abril de 2021, que exigiu o pagamento de resgate no valor de USD 5 milhões, ataque do qual aquele tribunal continua se recuperando até o momento da elaboração deste documento;
- Ataque ao STF – Supremo Tribunal Federal, ocorrido nos primeiros dias de maio de 2021, cujo foco foi o vazamento de informações por meio de robôs que exploraram vulnerabilidades em aplicações web. Esse ataque indisponibilizou o portal web e muitos serviços por vários dias;
- Ataque ao Portal SEBRAE Nacional e Estados – evento ocorrido em março de 2022, interrompeu os serviços do SEBRAE por mais de 48 horas em

todos os estados brasileiros.

Fica fácil e nítido perceber, infelizmente, que a velocidade com que os malwares vêm se desenvolvendo e sofisticando ultrapassam sobremaneira um possível contra-ataque ou mesmo estudos que viabilizem a blindagem dos sistemas existentes no Poder Judiciário como um todo.

Se por um lado, a presença do TRE-DF em soluções digitais tem aumentado com velocidade exponencial, por outro lado também têm aumentado a superfície de ataques, deixando o tribunal mais vulnerável. Mesmo estando às urnas eletrônicas seguras por sua proposital desconexão de redes de comunicação, muitas outras soluções estão expostas na Internet e precisam ser protegidas, pois eventuais incidentes diminuem a percepção de segurança da sociedade na prestação eleitoral como um todo.

Enquanto a Internet apresenta aos usuários e instituições muitas informações e serviços, também inclui diversos tipos de riscos. As ameaças cibernéticas estão aumentando em sofisticação e volume, com crescente número de cibercriminosos adotando um conjunto de diferentes tipos de “armas” para alcançar seus objetivos, muitas das vezes, meramente por simples vaidades ou mesmo com intenções mais sérias e graves.

Dentre os principais tipos de ameaças cibernéticas, podemos destacar, mas não esgotar:

- MALWARE – de forma bem simplificada, pode ser definido como um software mal-intencionado, que consegue acesso às redes corporativas por intermédio das vulnerabilidades nela encontradas. Os principais riscos gerados pelo malware incluem: a instalação de outros softwares ainda mais nocivos, comprometimento de componentes específicos da infraestrutura para torná-los inoperantes e obtenção de informações de caráter reservado.
- RAMSOMWARE – bastante difundido no meio de hackers, o ramsomware se caracteriza como um subconjunto de malwares que atuam no bloqueio dos dados que estão armazenados no dispositivo da vítima (um microcomputador desktop, notebook ou mesmo dispositivo móvel como smartphones e tablets), quase sempre a partir da criptografia. Uma vez que a invasão é bem-sucedida, o invasor solicita um determinado pagamento para o resgate das informações e para que o acesso seja restabelecido. Geralmente este resgate é exigido em criptomoedas, que são de difícil rastreabilidade.
- Ataques DDoS – o DDoS é considerado um dos ataques cibernéticos mais comuns e perigosos que podem afetar a atividade da rede corporativa. Também conhecido como ataque de negação de serviço distribuído, este tipo de ameaça utiliza computadores infectados dos mais diversos países, tendo como finalidade sobrecarregar a rede corporativa, fazendo com que a infraestrutura não consiga lidar com o alto volume de demandas, se tornando instável ou mesmo inacessível.

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

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

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

No que tange à responsabilidade da proteção de todos os sistemas informatizados existentes no ambiente do TRE-DF vale ressaltar que a simples adoção de soluções informatizadas em seu desenvolvimento apenas torna o trabalho mais eficiente. Estes sistemas exigem uma camada adicional de proteção, principalmente contra ameaças cibernéticas que buscam incessantemente fragilidades ou falhas nas soluções informatizadas como forma de obter êxito em suas investidas.

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

Dessa forma, o resultado esperado é a preservação da integridade, disponibilidade e conformidade de todos os sistemas informatizados da Justiça Eleitoral, além da sua imagem institucional.

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

2.2. **OBJETIVOS A SEREM ALCANÇADOS**:

2.2.1. Objetivo Geral: Prevenir ataques cibernéticos no âmbito do TRE-DF e demais Tribunais partícipes.

2.2.2. Objetivo(s) Específico(s):

2.2.2.1. Monitorar a rede interna e externa contra ameaças cibernéticas;

2.2.2.2. Evitar a suspensão dos serviços informatizados por conta de ataques de hackers;

2.2.2.3. Manter parque seguro contra ataques virtuais;

2.2.2.4. Prevenir ataques cibernéticos (internos e oriundos da WEB) no âmbito da Justiça Eleitoral, para os Tribunais partícipes;

2.2.2.5. Prover aos usuários/servidores em trabalho remoto consumo seguro dos serviços internos;

2.2.2.6. Corroborar para garantir a disponibilidade, integridade e confiabilidade aos dados e informações dos Tribunais partícipes;

2.2.2.7. Prover o apoio necessário para uma gestão eficiente, eficaz e efetiva da segurança da informação e da Cibersegurança;

2.2.2.8. Melhorar a maturidade na Gestão da Segurança da Informação e

da Cibersegurança para os Tribunais partícipes;

2.2.2.9. Promover a evolução tecnológica.

2.3. **BENEFÍCIOS DIRETOS E INDIRETOS**:

2.3.1. Monitoramento contínuo e visibilidade em tempo real de possíveis ameaças;

2.3.2. Redução das taxas de falsos positivos (decorrentes das análises isoladas pelas soluções existentes), considerando a adoção de avançados recursos, tais como inteligência artificial, *machine learning* não supervisionado e análise comportamental da rede e de seus componentes de forma autônoma e contínua se adaptando às variações de comportamento; e

2.3.3. Menor interferência humana na atividade de monitoramento das ameaças, o que beneficia também o fato da existência de reduzido quadro de servidores efetivos e terceirizados envolvidos com segurança da informação.

2.4. **ALINHAMENTO ESTRATÉGICO**:

2.4.1. A contratação está em consonância com:

a) Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD) 2021-2026, conforme objetivos: Aprimorar a Segurança da Informação e a Gestão de Dados; Promover serviços de infraestrutura e soluções coorporativas; Protocolo de prevenção de incidentes cibernéticos; e protocolo de investigação de ilícitos cibernéticos.

b) Planejamento Estratégico da Justiça Eleitoral 2021-2026, conforme Macrodesafio: Fortalecimento da Estratégia Nacional de TIC e de Proteção de Dados.

c) Plano Estratégico Institucional (PEI) TRE-DF 2021-2026, conforme Objetivo Estratégico: Fortalecimento da Estratégia Nacional de TIC e de Proteção de Dados.

d) Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) TRE-DF 2021-2022, conforme grupo 3 (Segurança da Informação e Proteção de dados): Aperfeiçoar as estruturas de segurança da informação.

e) Portaria nº 162, de 10 de junho de 2021, do Conselho Nacional de Justiça aprovou o estabelecimento dos seguintes Protocolos e Manuais:

- Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário

(PPINC-PJ), onde podemos destacar a aderência deste Termo de Referência 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.*
  Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário (PGCRC-PJ); e
  Protocolo de Investigação de Ilícitos Cibernéticos do Poder Judiciário (PIILC-PJ).
  Manual de Proteção de Infraestruturas Críticas de TIC;
  Manual de Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital;

2.5. **ESTUDOS PRELIMINARES**:

2.5.1. Em atendimento ao artigo 12, §§1º e 2º, da Resolução CNJ nº 182/2013, a Análise de Viabilidade da Contratação sobre a presente aquisição foi realizada e juntada ao processo SEI 0005153-57.2023.6.07.8100.

2.6. **RELAÇÃO ENTRE A DEMANDA PREVISTA E QUANTIDADE DE BENS/SERVIÇOS**:

2.6.1. A solução contratada deverá atender aos parâmetros listados abaixo, que representam exatamente o quantitativo que se pretende contratar, bem como os lotes que poderão ser licitados conforme o perfil definido e que o Tribunal partícipe foi enquadrado:

Lote	Item	Demanda Prevista	Unidade	Tipo do Perfil	Qtd	Tribunais Participantes
1	**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 única.	Unidade	1	2	TRE-AP e TRE-MS
	2	Serviço de Ativação da Solução	Unidade	**xxxxxxx**	**2**	**xxxxxxx**
	3	Serviço de Operação Assistida	Blocos de 4h	**xxxxxxx**	**220**	**xxxxxxx**
	4	Treinamento (por pessoa)	Alunos	**xxxxxxx**	**10**	**xxxxxxx**
2	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 única.	Unidade	2	5	TRE-AM, TRE-AL, TRE-MT, TRE-RR e TRE-AC
	2	Serviço de Ativação da Solução	Unidade	**xxxxxxx**	**5**	**xxxxxxx**
	3	Serviço de Operação Assistida	Blocos de 4h	**xxxxxxx**	**152**	**xxxxxxx**
	4	Treinamento (por pessoa)	Alunos	**xxxxxxx**	**21**	**xxxxxxx**
3	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 única.	Unidade	3	6	TRE-TO, TRE-CE, TRE-DF, TRE-ES, TRE-RN e TRE-RO
	2	Serviço de Ativação da Solução	Unidade	**xxxxxxx**	**6**	**xxxxxxx**
	3	Serviço de Operação Assistida	Blocos de 4h	**xxxxxxx**	**659**	**xxxxxxx**
	4	Treinamento (por pessoa)	Alunos	**xxxxxxx**	**34**	**xxxxxxx**

4	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 única.	Unidade	4	4	TRE-PI, TRE-PB, TRE-SE e TRE-MA
	2	Serviço de Ativação da Solução	Unidade	**xxxxxxx**	**4**	**xxxxxxx**
	3	Serviço de Operação Assistida	Blocos de 4h	**xxxxxxx**	**425**	**xxxxxxx**
	4	Treinamento (por pessoa)	Alunos	**xxxxxxx**	**21**	**xxxxxxx**
5	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 única.	Unidade	5	4	TRE-PR, TRE-RJ, TRE-BA e TRE-MG
	2	Serviço de Ativação da Solução	Unidade	**xxxxxxx**	**4**	**xxxxxxx**
	3	Serviço de Operação Assistida	Blocos de 4h	**xxxxxxx**	**538**	**xxxxxxx**
	4	Treinamento (por pessoa)	Alunos	**xxxxxxx**	**28**	**xxxxxxx**
6	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 única.	Unidade	6	1	TRE-RS
	2	Serviço de Ativação da Solução	Unidade	**xxxxxxx**	**1**	**xxxxxxx**
	3	Serviço de Operação Assistida	Blocos de 4h	**xxxxxxx**	**200**	**xxxxxxx**
	4	Treinamento (por pessoa)	Alunos	**xxxxxxx**	**10**	**xxxxxxx**
7	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 única.	Unidade	7	1	TRE-SP

	2	Serviço de Ativação da Solução	Unidade	**xxxxxxx**	**1**	**xxxxxxx**
	3	Serviço de Operação Assistida	Blocos de 4h	**xxxxxxx**	**180**	**xxxxxxx**
	4	Treinamento (por pessoa)	Alunos	**xxxxxxx**	**10**	**xxxxxxx**

2.6.2. As licenças de uso de softwares e suas funcionalidades, bem como os equipamentos que compõe a subscrição da solução, deverão ser dimensionados para atender ao que está determinado nos itens 1, 2, 3, 4 e 5 do Anexo I a este Termo de Referência, contemplando garantia, manutenção, instalação e configuração;

2.6.3. O Serviço de Operação Assistida durante a vigência contratual, deverá ser realizado conforme descrito no item 4.3, referente aos Requisitos Específicos neste Termo de Referência.

2.6.4. O treinamento para servidores do TRE-DF e Tribunais partícipes deverá ser realizado conforme descrito no item 4.4 deste Termo de Referência.

2.7. **LEVANTAMENTO DE MERCADO:**

2.7.1. O levantamento foi realizado dentro dos parâmetros previstos na **Instrução Normativa nº 73/2020**, junto a empresas do mercado.

2.7.2. Em atendimento às práticas adotadas pela Estratégia Nacional de Cibersegurança da Justiça Eleitoral, quanto às contratações conjuntas, visando elevar a maturidade da Gestão da Segurança da Informação e da Cibersegurança da JE como um todo, e com base nas informações passadas pelos Tribunais que responderam ao Ofício-Circular nº 09/2023 (SEI 1426231), consolidamos as mesmas no Anexo X, e fomos ao mercado para solicitar as estimativas de custo, conforme consta no item 2.1.16 da Análise de Viabilidade da Contratação.

2.7.3. Além das estimativas de custo solicitadas ao mercado, também analisamos alguns Contratos realizados pela Administração Pública Federal – APF, e destes, conseguimos utilizar apenas um dos itens analisados, para auxiliar na composição da estimativa de custos desta contratação, conforme item 2.1.8.5 da Análise de Viabilidade da Contratação.

2.7.4. Com base nas informações recebidas dos fabricantes CISCO, TRENDMICRO, DARKTRACE e FORTINET, consultamos as seguintes empresas abaixo relacionadas:

2.7.4.1. Parceiras TRENDMICRO

2.7.4.1.1. ServiceIT;

2.7.4.1.2. AllTech.

2.7.4.2. Parceiras CISCO

2.7.4.2.1. Logicalis;

2.7.4.2.2. Teletex;

2.7.4.2.3. Global;
2.7.4.2.4. WiseIT;
2.7.4.2.5. Atelecom;
2.7.4.2.6. Yssy;
2.7.4.2.7. Netsafecorp;
2.7.4.2.8. Teltecsolutions.

2.7.4.3. Parceiras DARKTRACE

2.7.4.3.1. RC2;
2.7.4.3.2. Grg Tech;
2.7.4.3.3. INN Tecnologia.

2.7.4.4. Parceiras FORTINET

2.7.4.4.1. Global Sectecnologia

2.7.5. Das empresas consultadas, recebemos retorno da ALLTECH (SEI 1453701), RATIONALE (SEI 1453693), INN_TECNOLOGIA (SEI 1453697), GARAGE TECH (SEI 1454816) e SERVICE IT (1458302), que foram consolidadas com a estimativa de preços retirada de contrato do TJRJ, conforme mencionado no item 2.7.3, e os valores unitários e totais por item e total por lote ficaram conforme tabela abaixo.

Lote	Item	Demanda Prevista	Unidade	Tipo do Perfil	Qtd	Tribunais	Valor Unitário	Valor Total
1	**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,	Und.	1	2	TRE-AP e TRE-MS	R$ 2.861.549,20	R$ 5.723.098,40

		garantia e manutenção pelo **período de 24 (vinte e quatro) meses,** e pagamento em parcela única.						
	2	Serviço de Ativação da Solução	Und.	**xxxxxxx**	**2**	**xxxxxxx**	R$ 93.913,20	R$ 187.826,40
	3	Serviço de Operação Assistida	Blocos de 4h	**xxxxxxx**	**220**	**xxxxxxx**	R$ 648,71	R$ 142.716,20
	4	Treinamento (por pessoa)	Alunos	**xxxxxxx**	**10**	**xxxxxxx**	R$ 22.839,73	R$ 228.397,34
	VALOR TOTAL DO LOTE 1							R$ 6.282.038,34
2	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,	Unidade	2	5	TRE-AM, TRE-AL, TRE-MT, TRE-RR e TRE-AC	R$3.420.916,10	R$ 17.104.580,50

		garantia e manutenção pelo **período de 24 (vinte e quatro) meses,** e pagamento em parcela única.						
	2	Serviço de Ativação da Solução	Unidade	**xxxxxxx**	**5**	**xxxxxxx**	R$95.673,20	R$ 478.366,00
	3	Serviço de Operação Assistida	Blocos de 4h	**xxxxxxx**	**152**	**xxxxxxx**	R$648,71	R$ 98.603,92
	4	Treinamento (por pessoa)	Alunos	**xxxxxxx**	**21**	**xxxxxxx**	R$22.839,73	R$ 479.634,41
	VALOR TOTAL DO LOTE 2							R$ 18.161.184,83
3	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,	Unidade	3	6	TRE-TO, TRE-CE, TRE-DF, TRE-ES, TRE-RN e TRE-RO	R$3.920.385,00	R$ 23.522.310,00

		garantia e manutenção pelo **período de 24 (vinte e quatro) meses,** e pagamento em parcela única.						
	2	Serviço de Ativação da Solução	Unidade	**xxxxxxx**	**6**	**xxxxxxx**	R$95.173,20	R$ 571.039,20
	3	Serviço de Operação Assistida	Blocos de 4h	**xxxxxxx**	**659**	**xxxxxxx**	R$648,71	R$ 427.499,89
	4	Treinamento (por pessoa)	Alunos	**xxxxxxx**	**34**	**xxxxxxx**	R$22.839,73	R$ 776.550,96
	VALOR TOTAL DO LOTE 3							R$ 25.297.400,05
4	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,	Unidade	4	4	TRE-PI, TRE-PB, TRE-SE e TRE-MA	R$4.868.637,80	R$ 19.474.551,20

		garantia e manutenção pelo **período de 24 (vinte e quatro) meses,** e pagamento em parcela única.						
	2	Serviço de Ativação da Solução	Unidade	**xxxxxxx**	**4**	**xxxxxxx**	R$96.833,20	R$ 387.332,80
	3	Serviço de Operação Assistida	Blocos de 4h	**xxxxxxx**	**425**	**xxxxxxx**	R$648,71	R$ 275.701,75
	4	Treinamento (por pessoa)	Alunos	**xxxxxxx**	**21**	**xxxxxxx**	R$22.839,73	R$ 479.634,41
	VALOR TOTAL DO LOTE 4							R$ 20.617.220,16
5	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,	Unidade	5	4	TRE-PR, TRE-RJ, TRE-BA e TRE-MG	R$6.037.522,60	R$ 24.150.090,42

		garantia e manutenção pelo **período de 24 (vinte e quatro) meses,** e pagamento em parcela única.						
	2	Serviço de Ativação da Solução	Unidade	**xxxxxxx**	**4**	**xxxxxxx**	R$91.813,20	R$ 367.252,80
	3	Serviço de Operação Assistida	Blocos de 4h	**xxxxxxx**	**538**	**xxxxxxx**	R$648,71	R$ 349.005,98
	4	Treinamento (por pessoa)	Alunos	**xxxxxxx**	**28**	**xxxxxxx**	R$22.839,73	R$ 639.512,55
	VALOR TOTAL DO LOTE 5							R$ 25.505.861,75
6	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,	Unidade	6	1	TRE-RS	R$9.297.366,84	R$ 9.297.366,84

		garantia e manutenção pelo **período de 24 (vinte e quatro) meses,** e pagamento em parcela única.						
	2	Serviço de Ativação da Solução	Unidade	**xxxxxxx**	**1**	**xxxxxxx**	R$92.673,20	R$ 92.673,20
	3	Serviço de Operação Assistida	Blocos de 4h	**xxxxxxx**	**200**	**xxxxxxx**	R$669,64	R$ 133.927,60
	4	Treinamento (por pessoa)	Alunos	**xxxxxxx**	**10**	**xxxxxxx**	R$22.839,73	R$ 228.397,34
	VALOR TOTAL DO LOTE 6							R$ 9.752.364,98
7	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,	Unidade	7	1	TRE-SP	R$14.824.605,53	R$ 14.824.605,53

		garantia e manutenção pelo **período de 24 (vinte e quatro) meses,** e pagamento em parcela única.						
	2	Serviço de Ativação da Solução	Unidade	**xxxxxxx**	**1**	**xxxxxxx**	R$103.013,20	R$ 103.013,20
	3	Serviço de Operação Assistida	Blocos de 4h	**xxxxxxx**	**180**	**xxxxxxx**	R$671,64	R$ 120.894,84
	4	Treinamento (por pessoa)	Alunos	**xxxxxxx**	**10**	**xxxxxxx**	R$22.839,73	R$ 228.397,34
	VALOR TOTAL DO LOTE 7							R$ 15.276.910,91
	VALOR TOTAL DA CONTRATAÇÃO							R$ 120.892.981,01

2.7.6. Comparando o valor médio total estimado desta contratação, considerando as estimativas enviadas pelas empresas mencionadas no item 2.7, com o valor médio total da mesma contratação realizada anteriormente no processo (0003372-34.2022.6.07.8100), considerando os devidos ajustes, quais sejam:

2.7.6.1. Nos quantitativos de partícipes, pois no processo anterior tínhamos 18 partícipes, e neste temos 23;

2.7.6.2. Na forma de pagamento, pois no processo anterior estava previsto o pagamento parcelado, realizado mensalmente, e neste será realizado pagamento em parcela única;

2.7.6.3. Na proposta de divisão em lotes por perfil e porte dos Tribunais partícipes, que no processo anterior era apenas um lote e neste serão 07 lotes;

2.7.6.4. Necessidade de igualar a quantidade de partícipes nos dois processos, incluindo na estimativa de custos do processo anterior, aonde 03 partícipes foram considerados como de porte e perfil 1 e os

outros 02 foram considerados como de porte e perfil 2.

2.7.7. Feitas as considerações e ajustes mencionados acima o valor total estimado para a contratação do processo anterior passaria a ser de R$ 172.090.589,19. Quando comparado com a estimativa de custos deste processo, que ficou no valor total de R$ 120.461.108,19, observamos uma economía inicial de R$ 51.629.481,00, o que equivale a uma redução de 30% no valor total previsto, considerando o mesmo objeto e prazo em ambos os projetos.

2.7.8. Cabe destacar que no documento de Análise de Viabilidade da Contratação, a tabela ao qual se refere o item 2.1.17, está com valor diferente da que consta neste, pois nesta, estão incluídos os preços de contratações da Administração Publica Federal – APF, enquanto naquela constam somente estimativa de preços coletados junto a empresas indicadas pelos fabricantes já mencionados.

2.7.9. Devido à heterogeneidade das infraestruturas e arquiteturas das redes dos Tribunais que compõe a rede da Justiça Eleitoral, e visando atender, possibilitar enquadrar os partícipes interessados em uma solução (hardware, softwares e serviços) que atenda às suas necessidades e aos preceitos e especificações técnicas previstas para esta contratação, de forma que os resultados esperados possam ser entregues conforme previsto, foi necessário estabelecer perfis específicos, balizados pelas seguintes informações: quantidade de ativos monitorados, throughput, quantidade de conexões por minuto e quantidade de caixas de e-mail VIP.

2.7.10. Abaixo seguem os 07 perfis criados.

PERFIL 1	
Throughput	até 500Mbps
Ativos Monitorados	até 1.500 ativos monitorados
Conexões por Minuto	até 25.000
E-mail VIP	50

PERFIL 2	
Throughput	de 501Mbps até 01Gbps
Ativos Monitorados	De 1.501 até 2.000 ativos monitorados
Conexões por Minuto	De 25.001 até 50.000 conexões por minuto
E-mail VIP	De 51 até 100 caixas de e-mail

PERFIL 3	
Throughput	De 01 Até 02 Gbps
Ativos Monitorados	De 2.001 até 2.500 ativos monitorados
Conexões por Minuto	De 50.001 Até 75.000 conexões por minuto
E-mail VIP	De 101 a 150 caixas de e-mail

PERFIL 4	
Throughput	De 02 até 03 Gbps
Ativos Monitorados	De 2.501 até 3.500 ativos monitorados
Conexões por Minuto	De 75.000 até 100.000 conexões por minuto
E-mail VIP	De 151 até 200 caixas de e-mail

PERFIL 5	
Throughput	De 03 até 05 Gbps
Ativos Monitorados	De 3.501 até 5.000 ativos monitorados
Conexões por Minuto	De 100.001 até 150.000 conexões por minuto
E-mail VIP	De 201 até 250 caixas de e-mail

PERFIL 6	
Throughput	De 10 até 15 Gbps
Ativos Monitorados	De 5.001 até 9.000 ativos monitorados
Conexões por Minuto	De 150.001 até 450.000 conexões por minuto
E-mail VIP	De 251 até 300 caixas de e-mail

PERFIL 7	
Throughput	De 15 até 20 Gbps
Ativos Monitorados	De 9.001 até 13.000 ativos monitorados
Conexões por Minuto	De 450.001 até 1,5 Milhão de conexões por minuto
E-mail VIP	300 caixas de e-mail

2.7.11. Após a inclusão de mais 22 (vinte e dois) outros Tribunais, além do TRE-DF como participes deste processo licitatório, foi necessária a criação dos Anexos IX e X.

2.7.11.1. O Anexo IX, referente à relação de Tribunais interessados em participar da Ata de Registro de preços, traz as seguintes

informações: A relação dos Tribunais partícipes, o endereço de entrega e as quantidades por item que cada partícipe indicou.

2.7.11.2. O Anexo X, referente aos perfis criados, traz as seguintes informações: Os tipos de perfis, parâmetros e quantidades por item que foram utilizados para definição do enquadramento nos perfis criados, e o enquadramento dos Tribunais nos perfis.

2.7.12. Após consolidarmos as informações passadas pelos Tribunais partícipes referente ao que foi solicitado no Ofício-Circular 09/2023 GDG/TER-DF, consultamos novamente todos os partícipes por e-mail (SEI 1443518) enviado dia 07/07/2023, a fim de ratificarem o enquadramento nos perfis criados, e informarem os quantitativos por item definido e as informações passadas pelos mesmos, foram consolidadas no Anexo X.

2.8. **NATUREZA DO OBJETO**:

2.8.1. O objeto a ser contratado possui características comuns e usuais encontradas atualmente no mercado de TIC, tendo em vista que são geralmente oferecidos por diversos fornecedores e são comparáveis entre si, de modo a permitir a decisão de compra com base no menor preço, por meio de especificações usuais praticadas no mercado, ou seja, os padrões de desempenho e qualidade são objetivamente definidos, nos termos do parágrafo único, do artigo 3º, inciso II, da Lei 10.520/2002 e Decreto nº 10.024/2019.

2.9. **PARCELAMENTO DO OBJETO**:

2.9.1. No contexto da solução apontada pela equipe de planejamento da contratação, e de acordo com as necessidades e requisitos previstos, a solução deve compreender o agrupamento de itens por lotes, tendo como referencia para o agrupamento, os itens e os lotes no quadro que integra o subitem 2.6.1 deste TR.

2.9.2. Cabe destacar, que a quantidade de licenças de softwares e equipamentos variam de fabricante para fabricante, não sendo possível desmembrar o item 1 do objeto em partes menores sem que se determine previamente o fabricante e sem impactar nos objetivos, entregas e benefícios esperados com a solução.

2.9.3. A Equipe de Planejamento da Contratação constata para melhor enquadramento dos Tribunais partícipes 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, com os princípios da Legalidade, Publicidade e Eficiência da APF, que o parcelamento do objeto desta contratação é viável.

2.10. **FORMA E CRITÉRIO DE SELEÇÃO DO FORNECEDOR**:

2.10.1. **MODALIDADE E TIPO DE LICITAÇÃO / ADJUDICAÇÃO**:

2.10.1.1 Considerando tratar-se de bens comuns de STIC, será adotada a modalidade pregão, em sua forma eletrônica, com fundamento no art. 1º da Lei nº. 10.520/2002 c/c o §1º do art. 1º do Decreto nº 10.024/2019.

2.10.1.2 O tipo de licitação será o "menor preço" e o critério de julgamento o "menor preço global" por lote.

2.10.1.3 A execução do objeto será efetivada de forma indireta e a contratação adotará o regime de execução empreitada por preço global (art. 6º, inciso VIII, letra "a", da Lei nº 8.666/1993).

2.10.1.4 Para a execução do objeto deverão ser observadas as especificações técnicas estabelecidas neste Termo de Referência e seus anexos.

2.10.1.5 Intenta-se, ademais, a formação de ARP – Ata de Registro de Preços, nos termos do Decreto nº 7.892, de 23 de janeiro de 2013, que regulamenta o Sistema de Registro de Preços previsto no art. 15 da Lei nº 8.666/93, com fundamento no inciso III do artigo 3º do Decreto nº 7.892/2013, alinhada a Estratégia Nacional de Cibersegurança da Justiça Eleitoral (Portaria nº 590/2022 do TSE), bem como à Resolução Nº 396/2021 do CNJ (ENSEC-PJ), que prevêem entre outras, as seguintes necessidades:

2.10.1.5.1 Elevar o nível de segurança das infraestruturas críticas;

2.10.1.5.2 Destinar recursos orçamentários específicos para as ações de segurança da informação;

2.10.1.5.3 Implementar a execução de programas, de projetos e de processos relativos à segurança da informação;

2.10.1.5.4. Utilizar de ferramentas e soluções automatizadas para gestão da Cibersegurança;

2.10.1.5.5 Capacitar equipe de tratamento e resposta a incidentes – ETIR;

2.10.1.5.6 Contratar serviços especializados para diagnóstico e análise de maturidade, e prover serviço especializado em Cibersegurança;

2.10.1.6 Esta aquisição propiciará o atendimento das recomendações mencionadas acima, especificamente por possibilitar compreender, abarcar à mais órgãos da Justiça Eleitoral,

conforme Anexo IX – Relação de Tribunais Interessados na ARP a este Termo de Referência.

2.10.1.7 Por não haver excepcionalidade, conforme orientações dos Acórdãos TCU nº 757/2015- Plenário e 2037/2019 – Plenário, o objeto da ARP não possibilitará adesões de outros órgãos da Administração Pública, com exceção dos Tribunais Regionais Eleitorais que não constam do Anexo IX - Relação de Tribunais Interessados na ARP a este Termo de Referência.

2.10.1.8 Aplica-se o Direito de Preferência previsto no Decreto nº 7.174/2010, no que couber.

2.10.2. **CRITÉRIO TÉCNICO DE HABILITAÇÃO JURÍDICA E REGULARIDADES JURÍDICA, FISCAL E ECONÔMICO-FINANCEIRA**: São as definidas no instrumento convocatório.

2.10.3. **QUALIFICAÇÃO TÉCNICA**:

2.10.3.1. As licitantes deverão comprovar aptidão para a prestação dos serviços em características, quantidades e prazos compatíveis com o objeto deste TR, mediante apresentação de Atestado(s) de Capacidade Técnica, fornecido(s) por pessoa jurídica de direito público ou privado, comprovando que a empresa já forneceu ou fornece bens/serviços(s) pertinente(s) e/ou similar(es) com o mesmo. Os atestados de capacidade técnica deverão ser emitidos no nome e com CNPJ da matriz e/ou filial da licitante.

2.10.3.1.1. Será considerado como serviço similar o fornecimento de soluções de segurança da informação e proteção de dados contemplando hardware, software e suporte, observados os requisitos do item 2.10.3.4. Estes são exemplos de serviços fornecidos similares que poderão ser acolhidos. Tal medida visa assegurar o perfeito cumprimento do contrato, por empresa idônea, e com *expertise* suficiente para evitar prejuízos ao Erário.

2.10.3.2. Os atestados deverão conter as seguintes informações mínimas: nome e cargo da pessoa que os assina, quantitativo, valor por item da solução fornecida, discriminação do serviço prestado e manifestação expressa de que a licitante presta (em caso de contrato vigente) ou prestou (em caso de contrato encerrado) satisfatoriamente os serviços contratados.

2.10.3.3. Os atestados deverão referir-se a serviços prestados no

âmbito da atividade econômica principal ou secundária especificadas no contrato social vigente da empresa licitante.

2.10.3.4. Para fins de comprovação de que trata a condição definida no **item 2.10.3.1**, os atestados deverão dizer respeito a serviços executados com as seguintes características mínimas:

2.10.3.4.1. Comprovação de expertise/experiência/proficiência na gestão de serviços de monitoramento proativo, e resposta a incidentes de segurança da informação, em ambientes com no mínimo 750 (setecentos e cinquenta) ativos/dispositivos compreendidos no escopo do serviço prestado.

2.10.3.4.2. Comprovação de experiência mínima de 06 (seis) meses na prestação de serviços de gestão de soluções de segurança da informação, em ambientes com no mínimo 750 (setecentos e cinquenta) usuários.

2.10.3.4.3. **METODOLOGIA ADOTADA PARA DEFINIÇÃO DAS CARACTERÍSTICAS MINIMAS DEFINIDAS NOS ITENS 2.10.3.4.1 e 2.10.3.4.2**

2.10.3.4.3.1. Por se tratar de contratação com objeto específico, e sem referência completa encontrada no mercado público e privado, somente há referencias parciais, que guardam similaridade e semelhança com esta, foi necessário mensurar e definir parâmetros e variáveis que pudessem assegurar e aferir a capacidade técnica, além da expertise mínima das licitantes, com o intuito de garantir partícipes que possam assegurar a qualidade necessária na prestação do serviço que se pretende contratar.

2.10.3.4.3.2. Toda contratação de solução (hardware, software e serviço) seja como serviço (*Solution as a Service*) ou não, as variáveis que impactam diretamente na qualidade, capacidade logística e expertise da entrega destes serviços, é a quantidade de usuários, a quantidade de ativos envolvidos, e a quantidade de locais onde serão prestados os serviços. Quanto maior for a quantidade de usuários, ativos e locais a serem atendidos, maior deverá ser a equipe técnica da licitante, a expertise/conhecimento dessa equipe e a capacidade de gestão necessária para desenvolver o projeto.

2.10.3.4.3.3. Em relação às quantidades para as variáveis definidas, foi feita uma análise em relação aos valores mínimos aceitáveis, com base nas informações fornecidas

pelos partícipes, e foi estimada uma quantidade mínima de 1000 usuários e 1000 dispositivos.

2.10.3.4.3.4. JUSTIFICATIVA PARA EXIGÊNCIA DA QUALIFICAÇÃO TÉCNICA

a. Considerando a abrangência da prestação dos serviços (vide Anexo IX) e com suporte nos Acórdãos TCU nº 1618/2002, 170/2007, 1417/2008 e 3070/2013, todos do Plenário, e visando resguardar a perfeita execução contratual em prol do interesse público, é imprescindível que a Administração "tenha as garantias necessárias para comprovação de que a empresa possui as condições técnicas para a boa execução dos serviços, tudo demonstrado no respectivo procedimento licitatório". Ademais, o Superior Tribunal de Justiça entende que:

"*ADMINISTRATIVO. LICITAÇÃO. INTERPRETAÇÃO DO ART. 30, II E §1º, DA LEI 8.666/93.*

1. Não se comete violação ao art. 30, II, da Lei nº 8.666/93, quando, em procedimento licitatório, exige-se a comprovação, em nome da empresa proponente, de atestados técnicos emitidos por operadoras de telefonia no Brasil de execução, em qualquer tempo, de serviço de implantação de cabos telefônicos classe 'L'e 'C' em período consecutivo de vinte e quatro meses, no volume mínimo de 60.000 HxH, devidamente certificados pela entidade profissional competente.

O exame do disposto no art. 37, XXI, da Constituição Federal, e sua parte final, referente a exigências de qualificação técnica e econômica indispensáveis à garantia do cumprimento das obrigações, revela que o propósito ai objetivado é oferecer iguais oportunidades de contratação com o Poder Público, não a todo e qualquer interessado, indiscriminadamente, mas sim, apenas a quem possa evidenciar que efetivamente dispõe de condições para executar aquilo a que se propõe (Adilson Dallari).

Mandado de segurança denegado em primeiro e segundo graus.". Recurso especial improvido. (Res. Nº 172.232-SP, rel. Min. José Delgado, DJU de 21.9.98, RSTJ 115/194).

ADMINISTRATIVO. PROCEDIMENTO LICITATÓRIO. ATESTADO TÉCNICO. COMPROVAÇÃO. AUTORIA. EMPRESA. LEGALIDADE.
Quando, em procedimento licitatório, exige-se comprovação, em nome da empresa, não está sendo violado o art. 30 §1º, II, caput, da Lei 8.666/1993. É de vital importância, no trato da coisa pública, a permanente perseguição ao binômio qualidade e eficiência, objetivando não só a garantir a segurança jurídica do contrato, mas também a consideração de certos fatores que integram a finalidade das licitações, máxime em se tratando daquelas de grande complexidade e de vulto financeiro tamanho que imponha ao administrador a elaboração de dispositivos, sempre em atenção à pedra de toque do ato administrativo – a lei – mas com dispositivos que busquem resguardar a Administração de aventureiros ou de licitantes de competência estrutural, administrativa e organizacional duvidosa.
Recurso provido." (Resp. nº 44.750-SP, rel. Ministro Francisco Falcão, 1ª T., unânime, DJ de 25.9.00) (grifos nosso)

2.10.3.5. O TRE-DF se reserva o direito de consultar a pessoa jurídica indicada no Atestado de Capacidade Técnica, visando obter informações sobre os serviços prestados, devendo a licitante sempre que solicitado, disponibilizar todas as informações necessárias à comprovação da legitimidade do(s) atestado(s) solicitado(s), apresentando, dentre outros documentos, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foram prestados os serviços, de acordo com o item 10.10 do Anexo VII-A da Instrução Normativa SEGES – ME nº 5/2017.

2.10.3.6. O atendimento poderá se dar por meio de um único atestado que contenha toda a comprovação da expertise prevista nos subitens 2.10.3.4.1 e 2.10.3.4.2, respectivamente, alinhados ao item 2.10.3.1.1, ou ainda por meio de vários atestados que, juntos, comprovem a experiência solicitada, conforme previsão contida no item 10.9 do Anexo VII-A da IN SEGES/ME nº 05/2017, desde que concomitantes, admitindo-se este para o

somatório de quantitativos de itens e não para o somatório de prazos.

2.10.3.7. Somente serão aceitos atestados expedidos após a conclusão do contrato ou decorrido, no mínimo, 06 (seis) meses do início de sua execução, exceto se firmado para ser executado em prazo inferior, conforme item 10.8 do Anexo VII-A da IN SEGES/ME nº 5/2017.

2.10.3.8. **A Justificativa para a exigência de atestado:** A exigência de atestados de capacidade técnica tem o objetivo de comprovar a aptidão da empresa no desempenho de atividade compatível com o objeto da licitação. Além disso, segundo entendimento do TCU, a comprovação da capacidade técnica da licitante é realizada por meio de atestados que reflitam a execução satisfatória de objeto compatível com as características do objeto licitado. Este documento deverá ser entregue junto com a proposta. (Acórdão nº 1.677/2014-TCU Plenário; Acórdão nº 3663/2013 – TCU – Plenário etc). A exigência objetiva ainda:

I. Garantir a contratação de empresa com experiência na prestação dos serviços ora pretendidos;
II. Evitar danos ao patrimônio público;
III. Maior relação custo X benefício X necessidade na execução dos trabalhos.

2.10.3.9. Para a comprovação do atendimento das especificações técnicas, a LICITANTE deverá apresentar documento detalhando as informações, local, site, páginas, documento, etc, necessários para aferição e atendimento de todos os itens da especificação técnica, ou seja, deverá apresentar uma espécie de índice, indicando o item, o documento que atende a especificação (nome do mesmo), O local onde está disponibilizado o documento (URL, Site, ou outro disponibilizado de forma digital), a página, e o texto que comprova o atendimento ao item.

2.10.3.10. Caso a LICITANTE não apresente o documento mencionado no item anterior, poderá ser realizada diligencia complementar conforme entendimento do pregoeiro.

2.10.4. **PERMISSÃO À PARTICIPAÇÃO DE EMPRESAS REUNIDAS EM CONSÓRCIO E DE COOPERATIVAS**:

2.10.4.1. Por meio deste vimos apresentar justificativa acerca da não participação de empresas enquadradas nas modalidades de Consórcio e Cooperativa no presente procedimento licitatório.

2.10.4.2. Acerca dos Consórcios este TRE, informa que a conveniência de admitir a participação dos mesmos em procedimento

licitatório é decisão meramente discricionária da Administração, conforme artigo 33 da Lei n.º 8.666/93.

2.10.4.3. Sobre o tema, Marçal Justen Filho (Comentários à lei de licitações e contratos administrativos, 12. ed., São Paulo: Dialética, p. 410) assevera:

> *O ato convocatório admitirá ou não a participação de empresas em consórcio. Trata-se de escolha discricionária da Administração Pública, o que evidentemente não significa autorização para decisões arbitrárias ou imotivadas.*

E assim conclui:

> *Admitir ou negar a participação de consórcios é o resultado de um processo de avaliação do mercado em face do objeto a ser licitado e da ponderação dos riscos inerentes à atuação de uma pluralidade de sujeitos associados para a execução do objeto.*

2.10.4.4. A vedação quanto à participação de consórcio de empresas no presente procedimento licitatório não limitará a competitividade.

2.10.4.5. Acerca das Cooperativas por sua vez atestamos que permitir a participação das mesmas representaria desrespeitar o Princípio Constitucional da Eficiência, previsto no Artigo 37 da Constituição Federal de 1988, considerando que todo e qualquer procedimento referente ao contrato, aos aditivos e pagamentos necessitariam obrigatoriamente da assinatura, e conseqüente anuência, de todos os cooperados dificultando, ou até impossibilitando, a célere execução do objeto pretendido.

2.10.5. **VISTORIA**

2.10.5.1. A licitante interessada poderá realizar vistoria prévia à abertura do certame, para verificar os ambientes onde será instalada a solução, bem como obter informações sobre os equipamentos e softwares de propriedade do TRE-DF existentes no mesmo ambiente. Não serão aceitas alegações posteriores de desconhecimento das condições do local, equipamentos e softwares relativos à prestação dos serviços.

2.10.5.2. Caso queira realizar a vistoria prévia, a licitante interessada poderá fazê-lo até 02 (dois) dias úteis antes da data designada para abertura do pregão, mediante agendamento prévio com 01 (um) dia útil de antecedência da data da vistoria, por meio dos telefones 3048-

4040/4480/4149, junto à Coordenadoria de Infraestrutura.

2.10.5.3. Não será permitida vistoria de duas ou mais empresas concomitantemente.

2.10.5.4. A prestação dos serviços objeto deste Instrumento ocorrerá nos endereços indicados no **Anexo IX** deste Termo de Referência.

2.10.5.5. A CONTRATADA ficará responsável pela execução integral do objeto do contrato, não podendo alegar desconhecimento de peculiaridades eventualmente existentes pela não realização da vistoria ou por omissões no momento da sua realização.

2.10.5.6. A licitante deverá apresentar o Termo de Vistoria ou, caso não a realize, o Termo de Ciência das condições de execução contratual, conforme modelos anexos (**Anexo V** a este TR), que será exigido como condição para habilitação.

2.11. **INFORMAÇÕES ACERCA DO IMPACTO AMBIENTAL:**

2.11.1. A CONTRATADA deverá assumir todas as responsabilidades e tomar as medidas cabíveis para a correção dos danos que vierem a ser causados, caso ocorra passivo ambiental, em decorrência da execução de suas atividades objeto desta contratação.

2.11.2. Os profissionais da CONTRATADA, quando nas dependências do TRE-DF, deverão observar todos os protocolos sanitários estabelecidos pela CONTRATANTE em função da pandemia de COVID-19, e os profissionais serão orientados pela CONTRATADA quanto aos protocolos e ao uso de máscaras, fornecidas pela CONTRATADA.

2.11.3. Os materiais, objeto desde Termo de Referência, deverão seguir, no que couberem, os seguintes normativos:

2.11.3.1. Art. 3º, caput, da Lei nº. 8.666/93, com redação pela Lei nº12.349/2010;

2.11.3.2. Decreto nº. 7.746, de 5 de junho de 2012;

2.11.3.3. Lei nº. 12.305, de 2 de agosto de 2010;

2.11.3.4. Decreto nº. 10.936, de 12 de janeiro de 2022;

2.11.3.5. Instrução Normativa nº. 01/2010, do atual Ministério da Economia;

2.11.3.6. Art. 225 da Constituição da República Federativa do Brasil de 1988;

2.11.3.7. Plano de Logística Sustentável do TREDF.

2.12. **CONFORMIDADE TÉCNICA E LEGAL:**

2.12.1. **Resolução nº 182/2013 CNJ** - Dispõe sobre diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação pelos órgãos submetidos ao controle administrativo e financeiro do Conselho Nacional de Justiça (CNJ).

2.12.2. **Resolução Administrativa 7760/2017 TRE-DF** – Institui o Plano

Estratégico de Tecnologia da Informação e Comunicação – PETIC do Tribunal Regional Eleitoral do Distrito Federal – TRE-DF, para o quadriênio 2017-2020 - PTIC.

2.12.3. **Portaria Presidência Nº 3/2018 TRE-DF/PR/GDG** – Regulamenta a elaboração do Plano de Contratações de Soluções de Tecnologia da Informação e Comunicação – PCSTIC, no âmbito do Tribunal Regional Eleitoral do Distrito Federal – TRE-DF.

2.12.4. **Portaria Presidência Nº 112/2018 TRE-DF/PR/GDG** - Institui a política de controle de acesso às informações e aos recursos de processamento da informação, no âmbito do Tribunal Regional Eleitoral do Distrito Federal (TRE-DF).

2.12.5. **Portaria Presidência Nº 113/2018 TRE-DF/PR/GDG** - Institui a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) no âmbito do Tribunal Regional Eleitoral do Distrito Federal.

2.12.6. **Portaria Presidência Nº 119/2018 TRE-DF/PR/GDG** - Nomeia o Gestor de Segurança da Informação no âmbito do Tribunal Regional Eleitoral do Distrito Federal.

2.12.7. **Portaria Presidência Nº 125/2018 TRE-DF/PR/GDG** - Institui a Política de Gestão de Continuidade de Negócios de Tecnologia da Informação, no âmbito do Tribunal Regional Eleitoral do Distrito Federal (TRE-DF) – PGCNTIC.

2.12.8. **Lei nº 8.666/1993** – "Regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências".

2.12.9. **Lei nº 10.520/2002: "***Institui, no âmbito da União, Estados, Distrito Federal e Municípios, nos termos do art. 37, inciso XXI, da Constituição Federal, modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns, e dá outras providências*.**".**

2.12.10. **Decreto nº 10.024/2019:** "*Regulamenta a licitação, na modalidade pregão, na forma eletrônica, para a aquisição de bens e a contratação de serviços comuns, incluídos os serviços comuns de engenharia, e dispõe sobre o uso da dispensa eletrônica, no âmbito da administração pública federal*".

2.12.11. **Decreto nº 7.892/1993: "***Regulamenta o Sistema de Registro de Preços previsto no art. 15 da Lei nº 8.666, de 21 de junho de 1993***".**

2.12.12. **Lei nº 9.609, de 19 de fevereiro de 1998** - "Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências.".

2.12.13. **Lei nº 13.853, de 8 de julho de 2019**: "Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências.".

2.12.14. **Resolução CNJ nº 370, de 28 de janeiro de 2021** - "Institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD).".

2.12.15. **Plano de Logística Sustentável do TRE/DF**, no que couber.

2.12.16. **Decreto nº 7174/2010:** Regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público, e pelas demais organizações sob o controle direto ou indireto da União.

2.13. **OBRIGAÇÕES CONTRATUAIS:**

2.13.1. **DEVERES E RESPONSABILIDADES DA CONTRATANTE:**

2.13.1.1. Promover o acompanhamento e a fiscalização da execução do contrato.

2.13.1.2. Recusar, a critério da fiscalização, qualquer bem ou serviço fornecido ou executado fora das condições contratadas.

2.13.1.3. Receber os bens e serviços na forma descrita neste Termo de Referência, no contrato e na Nota de Empenho.

2.13.1.4. Prestar as informações, recomendações e os esclarecimentos que venham a ser solicitados pela CONTRATADA.

2.13.1.5. Efetuar o pagamento à CONTRATADA, segundo as condições estabelecidas no termo contratual ou seu substitutivo.

2.13.1.6. Comunicar oficialmente à CONTRATADA quaisquer falhas verificadas na execução dos serviços, consignando prazo para saneamento das inconsistências.

2.13.1.7. Aplicar as sanções previstas no instrumento contratual, assegurando à CONTRATADA o contraditório e a ampla defesa.

2.13.2. **DEVERES E RESPONSABILIDADES DA CONTRATADA:**

2.13.2.1. Zelar pela perfeita execução contratual, indicando ao TRE-DF, por escrito e antes da data prevista para o início da execução contratual, um preposto idôneo com poderes para representar a empresa, no que toca às questões administrativas e, principalmente, no tocante à eficiência e agilidade na execução do contrato, fornecendo o telefone e e-mail de contato do referido preposto.

2.13.2.2. Responsabilizar-se pela entrega dos materiais e serviços conforme especificado, nos termos da legislação em vigor e neste Termo de Referência.

2.13.2.3. Fornecer o(s) produto(s), originais do(s) fabricante(s), no prazo e demais condições estipuladas neste Termo de Referência, no contrato e na proposta.

2.13.2.4. Monitorar o ambiente da CONTRATANTE 24x7x365 (vinte e quatro horas por dia, durante os sete dias da semana e nos doze meses do ano), durante o período de vigência da

contratação, informando sua equipe técnica sobre qualquer ocorrência que necessite de atuação, a fim de salvaguardar os serviços, sistemas e aplicações do Tribunal.

2.13.2.5. Manter durante a execução da contratação, todas as condições de habilitação e qualificação exigidas como condição para a celebração do contrato ou instrumento equivalente (inciso XIII do artigo 55 da Lei nº 8.666/1993).

2.13.2.6. Fornecer materiais de primeira qualidade e que atendam as normas do Código de Defesa do Consumidor, no que couber.

2.13.2.7. Responder, por todas as despesas decorrentes da execução do objeto e por outras correlatas, tais como frete, obrigações trabalhistas, seguros de acidentes, encargos fiscais e comerciais, encargos sociais, tributos e emolumentos e outras que porventura venham a ser criadas e exigidas pelo Poder Público.

2.13.2.8. Respeitar as normas e procedimentos de controle interno, inclusive de acesso às dependências do TRE-DF.

2.13.2.9. Responder pelos danos causados diretamente ao TRE-DF, ou a terceiros, decorrentes de sua culpa ou dolo, não excluindo ou reduzindo dessa possibilidade a fiscalização ou o acompanhamento pelo TRE-DF.

2.13.2.10. Comunicar ao TRE-DF qualquer anormalidade constatada e prestar os esclarecimentos solicitados.

2.13.2.11. Abster-se de subcontratar outra empresa para a execução do objeto deste procedimento, sem autorização do TRE-DF.

2.13.2.12. Informar ao TRE-DF, através de Declaração, caso haja alteração em seus dados bancários.

2.13.2.13. Informar ao TRE-DF, através de declaração entregue com protocolo, caso haja alteração de endereço, telefone ou e-mail, sendo consideradas válidas todas as notificações, intimações, correspondências e avisos que lhe forem dirigidas para o endereço contratual, telefone ou e-mail originalmente indicado, caso não seja procedida à mencionada alteração.

2.13.2.14. Reportar formal e imediatamente ao gestor do contrato quaisquer problemas, anormalidades, erros ou irregularidades que possam comprometer a execução do objeto, utilizando-se das formas de comunicação estabelecidas neste Termo de Referência.

2.13.2.15. Seguir as instruções e observações efetuadas pelo gestor do contrato, bem como, reparar, corrigir ou substituir às suas expensas, no todo ou em parte, os itens que se constituem o objeto quando se verificarem vícios, defeitos ou incorreções.

2.13.2.16. Responder integralmente por quaisquer perdas ou danos causados ao CONTRATANTE ou a terceiros em razão de

ação ou omissão, dolosa ou culposa, sua ou dos seus profissionais em razão da execução do objeto, independentemente de outras cominações contratuais ou legais a que estiver sujeita.

2.13.2.17. Fornecer, quando solicitado, relatórios impressos nos formatos PDF e/ou CSV.

2.13.2.18. Fornecer, quando solicitado, a exportação de dados no padrão PCAP.

3. ESPECIFICAÇÃO TÉCNICA DETALHADA:

3.1. MODELO DE EXECUÇÃO E DE GESTÃO DO CONTRATO:

3.1.1. PAPEIS E RESPONSABILIDADES:

Papel	Entidade	Responsabilidade
Equipe de Apoio à Contratação	TRE-DF	Equipe responsável por subsidiar a Área de Licitações em suas dúvidas, respostas aos questionamentos, recursos e impugnações, bem como na análise e julgamento das propostas das licitantes.
Equipe de Gestão da Contratação	TRE-DF	Equipe composta pelo Gestor do Contrato, responsável por gerir a execução contratual e, sempre que possível e necessário, pelos Fiscais Demandante, Técnico e Administrativo, responsáveis por fiscalizar a execução contratual, consoante às atribuições regulamentares.
Fiscal Demandante do Contrato	TRE-DF	Servidor representante da Área Demandante da Solução de Tecnologia da Informação e Comunicação, indicado pela respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos funcionais da solução.
Fiscal Técnico do Contrato	TRE-DF	Servidor representante da Área de Tecnologia da Informação e Comunicação, indicado pela respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos técnicos da solução.
Fiscal Administrativo do Contrato	TRE-DF	Servidor representante da Área Administrativa, indicado pela respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos administrativos da execução, especialmente os referentes ao recebimento, pagamento, sanções, aderência às normas, diretrizes e obrigações contratuais.
Gestor do Contrato	TRE-DF	Servidor com atribuições gerenciais, técnicas ou operacionais relacionadas ao processo de gestão do contrato, indicado por autoridade competente do órgão.
Preposto	Contratada	Funcionário representante da empresa contratada, responsável por acompanhar a execução do contrato e

		atuar como interlocutor principal junto ao órgão contratante, incumbido de receber, diligenciar, encaminhar e responder as questões técnicas, legais e administrativas referentes ao andamento contratual.

3.1.2. **DINÂMICA DE EXECUÇÃO:**

3.1.2.1. **Evento: Assinatura da Ata de Registro de Preços – ARP**

3.1.2.1.1. A assinatura da ARP ocorrerá após a homologação do Pregão Eletrônico.

3.1.2.2. **Evento: Assinatura do Contrato.**

3.1.2.2.1. A assinatura do contrato ocorrerá após a assinatura da ARP pelas partes.

3.1.2.3. **Evento: Emissão da Ordem de Serviço.**

3.1.2.3.1. Ocorrerá em até 05 (cinco) dias úteis após a assinatura do contrato, cabendo ao Gestor do contrato, emitir a Ordem de Serviço (OS).

3.1.2.4. **Evento: Elaboração e Entrega do Plano de Instalação.**

3.1.2.4.1. A CONTRATADA deverá apresentar em até 10 dias corridos, após a emissão da Ordem de Serviço, o Plano de Projeto/Instalação, para análise e validação da CONTRATANTE, que terá 05 dias corridos, para entregar suas considerações e ajustes ao Plano, para que a CONTRATADA por sua vez, em até 03 dias corridos, faça todos os ajustes necessários e o mesmo, possa ser aprovado para iniciar a preparação do ambiente para início da execução do Plano de Instalação da solução.

3.1.2.5. **Evento: Entrega da solução.**

3.1.2.5.1. A entrega da solução (hardware em comodato e softwares que serão utilizados) deverá acontecer em até 60 (sessenta) dias corridos após a aprovação do Plano de Instalação pela CONTRATANTE.

3.1.2.6. **Evento: Ativação/Instalação da solução**

3.1.2.6.1. A ativação da solução deverá ocorrer em até 15 dias úteis após a entrega da solução.

3.1.2.7. **Evento: Aceite provisório.**

3.1.2.7.1. O gestor emitirá termo circunstanciado referente ao aceite provisório após o início da execução do serviço, em no máximo 05 dias corridos, contados da entrega da solução (licenças, softwares e hardwares), conforme item 3.1.2.5.1.

3.1.2.8. **Evento: Emissão do aceite definitivo.**

3.1.2.8.1. A Comissão de Recebimento Definitivo emitirá termo circunstanciado de recebimento definitivo, após a verificação de conformidade e atendimento do previsto no item 4.2.11 deste

TR, em até 10 dias corridos, após a finalização da instalação, implementação, parametrização e verificação do atendimento aos requisitos e ao objeto definido.

3.1.2.9. A prestação dos serviços referentes à solução, dar-se-á nas localidades e nos endereços definidos e apresentados no **Anexo IX** deste TR.

3.1.2.10. Abaixo, segue cronograma macro com os eventos, descrição das ações referentes à execução do contrato, bem como os prazos previstos para realização das mesmas.

Evento	Descrição	Prazo previsto	Responsável
1	Publicação da ARP	Após a homologação do certame.	TRE-DF/SAO
2	Assinatura do Contrato	Em até 05 dias úteis após a assinatura da ARP.	TRE-DF/DG - CONTRATADA
3	Emissão da Ordem de Serviço	Em até 03 dias úteis após o evento 2.	GESTOR DO CONTRATO
4	Elaboração e Entrega do Plano de Instalação	Em até 10 dias corridos, após o evento 3.	CONTRATADA
5	Entrega da solução	Em até 60 dias corridos, após o evento 4.	CONTRATADA
6	Ativação/Instalação da solução	Em até 15 dias úteis, após o evento 5.	CONTRATADA
7	Aceite provisório	Em até 05 dias corridos, após o evento 5.	GESTOR DO CONTRATO
8	Aceite definitivo	Em até 10 dias corridos, após o evento 6.	COMISSÃO DE RECEBIMENTO DEFINITIVO

3.1.3. **INSTRUMENTOS DE SOLICITAÇÃO DOS BENS E/OU DE SERVIÇOS:**

3.1.3.1. Nota de empenho: De natureza orçamentária, o qual se reserva o montante financeiro para a execução do contrato.

3.1.3.2. Ordem de Serviço: Documento emitido pelo gestor a fim demandar ação da CONTRATADA para execução de parte ou o todo de um determinado serviço ou fornecimento.

3.1.3.3. Chamado técnico: Dispositivo pelo qual o CONTRATANTE acionará a CONTRATADA para tirar dúvidas ou resolver problemas relacionados às licenças. Neste caso, a assistência técnica que prestará o serviço deverá dispor de um número telefônico para suporte técnico e abertura de chamados técnicos, sem ônus para o CONTRATANTE.

3.1.4. **GARANTIA E SUPORTE TÉCNICO:**

3.1.4.1. **GARANTIA:**

3.1.4.1.1. Deverá ser considerado o período mínimo de 24 (vinte e quatro) meses de suporte técnico e atualização do

fabricante na modalidade 24x7x365 (vinte e quatro horas do dia, em todos os dias da semana, durante o ano inteiro) sem custos adicionais ao CONTRATANTE, contados a partir da emissão do Termo de Recebimento Definitivo da Solução.

3.1.4.1.1.1. A garantia deverá cobrir falhas nos serviços de ativação, configuração e nos entregáveis da solução e dos serviços prestados, no fornecimento de correção de software, substituições de hardware defeituoso e fornecimento de atualizações corretivas e evolutivas de software integrante da solução.

3.1.4.1.2. O Prazo de garantia deverá ser aferido pelo sítio eletrônico do(s) fabricante(s), durante a fase de recebimento.

3.1.4.1.3. Prover suporte e atualização contendo as seguintes características:

3.1.4.1.3.1. Atualizações de programas, correções, alertas de segurança e atualizações críticas e essenciais para garantia de pleno funcionamento do produto durante 24 x 7 x 365;

3.1.4.1.3.2. Scripts de atualização;

3.1.4.1.3.3. Versões principais de softwares, o que inclui atualização para novas versões dos programas, versões de manutenção geral, versões de funcionalidades escolhidas e atualizações de documentação;

3.1.4.1.4. A CONTRATADA deverá fornecer ao CONTRATANTE as atualizações, correções, modificações e/ou melhorias introduzidas nos softwares objetos da contratação tão logo ocorra a sua homologação, publicação e disponibilização pelo fabricante, sem custos adicionais ao contrato;

3.1.4.1.5. A CONTRATADA deverá informar proativamente ao CONTRATANTE sobre a descoberta de bugs e as suas respectivas correções nos softwares relacionados desta contratação, emitindo relatório técnico para a CONTRATANTE, durante todo o período de vigência do contrato/garantia;

3.1.4.1.6. A CONTRATADA deverá fornecer ao CONTRATANTE informações detalhadas por meio de relatório técnico e toda a documentação aplicável sobre os erros ou bugs e seus possíveis impactos;

3.1.4.1.7. O CONTRATANTE terá como opção executar ou não as atualizações de software disponibilizadas;

3.1.4.1.8. Caberá a CONTRATADA, resolver dúvidas e

esclarecimentos relativos à utilização e configuração das funcionalidades relacionadas ao objeto contratado;

3.1.4.1.9. Caberá a CONTRATADA, resolver problemas de desempenho e estabilidade do ambiente;

3.1.4.1.10. Caberá a CONTRATADA, resolver problemas que limitem ou impeçam o desenvolvimento e/ou execução das aplicações do CONTRATANTE que façam uso efetivo das funcionalidades de software que compõe a solução;

3.1.4.1.11. A CONTRATADA deverá prestar serviço de suporte nas modalidades, telefônica, via Web e/ou presencial On-Site;

3.1.4.1.12. O Serviço de suporte telefônico do fabricante poderá ser em inglês ou português do Brasil, conforme políticas do fabricante;

3.1.4.1.13. A CONTRATADA deverá garantir que o CONTRATANTE possa efetuar um número ilimitado de chamados de suporte durante o período de garantia, para suprir suas necessidades de utilização dos softwares, sem ônus adicional;

3.1.4.1.14. A CONTRATADA deverá fornecer ao CONTRATANTE acesso ao sistema de suporte on-line que permita a abertura e acompanhamento de chamados.

3.1.4.2. **SUPORTE TÉCNICO:**

3.1.4.2.1. A CONTRATADA deverá fornecer através do suporte do fabricante, tempo de resposta máximo de acordo com níveis de severidade, a partir da abertura do chamado técnico:

3.1.4.2.1.1. Severidade 1: O funcionamento da solução é interrompido ou tão severamente impactado que não é possível trabalhar ou utilizar/operar a mesma. A perda do serviço é total. A operação é essencial para o negócio e trata-se de uma emergência. Uma solicitação de serviço severidade 1 tem uma ou mais das seguintes características:

I. dados corrompidos;
II. uma função crítica documentada não está disponível;
III. A solução ou parte da mesma trava indefinidamente, gerando impacto inaceitável ao serviço, impactando recursos, respostas e a operação do serviço;
IV. O sistema falha repetidamente após várias tentativas de reinicialização.

3.1.4.2.1.2. Severidade 2: A perda do serviço é pequena. O problema gera inconvenientes que podem requerer uma solução temporária para restauração de funcionalidade ou

serviço.

3.1.4.2.1.3. Severidade 3: Solicitação de informações, melhorias ou esclarecimentos relativos ao software e/ou hardware, mas não há impacto na operação do mesmo. Não há perda de serviço. O resultado não impede o funcionamento do sistema.

3.1.4.2.2. O prazo de início do atendimento dos chamados técnicos deverá ocorrer conforme os níveis mínimos de serviço detalhados abaixo, contados da abertura do chamado.

Severidade	Tempo máximo de início do atendimento	Disponibilidade para atendimento
1	Os chamados de Severidade 1 deverão ser iniciados no prazo de 4 (quatro) horas	24 horas por dia, 7 dias por semana
2	Os chamados de Severidade 2 deverão ser iniciados no prazo de 8 (oito) horas	24 horas por dia, 7 dias por semana
3	Os chamados de Severidade 3 deverão ser iniciados no prazo de 24 (vinte e quatro) horas	24 horas por dia, 7 dias por semana

3.1.4.2.3. Caso seja identificado um defeito no software (bugs, erros e/ou falhas que não impactem o funcionamento do mesmo, ou que impeça a realização dos serviços para o qual a solução foi construída, implementada), o mesmo deverá ser resolvido em até 30 (trinta) dias corridos a contar da abertura do chamado. Não sendo resolvido neste prazo, deverá ser providenciada uma solução de contorno dentro do intervalo dos 30 dias supracitado, até que a solução definitiva seja efetivada.

3.1.4.2.3.1. No caso de aplicação de solução de contorno, a solução definitiva deverá ser entregue em até 45 (quarenta e cinco) dias corridos, incluídos os 30 dias mencionados no caput deste.

3.1.4.2.4. Caso seja identificado um defeito no hardware (peças defeituosas), o mesmo deverá ser resolvido em até 48 (quarenta e oito) horas a contar da abertura do chamado ou, não resolvendo neste prazo, deverá ser providenciada uma solução de contorno, dentro do prazo de 48 horas supracitado, até que a solução definitiva seja efetivada.

3.1.4.2.4.1. No caso de aplicação de solução de contorno, a solução definitiva deverá ser entregue em até 30 (trinta) dias úteis.

3.1.4.3. **SANÇÕES APLICÁVEIS**

3.1.4.3.1. Caberá à CONTRATADA até o 5º dia útil de cada mês após o efetivo início da prestação dos serviços, emitir relatório contendo todas as informações necessárias para demonstrar o cumprimento e entrega do:

3.1.4.3.1.1. Índice de disponibilidade do serviço da solução implementada, em minutos por mês;

3.1.4.3.1.2. Índice de efetividade nas intervenções e detecções realizadas.

3.1.4.3.1.3. Relatório de execução das Ordens de Serviço referentes às demandas de serviços de Operação Assistida.

3.1.4.3.2. Os relatórios mencionados no **item 3.1.4.3.1**, deverão ser armazenados em local a ser definido entre as partes, e sempre que solicitados pela CONTRATANTE, deverão estar disponíveis para consulta e análise por parte de sua equipe.

3.1.4.3.3. O serviço prestado pela CONTRATADA, conforme previsto neste item será pago conforme definido no **Item 3.1.7** deste TR, e sempre que necessário for, este serviço será avaliado conforme relatórios previstos no **item 3.1.4.3.1**.

3.1.4.3.4. Os relatórios mencionados no **item 3.1.4.3.1** deverão demonstrar os incidentes que ocorreram durante o período, as soluções e intervenções propostas e que efetivamente foram adotadas, além da descrição detalhada dos procedimentos operacionais realizados nas intervenções.

3.1.4.3.5. Caberá à CONTRATADA, emitir ainda relatórios diários quando a situação do incidente identificado motive a ciência da equipe da CONTRATANTE, devido a criticidade do mesmo, e este deverá conter minimamente:

3.1.4.3.5.1. Detalhamento e descrição do incidente;

3.1.4.3.5.2. Ativos e portas envolvidas;

3.1.4.3.5.3. Ações e procedimentos realizadas;

3.1.4.3.5.4. Impacto observado quando for o caso;

3.1.4.3.5.5. Recomendações para correção da vulnerabilidade quando for o caso.

3.1.4.3.6. Os indicadores e as metas dos níveis de serviço mínimos esperados para os índices definidos no item 3.1.4.3.1, estão descritos na tabela a seguir.

ITEM	NOME DO INDICADOR	FÓRMULA DE CÁLCULO	NÍVEL DE SERVIÇO (METAS)	% DE MULTA
1	Índice de disponibilidade da solução	IDS = ((TM – TI) / TM) x 100	Maior ou igual a 90%	Entre 90% e 100% - 0%; Entre 89,99 e 85% - 1% sobre o valor

				total do contrato; Entre 84,99 a 80% - 2% sobre o valor total do contrato; Entre 79,99 a 75% - 3% sobre o valor total do contrato.
2	Índice de efetividade nas intervenções	IEI = ((QTI – QFP - QIR) x 100	Maior ou igual a 90%	Entre 90% e 100% - 0%; Entre 89,99 e 85% - 1% sobre o valor total do contrato; Entre 84,99 a 80% - 2% sobre o valor total do contrato; Entre 79,99 a 75% - 3% sobre o valor total do contrato.
3	Demandas de Operação Assistida	DOA = (QOS / TOS) x 100	Maior ou igual a 90%	Entre 90% e 100% - 0%; Entre 89,99 e 85% - 0,4% sobre o valor total do contrato; Entre 84,99 a 80% - 0,6% sobre o valor total do contrato; Entre 79,99 a 75% - 0,8% sobre o valor total do contrato.

Tabela de Multas Aplicáveis

3.1.4.3.7. Sendo:

3.1.4.3.7.1. IDS: Índice de Disponibilidade da Solução;

3.1.4.3.7.2. TTF: Tempo Total de Funcionamento da Solução,

em minutos por mês;

3.1.4.3.7.3. TTI: Tempo Total de Indisponibilidade da Solução, em minutos por mês;

3.1.4.3.7.4. IEI: Índice de Efetividade nas Intervenções Realizadas;

3.1.4.3.7.5. QTI: Quantidade Total de Incidentes Identificados;

3.1.4.3.7.6. QIR: Quantidade de Intervenções Não Realizadas;

3.1.4.3.7.7. DOA: Demandas de Operação Assistida;

3.1.4.3.7.8. TOS: Total de Ordens de Serviço de Operação Assistida abertas no mês;

3.1.4.3.7.9. QOS: Quantidade de Ordens de Serviços de Operação Assistida finalizadas no mês;

3.1.4.3.8. O Índice de Disponibilidade da Solução – IDS, será medido pela disponibilidade de toda a solução, incluídas todas as ferramentas, hardwares, softwares, licenciamentos, subscrições e demais itens que façam parte da solução entregue e implementada pela CONTRATADA, em atendimento ao previsto neste TR.

3.1.4.3.9. Caso a indisponibilidade da solução seja motivada por falha na infraestrutura da CONTRANTE, o período referente a essa indisponibilidade, não será consideração para o cálculo do IDS.

3.1.4.3.10. O Índice de Efetividade nas Intervenções Realizadas – IEI, será medido com base nos incidentes efetivamente validados, efetivos, não serão considerados os falsos positivos registrados.

3.1.4.3.11. As intervenções não realizadas (QIR), são aquelas que a CONTRATADA, mesmo sabendo que havia necessidade de intervir, e que tinha autonomia a partir da solução implementada para intervir e não tomou a ação para a devida intervenção.

3.1.4.3.12. Caso a intervenção não tenha sido realizada pela CONTRATADA, por que extrapolava sua autonomia, ou seja, somente a equipe da CONTRATANTE poderia intervir, esta não será considerada no cálculo do IEI.

3.1.4.3.13. Caberá á CONTRATADA, apresentar as devidas justificativas para não ter realizado alguma intervenção relacionada a incidente validado, ou que tenha relação com indisponibilidade da solução no relatório mensal.

3.1.4.3.14. O cálculo mensal dos indicadores levará em conta o período entre o primeiro e o último dia de cada mês.

3.1.4.3.15. A CONTRATANTE se reserva o direito de auditar os indicadores a qualquer momento e também referente a qualquer período pretérito, podendo ocorrer multas retroativas caso sejam constatados erros.

3.1.4.3.16. Caso as metas estabelecidas (conforme item 3.1.4.3.6) para os indicadores não sejam alcançadas por 3 (três) meses

consecutivos ou por 3 (três) meses intercalados, em um período de 6 (seis) meses seguidos, a CONTRATADA estará sujeita às sanções cabíveis conforme a lei de licitações vigente e demais aplicáveis.

3.1.4.3.17. Os valores fracionados que porventura venham a ser medidos, referente ao % de Multa que será aplicado, deverão sempre considerar o maior número inteiro, próximo do Percentual/Faixa que se está querendo enquadrar, ou seja, caso tenhamos um valor Percentual/Faixa de 84,94%, deve-se considerar o atendimento do Percentual/Faixa entre 89,99% e 85%, aplicando uma multa de 1% sobre o valor total do contrato.

3.1.4.3.18. A CONTRATADA deverá atender mensalmente aos relatórios que deverão ser entregues conforme previsto no **Anexo VI**, estando sujeita às sanções aplicáveis conforme o caso e a meta estabelecida e não cumprida (item 3.1.4.3.6).

3.1.4.3.19. Caso a CONTRATADA entregue entre 90 a 100% dos relatórios obrigatórios por mês dentro do prazo, não se aplica multa. Nos demais casos, a CONTRATADA será advertida pelo descumprimento.

3.1.4.3.20. Caso a CONTRATADA mesmo após advertidas, descumpra por 3 (três) meses consecutivos ou por 3 (três) meses intercalados, em um período de 6 (seis) meses seguidos, os percentuais estabelecidos para entrega dos relatórios previstos no **Anexo VI**, a mesma estará sujeita a multa de 0,2% sobre o valor do contrato.

3.1.4.3.21. Os casos omissos que se apresentarem serão tratados entre as partes, e apreciados à luz da legislação vigente sobre a matéria.

3.1.4.3.22. As informações que precisarão ser fornecidas conforme solicitado no **Anexo VI – Entregáveis**, e que estão com a periodicidade definida como **"MENSAL SOB DEMANDA"**, somente deverão ser fornecidas quando solicitadas pela CONTRATANTE, via OS, conforme modelo definido no **Anexo VII**.

3.1.4.3.23. Os entregáveis com periodicidade definida como **"MENSAL SOB DEMANDA",** não terão custos a mais ao CONTRATANTE.

3.1.4.4. Demais previsões de sanções serão definidas em cláusula específica do contrato.

3.1.5. **<u>MECANISMOS FORMAIS DE COMUNICAÇÃO:</u>**

3.1.5.1. **Função de Comunicação**: Emissão da Ordem de Serviço.

- Documento: Ordem de serviço.
- Emissor: Gestor ou Fiscal do contrato.

- Destinatário: Preposto da CONTRATADA.
- Meio: As comunicações realizadas entre a CONTRATANTE e a CONTRATADA relacionadas sobre a gestão do contrato deverão ser registradas prioritariamente por escrito no sistema SEI e enviadas por e-mail, nesse mesmo sistema e também via e-mail institucional dos responsáveis pela comunicação, Gestor ou Fiscal do contrato.
- Periodicidade: A Ordem de Serviço será emitida em até 05 dias úteis, após a assinatura do contrato, conforme definido no item 3.1.2.3.

3.1.5.2. **Função de Comunicação**: Abertura de chamados.

- Documento: Chamado.
- Emissor: Gestor ou Fiscal de Contrato.
- Destinatário: Preposto da Contratada
- Meio: As comunicações realizadas entre a CONTRATANTE e a CONTRATADA deverão ser por telefone 0800, e-mail ou registro na página desta última. Em casos de urgência, poderão ser utilizados meios alternativos como aplicativos de *smartphones* ou até mesmo pelo *WhatsApp*.
- Periodicidade: Eventual ou sempre que necessário para a solução de problemas ou esclarecimento de dúvidas, de modo célere e tempestivo.
- As comunicações e acordos realizados pessoalmente em reuniões ou por meio de ligações telefônicas deverão ser formalizados, em até 24 horas, por escrito nos mesmos meios supracitados, pelo Preposto da CONTRATADA, ou seu representante e enviada aos participantes para validação e considerações.

3.1.6. **FORMA DE RECEBIMENTO E AVALIAÇÃO DA QUALIDADE:**

3.1.6.1. **Condição de Aceite:** Após aferição do atendimento das condições técnicas, serão emitidos os termos descritos nos itens 3.1.2.7 (provisório) e 3.1.2.8 (definitivo), referentes à Dinâmica de execução contratual, e seus subitens.

3.1.6.2. **METODOLOGIA DE AVALIAÇÃO DA QUALIDADE*:***

- Etapa / Fase / Item: Recebimento da solução.
- Método de Avaliação: Verificação da aderência aos requisitos técnicos discriminados no item 4.1, 4.2 e respectivos subitens deste Termo de Referência, bem como no **Anexo I** a este TR. O objeto entregue em desconformidade com o especificado neste Termo de Referência e na proposta comercial será rejeitado parcial ou totalmente, conforme o caso, obrigando-se a CONTRATADA a entregar novo objeto no prazo máximo de 5 (cinco) dias úteis, contados da data do recebimento da

notificação pela CONTRATANTE.

3.1.7. **<u>CONDIÇÕES PARA PAGAMENTO</u>:**

3.1.7.1. Etapa / Fase / Item: Início de execução dos serviços prestados pela solução.

3.1.7.2. Condição de Pagamento: O pagamento dos itens 1 e 2 de cada lote da tabela que integra o **item 2.6.1** deste TR, se dará cada um em parcela única, à medida que forem entregues e executados conforme será previsto no instrumento contratual e desde que atendidos os requisitos, prazos e condições estabelecidos para os mesmos neste TR.

3.1.7.3. Os serviços sob demanda (Operação Assistida), previstos no item 3 de cada lote da tabela que integra o **item 2.6.1** deste TR, serão pagos no mês posterior à prestação dos serviços, desde que atendidos os requisitos, prazos e condições estabelecidos para os mesmos neste TR.

3.1.7.4. O pagamento do item 4 de cada lote da tabela que integra o **item 2.6.1** deste TR, será realizado após a entrega definitiva e execução total do item, desde que cumpridas todas as exigências previstas neste Termo de Referência.

3.1.7.5. O pagamento em parcela única do item 1 de cada lote da tabela apresentada no **item 2.6.1**, se justifica pelos seguintes motivos:

3.1.7.5.1. **REDUÇÃO DE CUSTOS**

3.1.7.5.1.1. O pagamento em parcela única geralmente resulta em custos totais menores em comparação com o pagamento mensal. Isso ocorre porque as empresas licitantes podem obter descontos significativos com os fabricantes, uma vez que não precisam se preocupar com a administração de pagamentos mensais e os riscos associados à cobrança, como atraso nos pagamentos e possível incidência de juros ás licitantes, reduzindo a margem de lucro das mesmas, o que corrobora com a redução do preço final para a CONTRATANTE;

3.1.7.5.1.2. A não incidência de juros do financiamento da solução junto aos fabricantes das ferramentas (hardware e licenciamento/subscrição), ou mesmo junto aos bancos, que estaria embutido no preço mensal e final estimado da solução ofertada, é menor, ou até mesmo não existe quando há previsão de pagamento em parcela única, o que impacta sobre maneira na redução dos custos e valores finais estimados para a CONTRATANTE;

3.1.7.5.1.3. A variação dos preços dos componentes da solução ofertada que são baseadas em moeda Americana ($US – Dolar), também reduz os custos totais de contratos com pagamento em parcela única, frente aos contratos com pagamento parcelado mensal, pois sobre estes pode incidir variação, aumento no valor da moeda Americana, o que resultaria em um custo maior, e conseqüentemente um risco maior, o que impactaria no repasse desse custo ao valor do pagamento mensal e no valor final da solução, ao final do período de vigência contratual, e não havendo esta variação no valor da moeda Americana, não há repasse desse valor na estimativa de custos para a CONTRATANTE;

3.1.7.5.1.4. Todos os itens acima corroboram com a redução do preço final para a CONTRATANTE.

3.1.7.5.2. **AGILIDADE NA IMPLEMENTAÇÃO**

3.1.7.5.2.1. Em função do pagamento em parcela única, a empresa CONTRATADA poderá acelerar a implementação da solução, a mesma pode ocorrer de forma mais rápida e eficiente, o que beneficiaria a CONTRATANTE, com a entrega da solução operacional em um prazo menor;

3.1.7.5.2.2. Ganho no resultado e na proteção do ambiente com a implementação da solução de forma mais célere, antes do tempo previsto em contrato, resultando na redução de riscos relacionados e aproveitamento mais rápido dos benefícios advindos da solução contratada pela CONTRATANTE.

3.1.7.5.3. **REDUÇÃO NO ÔNUS ADMINISTRATIVO**

3.1.7.5.3.1. O pagamento em parcela única reduz a burocracia e a complexidade administrativa mensal para gestão do contrato pela equipe da CONTRATANTE;

3.1.7.5.3.2. Não há necessidade de validação mensal de entregas, que em contratos com pagamento mensal são necessárias, e se descumpridas condicionam o pagamento e impõe a aplicação de glosas, situação que exige da equipe de gestão do contrato grande esforço.

3.1.7.5.3.3. Em contrapartida, em contratos com pagamento

em parcela única, o ônus administrativo para equipe de gestão do contrato, é mínima, normalmente quando há necessidade de acionar o serviço de garantia e suporte previstos em contrato.

3.1.7.6. Além dos motivos elencados acima, o emprego de um modelo de parcela única em um contrato é proveniente da análise de circunstâncias, cenários e benefícios para sua adoção.

3.1.7.7. A Lei n. 8.666/1993, por exemplo, em seu art. 7º, § 2º, determina que serviços somente poderão ser licitados quando houver previsão de recursos orçamentários que assegurem o pagamento das obrigações decorrentes de obras ou serviços a serem executadas no exercício financeiro em curso, de acordo com o respectivo cronograma, e a previsão para pagamento em parcela única propicia isso.

3.1.7.8. O art. 15º, Incisos III e IV, também da Lei nº 8.666/1993, por exemplo reza que as compras deverão sempre que possível, submeter-se às condições de aquisição e pagamento semelhantes às do setor privado, se dividindo em tantas parcelas quantas necessárias para aproveitar as peculiaridades do mercado, visando economicidade. Como demonstrado nos itens acima, em função dos descontos dados pelos fabricantes, a redução dos juros e a pequena variação no preço da moeda Americana em aquisições com pagamento em parcela única, corroboram sobremaneira com a economicidade prevista nos incisos mencionados acima.

3.1.7.9. O princípio da economicidade é um dos princípios fundamentais que norteiam a administração pública. Ele estabelece que a gestão dos recursos públicos deve ser realizada de forma eficiente e econômica, visando à obtenção dos melhores resultados possíveis com o menor custo possível, e o pagamento em parcela única, frente ao pagamento mensal, demonstra a aplicação efetiva deste princípio.

3.1.7.10. A escolha pelo modelo de pagamento em parcela única aumenta muito o poder de negociação das licitantes junto aos fabricantes, afinal, a previsão de recebimento de forma única, concede a possibilidade de solicitar descontos mais agressivos e negociações com reduções maiores dos preços, o que resulta em uma oferta mais vantajosa para a Administração, para a CONTRATANTE.

3.1.7.11. Corrobora ainda com o a adoção de pagamento em parcela única o fato de que para soluções de Tecnologia da Informação esse modelo é uma praxe do mercado, e como exemplo podemos citar

contratações de soluções de Microsoft, como o pacote Microsoft 365, oferecido pelos parceiros da mesma, que são normalmente pagos em parcela única. Outros exemplos seriam as contratações conjuntas realizadas em 2022 pelos Tribunais Regionais Eleitorais, todas também foram realizadas dessa forma.

3.1.7.12. Conclui-se assim, que a adoção do modelo de pagamento me parcela única é administrativa e economicamente mais vantajosa para a CONTRATANTE.

3.1.8. **TRANSFERÊNCIA DE CONHECIMENTO:**

3.1.8.1. A transferência de conhecimento dar-se-á mediante a execução do Treinamento previsto no item 4.4 deste Termo de Referência.

3.1.8.2. A transferência de conhecimento para a equipe técnica do CONTRATANTE, também será realizada por meio de todos os novos serviços implantados ou modificados, mediante documentação técnica em repositório adotado pelo TRE-DF para esse fim.

3.1.9. **PROPRIEDADE, SIGILO E RESTRIÇÕES:**

3.1.9.1. Direito de Propriedade: Os direitos autorais e os direitos de propriedade intelectual gerados a partir da Solução de Tecnologia da Informação fornecida pela CONTRATADA, especificamente aqueles relacionados aos diversos artefatos e produtos produzidos ao longo do contrato, como a documentação, os modelos de dados e as bases de dados com seus respectivos dicionários de dados pertencerão ao TRE-DF e aos Tribunais partícipes, devendo ser justificado os casos em que isso não ocorrer, e deverão ser entregues à CONTRATANTE ao final do contrato.

3.1.9.2. Portanto caberá à CONTRATADA para viabilizar o entendimento dos dados que por ventura sejam entreguea á CONTRATANTE ao final do contrato, passar todas as informações necessárias, para que essa Inteligência com base nos dados e informações gerados ao longo do contrato, possam ser reaproveitados em contratos futuros.

3.1.9.3. No caso de haver fornecimento de base de dados conforme mencionado nos itens anteriores caberá ainda a CONTRATADA, entregar a base de dados em formato padrão utilizado pelo mercado.

3.1.9.4. Condição de Manutenção de Sigilo: A CONTRATADA obriga-se a manter o mais rigoroso sigilo sobre quaisquer dados, informações, documentos e especificações que a ela venham a ser confiados, ou que venha a ter acesso em razão da

contratação a ser efetivada, não podendo, sob qualquer pretexto, revelá-los, divulgá-los, reproduzi-los na sua totalidade ou em partes, ou deles dar conhecimento a quaisquer terceiros, sendo obrigatória a assinatura do Termo de confidencialidade – **Anexo IV** deste Termo de Referência.

3.1.10. **QUALIFICAÇÃO TÉCNICA/PROFISSIONAL:**

3.1.10.1. A CONTRATADA deverá apresentar após assinatura do contrato, no prazo de até 10 (dez) dias contados da publicação do extrato do Contrato no Diário Oficial da União, a documentação associada ao(s) profissional(is) envolvidos e certificações mínimas associadas à execução dos serviços.

3.1.10.2. A CONTRATADA deverá disponibilizar, para o suporte técnico da solução objeto deste Termo de Referência e do instrumento contratual, uma equipe com perfil técnico adequado e qualificado para a perfeita execução das atividades necessárias à operação, sustentação e manutenção da solução durante o período da validade/vigência contratual, sem qualquer custo a mais para o CONTRATANTE.

3.1.10.3. Para a comprovação da qualificação técnica necessária, dos profissionais que irão desempenhar os serviços previstos, como planejamento, instalação/implementação, operacionalização e suporte, a CONTRATADA, deverá apresentar minimamente, mas não limitado: Comprovação de experiência de pelo menos 05 anos em Gestão de Cibersegurança/Segurança da Informação, ou certificação em Cibersegurança/Segurança da informação emitida por instituições renomadas na área, como ISO, Exin, Sans, CompTIA, NIST,ECCOUNCIL,ISACA, ISC2, entre outras.

3.1.10.4. Caso a CONTRATADA não tenha em seu quadro o profissional com o perfil e experiências aqui especificadas, a mesma terá o prazo de até 60 dias corridos, para apresentar a documentação que comprove o atendimento das condições estabelecidas para a qualificação técnica.

3.1.10.4.1. Caso a CONTRATADA não atenda ao prazo estabelecido no **item 3.1.10.1**, o CONTRATANTE terá autonomia para solicitar a troca do profissional indicado a qualquer tempo. O TRE-DF não autorizará o início dos serviços enquanto não for apresentado técnico/analista, que cumpra as exigências definidas no **item 3.1.10** e seus subitens.

3.1.10.5. As certificações profissionais serão verificadas/aferidas no início dos serviços pela equipe de fiscalização do Contrato.

3.1.10.6. Em caso de descumprimento das obrigações citadas no item 3.1.10 e respectivos subitens, aplicar-se-á o previsto no item 3.1.11 deste TR.

3.1.11. **DESCUMPRIMENTO DAS OBRIGAÇÕES CONTRATUAIS:**

3.1.11.1. As sanções aplicáveis são as estabelecidas no instrumento contratual, com observância da legislação que rege a matéria e demais definidas conforme item 3.1.4.3.6.

4. REQUISITOS TÉCNICOS ESPECÍFICOS:

4.1. **ITEM 01 - 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 ÚNICA - CARACTERÍSTICAS TÉCNICAS**

4.1.1. 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. As características técnicas da solução estão dispostas no **Anexo I** deste Termo de Referência.

4.1.2. A solução (hardware, software e serviço) entregue, a ser fornecida deverá ter acompanhamento e monitoramento presencial ou remoto (não presencial) pela equipe da CONTRATADA durante toda e vigência contratual, (24 meses), visando atender, operar e solucionar todos os incidentes detectados, que possam causar dano, indisponibilizar serviços e risco às informações, à imagem e aos serviços da CONTRATANTE durante esse período.

4.1.3. O início da prestação do serviço mencionado no item 4.1.2 ocorrerá no dia útil posterior à emissão e assinatura do **Termo de Recebimento Definitivo (TRD)** da instalação e operacionalização de toda a solução pela CONTRATANTE.

4.1.4. A CONTRATADA deverá apoiar o início das atividades técnicas da nova solução, garantindo apoio imediato e acesso rápido às soluções para alterar ou aplicar configurações necessárias ao ajuste, caso necessário, do ambiente de produção.

4.1.5. A CONTRATADA deverá manter à disposição da CONTRATANTE, durante a vigência contratual, pessoal técnico especializado e qualificado para o acompanhamento e verificação do desempenho operacional da solução, eliminando de imediato eventuais falhas detectadas na mesma.

4.1.6. A equipe técnica da CONTRATADA, a qual será responsável pela prestação dos serviços, deverá possuir certificação e/ou ter experiência mínima, conforme condições estabelecidas no **item 3.1.10** e respectivos subitens deste Termo de Referência.

4.1.7. A equipe da CONTRATADA deverá monitorar o ambiente da

CONTRATANTE 24x7x365 (vinte e quatro horas por dia, durante os sete dias da semana e nos doze meses do ano), durante o período de vigência da contratação, informando a equipe técnica do Tribunal sobre qualquer ocorrência que necessite de atuação, a fim de salvaguardar os serviços, sistemas e aplicações do Tribunal.

4.1.8. A contratada deverá propor e tomar todas as ações necessárias para a prevenção contra repetição de falhas que ocorrerem durante o período de execução dos serviços e soluções implementadas e relacionadas à este item 4 (Requisitos Técnicos Específicos).

4.1.9. A CONTRATADA deverá realizar os ajustes, configurações, parametrizações, análises e demais serviços que compreendem a monitoração e fazem parte da solução implementada.

4.1.10. A CONTRATADA deverá realizar todas as ações e procedimentos necessários para o perfeito funcionamento da solução, visando assegurar a disponibilidade e desempenho do ambiente, sempre que demandada, ou de forma voluntária, preventiva durante o período de vigência contratual.

4.2. **ITEM 02 – INSTALAÇÃO/ATIVAÇÃO DA SOLUÇÃO.**

4.2.1. Os serviços de instalação física e lógica serão executados pela CONTRATADA e deverão ser estruturados conforme as fases a seguir.

4.2.1.1. **Fase de Planejamento**

4.2.1.1.1. A CONTRATADA deverá elaborar plano de projeto da implementação/instalação seguindo minimamente, mas não restrita às mesmas, as seguintes etapas;

4.2.1.1.1.1. Definir escopo do projeto;

4.2.1.1.1.2. Validar objetivos e premissas do projeto;

4.2.1.1.1.3. Definir e analisar riscos e restrições do projeto;

4.2.1.1.1.4. Identificar e validar os requisitos do projeto;

4.2.1.1.1.5. Efetuar o levantamento de informações sobre o ambiente atual, em complementação ao conjunto de informações apresentado nesta especificação técnica;

4.2.1.1.1.6. Definir as pessoas envolvidas por parte da CONTRATANTE no projeto;

4.2.1.1.1.7. Reunir as equipes da CONTRATADA e CONTRATANTE;

4.2.1.1.1.8. Definir os parâmetros de configuração básicos e avançados a serem implementados;

4.2.1.1.1.9. Apresentar para análise e aprovação da CONTRATANTE, a arquitetura prevista para implementação da solução;

4.2.1.1.1.10. Apresentação do cronograma do projeto com os prazos e responsabilidades;

4.2.1.1.1.11. Verificar os pré-requisitos do projeto e validar

com a CONTRATANTE;

4.2.1.1.1.12. Apresentar plano do projeto para a homologação por parte da CONTRATANTE.

4.2.1.2. **Fase de Execução**

4.2.1.2.1. O serviço de instalação consiste na colocação do(s) equipamento(s) previstos em pleno funcionamento, em conformidade com o disposto nesta especificação técnica, no Edital e seus Anexos e em perfeitas condições de operação, de forma integrada ao ambiente da CONTRATANTE, bem como instalar, configurar e parametrizar os serviços (softwares) previstos na solução, e estes devem contemplar, no mínimo, o seguinte:

4.2.1.2.1.1. Deverão ser realizados por conta da CONTRATADA o armazenamento, a embalagem, o transporte, a entrega e a instalação de todo e qualquer item do objeto deste TR, de tal maneira que a CONTRATADA será responsável pela remessa dos equipamentos para o(s) endereços informados no **Anexo IX**, locais esses onde a solução de segurança será efetivamente implantada;

4.2.1.2.1.2. A CONTRATADA deverá efetuar instalação e configuração de toda a solução (hardware, software (licenças, subscrições e demais serviços ofertados) de acordo com as recomendações do fabricante;

4.2.1.2.1.3. A CONTRATADA deverá efetuar a instalação da solução na infraestrutura indicada pelo CONTRATANTE, onde a configuração realizada deverá estar em conformidade com as recomendações do fabricante, e precisarão atender às necessidades dos serviços que serão prestados pela solução, devendo minimamente atender aos seguintes requisitos:

a. Conexão e configuração de todos os equipamentos e/ou demais componentes da solução (softwares) no ambiente do CONTRATANTE;

b. Atualização de softwares, firmwares e drivers que compõem a solução;

c. Fornecer quando for o caso, todos os equipamentos, componentes, acessórios e cabos de conexão para interligar física e lógicamente todos os componentes da solução entregue;

d. Aplicação das licenças e ou subscrições necessárias ao funcionamento da solução entregue;

e. Realizar testes da solução, incluindo testes de *failover*;

f. Documentação do ambiente configurado e instalado (*AS BUILT*).

4.2.2. Os serviços de instalação e configuração deverão se basear nas melhores práticas estabelecidas pelo respectivo fabricante em seus manuais de instalação e configuração ou artigos técnicos.

4.2.3. A solução deverá ser entregue com todas as funcionalidades, recursos, componentes, acessórios, softwares e licenciamentos necessários ao seu pleno funcionamento.

4.2.4. Todas as informações da infraestrutura interna da rede do Tribunal, que forem necessárias à implantação da solução, serão fornecidas pelo CONTRATANTE á CONTRATADA.

4.2.5. A instalação da solução, incluindo o fornecimento de todos os componentes e acessórios necessários para o pleno funcionamento da solução, serão fornecidos e será realizada pela CONTRATADA, com acompanhamento de uma equipe destacada pela CONTRATANTE.

4.2.6. A CONTRATADA deverá providenciar um profissional com a expertise e conhecimento, conforme critérios estabelecidos no item 3.1.10 e respectivos subitens, para garantir a conformidade da instalação e a configuração dos equipamentos e softwares que compõem a solução.

4.2.7. A instalação, configuração e testes do equipamento deverão ser realizados com o acompanhamento de técnicos/analistas da CONTRATANTE, visando o repasse de conhecimento, e durante esse procedimento, deverão ser observados os padrões de gerenciamento de credenciais e acessos, de manutenção e de segurança do CONTRATANTE.

4.2.8. A critério do CONTRATANTE, os serviços poderão ser executados fora do horário comercial e/ou em finais de semana ou feriados sem custo adicional para o mesmo, visando minimizar os transtornos aos usuários devido a uma eventual indisponibilidade dos serviços. Por conseguinte, as atividades que não tenham impacto de indisponibilidade ou que não venham a requerer a parada dos equipamentos e/ou serviços internos, poderão ser executadas em horário comercial.

4.2.9. Para as atividades que tenham impacto de disponibilidade ou que venham a requerer a parada de equipamentos e/ou serviços, estes deverão ser executadas fora do horário de expediente, inclusive em feriados ou finais de semana, de acordo com o estabelecido entre a CONTRATADA e o CONTRATANTE.

4.2.10. O serviço de implantação/instalação da solução deverá ser concluído no prazo máximo de 15(quinze) dias úteis, após a entrega da solução pela CONTRATADA.

4.2.11. Para todos os efeitos, a conclusão dos serviços de instalação e configuração será atestada pela entrega do sistema em pleno funcionamento, incluindo a documentação "*As Built*", contendo planejamento, relatório de instalação, configuração adotada, testes realizados e seus resultados, de acordo com as especificações do(s)

fabricante(s) e demais condições, requisitos e especificações estabelecidas neste TR.

4.2.12. A CONTRATADA iniciará a instalação e ativação da solução nas dependências do Tribunal após a entrega da solução, observado o prazo estabelecido no item 3.1.2.5 (60 dias corridos);

4.2.13. A CONTRATADA deverá apresentar em até 10 dias corridos, após a emissão da Ordem de Serviço, o Plano de Projeto/Instalação, para análise e validação da CONTRATANTE, que terá 05 dias corridos, para entregar suas considerações e ajustes ao Plano, para que a CONTRATADA por sua vez, em até 03 dias corridos, faça todos os ajustes necessários e o mesmo, possa ser aprovado para iniciar a implementação.

4.2.14. Caberá à CONTRATADA apresentar todas as demais documentações técnicas detalhadas contendo todas as informações referentes a ativação e a configuração da solução.

4.2.14.1. O Plano de Instalação, bem como a documentação técnica detalhada deverão contemplar os números de registro (ou informações similares - part numbers por exemplo) que possam identificar todos os recursos tecnológicos utilizados na ativação e configuração da solução.

4.2.15. O serviço de Ativação da Solução contempla a configuração dos itens de hardware e software fornecidos pela CONTRATADA e será considerada como ativada quando for possível verificar os primeiros registros de monitoramento da rede do Tribunal.

4.2.16. A CONTRATANTE dará o aceite definitivo da Ativação da Solução no prazo de até 10 (dez) dias corridos após a emissão do Termo de Recebimento Provisório e cumprimento das obrigações previstas nos itens 3.1.2.8, 4.2.11 e 4.2.13.

4.3. **ITEM 03 – OPERAÇÃO ASSISTIDA**

4.3.1. A CONTRATADA deverá prover o serviço de Operação Assistida, com atendimento remoto para solução.

4.3.2. **O serviço de Operação Assistida consiste:**

4.3.2.1. No fornecimento de informações e esclarecimentos solicitados pela CONTRATANTE;

4.3.2.2. Em intervenções técnicas para solução de incidentes e problemas que estejam impactando a solução;

4.3.2.3. Em orientações técnicas sobre melhores práticas para uso da solução;

4.3.2.4. Em intervenções técnicas para parametrização e configuração da solução.

4.3.3. O início da Operação Assistida ocorrerá no dia útil posterior à emissão e assinatura do **Termo de Recebimento Definitivo (TRD)** da

solução pela CONTRATANTE.

4.3.4. O serviço de Operação Assistida não pode ser confundido com os serviços de suporte/garantia e manutenção, já contemplados na solução.

4.3.5. A CONTRATANTE deverá utilizar Ordens de Serviço - OS, conforme modelo definido no **Anexo VII** deste TR, para solicitar quando necessário os serviços específicos de Operação Assistida, utilizando para tal, o catálogo de serviços definido no **Anexo VIII,** também deste TR.

4.3.6. Aplica-se aqui também os mesmos parâmetros de qualidade definidos no **item 4.1.10.1**, para os entregáveis previstos no **Anexo VIII** quando demandados pela CONTRATANTE.

4.3.7. O dimensionamento da quantidade de horas estimadas para este item foi baseada em outros contratos com serviços similares, relacionados, pois não tínhamos base de cálculo interna, por se tratar de contratação nova, de serviço ainda não previsto por este Tribunal. As estimativas de horas previstas no **Anexo VIII**, referente ao catálogo de serviço de Operação Assistida foram definidas pela complexidade estimada prevista para a realização de cada uma das atividades e entregas descritas no mesmo.

4.3.8. Ao final de cada Ordem de Serviço - OS entregue e devidamente aprovada pela CONTRATANTE, será emitido o Termo de Recebimento Definitivo – TRD em até 05 dias corridos, o qual será requisito para a realização do pagamento da OS relacionada.

4.4. **ITEM 04 - TREINAMENTO**

4.4.1. Deverá ser fornecido treinamento com carga horária mínima de 40 horas, abarcando todo o conteúdo necessário para a perfeita compreensão e operação de todos os componentes e requisitos da solução ofertada pela CONTRATADA.

4.4.2. O treinamento deverá ser fornecido em turma sempre que possível, e nestas mais de um Tribunal poderá ser envolvido, desde que haja alinhamento na disponibilidade de horário dos alunos participantes.

4.4.2.1. Caso não seja possível o alinhamento de horário dos alunos participantes, os treinamentos deverão ocorrer em separado por cada Tribunal.

4.4.3. O início do treinamento ocorrerá em até 10 (dez) dias úteis do recebimento do pedido de realização do treinamento emitido pela CONTRATANTE, à CONTRATADA.

4.4.4. Sua prestação deverá ser realizada na forma remota, de forma virtual (pela internet), ficando a CONTRATADA, responsável pela produção e fornecimento de todo material didático e demais informações necessárias para o acesso seguro (uso de https) ao treinamento para todos os treinandos.

4.4.5. Ao final do treinamento, a CONTRATADA deverá fornecer um

certificado de conclusão aos servidores efetivos participantes, contendo as seguintes informações mínimas: nome do curso, nome do participante, carga horária total e ementa resumida do treinamento.

4.4.6. Ao final do treinamento a CONTRATADA deverá aplicar o Formulário de Avaliação, conforme modelo constante no **Anexo II** deste Termo de Referência.

4.4.6.1. No questionário, será utilizada escala de até 5 (cinco) pontos para cada quesito.

4.4.6.2. Para fins de entendimento, a escala deverá representar os seguintes conceitos:

4.4.6.2.1. 1 (um) - Discordo totalmente

4.4.6.2.2. 2 (dois) - Discordo Parcialmente

4.4.6.2.3. 3 (três) – Concordo

4.4.6.2.4. 4 (quatro) – Concordo Parcialmente

4.4.6.2.5. 5 (cinco) – Concordo Totalmente

4.4.6.3. No mínimo 70% dos participantes deverão atribuir grau igual ou superior a 3 (três), para o item avaliado ser considerado proveitoso.

4.4.6.4. O resultado positivo da Avaliação será utilizado como critério de aceite do treinamento, devendo ser considerado pela amostra de participantes como “proveitoso” para no mínimo 70% (setenta por cento) dos itens avaliados.

4.4.6.5. Caso o resultado da Avaliação de Instrutor seja considerado “não proveitoso”, o treinamento fornecido será considerado não aceito.

4.4.6.5.1. Na hipótese de não aceitação, a CONTRATADA deverá oferecer outro treinamento, com a mesma carga horária, com outro instrutor, sem qualquer ônus para os Tribunais participantes.

4.4.6.5.2. O novo treinamento deverá ser realizado no prazo de 30 (trinta) dias corridos, contados da não aceitação do curso anterior, considerando-se os critérios previamente estabelecidos.

4.4.7. Ao final do treinamento estando cumpridas todas as condições estabelecidas no item 4.4.6 e respectivos subitens, será emitido o Termo de Recebimento Definitivo – TRD pela CONTRATANTE em até 05 dias corridos, o qual será requisito para a realização do pagamento.

5. GARANTIA DE EXECUÇÃO DO CONTRATO:

5.1. Será obrigatória à CONTRATADA a apresentação de garantia no percentual de 5% (cinco por cento) do valor total do contrato, nos termos do artigo 56 da Lei nº 8.666/93, com validade durante toda a vigência, de acordo com as regras fixadas no instrumento contratual.

6. DOTAÇÃO ORÇAMENTÁRIA:

6.1. A demanda se classifica na Ação 21EE: Plano Orçamentário SEG0 - Segurança da Informação, na natureza de despesa 3390.40 - Serviços de Tecnologia da Informação e Comunicação - PJ, no subitem 21 – Serviços Técnicos Profissionais de TIC.

6.2. Conforme informação da SEPEO/CORF no Despacho SEI 1100347, há disponibilidade orçamentária para fazer face à contratação no valor estimado de R$ 3.684.925,60, nos termos do item 3 do DOD (SEI 1419529).

6.3. Ainda no mesmo Despacho a SEPEO/CORF, detalha o saldo disponível para execução na Ação 21EE:

Ação: Plano Orçamentário	GND	Valor Descentralizado pelo TSE (R$)	Valor Disponível para Execução (R$)
Ação 21EE: PO SEG0 - Segurança da Informação	3	3.828.925,60	3.698.325,60
Ação 21EE: PO SEG0 - Segurança da Informação	4	2.112.221,76	2.112.221,76

7. VIGÊNCIA DO CONTRATO E CRITÉRIOS PARA PRORROGAÇÃO SE FOR O CASO:

7.1. O contrato vigerá pelo prazo de 24 (vinte e quatro) meses, pois o custo para inserção da empresa nos órgãos participantes da Ata de Registro de Preços é alto, de modo que em um período menor, tem-se o risco de não haver prorrogação, pois esta não tem o direito subjetivo à mesma, o que tenderia ao aumento nos preços ofertados.

7.2. O início do período de garantia e suporte iniciará a partir da emissão do Termo de Recebimento Definitivo - TRD, e poderá ser prorrogado até o limite de 48 (quarenta e oito) meses, nos termos do inciso IV do artigo 57 da Lei nº 8.666/1993, desde que haja autorização formal da autoridade competente e observados os seguintes requisitos:

7.2.1. Os serviços foram prestados regularmente;

7.2.2. A Administração tem interesse na continuidade da realização do serviço;

7.2.3. A contratada manifestou expressamente interesse na prorrogação.

7.3. Somente o item 1 previsto em todos os lotes poderá ser prorrogado conforme definido no item 7.2.

7.4. A Contratada não tem direito subjetivo à prorrogação contratual.

8. EQUIPE DE FISCALIZAÇÃO:

- Gestor Titular: José Fernando Valim Batelli, Técnico Judiciário, 0538,

SESOP/COIE/STIC.

- Gestor Substituto: Anderson de Souza Meneses, Técnico Judiciário, 1589, SESOP/COIE/STIC.

9. INFORMAÇÕES GERAIS E FINAIS:

9.1. As partes não estão eximidas do cumprimento de obrigações e responsabilidades previstas na legislação vigente e não expressas neste Termo de Referência.

9.2. De acordo com a RESOLUÇÃO N.º 07, DE 18 DE OUTUBRO DE 2005, do Conselho Nacional de Justiça (CNJ), ficam as PROPONENTES cientificadas de que é vedada a contratação de pessoa jurídica que tenha em seu quadro societário cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade até o terceiro grau, inclusive, dos magistrados ocupantes de cargos de direção ou no exercício de funções administrativas, assim como de servidores ocupantes de cargos de direção, chefia e assessoramento, vinculados direta ou indiretamente às unidades situadas na linha hierárquica da área encarregada da licitação.

10. MODELOS (TEMPLATES):

Segue proposta de modelos (templates) a serem utilizados na contratação:

10.1. Especificações Técnicas da Solução: Anexo I
10.2. Avaliação de Treinamento: Anexo II
10.3. Proposta Comercial: Anexo III.
10.4. Termo de confidencialidade: Anexo IV.
10.5. Termo de Vistoria ou Ciência: Anexo V.
10.6. Relação de Entregáveis: Anexo VI.
10.7. Modelo de Ordem de Serviço – OS: Anexo VII.
10.8. Catálogo de Serviço da Operação Assistida: Anexo VIII.
10.9. Relação de Tribunais Participantes da ARP: Anexo IX.
10.10. Definição dos Tipos de Perfil por Tribunal participante – Anexo X.

A Equipe de Planejamento da Contratação, composta pelos Integrantes Demandante, Técnico e Administrativo, abaixo elencados, assina e data este documento eletronicamente:

Equipe de Planejamento da Contratação		
Integrante Demandante	**Integrante Técnico**	**Integrante Administrativo**
João Paulo Carneiro Rodrigues **Analista Judiciário - 2103**	**Marcelo Nogueira Lino** **Técnico Judiciário - 2409**	**José Fernando Valim Batelli** **Técnico Judiciário - 0538**

O **Gestor da Área Demandante** aprova este documento, **assinando-o e datando-o eletronicamente**:

Brasília (DF), 04 de setembro de 2023.

João Paulo Carneiro Rodrigues
Analista Judiciário - COIE

ANEXO I AO TERMO DE REFERÊNCIA –
PREGÃO ELETRÔNICO N.º xx/xxxx
- ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO–
PA SEI - Nº 0005153-57.2023.6.07.8100

1. CARACTERÍSTICAS GERAIS DA SOLUÇÃO

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.

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.

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;

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:

- **1.4.1.** Machine learning não supervisionado
- **1.4.2.** Machine learning supervisionado
- **1.4.3.** Deep Learning
- **1.4.4.** Redes Neurais

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-DF.

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

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.

1.8. Não serão aceitos produtos ou serviços OpenSource.

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

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

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-DF para o funcionamento da solução.

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.

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

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.

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

- **1.15.1.** Amazon AWS;
- **1.15.2.** Microsoft Azure;
- **1.15.3.** Google G-Suite;
- **1.15.4.** Office 365/Microsoft 365;
- **1.15.5.** Dropbox enterprise;
- **1.15.6.** Componentes virtuais (máquinas virtuais);
- **1.15.7.** Endpoint para Sistemas Operacionais;
- **1.15.8.** Docker e Kubernet.

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

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

1.18. Deverá possuir integração através de feeds com a ferramenta de análise interna.
1.19. Deverá ter capacidade de direcionar as pesquisas por ameaças cibernéticas levando em consideração os ativos críticos do TRE-DF, outros segmentos do mercado, localização e ameaças direcionadas.
1.20. Deve possuir características para enfatizar as ameaças urgentes e priorizá-las automaticamente.
1.21. Deve permitir que os usuários criem alertas dedicados com base em parâmetros definidos.
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.
1.23. A solução deve permitir que os usuários realizem consultas ad-hoc ilimitadas para uma ou mais de suas fontes de dados.
1.24. A solução deve disponibilizar, permitir o monitoramento e coleta 24 horas por dia e 7 dias por semana dos fóruns fechados da Deep e Dark Web.
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;
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:
  1.26.1. Prevenção de Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ);
  1.26.2. Gerenciamento de Crises Cibernéticas do Poder Judiciário (PGCRC-PJ);
  1.26.3. Investigação de Ilícitos Cibernéticos do Poder Judiciário (PIILC-PJ).
1.27. Possuir acesso no mínimo às seguintes redes anônimas; Darknet e Zeronet.
1.28. A coleta de dados para análise de ameaças deverá ser realizada diariamente.
1.29. A solução deverá permitir habilitar sua integração com vários produtos de inteligência do(s) fabricante(s).
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.
1.31. A solução não deve depender de assinaturas predefinidas para respostas.
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.
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.
1.34. A solução deverá oferecer *features* de respostas proativas contra ameaças, sem interromper as atividades do Tribunal.
1.35. Possuir funcionalidade de bloquear as ameaças de forma proativa.
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.
1.37. Solução deverá possuir capacidade de bloquear downloads de arquivos maliciosos de fontes não confiáveis.
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.
1.39. A solução deverá possuir uma lista, na ferramenta de gestão, para escolha dos firewalls que poderão ser instruídos quanto aos ataques cibernéticos.
1.40. A solução deverá, de forma automática, bloquear apenas a porta daquele dispositivo que está comprometido.
1.41. A solução deverá ser habilitada no console de uso de todas as outras ferramentas do(s) fabricante(s).
1.42. A solução deverá funcionar 24h x 7d x 365 dias do ano.
1.43. Possuir mecanismos de proteção para usuários Vips.
1.44. A solução não deve trabalhar com defesas pré-programadas.
1.45. A solução deverá reconhecer um ataque mesmo que não tenha sido identificado ou definido pelos padrões e frameworks em uso pelo mercado.
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).

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.

1.48. A solução deverá possuir capacidade de uso em aplicativos moveis.

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

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.

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.

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

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.

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 *DarkWe*b sobre essa 'expressão'", o Tribunal pode executar uma consulta a uma fonte específica como fórum particular de hackers russos.

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.

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.

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.

1.57. A solução dever 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.

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*.

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

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

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.

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.

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.

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.

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.

2. CARACTERÍSTICAS TÉCNICAS DA SOLUÇÃO

2.1. A solução deve 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:
- **2.1.1.** Classificação do tipo de dispositivo (desktop, servidor, Impressora, câmera, iot, etc);
- **2.1.2.** IP do dispositivo;
- **2.1.3.** Mac Address ;
- **2.1.4.** Nome DNS do dispositivo;
- **2.1.5.** Primeira vez que o dispositivo/IP foi visto na rede ;
- **2.1.6.** Última vez que o dispositivo foi visto na rede;
- **2.1.7.** Deve ser possível visualizar o histórico de IPs de um determinado dispositivo baseado no IP provido pelo servidor DHCP.

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.

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.

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

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.

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.

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

2.8. A solução deve ser comprovadamente baseada em análise de comportamento permitindo a detecção de, no mínimo, as seguintes anomalias:
- **2.8.1.** Dispositivo realizando conexões para destinos raros na internet não freqüentemente visitados por dispositivos da rede interna.
- **2.8.2.** Dispositivo se comunicando com um servidor externo usando um certificado auto assinado.
- **2.8.3.** Dispositivo se comunicando com um servidor usando um certificado expirado.
- **2.8.4.** Dispositivo se comunicando com um dispositivo externo usando um certificado inválido.
- **2.8.5.** Dispositivo iniciando várias conexões para um IP externo raro de maneira regular. (Beaconing)
- **2.8.6.** Dispositivo gerando um grande número de solicitações para servidores Web internos o qual está retornando códigos de erro HTTP.
- **2.8.7.** Novo dispositivo entrou na rede e começou a utilizar o software de teste de penetração ou escaneamento de rede.
- **2.8.8.** Vários dispositivos internos começaram a desviar de suas atividades normais e escanearam a rede interna.
- **2.8.9.** Dispositivo fazendo requisições de DNS repetidas recebendo respostas com registro TXT. (Tunelamento via DNS).
- **2.8.10.** Dispositivo se comunicando externamente via DNS de maneira consistente com o tunelamento de DNS.
- **2.8.11.** Dispositivo fazendo conexões criptografadas para um domínio relacionado a DNS Dinâmico.
- **2.8.12.** Dispositivo gerando um volume anormalmente alto de solicitações DNS.
- **2.8.13.** Dispositivo fazendo uma série de conexões utilizando Hostnames raros que parecem não ter uma resolução de DNS legítima.
- **2.8.14.** Um servidor DNS interno está agindo como um resolvedor de DNS aberto (OpenDns).
- **2.8.15.** Dispositivo se comunicando com o serviço de anonimização da rede TOR.
- **2.8.16.** Dispositivo se comunicando com a rede Tor por meio de um Web Service intermediário.
- **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.
- **2.8.18.** Dispositivo executando comandos PsExec em uma máquina remota que nunca havia recebido tráfego similar anteriormente.
- **2.8.19.** Dispositivo se conectando repetidamente a destinos externos que não possuem nomes legíveis para humanos.
- **2.8.20.** Dispositivo detectado conectando-se a hostnames identificados como trojans financeiros.
- **2.8.21.** Dispositivo fazendo conexões com hostnames raros associados a uma botnet.
- **2.8.22.** Dispositivo solicitando um domínio conhecido por hospedar malwares.
- **2.8.23.** Dispositivo gravando arquivos com nomes suspeitos, relacionado a ransomware, em Servidores de arquivos da rede SMB.

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.
2.8.25. Dispositivo fazendo download de dados de um sistema interno e fazendo upload de volumes de dados semelhantes para destino externo.
2.8.26. Dispositivo se comunicando com domínios suspeitos na internet e, ao mesmo tempo, realizando comportamentos incomuns de SMB na rede interna.
2.8.27. Dispositivo acessando uma grande quantidade de compartilhamentos SMB que não foram acessados anteriormente pelo mesmo dispositivo.
2.8.28. Dispositivo enviando um grande volume de dados para um IP externo que raramente é utilizado por qualquer dispositivo na rede interna.
2.8.29. Dispositivo fazendo conexões web externas sem usar um proxy web.
2.8.30. Dispositivo sendo bloqueado repetidamente por um proxy web durante um período de várias horas.
2.8.31. Dispositivo solicitando informações de configuração de proxy (WPAD) para um IP externo.
2.8.32. Dispositivo fazendo conexões HTTP suspeitas, de forma repetitiva, diretamente para um endereço IP sem utilizar um Hostname.
2.8.33. Dispositivo foi redirecionado para um Hostname HTTP raro e em seguida baixou um executável ou outro arquivo binário.
2.8.34. Dispositivo causando repetidos picos de conexões HTTP ou SSL na rede interna ou para a internet.
2.8.35. Dispositivo fazendo requisições HTTP suspeitas repetidamente em portas não padrão.
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.
2.8.37. Dispositivo fazendo download de arquivo executável vindo de uma fonte a qual não é comumente acessada por dispositivos da rede interna.
2.8.38. Dispositivo fazendo download de arquivo comprimido vindo de uma fonte a qual não é comumente acessada por dispositivos da rede interna.
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.
2.8.40. Dispositivo usando uma plataforma externa de armazenamento de arquivos de terceiros.
2.8.41. Dispositivo enviando dados para o Pastebin.
2.8.42. Dispositivo usando um sistema terceiro de mensageria (Whatsapp ou similares).
2.8.43. Dispositivo acessando rede social (Facebook ou similares).
2.8.44. Dispositivo se comunicando com um destino raro na internet usando portas normalmente usadas apenas na rede interna.
2.8.45. Dispositivo fazendo conexões peer-to-peer BitTorrent.
2.8.46. Dispositivo recebeu um número anormalmente grande de conexões de entrada de IP externos raros.
2.8.47. Dispositivo fazendo conexões SQL para IPs externos a rede.
2.8.48. Dispositivo enviando uma quantidade anormal alta de dados para destinos fora da rede.
2.8.49. Dispositivo trocando um volume de dados anormal com outro dispositivo na rede interna.
2.8.50. Dispositivo enviando uma quantidade anormalmente alta de dados externamente para um local para o qual a rede não enviou dados anteriormente.
2.8.51. Dispositivo explorando vulnerabilidade Heartbleed na rede interna.
2.8.52. Dispositivo se conectando a um DNS SinkHole conhecido.
2.8.53. Dispositivo realizando grandes volumes de pequenas conexões SSH e/ou RDP.
2.8.54. Dispositivo iniciando um grande número de conexões para um servidor RDP e/ou SSH.
2.8.55. Dispositivo recebendo um grande número de conexões RDP de entrada de IPs externos raros.
2.8.56. Alteração no comportamento de tráfego DHCP.
2.8.57. Novo servidor DNS na rede.
2.8.58. Novo servidor de proxy web na rede.
2.8.59. Uma senha de credencial de alto privilégio foi alterada no domínio Windows.
2.8.60. Uma credencial efetuando login de uma origem incomum.
2.8.61. Uma credencial foi usada em múltiplos dispositivos internos.
2.8.62. Um dispositivo gerou um grande número de falhas de sessão SMB.
2.8.63. Um dispositivo desviou de suas atividades normais criando várias falhas de login Kerberos.

2.9. Deve ser possível criar regras utilizando um ou mais dos componentes do item acima.
2.10. Todos os dados processados pela solução devem ser armazenados para posterior análise independentemente de terem gerado alertas ou não.
2.11. A solução deve possuir mecanismos para exportar os dados armazenados no padrão de extensão ‘.pcap’.

2.12. Deve ser capaz de agrupar de forma autônoma dispositivos em grupos baseado em sua similaridade de comportamento.
2.13. Deve ser capaz de tomar ações baseadas em desvio de comportamento.
2.14. Deve possuir a capacidade de quarentenar ou semi-quarentenar temporariamente dispositivos na rede.
2.15. Deve possuir a habilidade para responder e/ou parar ameaças autonomamente.
2.16. Deve ser capaz de marcar dispositivos automaticamente para decisões de resposta e ajuste fino.
2.17. Deve ser altamente configurável permitindo vários níveis de resposta a uma anomalia na rede.
2.18. Deve se capaz de registrar todas as ações de resposta para propósitos de auditoria.
2.19. Deve ser configurável para supervisão e aprovação de analistas em ações de tomada de decisão / resposta.
2.20. Capacidade de personalizar a sua busca por ameaças cibernéticas.
2.21. Deverá possuir integração através de feeds com a ferramenta de análise interno.
2.22. Capacidade de direcionar as pesquisas por ameaças cibernéticas levando em consideração ativos críticos do TRE-DF, outros segmentos do mercado, localização e ameaças direcionadas.
2.23. Possuir funcionalidade de personalização dos usuários, para acesso fácil as ameaças ao TRE-DF.
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.
2.25. Possuir características para enfatizar as ameaças urgentes e priorizá-las automaticamente.
2.26. Permitir que os usuários criem alertas dedicados com base em parâmetros definidos.
2.27. Oferecer análise constante de fluxo de inteligência acionável, baseada em contexto e que possa alertar os usuários sobre atividades cibernéticas suspeitas.
2.28. Oferecer cruzamento automático das descobertas de ameaças com um repositório de inteligência final e histórico para aumentar a consciência situacional da organização.
2.29. Permitir que os usuários possam gerenciar os incidentes.
2.30. A solução deverá disponibilizar um conjunto pré-configurado de filtros estatísticos dedicados ao campo de inteligência de ameaças.
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.
2.32. A solução de inteligência cibernética, deverá possuir recursos necessários para compreensão de ameaças em mais de 20 idiomas, incluindo:
  2.32.1. Russo;
  2.32.2. Chinês;
  2.32.3. Farsi;
  2.32.4. Árabe;
  2.32.5. Idiomas europeus;
  2.32.6. Inglês;
  2.32.7. Hebraico.
2.33. Disponibilizar monitoramento e coleta 24 horas por dia e 7 dias por semana dos fóruns fechados da Deep e Dark Web.
2.34. Disponibilizar monitoramento e coletas 24 horas por dia e 7 dias por semana dos marketplaces fraudulentos.
2.35. Permitir acesso a possíveis dados do TRE-DF 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).
2.36. Possuir domínios de especialização, incluindo minimamente, crimes financeiros, hacktivismo e ciberterrorismo.
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:
  2.37.1. Prevenção de Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ);
  2.37.2. Gerenciamento de Crises Cibernéticas do Poder Judiciário (PGCRC-PJ);
  2.37.3. Investigação de Ilícitos Cibernéticos do Poder Judiciário (PIILC-PJ).
2.38. Possuir acesso as seguintes redes anônimas; Darknet e Zeronet.
2.39. A coleta de dados para análise de ameaças deverá ser realizada diariamente.

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.
2.41. A solução, deverá possuir documentação que habilite a integração da solução com vários produtos de inteligência do fabricante.
2.42. Disponibilizar painel com KPIs de segurança que pode ser customizado pelo TRE-DF.
2.43. Obter informações de repositórios de códigos GitHub.
2.44. Obter informações da Zeronet.
2.45. Permitir ao TRE-DF organizar plano de mitigação de ameaça por dentro da solução, trazendo também recomendações pré configuradas.
2.46. Solução deve ter algoritmo de threat scoring para priorizar as ameaças identificadas.
2.47. A solução deverá suportar, no mínimo, os seguintes servidores/serviços de e-mail:
- **2.47.1.** Google Gmail e Microsoft Exchange (Microsoft 365 ou Office 365);
- **2.47.2.** A solução deverá considerar o quantitativo de 150 caixas postais prioritárias, estabelecidas pelo TRE-DF e que serão informadas oportunamente a CONTRATADA;
- **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.

2.48. A solução deve realizar a inspeção de todos os e-mails recebido e enviados de forma offline, ou seja, sem a necessidade da alteração do fluxo de e-mails entre clientes e MTA (Mail Tranfer Agent) do órgão.
2.49. A solução deverá armazenar o histórico de e-mails enviados e recebidos independentemente se estes foram considerados anômalos ou não.
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.
2.51. A solução deve identificar e proteger o ambiente de e-mail do órgão contra as seguintes anomalias:
- **2.51.1.** Spoofing;
- **2.51.2.** Links anômalos/suspeitos;
- **2.51.3.** Anexos suspeitos;
- **2.51.4.** SPAM;
- **2.51.5.** Phising/Spearphishing;
- **2.51.6.** Sequestro de conta de e-mail;
- **2.51.7.** Envio de dados sensíveis para fora do órgão.

2.52. A solução deve realizar a inspeção e apresentar os dados de, no mínimo, os seguintes parâmetros para cada e-mail:
- **2.52.1.** Sender Policy Framework (SPF);
- **2.52.2.** Domain Keys Identified Mail (DKIM);
- **2.52.3.** Forwarded-confirmed Reverse DNS (FCRDNS);
- **2.52.4.** IP do servidor de e-mail de origem e seu ASN correspondente;
- **2.52.5.** Todos os cabeçalhos do e-mail;
- **2.52.6.** Anexos (se existentes), nome dos anexos, tamanho, mime type, quantidade de vezes em que o anexo foi observado em caixas postais.

2.53. A solução deve permitir a tomada de ações contra e-mails como:
- **2.53.1.** Reter o e-mail no servidor de e-mail evitando que a correspondência anômala seja enviada para o destinatário;
- **2.53.2.** Entregar o e-mail para o cliente direcionando-o para a pasta de lixo eletrônico do cliente;
- **2.53.3.** Substituir um link considerado anômalo por um link gerado pela solução afim 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);
- **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;
- **2.53.5.** Remover anexos do e-mail original antes do envio para o cliente;
- **2.53.6.** Converter anexos anômalos para o padrão PDF. Quando a conversão não for possível o anexo deverá ser removido;
- **2.53.7.** Remover o nome do remetente (unspoof) apresentando o endereço de e-mail completo do mesmo;
- **2.53.8.** Adicionar banner (mensagem customizada) ao e-mail antes do envio para o cliente;
- **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;

2.54. A solução deve apresentar, para cada e-mail identificado como anômalo:
- **2.54.1.** Índice de anomalia do e-mail;
- **2.54.2.** Categoria(s) que apresentam o motivo da anomalia;
- **2.54.3.** Ações tomadas contra o e-mail, de acordo com item 2.53;
- **2.54.4.** Dados sobre o remetente de acordo com item 2.52;

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.

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:

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

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

2.55.3. Mapa de interações freqüentes com usuários externos agrupados por domínio;

2.55.4. Lista de Alias da caixa postal;

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

2.55.6. Índice de risco da caixa postal;

2.55.7. Índice de prevalência para spoofing da caixa postal;

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;

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

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

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.

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.

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

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.

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.

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

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

2.61.2. Apresentar posts realizados pelo ator de ameaça em cada fonte;

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

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

2.62. A solução deve permitir:

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

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

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

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

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

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

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

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

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

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

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

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.

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

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

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

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

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

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.

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

3. CARACTERÍSTICAS DE GERENCIAMENTO

3.1. O gerenciador deve possuir controle de interface gráfica (GUI: Graphical User Interface) e interface texto (CLI).
3.2. A interface de texto (CLI) deve possuir comandos para permitir a realização de troubleshooting.
3.3. A interface gráfica não deve ser desenvolvida ou conter componentes baseados em java por questões de compatibilidade com browsers modernos.
3.4. A interface gráfica deve possuir no mínimo:
- **3.4.1.** Lista de alertas de anormalidade identificadas;
- **3.4.2.** Critérios de filtro dos alertas de anormalidade por categoria de alerta, dispositivo ou usuários;
- **3.4.3.** Critérios de filtro de período (data e horário) para os alertas de anormalidade;
- **3.4.4.** Critérios de filtro de prioridade (risco) para os alertas de anormalidade;
- **3.4.5.** Apresentar a posição geográfica das redes no ambiente de TI;
- **3.4.6.** Opções de configuração do sistema;
- **3.4.7.** Área de gerenciamento de usuários;
- **3.4.8.** Área para gerenciamento de arquivos pcap, exportação e visualização na própria interface;
- **3.4.9.** Área de busca de dados na base de dados da solução.

3.5. Os alertas de anomalia devem conter no mínimo os seguintes dados:
- **3.5.1.** Identificador único (Unique ID);
- **3.5.2.** Data e horário;
- **3.5.3.** Dispositivo que originou a ação;
- **3.5.4.** Apresentar o IP de origem do dispositivo;
- **3.5.5.** Apresentar o MAC address do dispositivo;
- **3.5.6.** Apresentar o Hostname (DNS) do dispositivo;
- **3.5.7.** Apresentar o (s) usuário(s) que se eventualmente se logaram no dispositivo nas últimas horas;
- **3.5.8.** Apresentar o a rede a qual o dispositivo estava conectado;
- **3.5.9.** Descrição técnica do evento;
- **3.5.10.** Gráfico apresentando a quantidade de eventos similares e evolução do nível de risco;
- **3.5.11.** Atalho para acesso rápido às configurações da política que gerou o alerta;
- **3.5.12.** Dados técnicos resumidos das ações que causaram a anomalia e subsequente alerta;
- **3.5.13.** Atalho para acessar dados detalhados das ações que causaram a anomalia e subsequente alerta;
- **3.5.14.** Durante a investigação de uma anomalia/alerta o administrador pode acessar os dados abaixo utilizando apenas o mouse:
  - **3.5.14.1.** Dados detalhados do dispositivo que originou a anomalia;
  - **3.5.14.2.** IP do dispositivo;
  - **3.5.14.3.** Mac Address;
  - **3.5.14.4.** Nome DNS do dispositivo;
  - **3.5.14.5.** Primeira vez que o dispositivo/IP foi visto na rede;
  - **3.5.14.6.** Última vez que o dispositivo foi visto na rede;
  - **3.5.14.7.** Apresentar o (s) usuário(s) que se eventualmente se logou(aram) no dispositivo;
  - **3.5.14.8.** Apresentar a rede a qual o dispositivo estava conectado;
  - **3.5.14.9.** Acesso a todas as comunicações realizadas pelo dispositivo na rede;
  - **3.5.14.10.** Acesso a todas as anomalias as quais o dispositivo gerou na rede.

3.6. Acesso a ferramenta para geração de gráficos que facilitem a investigação utilizando critérios como, mas não limitados a:
- **3.6.1.** Dados relacionados a conexões;
- **3.6.2.** Tráfego de dados;
- **3.6.3.** Requisições DNS;
- **3.6.4.** Erros de Login;
- **3.6.5.** Ações utilizando SMB;
- **3.6.6.** Apresentar gráfico representando os fluxos de comunicação entre os dispositivos que originaram e receberam tráfego anômalo;

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:
- **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;
- **3.7.2.** Apresentação individual de cada alerta contendo:
  - **3.7.2.1.** Descrição do comportamento anômalo e riscos associados.

3.7.3. Dados técnicos relacionados ao alerta como:
3.7.3.1. Período em que a anomalia foi observada;
3.7.3.2. IP de origem;
3.7.3.3. IP(s) de destino;
3.7.3.4. Credencial de usuário observada no dispositivo;
3.7.3.5. Ação anômala identificada pela solução;
3.7.3.6. Acesso aos logs do tráfego anômalo;
3.7.3.7. Deverá classificar cada alerta baseado em fases de ataque.
3.7.4. Deve permitir ao administrador exportar todas as informações do item 3.7.3 em documento padrão .pdf.

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.

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

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'.

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.

3.12. O administrador pode gerar arquivos '.pcap' para quaisquer comunicação inspecionada pela solução.

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.

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

3.15. A solução deve possuir mecanismo de gerenciamento de usurários da interface web permitindo:
3.15.1. Criação, modificação ou remoção de usuários;
3.15.2. Gerenciamento de permissionamento dos usuários;
3.15.3. Opção de gerar usuário com permissão de leitura apenas;
3.15.4. Deve possuir interface para visualização dos aspectos do sistema como:
3.15.4.1. A versão de software, espaço utilizado em disco, consumo de CPU e consumo de memória;
3.15.4.2. Informação de todas as interfaces ativas e respectivo tráfego recebido através de cada uma delas;
3.15.4.3. Total de banda processada no momento, a média de banda processada e o pico de banda registrado nas últimas semanas;
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;
3.15.6. Listagem de todas as sub redes identificadas no ambiente bem como a quantidade de dispositivos em cada sub rede.

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

3.17. Deve permitir o envio de logs para sistemas externos utilizando os seguintes padrões:
3.17.1. CEF;
3.17.2. LEEF;
3.17.3. JSON;
3.17.4. Syslog.

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

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

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

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

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

4. CARACTERÍSTICAS DE GERENCIAMENTO DE RELATÓRIOS

4.1. Deve permitir a criação automática de relatórios executivos cobrindo no mínimo:
4.1.1. Indicação da quantidade total de dispositivos, quantidade total de sub redes e banda média processada;
4.1.2. Sumário das violações por fase do ataque;
4.1.3. Sumário dos dispositivos com maior nível de brechas não usuais;
4.1.4. Sumário dos top dispositivos que mais violaram comportamentos anômalos;

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;

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

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

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

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

4.4.1. Data e Horário;
4.4.2. Endereços IPs de origem e destino;
4.4.3. Versão do protocolo IP;
4.4.4. Protocolo de comunicação;
4.4.5. Estado da conexão;
4.4.6. Dados trafegados de entrada e saída;
4.4.7. Método HTTP;
4.4.8. Cabeçalhos HTTP;
4.4.9. Versão do SSL;
4.4.10. Cifragem da Conexão SSL;
4.4.11. Logins Kerberos;
4.4.12. Comunicações DNS;
4.4.13. Comunicações FTP;
4.4.14. Comunicações LDAP;
4.4.15. Comunicações Kerberos;
4.4.16. Comunicações de mineração de criptomoedas;
4.4.17. Comunicações SMB;
4.4.18. Comunicações Radius;
4.4.19. Comunicações RDP;
4.4.20. Comunicações SIP;

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

5. CARACTERÍSTICAS GERAIS DO HARDWARE

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.

5.2. 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.

5.3. 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.

5.4. 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:

5.4.1. Equipamento Tipo 1

5.4.1.1. Deverá suportar throughput de até 500Mbps;
5.4.1.2. Deverá ter capacidade de analisar e identificar 1.500 dispositivos;
5.4.1.3. Deverá suportar e analisar até 25.000 conexões por minuto;
5.4.1.4. Deverá considerar a inspeção de até 50 caixas postais prioritárias (VIP's);
5.4.1.5. Deverá possuir 1 (uma) interface padrão 100/1000 BASE-T para atuar como interface de administração;
5.4.1.6. Deverá possuir pelo menos 2 (duas) interfaces padrão 100/1000 BASE-T para atuarem como interfaces de análise de tráfego;
5.4.1.7. Deverá possuir pelo menos 2 (duas) interfaces padrão 10 Gbe SFP+ para atuarem como interface de análise de tráfego;
5.4.1.8. O hardware fornecido deverá possuir fonte de alimentação redundante.

5.4.2. Equipamento Tipo 2

5.4.2.1. Deverá suportar throughput de até 01Gbps;
5.4.2.2. Deverá ter capacidade de analisar e identificar 2.000 dispositivos;

5.4.2.3. Deverá suportar e analisar até 50.000 conexões por minuto;
5.4.2.4. Deverá considerar a inspeção de até 100 caixas postais prioritárias (VIP's);
5.4.2.5. Deverá possuir 1 (uma) interface padrão 100/1000 BASE-T para atuar como interface de administração;
5.4.2.6. Deverá possuir pelo menos 2 (duas) interfaces padrão 100/1000 BASE-T para atuarem como interfaces de análise de tráfego;
5.4.2.7. Deverá possuir pelo menos 2 (duas) interfaces padrão 10 Gbe SFP+ para atuarem como interface de análise de tráfego;
5.4.2.8. O hardware fornecido deverá possuir fonte de alimentação redundante.

5.4.3. Equipamento Tipo 3

5.4.3.1. Deverá suportar throughput de até 02Gbps;
5.4.3.2. Deverá ter capacidade de analisar e identificar 2.500 dispositivos;
5.4.3.3. Deverá suportar e analisar até 75.000 conexões por minuto;
5.4.3.4. Deverá considerar a inspeção de até 150 caixas postais prioritárias (VIP's);
5.4.3.5. Deverá possuir 1 (uma) interface padrão 100/1000 BASE-T para atuar como interface de administração;
5.4.3.6. Deverá possuir pelo menos 2 (duas) interfaces padrão 100/1000 BASE-T para atuarem como interfaces de análise de tráfego;
5.4.3.7. Deverá possuir pelo menos 2 (duas) interfaces padrão 10 Gbe SFP+ para atuarem como interface de análise de tráfego;
5.4.3.8. O hardware fornecido deverá possuir fonte de alimentação redundante.

5.4.4. Equipamento Tipo 4

5.4.4.1. Deverá suportar throughput de até 03Gbps;
5.4.4.2. Deverá ter capacidade de analisar e identificar 3.500 dispositivos;
5.4.4.3. Deverá suportar e analisar até 100.000 conexões por minuto;
5.4.4.4. Deverá considerar a inspeção de até 200 caixas postais prioritárias (VIP's);
5.4.4.5. Deverá possuir 1 (uma) interface padrão 100/1000 BASE-T para atuar como interface de administração;
5.4.4.6. Deverá possuir pelo menos 2 (duas) interfaces padrão 100/1000 BASE-T para atuarem como interfaces de análise de tráfego;
5.4.4.7. Deverá possuir pelo menos 2 (duas) interfaces padrão 10 Gbe SFP+ para atuarem como interface de análise de tráfego;
5.4.4.8. O hardware fornecido deverá possuir fonte de alimentação redundante.

5.4.5. Equipamento Tipo 5

5.4.5.1. Deverá suportar throughput de até 05Gbps;
5.4.5.2. Deverá ter capacidade de analisar e identificar 5.000 dispositivos;
5.4.5.3. Deverá suportar e analisar até 150.000 conexões por minuto;
5.4.5.4. Deverá considerar a inspeção de até 250 caixas postais prioritárias (VIP's);
5.4.5.5. Deverá possuir 1 (uma) interface padrão 100/1000 BASE-T para atuar como interface de administração;
5.4.5.6. Deverá possuir pelo menos 2 (duas) interfaces padrão 100/1000 BASE-T para atuarem como interfaces de análise de tráfego;
5.4.5.7. Deverá possuir pelo menos 2 (duas) interfaces padrão 10 Gbe SFP+ para atuarem como interface de análise de tráfego;
5.4.5.8. O hardware fornecido deverá possuir fonte de alimentação redundante.

5.4.6. Equipamento Tipo 6

5.4.6.1. Deverá suportar throughput de 10 a 15Gbps;
5.4.6.2. Deverá ter capacidade de analisar e identificar 9.000 dispositivos;
5.4.6.3. Deverá suportar e analisar até 450.000 conexões por minuto;
5.4.6.4. Deverá considerar a inspeção de até 300 caixas postais prioritárias (VIP's);
5.4.6.5. Deverá possuir 1 (uma) interface padrão 100/1000 BASE-T para atuar como interface de administração;
5.4.6.6. Deverá possuir pelo menos 2 (duas) interfaces padrão 100/1000 BASE-T para atuarem como interfaces de análise de tráfego;
5.4.6.7. Deverá possuir pelo menos 2 (duas) interfaces padrão 10 Gbe SFP+ para atuarem como interface de análise de tráfego;
5.4.6.8. O hardware fornecido deverá possuir fonte de alimentação redundante.

5.4.7. Equipamento Tipo 7

5.4.7.1. Deverá suportar throughput de até 20Gbps;
5.4.7.2. Deverá ter capacidade de analisar e identificar 13.000 dispositivos;
5.4.7.3. Deverá suportar e analisar até 1,5 milhões de conexões por minuto;
5.4.7.4. Deverá considerar a inspeção de até 300 caixas postais prioritárias (VIP's);
5.4.7.5. Deverá possuir 1 (uma) interface padrão 100/1000 BASE-T para atuar como interface de administração;
5.4.7.6. Deverá possuir pelo menos 2 (duas) interfaces padrão 100/1000 BASE-T para atuarem como interfaces de análise de tráfego;
5.4.7.7. Deverá possuir pelo menos 2 (duas) interfaces padrão 10 Gbe SFP+ para atuarem como interface de análise de tráfego;
5.4.7.8. O hardware fornecido deverá possuir fonte de alimentação redundante.