TRIBUNAL REGIONAL ELEITORAL DO ESPÍRITO SANTO
Rua João Batista Parra 575 - Bairro Praia do Suá - CEP 29052-123 - Vitória - ES

ESTUDO TÉCNICO PRELIMINAR (TIC) Nº 06/2023 - TRE-ES/PRE/DG/STI/CIS/NSC

(este documento deve seguir as orientações da Resolução TRE/ES nº 261/2018)

SUMÁRIO

ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO

[Obrigatório mesmo para prorrogações, art. 19, § único, resolução TRE-ES nº 261/2018]

1. CARACTERIZAÇÃO DA DEMANDA

1.1. DESCRIÇÃO SUCINTA

1.1.1.Contratação de empresa especializada para fornecimento de bens e serviços de inteligência cibernética, no formato de prestação de serviço, voltados para análise do ambiente interno da infraestrutura de rede e monitoramento do ambiente externo a infraestrutura do TRE-ES, sobre ameaças cibernéticas do seu ambiente, com adoção de tecnologias de análise de comportamento, inteligência artificial, *machine learning* não supervisionado, incorporando os incidentes identificados em sua base com a inteligência cibernética.

1.2. JUSTIFICATIVA DA NECESSIDADE E RESULTADOS

1.1.2. 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.

1.1.3. 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.;

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

1.1.5. Em novembro de 2020 o Superior Tribunal de Justiça – STJ foi alvo do maior ataque cibernético já realizado ao um órgão do Governo Brasileiro. Foram mais de 7 dias com todos os sistemas indisponíveis. O foco do ataque foi a infraestrutura do Datacenter do STJ;

1.1.6. 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.

1.1.7. 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:

1.1.7.1. Acesso e exposição indevidos de dados administrativos do próprio TSE, na data do primeiro turno das eleições municipais de 2020 (15/11/20);

1.1.7.2. 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;

1.1.7.3. 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;

1.1.7.4. 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;

1.1.7.5. 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;

1.1.7.6. Ataque à Procuradoria do Município de Vitória, Espírito Santo, ocorrido em 10 de novembro de 2020, acarretando suspensão dos serviços informatizados;

1.1.7.7. 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;

1.1.7.8. 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

1.1.7.9. Ataque à Biblioteca Nacional que, da mesma forma, teve seus serviços de TI interrompidos por 15 dias, até que fossem restaurados com segurança;

1.1.7.10.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;

1.1.7.11.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.

1.1.7.12.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 estados brasileiros.

1.1.8. 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.

1.1.9. Se por um lado, a presença do TRE-ES em soluções digitais tem aumentado com velocidade, por outro lado também têm aumentado as tentativas de ataques à presença de suas instituições no ciberespaço. Mesmo estando as 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.

1.1.10. 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.

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

1.1.11.1.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.

1.1.11.2.RAMSOMWARE – bastante difundido no meio de hackers, o ramsomware se caracteriza como um subconjunto de malwares que atuam no bloqueio de 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.

1.1.11.3.Ataques DDoS – o DDoS é considerado um dos ataques cibernéticos mais comuns e perigosos para uma 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.

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

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

1.1.12.2.Sistemas administrativos: SEI e SGRH, sistema de patrimônio ASI, sistema de pagamento, controle de ponto, dentre outros;

1.1.12.3.Sistemas Eleitorais: Cadastro Nacional de Eleitores (ELO), Sistema Batimento Biométrico, dentre outros;

1.1.12.4.Sistemas Jurisdicionais: PJe-TRE-ES, Jurisprudência, Nada consta com a Justiça Eleitoral, dentre outros;

1.1.12.5.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.

1.1.13. No que tange à responsabilidade da proteção de todos os sistemas informatizados existentes no ambiente do TRE-ES 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.

1.1.14. 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.

1.1.15. 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.

1.1.16. 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-ES perante a sociedade de forma geral.

1.1.17. O TRE-DF por meio do Ofício-Circular GAB-DG TSE nº 144/2023 foi definido como responsável pela aquisição conjunta a ser realizada em 2023, de solução de análise de rede com inteligência artificial e Inteligência Cibernética, referente ao Eixo Estruturante E3 – Ferramentas Automatizadas em atendimento a Estratégia Nacional de Cibersegurança e Arquitetura de Cibersegurança para o período 2021-2024.

1.1.18. A contratação tem como finalidade atender as necessidades do Tribunal Regional Eleitoral do Distrito Federal – TRE-DF, bem como outros TRE’s partícipes quem venham a se interessar em entrar na Ata de registro de preços que será formada. Conforme processo SEI nº 0003000-33.2023.6.08.8000 o TRE-ES será partícipe desta contratação.

2. ESPECIFICAÇÃO DOS REQUISITOS FUNCIONAIS

Contratação de empresa especializada para fornecimento de bens e serviços de inteligência cibernética, no formato de prestação de serviço, voltados para análise do ambiente interno da infraestrutura de rede e monitoramento do ambiente externo a infraestrutura do TRE-ES, sobre ameaças cibernéticas do seu ambiente, com adoção de tecnologias de análise de comportamento, inteligência artificial, *machine learning* não supervisionado, incorporando os incidentes identificados em sua base com a inteligência cibernética, nos termos dos requisitos listados no item 2.1 deste ETP.

2.1. REQUISITOS RELACIONADOS AO NEGÓCIO

2.2.1. Características Gerais:

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

2.2.1.2. A solução, composta de hardware, software e serviços, deve ser fornecida através de aquisição por meio de subscrição de direito de uso durante o período contratual, na versão mais recente publicada pelo desenvolvedor e com prazo de garantia (atualização, manutenção e suporte técnico) mínimo de 24 (vinte e quatro) meses, com possibilidade de renovação até 60 meses.

2.2.1.3. A solução poderá ser formada por vários fabricantes ou serviços integrados por meio de API's (Application Programming Interface) ou única, sem a necessidade de desenvolvimento, desde que atenda todas as especificações técnicas desta Análise de Viabilidade;

2.2.1.4. A solução terá prazo de garantia de 24 meses, com o seu pagamento sendo realizado em parcela única, após a homologação da entrega, com devidos aceites, exceto para os treinamentos e os serviços sob demanda, que serão liquidados e pagos a medida de sua execução.

2.2. REQUISITOS DE CAPACITAÇÃO, AMBIENTAIS, CULTURAIS E SOCIAIS

2.2.1. Deverá ser fornecido treinamento oficial, com carga horária mínima de 40 horas, abarcando a solução, no conteúdo necessário para a perfeita compreensão e operação de todos os seus requisitos. Ações complementares como workshops internos e treinamentos no formato hands-on podem ser também considerados no escopo do treinamento. O treinamento poderá também ser realizado de forma remoto, via videoconferência, objetivando agilizar a capacitação das equipes envolvidas e a possibilidade de atender de forma simultânea vários Tribunais.

2.2.2. O treinamento deverá ser fornecido, por turma, para no mínimo 5 (cinco) servidores detentores de cargos efetivos do TRE-ES, com emissão de certificados e pesquisa de satisfação ao final do treinamento, estando sujeita a CONTRATADA a atingir uma qualidade mínima, sob pena de sanção aplicável, a ser definida no Termo de Referência;

2.2.3. Poderão ser indicados mais participantes na categoria de ouvintes, sem a exigência de certificado de participação e material (limitando-se a 4 participantes adicionais do tipo “ouvintes”).

2.2.4. Todas as despesas referentes à realização do treinamento ou ao custeio de insumos deverão estar inclusas no valor contratado.

2.2.5. Todos os manuais, guias de instruções e ajuda deverão ser disponibilizados preferencialmente para o idioma português do Brasil – Pt-BR e fornecidos em meio digital.

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

2.2.7. Quanto aos requisitos sociais, os profissionais da CONTRATADA, quando nas dependências do TRE-ES, deverão apresentar-se com crachá de identificação, vestidos de forma adequada ao ambiente de trabalho, evitando-se o vestuário que caracterize o comprometimento da boa imagem institucional do TRE- ES.

2.2.8. Os profissionais da CONTRATADA, quando nas dependências do TRE-ES, 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.

2.2.9. Os profissionais também deverão respeitar todos os servidores, funcionários e colaboradores em qualquer posição hierárquica, preservando a comunicação e o relacionamento interpessoal construtivo.

2.2.10. Para fins do disposto no inciso XXXIII do art. 7º da Constituição Federal, de 5 de outubro de 1988, e no inciso V do art. 27 da Lei no 8.666, de 21 de junho de 1993, acrescido pela Lei nº 9.854, de 27 de outubro de 1999, a CONTRATADA não poderá possuir em seu quadro de pessoal empregado(s) com menos de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre, e em qualquer trabalho menores de 16 (dezesseis) anos, salvo na condição de aprendiz a partir de 14 (quatorze) anos.

2.2.11. Os materiais, objeto desta Análise de Viabilidade, deverão seguir, no que couberem, os seguintes normativos:

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

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

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

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

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

2.2.11.6. art. 225 da Constituição da República Federativa do Brasil de 1988;

2.3. REQUISITOS DE MANUTENÇÃO E GARANTIA

2.3.1. A solução deverá ser ofertada com garantia e manutenção do fabricante e deverá ser prestado na modalidade 24 horas por dia e 7 dias por semana (24x7), pelo prazo de 24 meses, sem custos adicionais ao TRE-ES, contados a partir da emissão do Termo de Recebimento Definitivo da Solução.

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

2.3.3. O acionamento da garantia ocorrerá por meio de abertura dos chamados técnicos via número de telefone de discagem gratuita (0800), envio de e-mail ou acesso ao site oficial de suporte do fabricante, obedecendo aos seguintes padrões de severidade:

2.3.3.1. Severidade 1: O uso do sistema de programa suportado é interrompido ou tão severamente impactado que não é possível trabalhar ou operar de modo razoável. 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:

2.3.3.1.1. dados corrompidos;

2.3.3.1.2. uma função crítica documentada não está disponível;

2.3.3.1.3. a solução ou parte da mesma trava indefinidamente, gerando impacto inaceitável ao serviço, impactando recursos, respostas e a sua operação;

2.3.3.1.4. a solução ou parte da mesma falha repetidamente após tentativas de reinicializações.

2.3.3.1.5. Caso seja identificado um defeito no software (bugs, erros e/ou falhas), o mesmo deverá ser resolvido em até 30 (trinta) dias úteis a contar da abertura do chamado ou, não resolvendo neste prazo, deverá ser providenciada uma solução de contorno dentro do intervalo, de 30 dias supracitado, até que a solução definitiva seja efetivada.

2.3.3.1.6. No caso de aplicação de solução de contorno, a solução definitiva deverá ser entregue em até 45 (quarenta e cinco) dias.

2.3.3.1.7. 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.

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

2.3.3.2. Severidade 2: A perda da solução é pequena. O problema gera inconvenientes que podem requerer uma solução temporária para restaurar a funcionalidade. O impacto no serviço é mínimo e não compromete o uso e as principais funcionalidades da operação.

2.3.3.3. Severidade 3: Solicitação de informações, melhorias ou esclarecimentos relativos à Solução, mas não há impacto na operação dela. Não há perda de serviço. O resultado não impede o seu funcionamento.

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

2.4. REQUISITOS TEMPORAIS

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

2.4.2. Todos os prazos citados, quando não expresso de forma contrária, serão considerados em dias úteis (ou horas úteis, quando definido em horas).

2.4.3. Todos os eventos de trabalho que envolva participação de integrantes do TRE-ES serão realizados durante os horários de expediente adotados, de segunda-feira a sexta-feira, exceto feriados, salvo casos de urgência e/ou acordo entre as partes, desde que tempestivamente informados e solicitados.

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

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

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

2.5. REQUISITOS DE SEGURANÇA DA INFORMAÇÃO

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

2.5.2. A solução deverá proporcionar a disponibilidade, a integridade e a segurança de todas as informações do TRE-ES por ela gerenciadas e armazenadas.

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

2.5.4. O Tribunal deverá adotar precauções e medidas para que as obrigações oriundas do presente instrumento sejam efetivamente observadas a todos os seus representantes.

2.5.5. A CONTRATADA deverá informar imediatamente ao TRE qualquer violação das regras de sigilo ora estabelecidas que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo, bem como de seus empregados, prepostos e prestadores de serviço.

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

2.5.7. A CONTRATADA deverá respeitar as diretrizes constantes da Política de Segurança da Informação da Justiça Eleitoral (Resolução TSE Nº 23.644, de 1º de julho de 2021), obrigando-se a manter sigilo a respeito de quaisquer informações, dados, processos, fórmulas, códigos, cadastros, fluxogramas, diagramas lógicos, dispositivos, modelos ou outros materiais de propriedade do TRE-ES, aos quais tiver acesso em decorrência do objeto da presente contratação, ficando terminantemente proibida de fazer uso ou revelação destes sob qualquer justificativa;

2.5.8. O TRE-ES terá propriedade sobre todos os documentos e procedimentos operacionais produzidos no escopo da presente contratação;

2.5.9. A CONTRATADA assinará no ato da entrega da solução e do início dos serviços, Termo de Confidencialidade, em que se comprometerá a não acessar, não divulgar e a proteger todos os dados de infraestrutura e de vulnerabilidades do CONTRATANTE a que tiver acesso, que abrangerá todos os seus colaboradores e terceiros, sob ônus e penas aplicáveis referentes à legislação vigente.

2.6. REQUISITOS DE GARANTIA DA SOLUÇÃO

2.6.1. A solução deverá ter garantia/suporte por 24 (vinte e quatro) meses, incluindo software, hardware, atualizações e, se necessário, substituição de peças e equipamentos;

2.6.2. O contrato poderá ser prorrogado por até 60 meses, conforme condições estabelecidas pela legislação vigente.

2.7. REQUISITOS OPERAÇÃO ASSISTIDA DA SOLUÇÃO

2.7.1. A solução deverá possuir Operação Assistida, sob demanda, com atendimento remoto ou presencial para solução de qualquer solicitação de esclarecimentos por parte da equipe técnica do tribunal, que envolva a solução ofertada.

2.7.2. O serviço de Operação Assistida será consumido em blocos de 4 (quatro) horas;

2.7.3. Cada acionamento de bloco mínimo ocorrerá por intermédio de emissão de Ordem de Serviço (OS);

2.7.4. Este serviço não pode ser confundido com os serviços de garantia, manutenção e sustentação da solução, que deverão obedecer ao regime de 24x7x365 (vinte e quatro horas do dia, nos sete dias da semana, em todos os dias do ano)

2.7.5. Se for observado pela equipe de planejamento da contratação a necessidade de aprimorar os requisitos para o serviço de Operação Assistida, estes poderão ser incluídos no Termo de Referência.

2.8. REQUISITOS DE METODOLOGIA DE TRABALHO

2.8.1. A solução deve ser instalada, preferencialmente, nas dependências do TRE-ES;

2.8.2. Deverá ser apresentada documentação técnica detalhada contendo todas as informações referentes a instalação e a configuração de todos os itens que compõe a solução, com plano de ação detalhando as ações e procedimentos realizados.

2.8.3. Se for observado pela equipe de planejamento da contratação a necessidade de aprimorar os requisitos referentes à metodologia de trabalho, estes poderão ser incluídos no Termo de Referência.

2.9. REQUISITOS DE EXPERIÊNCIA PROFISSIONAL DA EQUIPE DA CONTRATADA

2.9.1. A CONTRADADA deverá comprovar aptidão e experiência técnica e profissional para a prestação dos serviços em características, quantidades e prazos compatíveis com o que for definido como o mínimo aceitável para prestação e realização dos serviços.

3. ESPECIFICAÇÃO DOS REQUISITOS TECNOLÓGICOS

3.1. CARACTERÍSTICAS GERAIS

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

3.1.2. 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.

3.1.3. A solução, composta de hardware e software, deve ser fornecida através de aquisição por meio de serviços de subscrição de direito de uso durante o período contratual, na versão mais recente publicada pelo desenvolvedor e com prazo de garantia (atualização, manutenção e suporte técnico) mínimo de 24 (vinte e quatro) meses;

3.1.4. A solução poderá ser formada por vários fabricantes ou serviços integrados por meio de API's (Application Programming Interface) ou única, sem a necessidade de desenvolvimento, desde que atenda todas as especificações técnicas desta Análise de Viabilidade.

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

3.1.5.1. Machine learning não supervisionado

3.1.5.2. Machine learning supervisionado

3.1.5.3. Deep Learning

3.1.5.4. Redes Neurais

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

3.1.7. 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.

3.1.8. Não serão aceitos produtos ou serviços OpenSource.

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

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

3.1.11. 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-ES para o funcionamento da solução.

3.1.12. 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.

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

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

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

3.1.15.1. Amazon AWS

3.1.15.2. Microsoft Azure

3.1.15.3. Google G-Suite

3.1.15.4. Office 365

3.1.15.5. Dropbox enterprise

3.1.15.6. Componentes virtuais (máquinas virtuais)

3.1.15.7. Endpoint para Sistemas Operacionais.

3.1.15.8. Docker e Kubernets.

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

3.1.17. Capacidade de personalizar a sua busca por ameaças cibernéticas;

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

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

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

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

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

3.1.23. A solução permite que os usuários realizem consultas ad-hoc ilimitadas para uma ou mais de suas fontes de dados;

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

3.1.25. 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;

3.1.26. Possuir no mínimo, uma base de análise de 150 milhões de registros em sites de vendas de cartões. Como pode ser demonstrado no link https://www.tse.jus.br/comunicacao/noticias/2023/Janeiro/eleitores-podem-quitar-debitos-com-a-justica-eleitoral-via-pix-ou-cartao-de-credito#:~:text=Eleitores%20podem%20quitar%20d%C3%A9bitos%20com,de%20cr%C3%A9dito%20%E2%80%94%20Tribunal%20Superior%20Eleitoral a Justiça Eleitoral aceita o pagamento de débitos por intermédio de Pix ou cartões de créditos. Desta forma o monitoramento de marketplaces fraudulentos e de sites que vendem cartões de crédito podem mitigar possíveis usos indevidos. 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).

3.1.27. Possuir domínios de especialização, incluindo, crimes financeiros, hacktivismo e ciberterrorismo;

3.1.28. Possuir acesso a mais de 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:

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

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

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

3.1.29. Possuir acesso as seguintes redes anônimas; Darknet e Zeronet;

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

3.1.31. Todos os requisitos mencionados a partir do item 3.1.17 desse documento, deverão ser suportados e monitorados através da CONTRATADA, podendo ser externo ao ambiente do TRE-ES;

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

3.1.33. 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;

3.1.34. A solução não deve depender de assinaturas predefinidas para respostas;

3.1.35. 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;

3.1.36. 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.

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

3.1.38. Possuir funcionalidade de bloquear as ameaças de forma proativa;

3.1.39. 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;

3.1.40. Solução deverá possuir capacidade de bloquear downloads de arquivos maliciosos de fontes não confiáveis;

3.1.41. 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;

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

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

3.1.44. A solução deverá ser habilitada no console de uso de todas as outras ferramentas do fabricante;

3.1.45. A solução deverá funcionar 24h x 7d x 365 d;

3.1.46. Possuir mecanismos de proteção para usuários Vips;

3.1.47. A solução não deve trabalhar com defesas pré-programadas;

3.1.48. A solução deverá reconhecer um ataque mesmo que não tenha sido identificado pelos padrões e frameworks do mercado;

3.1.49. 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);

3.1.50. 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 e dispositivos de rede sobre ataques ocorridos;

3.1.51. A solução deverá possuir capacidade de uso em aplicativos moveis;

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

3.1.53. 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.

3.1.54. 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.

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

3.1.55.1. 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.

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

3.1.57. 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

3.1.58. 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.

3.1.59. 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.

3.1.60. 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.

3.1.61. 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.

3.2. CARACTERÍSTICAS TÉCNICAS DA SOLUÇÃO

3.2.1. 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:

3.2.1.1. Classificação do tipo de dispositivo (desktop, servidor, impressora, câmera, iot, etc)

3.2.1.2. IP do dispositivo

3.2.1.3. Mac Address

3.2.1.4. Nome DNS do dispositivo

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

3.2.1.6. Última vez que o dispositivo foi visto na rede

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

3.2.2. 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.

3.2.3. 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.

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

3.2.5. A solução deve criar métricas, de forma autônoma, de raridade de Ips, domínios DNS, dispositivos etc. baseados na frequência que estes são acessados através da rede.

3.2.6. 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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3.2.8.22. Dispositivo solicitando um domínio conhecido por hospedar malwares.

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

3.2.8.24. 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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3.2.8.39. 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.

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

3.2.8.41. Dispositivo enviando dados para o Pastebin.

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

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

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

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

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

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

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

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

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

3.2.8.51. Dispositivo explorado vulnerabilidade Heartbleed na rede interna. 4

3.2.8.52. Dispositivo se conectando a um DNS SinkHole conhecido.

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

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

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

3.2.8.56. Alteração no comportamento de tráfego DHCP.

3.2.8.57. Novo servidor DNS na rede.

3.2.8.58. Novo servidor de proxy web na rede.

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

3.2.8.60. Uma credencial efetuando login de uma origem incomum.

3.2.8.61. Uma credencial foi usada em múltiplos dispositivos internos.

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

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

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

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

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

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

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

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

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

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

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

3.2.17. Deve se capaz de registrar todas as ações de resposta para propósitos de auditoria.

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

3.2.19. Capacidade de personalizar a sua busca por ameaças cibernéticas;

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

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

3.2.22. Possuir funcionalidade de personalização dos usuários, para acesso fácil as ameaças ao TRE-ES;

3.2.23. 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;

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

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

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

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

3.2.28. Permitir que os usuários possam gerenciar os incidentes;

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

3.2.30. A solução permite que os usuários realizem consultas ad-hoc ilimitadas para uma ou mais de suas fontes de dados;

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

3.2.31.1. Russo;

3.2.31.2. Chinês;

3.2.31.3. Farsi;

3.2.31.4. Árabe;

3.2.31.5. Idiomas europeus;

3.2.31.6. Inglês;

3.2.31.7. Hebraico;

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

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

3.2.34. Possuir acesso a mais de 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:

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

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

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

3.2.35. Possuir domínios de especialização, incluindo, crimes financeiros, hacktivismo e ciberterrorismo;

3.2.36. Possuir acesso as seguintes redes anônimas; Darknet e Zeronet;

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

3.2.38. Todos os requisitos mencionados entre os itens 4.2.4.20 e 4.2.4.41 desta Análise de Viabilidade, deverão ser suportados e monitorados através da CONTRATADA, podendo ser externo ao ambiente do TRE- ES;

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

3.2.40. Disponibilizar painel com KPIs de segurança que pode ser customizado pelo TRE-ES;

3.2.41. Obter informações de repositórios de códigos GitHub;

3.2.42. Obter informações da Zeronet;

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

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

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

3.2.45.1. Microsoft Office 365 Exchange Online e Google Gmail;

3.2.45.2. A solução deverá considerar o quantitativo de 150 caixas postais prioritárias, estabelecidas pelo TREES e que serão informadas oportunamente a contratada.

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

3.2.46. 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.

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

3.2.48. 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.

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

3.2.49.1. Links anômalos/suspeitos

3.2.49.2. Anexos suspeitos

3.2.49.3. SPAM

3.2.49.4. Phising/Spearphishing.

3.2.49.5. Sequestro de conta de e-mail.

3.2.49.6. Spoofing

3.2.49.7. Envio de dados sensíveis para fora do órgão.

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

3.2.50.1. Sender Policy Framework (SPF).

3.2.50.2. Domain Keys Identified Mail (DKIM).

3.2.50.3. Forwarded-confirmed Reverse DNS (FCRDNS).

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

3.2.50.5. Todos os cabeçalhos do e-mail.

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

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

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

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

3.2.51.3. 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).

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

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

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

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

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

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

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

3.2.52.1. Índice de anomalia do e-mail.

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

3.2.52.3. Ações tomadas contra o e-mail, de acordo com item 3.2.49 e seus subitens.

3.2.52.4. Dados sobre o remetente de acordo com item 3.2.48

3.2.52.5. 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.

3.2.53. 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:

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

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

3.2.53.3. Mapa de interações frequentes com usuários externos agrupados por domínio.

3.2.53.4. Lista de Alias da caixa postal.

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

3.2.53.6. Apresentar informações sobre o dispositivo de acordo com item 3.2.1 e seus subitens

3.2.53.7. Índice de risco da caixa postal.

3.2.53.8. Índice de prevalência para spoofing da caixa postal.

3.2.53.9. Lista de ações tomadas a e-mails anômalos, de acordo com o item 3.2.49 e seus subitens, e a respectiva quantidade de ações tomadas.

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

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

3.2.55. A solução deve possuir interface apresentando a quantidade de e-mails recebidos em um período, a quantidade de ações tomadas conta e-mails de acordo com o item 3.2.49 e o percentual total de ações tomadas.

3.2.55.1. 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.

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

3.2.57. 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.

3.2.58. 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.

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

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

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

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

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

3.2.60. A solução deve permitir:

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

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

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

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

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

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

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

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

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

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

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

3.2.69. 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.

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

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

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

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

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

3.2.75. 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.

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

3.3. CARACTERÍSTICAS DE GERENCIAMENTO

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

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

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

3.3.4. A interface gráfica deve possuir no mínimo:

3.3.4.1. Lista de alertas de anormalidade identificadas.

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

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

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

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

3.3.4.6. Opções de configuração do sistema

3.3.4.7. Área de gerenciamento de usuários

3.3.4.8. Área para gerenciamento de arquivos pcap, exportação e visualização na própria interface. 3.2.10. Área de busca de dados na base de dados da solução.

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

3.3.5.1. Identificador único (Unique ID).

3.3.5.2. Data e horário.

3.3.5.3. Dispositivo que originou a ação.

3.3.5.4. Apresentar o IP de origem do dispositivo.

3.3.5.5. Apresentar o MAC address do dispositivo.

3.3.5.6. Apresentar o Hostname (DNS) do dispositivo.

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

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

3.3.5.9. Descrição técnica do evento.

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

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

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

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

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

3.3.5.15. Dados detalhados do dispositivo que originou a anomalia.

3.3.5.16. IP do dispositivo

3.3.5.17. Mac Address

3.3.5.18. Nome DNS do dispositivo

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

3.3.5.20. Última vez que o dispositivo foi visto na rede

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

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

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

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

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

3.3.6.1. Dados relacionados a conexões.

3.3.6.2. Tráfego de dados.

3.3.6.3. Requisições DNS.

3.3.6.4. Erros de Login.

3.3.6.5. Ações utilizando SMB.

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

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

3.3.8. 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, e apresentação individual de cada alerta contendo a descrição do comportamento anômalo e riscos associados, e dados técnicos relacionados ao alerta como:

3.3.8.1. Período em que a anomalia foi observada;

3.3.8.2. IP de origem;

3.3.8.3. IP(s) de destino;

3.3.8.4. Credencial de usuário observada no dispositivo;

3.3.8.5. Ação anômala identificada pela solução;

3.3.8.6. Acesso aos logs do tráfego anômalo.

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

3.3.10. Deverá permitir ao administrador exportar todas as informações acima do item 3.3.8. em documento padrão .pdf.

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

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

3.3.13. 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’.

3.3.14. 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.

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

3.3.16. 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.

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

3.3.18. A solução deve possuir mecanismo de gerenciamento de usurários da interface web permitindo:

3.3.18.1. Criação, codificação ou remoção de usuários

3.3.18.2. Gerenciamento de permissionamento dos usuários.

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

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

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

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

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

3.3.18.8. 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.

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

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

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

3.3.20.1. CEF

3.3.20.2. LEEF

3.3.20.3. JSON

3.3.20.4. Syslog

3.3.21. Deve permitir a integração nativa com plataforma de gerenciamento de chamados como Atlassian JIRA e ServiceNow.

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

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

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

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

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

3.4. CARACTERÍSTICAS DE GERENCIAMENTO DE RELATÓRIOS

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

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

3.4.1.2. Sumário das violações por fase do ataque.

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

3.4.1.4. Sumario dos top dispositivos que mais violaram comportamentos anômalos.

3.4.1.5. 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, dentre outros.

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

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

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

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

3.4.4.1. Data e Horário;

3.4.4.2. Endereços IPs de origem e destino;

3.4.4.3. Versão do protocolo IP;

3.4.4.4. Protocolo de comunicação;

3.4.4.5. Estado da conexão;

3.4.4.6. Dados trafegados de entrada e saída;

3.4.4.7. Método HTTP;

3.4.4.8. Cabeçalhos HTTP;

3.4.4.9. Versão do SSL;

3.4.4.10. Cifragem da Conexão SSL;

3.4.4.11. Logins Kerberos;

3.4.4.12. Comunicações DNS;

3.4.4.13. Comunicações FTP;

3.4.4.14. Comunicações LDAP;

3.4.4.15. Comunicações Kerberos;

3.4.4.16. Comunicações de mineração de criptomoedas;

3.4.4.17. Comunicações SMB;

3.4.4.18. Comunicações Radius;

3.4.4.19. Comunicações RDP;

3.4.4.20. Comunicações SIP.

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

3.5. CARACTERÍSTICAS GERAIS DO HARDWARE

3.5.1. Deverá ser fornecido para monitoramento do ambiente interno na modalidade física, equipamentos *Appliances* capazes de processar o tráfego do TRE-ES. As informações contidas nesse equipamento, não devem ser processadas fora do ambiente dos Tribunais envolvidos na contratação, somente internamente.

3.5.2. 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.

3.5.3. 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.

3.5.4. Detalhamento do equipamento:

3.5.4.1. Deverá suportar throughput de até 02Gbps;

3.5.4.2. Deverá ter capacidade de analisar e identificar 2.500 dispositivos;

3.5.4.3. Deverá suportar e analisar até 75.000 conexões por minuto;

3.5.4.4. Deverá considerar a inspeção de até 150 caixas postais prioritárias (VIP's);

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

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

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

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

3.6. ANÁLISE DA DEPENDÊNCIA TECNOLÓGICA

3.6.1. FORMA DE TRANSFERÊNCIA DE CONHECIMENTO TECNOLÓGICO:

3.6.1.1. A empresa contratada deverá realizar treinamento oficial dos fabricantes envolvidos, em carga horária definida pelo TRE-ES a seus servidores efetivos, para pleno conhecimento e entendimento do uso da solução.

3.6.2. DIREITOS DE PROPRIEDADE INTELECTUAL E AUTORAIS DA SOLUÇÃO DE TIC:

3.6.2.1. Com essa contratação, o TRE-ES irá adquirir subscrição dos softwares e hardwares que compõe a solução, não sendo detentor de propriedade intelectual dos mesmos. Ressalte-se que os direitos autorais dos fabricantes dos softwares utilizados na solução são resguardados e garantidos por legislação nacional e internacional.

3.6.2.2. Toda a documentação gerada ao longo da contratação é de propriedade do TRE-ES.

4. IDENTIFICAÇÃO E COMPARAÇÃO DAS SOLUÇÕES ADERENTES AOS REQUISITOS

4.1. SOLUÇÕES DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO SIMILAR ENCONTRADAS EM OUTROS ÓRGÃOS OU ENTIDADES DA ADMINISTRAÇÃO:

4.1.1. O mercado de tecnologia voltado para segurança da informação tem se direcionado basicamente para duas vertentes:

4.1.1.1. Solução 01 – Serviço continuado de inteligência cibernética, incluindo serviços gerenciados de ferramentas de segurança da informação, análise de incidentes cibernéticos e prevenção de eventos;

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

4.1.2. É habitual em ambos os cenários, a adoção de 2 (dois) ou mais fabricantes e/ou ferramentas na definição da solução para pleno atendimento ao objeto que a APF contratou.

4.1.3. Não foram localizados no mercado soluções aderentes ao que está se buscando nesta Análise de Viabilidade realizada pelo o TRE-ES, ou seja, nem contratações da Solução 01, nem as contratações da Solução 02, se enquadram à proposta que está prevista neste documento.

4.1.4. A proposta aqui prevista seria uma **Solução 03**, uma contratação envolvendo tanto segurança cibernética para rede interna e externa, com uso de inteligência artificial, respostas autônomas e *machine learning* não supervisionado, integrados com recursos de inteligência cibernética, fornecida como serviço e pagamento em parcela única.

4.1.5. Algumas contratações existentes, já licitadas pela APF podem atender parcialmente aos requisitos desejados, contudo, pela complexidade da solução aqui proposta, entendemos que será necessária a composição de ferramentas, que se devidamente integradas, poderão atender a solução que está desenhada nesta Análise de Viabilidade.

4.1.6. Foram identificados alguns órgãos que realizaram contratações cujo objeto apresenta similaridade com o que foi apresentado aqui e no item 2. Importante ressaltar que não foi encontrada nenhuma contratação que pudesse ser utilizada complemente para comparação e estimativa de custos.

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

4.1.8. Seguem abaixo algumas contratações identificadas na APF e os respectivos itens que poderão ser utilizados como referência para comparação de custos:

4.1.8.1. Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira – INEP

4.1.8.1.1. Nº pregão: 009/2017

4.1.8.1.2. UASG: 153978

4.1.8.1.3. Vigência: 12 meses

4.1.8.1.4. Valor contratado: R$4.524.800,00

4.1.8.1.5. Similar a solução 01, mas contemplando rol de serviços adicionais que vão além dos demandados pelo TRE-ES;

ITEM	DESCRIÇÃO	UNIDADE	QTD	VLR UNIT	VLR TOTAL	
1	SOLUÇÃO INTEGRADA DE SERVIÇOS GERENCIADOS DE SEGURANÇA	MÊS	12	R$340.900,00		R$4.090.800,00
2	SERVIÇOS TÉCNICOS EVOLUTIVOS	HORAS	2000	R$217,00		R$434.000,00

4.1.8.2. Tribunal de Contas da União - TCU

4.1.8.2.1. Nº pregão: 034/2017 2.1.4.2.2. UASG: 30001

4.1.8.2.3. Vigência: 60 meses

4.1.8.2.4. Valor contratado: R$10.000.000,00

4.1.8.2.5. Similar a solução 01, mas contemplando rol de serviços adicionais que vão além dos demandados pelo TRE-ES;

ITEM	DESCRIÇÃO	UNIDADE	QTD	VLR UNIT	VLR TOTAL

1	SOLUÇÃO INTEGRADA DE SERVIÇOS GERENCIADOS DE SEGURANÇA	MÊS	60	R$161.987,29	R$ 9.719.237,40
2	SERVIÇOS TÉCNICOS EVOLUTIVOS	HORAS	2000	R$109,34	R$ 218.680,00
3	TREINAMENTOS	TURMAS	1	R$62.039,21	R$62.039,21

4.1.8.3. Conselho da Justiça Federal – CJF

4.1.8.3.1. Nº pregão: 001/2020

4.1.8.3.2. UASG: 90026

4.1.8.3.3. Vigência: 24 meses

4.1.8.3.4. Valor contratado: R$3.602.025,36

4.1.8.3.5. Similar a solução 01, mas contemplando rol de serviços adicionais que vão além dos demandados pelo TRE-ES;

ITEM	DESCRIÇÃO	UNIDADE	QTD	VLR UNIT	VLR TOTAL
1	SOLUÇÃO INTEGRADA DE SERVIÇOS GERENCIADOS DE SEGURANÇA	MÊS	24	R$ 142.891,64	R$3.602.025,36

4.1.8.4. Supremo Tribunal Federal - STF

4.1.8.4.1. Nº pregão: 008/2023

4.1.8.4.2. UASG: 40001

4.1.8.4.3. Vigência: 12 meses

4.1.8.4.4. Valor contratado: R$3.522.999,92

4.1.8.4.5. Similar a solução 02, mas contemplando rol de serviços adicionais que vão além dos demandados pelo TRE-ES;

GRUPO	ITEM	DESCRIÇÃO	UNIDADE	QTDE	VLR UNITÁRIO	VLR TOTAL
1	1	Serviço de Operação e Atendimento a Requisições	MÊS	12	R$33.530,00	R$402.360,00
	2	Serviço de Gestão de Vulnerabilidades	SERVIÇO	4	R$41.348,00	R$165.392,00
	4	Serviço de Gestão de Incidentes de Segurança (CSIRT - Blue Team)	SERVIÇO	4	R$71.463,00	R$285.852,00
	5	Serviço de Testes de Invasão (Red Team)	SERVIÇO	4	R$21.042,00	R$84.168,00
	6	Serviço de Operação, Controle e Suporte à Infraestutura	MÊS	12	R$123.333,33	R$1.479.999,96
	7	Serviço de Análise de Inteligência em Ameaças Cibernéticas (CIT)	MÊS	12	R$29.583,33	R$354.999,96

4.1.8.5. Tribunal de Justiça do Estado do Rio de Janeiro - TJRJ

4.1.8.5.1. Nº pregão: 050/2022

4.1.8.5.2. UASG: 30100

4.1.8.5.3. Vigência: 24 meses

4.1.8.5.4. Valor contratado: R$45.608.000,00

4.1.8.5.5. Similar a solução 02, mas contemplando rol de serviços adicionais que vão além dos demandados pelo TRE-ES;

ITEM	DESCRIÇÃO	VALOR MENSAL ESTIMADO	Meses	VALOR TOTAL ESTIMADO (24 MESES)

3	SERVIÇO DE PRIVACIDADE E PROTEÇÃO DE DADOS	R$542.527,08	24	R$13.020.649,92
4	SERVIÇO DE GESTÃO DE SEGURANÇA DE ATIVOS	R$49.352,00	24	R$1.184.448,00
5	SERVIÇO DE GESTÃO DE INCIDENTES DE SEGURANÇA, VULNERABILIDADES E AMEAÇAS	R$1.031.846,24	24	R$24.764.309,76
7	SERVIÇO DE GESTÃO DE PROBLEMAS	R$69.481,53	24	R$1.667.556,72
12	SERVIÇO DE AUDITORIA E INVESTIGAÇÃO	R$60.560,67	24	R$1.453.456,08
13	SERVIÇO DE MELHORIAS	R$34.005,19	24	R$816.124,56

4.1.8.6. Banco da Amazonia - BASA

4.1.8.6.1. Nº pregão: 043/2021

4.1.8.6.2. UASG: 179007

4.1.8.6.3. Vigência: 36 meses

4.1.8.6.4. Valor contratado: R$11.636.999,44

4.1.8.6.5. Similar a solução 02, mas contemplando rol de serviços adicionais que estão aquém dos demandados pelo TRE-ES;

Item	Subitem	DESCRIÇÃO	QTD	UNIDADE	PREÇO UNITÁRIO	PREÇO TOTAL
1	1	Serviço de monitoramento de incidentes	36	mês	R$126.388,88	R$4.549.999,68
	2	Serviço de resposta a incidentes	36	mês	R$33.333,33	R$1.199.999,88
	3	Serviço de gestão de vulnerabilidades	36	mês	R$7.361,11	R$3.144.999,96
	4	Serviço de feeds de inteligência, detecção e proteção de ameaças direcionadas	36	mês	R$49.722,22	R$1.789.999,92
	5	Serviços técnicos especializados em segurança da informação - UST (sob demanda)	2000	UST	R$390,00	R$780.000,00
	6	Serviço de capacitação nos produtos e softwares utilizados para atender aos requisitos desta contratação (sob demanda) com carga horária de 24 horas	1	Turma c/ 15 participantes	R$80.000,00	R$80.000,00
	7	Serviço de capacitação em Security Analytics (sob demanda) com carga horária de 40 horas	1	Turma c/ 15 participantes	R$92.000,00	R$92.000,00

4.1.8.7. Instituto Brasileiro de Geografia e Estatística - IBGE

4.1.8.7.1. Nº pregão: 011/2021

4.1.8.7.2. UASG: 114637

4.1.8.7.3. Vigência: 24 meses

4.1.8.7.4. Valor contratado: R$3.229.999,68

4.1.8.7.5. Similar a solução 02, mas contemplando rol de serviços adicionais aquém dos demandados pelo TRE-ES;

Item	ESPECIFICAÇÃO DOS SERVIÇOS	QTDE	UNID	PREÇO UNITÁRIO	PREÇO TOTAL
1	Gestão de Riscos - Processo integrado envolvendo a Gestão de Vulnerabilidades, Gestão de Riscos, Compliance e Monitoração de Marca.	24	MÊS	R$59.583,33	R$1.429.999,92
2	Gestão de Incidentes - Processo integrado envolvendo a Análise de Incidentes Globais e o Monitoramento de Incidentes.	24	MÊS	R$45.833,33	R$1.099.999,92
3	Resposta aos Incidentes - Processo integrado envolvendo a prevenção, bloqueio e resposta aos incidentes, bem como a	24	MÊS	R$29.166,66	R$699.999,84

	análise de sua causa raiz.				

4.1.8.8. **TCERR**

017/2021 OPERAÇÃO ASSISTIDA

ITEM	DESCRIÇÃO	UNIDADE	QTD	VLR UNIT	VLR TOTAL
4	Serviço de Operação Assistida e consultoria especializada com bloco de 4 horas	horas	40	R$300,00	R$12.000,00

4.1.8.9. **TSE**

058/2021 OPERAÇÃO ASSISTIDA

ITEM	DESCRIÇÃO	UNIDADE	QTD	VLR UNIT	VLR TOTAL
29	Operação Assistida 10 dias úteis de 8h diárias	horas	80	R$271,49	R$21.719,20

4.1.8.10. **TCE-MT**

06/2020 OPERAÇÃO ASSISTIDA

ITEM	DESCRIÇÃO	UNIDADE	QTD	VLR UNIT	VLR TOTAL
29	Serviço de Operação Assistida	horas	2.112	R$397,72	R$869.760,00

4.1.8.11. **TELEBRAS**

007/2021 OPERAÇÃO ASSISTIDA

ITEM	DESCRIÇÃO	UNIDADE	QTD	VLR UNIT	VLR TOTAL
29	Operação Assistida por blocos de 8 dias corridos	horas	2.880	R$326,01	R$938.892,15

4.1.8.12. **TCU 034/2017**

ITEM	DESCRIÇÃO	UNIDADE	QTD	VLR UNIT	VLR TOTAL
3	TREINAMENTOS	TURMAS	1	R$62.039,21	R$62.039,21

4.1.8.13. **CNJ 036/2019**

ITEM	DESCRIÇÃO	UNIDADE	QTD	VLR UNIT	VLR TOTAL
3	TREINAMENTOS	TURMAS	1	R$20.050,00	R$20.050,00

4.1.9. **Solução Proposta** – Dentro da análise realizada nas contratações acima mencionadas, fica evidente a necessidade de levantamentos adicionais para a apuração mais refinada dos custos relacionados com a contratação pretendida, aqui nomeada como **(Solução 03)**.

4.1.10. A complexidade na análise das contratações da APF identificadas e já realizadas que podem ter alguma similaridade com a **Solução 03**, impede uma comparação mais assertiva, tanto das contratações aqui classificadas como **Solução 01** quanto aquelas consideradas como **Solução 02**, que possibilite o uso dos preços de alguns dos itens dessas contratações como referência para estimativa de custos da solução proposta.

4.1.11. De toda forma, mesmo assim os subitens do item 4.1.8, poderão ser utilizados como referência para auxiliarem na composição e definição de custos para Solução Proposta (Solução 03).

4.2. SOLUÇÕES EXISTENTES NO PORTAL DE SOFTWARE PÚBLICO BRASILEIRO (http://www.softwarepublico.gov.br):

4.2.1. Não foram identificadas soluções no Portal do Software Público Brasileiro capazes de atender plenamente as necessidades e requisitos desta contratação.

4.3. SOLUÇÕES DISPONÍVEIS NO MERCADO DE TIC, INCLUSIVE A EXISTÊNCIA DE SOFTWARE LIVRE OU SOFTWARE PÚBLICO:

4.3.1. Observância às políticas, premissas e especificações técnicas definidas no Modelo Nacional de Interoperabilidade (MNI) do Poder Judiciário:

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

4.3.2. Aderência às regulamentações da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), quando houver necessidade de utilização de certificação digital, observada a legislação sobre o assunto:

4.3.2.1. As alternativas de solução levantadas são capazes de fazer uso dos recursos tecnológicos disponíveis em certificados digitais, estando alinhadas à Infraestrutura de Chaves Públicas – ICP Brasil e em conformidade com a MP nº 2.200-2 – de 24 de agosto de 2001 - e demais arcabouços normativos aplicáveis a solução, instituídos pelo Instituto Nacional de Tecnologia da Informação (ITI).

4.3.3. Observância às orientações, premissas e especificações técnicas e funcionais definidas no Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário (Moreq-Jus):

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

4.4. Foram identificadas as seguintes soluções de mercado:

4.4.1. **TREND Micro** - a solução da Trend apresenta extenso portfólio de soluções de segurança, possuindo características de integração com diversas outras ferramentas do próprio fabricante. A solução é constituída de plataforma e diversas integrações, exemplo, *endpoint security, server security, cloud security, email security e network security*.

4.4.1.1. O *Trend Vision One*, aplica IA e a análise especializada mais eficaz aos dados de atividade coletadas de sensores nativos no ambiente para produzir menos alertas de maior fidelidade. A inteligência global de ameaças da Trend Micro, combinada com regras de detecção especializadas continuamente atualizadas por seus especialistas em ameaças maximizam o poder da IA e dos modelos analíticos de maneira incomparáveis.

4.4.1.2. A Trend Vision One é uma plataforma única que oferece suporte a integração com as seguintes tecnologias:

4.4.1.2.1. A solução de endpoint, gera uma gravação do comportamento do sistema e dos eventos que ocorrem nos níveis do usuário e do kernel. Para obter esse tipo de análise o serviço utiliza de agente e ferramentas de proteção de endpoint.

4.4.1.2.2. A solução de network, utiliza tecnologias de inspeção profunda no tráfego da rede. A inspeção é uma solução de dispositivo de rede que monitora portas e protocolos de rede, tentando detectar ameaças avançadas ou ataques direcionados que se movem lateralmente pela rede, bem como dentro e fora da rede.

4.4.1.2.3. Compondo com ferramentas de mensagens a solução protege os e-mails evitando o escalonamento e técnicas de phishing. Além de proteger recursos de e-mail, essa composição de ferramentas, oferece proteção avançada contra ameaças e ajuda a proteger o compartilhamento de arquivos e e-mails de serviços como Gmail, Dropbox, entre outros.

4.4.1.2.4. As ferramentas juntas, formam uma solução de proteção onde possuem itens de:

- Detecção;
- Investigação;
- Resposta;
- Relatório.

4.4.1.3. Vantagens:

4.4.1.3.1. O Trend Vision One analisa dados de atividades coletados por sensores para fornecer detecções e alertas inteligentes e de alta fidelidade.

4.4.1.3.2. A plataforma obtém uma visão geral dos aplicativos e recursos disponíveis do Trend Vision One e personaliza a barra de menus.

4.4.1.3.3. Visualiza as informações da sua conta, altera a senha da sua conta e redefine seu dispositivo de autenticação de dois fatores.

4.4.1.3.4. Visualiza o ID de sua empresa e atualiza as suas informações.

4.4.1.3.5. Utiliza script de demonstração para simular ataques.

4.4.1.3.6. Solução de segurança é bem difundida no mercado corporativo e conhecido por defender grandes empresas e seus sistemas, além de seus dados de ameaças sofisticadas. A detecção de rede, sandbox personalizado, compartilhamento de inteligência de ameaças e outras funcionalidades avançadas estão incluídas no software.

4.4.1.3.7. Ele é altamente eficiente na detecção e análise de malware avançado e ataques direcionados. Além disso, a plataforma é conhecida por sua simplicidade de operação, durabilidade e excelente suporte ao cliente.

4.4.1.3.8. Possui visibilidade em toda a rede, fornecendo uma visão completa, permitindo que os usuários detectem e avaliem possíveis violações de segurança numa única interface. Oferece ainda um gerenciamento centralizado, permitindo que lidemos com políticas de segurança e alertas em vários pontos e locais a partir de um único console. Isso simplifica a gerência em toda a organização, tornando-a capaz de responder rapidamente.

4.4.1.4. Desvantagens:

4.4.1.4.1. Consumo de memória, espaço e muitos recursos da infraestrutura tecnológica, causando problemas de desempenho para os demais sistemas que estão sendo executados na mesma plataforma.

4.4.1.4.2. A precificação é baseada na compra de sensores, que têm custos variados com base no dimensionamento da infraestrutura de rede. Além disso a licença de entrada de telemetria para ingestão de NDR está disponível por um custo adicional, tornando assim a alternativa mais onerosa.

4.4.1.4.3. A configuração, pode se tornar extremamente complexa em função das integrações.

4.4.1.4.4. A solução não contempla funcionalidades de inteligência cibernética.

4.4.2. **DARKTRACE** – a solução é constituída de 3 grandes pilares:

4.4.2.1. **Enterprise Imunne System:**

4.4.2.1.1. Sua principal característica é a Detecção por autoaprendizagem – sem regras ou referências físicas.

4.4.2.1.2. Ele aproveita o machine learning não supervisionado, o que significa que aprende na prática, sem qualquer conhecimento anterior ou dados de treinamento.

4.4.2.1.3. A aprendizagem não supervisionada é exclusiva e permite que seja detectado algo que não corresponda ao "se" e que não foi observado antes – seja uma ameaça interna, um ataque externo, ou simplesmente uma configuração incorreta não conhecida que precise ser corrigida

4.4.2.2. **Cyber AI Analyst - Sua principal característica é a Investigação automatizada.**

4.4.2.2.1. O Cyber AI Analyst analisa as alertas, reúne-os, mostra para o usuário a fase do ataque e até mesmo sugere quais ações precisam ser tomadas.

4.4.2.2.2. Reduz o tempo de triagem em até 92%, possibilitando a geração de relatórios de maneira automática. Com isso a equipe de segurança cibernética pode concentrar seu tempo em tarefas mais relevantes.

4.4.2.2.3. Foi construído aprendendo como os analistas humanos investigam, fazem a triagem e relatam ameaças. Portanto, em vez de receber 20 alertas, a equipe visualiza os dois incidentes de segurança pós-triagem que realmente interessam. Esta funcionalidade pode usar o processamento de linguagem natural para explicar isso em um relatório que qualquer pessoa é capaz de entender.

4.4.2.3. **Antigena - Sua principal característica é a Resposta Autônoma.**

4.4.2.3.1. Esta funcionalidade toma medidas com grande precisão para impedir a propagação de ataques em andamento. Ela funciona com extrema velocidade, e a parte mais importante aqui é a tomada de decisão – no cérebro da IA, que toma a decisão sobre quando e em quais cenários as ações devem ser tomadas.

4.4.2.3.2. Antigena faz continuamente julgamentos sobre a melhor forma de conter a ameaça, minimizando qualquer impacto nas atividades digitais e permitindo que as operações continuem normalmente.

4.4.2.4. **Vantagens**

4.4.2.4.1. Utilização de ferramenta de Inteligência Artificial (IA) reduz a participação humana e cria as condições de agilidade e eficiência para que os poucos recursos humanos envolvidos possam participar efetivamente do que se faz necessário no combate às ameaças cibernéticas;

4.4.2.4.2. Módulos de resposta autônoma voltados para ambientes Office365 e Google WorkSpace.

4.4.2.4.3. Não há necessidade de instalação de agentes em equipamentos servidores e desktops.

4.4.2.4.4. Equipamentos appliance tanto físicos quanto virtuais, permitindo se adequar a qualquer tipo de tamanho de infraestrutura;

4.4.2.4.5. Formato de licenciamento OnPremisse, Cloud ou híbrida;

4.4.2.4.6. Possibilidade de notificações proativas de atividades de ameaças 24x7 por intermédio do SOC especializado da DarkTrace;

4.4.2.4.7. Automatiza as investigações de ameaças com velocidade e abrangência, reduzindo em até 92% o tempo de triagem.

4.4.2.4.8. DarkTrace trabalha com o conceito de Open API que permite facilmente a integração com outras ferramentas de segurança, tais como:

- SIEM e SOAR;
- Soluções de ITSM;
- Firewalls, NACLs & Preventative Controls;
- VPN & Zero-Trust Technologies;
- Endpoints
- Asset / Inventory Management

4.4.2.4.9. Possui tecnologia capaz de disparar respostas a incidentes via Mobile App;

4.4.2.4.10. Uma única solução consegue orquestrar, por intermédio de integração via API, com diversas tecnologias de segurança existentes no âmbito dos tribunais.

4.4.2.4.11. No contexto do estudo realizado pelo Gartner PeerInsights a solução recebeu nota 4,6 onde o máximo era 5,0, com 141 avaliações.

4.4.2.5. **Desvantagens**

4.4.2.5.1. A solução não contempla funcionalidades de inteligência cibernética.

4.4.3. **CISCO STEALWATCH:** A solução Cisco Stealwatch oferece duas opções de implantação:

4.4.3.1. Stealthwatch Enterprise - coleta, armazena e analisa informações no ambiente do cliente; e

4.4.3.2. Stealthwatch Cloud - é uma oferta SaaS. Ele pode monitorar a rede privada de um cliente ou um ambiente de nuvem pública (através de integrações com AWS, Azure ou Google Cloud Platform).

4.4.3.3. O Cisco Stealthwatch é composto pelos seguintes componentes:

4.4.3.3.1. StealthWatch Management Console (SMC)

4.4.3.3.2. Flow Sensor (FS)

4.4.3.3.3. Flow Collector (FC)

4.4.3.3.4. UDP Directory (UDPD)

4.4.3.3.5. Flow Replicator (optional)

4.4.3.4. O Stealthwatch detecta tráfego suspeito principalmente analisando registros do NetFlow, IPFIX ou sFlow.

4.4.3.5. Stealthwatch usa várias técnicas analíticas para detectar tráfego suspeito, incluindo aprendizado de máquina supervisionado, aprendizado de máquina não supervisionado e alguns algoritmos de aprendizagem profunda.

4.4.3.6. A solução não descriptografa o tráfego TLS. O Stealthwatch usa a funcionalidade ETA (Encrypted Traffic Analysis, análise de tráfego criptografado) da Cisco para analisar o tráfego do TLS sem descriptografá-lo.

4.4.3.7. O Stealthwatch fornece informações históricas para permitir que um analista de segurança responda manualmente a incidentes. Ele também permite respostas automatizadas por meio da integração com o ISE (Identity Services Engine, mecanismo de serviços de identidade) da Cisco. Alarmes e eventos do Stealthwatch podem ser compartilhados com a plataforma SecureX da Cisco, onde as respostas podem ser automatizadas através de cartilhas SecureX.

4.4.3.8. Stealthwatch é vendido como uma assinatura com base nos fluxos necessários por segundo, contagem de dispositivos de rede ou fluxos mensais totais.

4.4.3.9. Vantagens

4.4.3.9.1. - Maior competitividade na licitação.

4.4.3.9.2. - No contexto do estudo realizado pelo Gartner PeerInsights a solução recebeu nota 4,8 onde o máximo era 5,0, com 16 avaliações.

4.4.3.10. Desvantagens

4.4.3.10.1. - A solução não é integrada, exigindo a adoção de todos os módulos, não possuindo recursos nativos de IA nem recursos de resposta autônoma. Fica a impressão de que a CISCO adquiriu tecnologias, mas não integrou, apenas transformou em recursos a parte, criando um cenário conturbado para sua instalação e configuração.

4.4.3.10.2. - Compatibilidade limitada com outros fabricantes, buscando direcionar o comprador para soluções proprietárias CISCO.

4.4.3.10.3. - O modelo de licenciamento é complexo, e passível de erros, como pode ser verificado em https://ciscolicense.com/lic/cat/security/stealthwatch/.

4.4.3.10.4. A solução não contempla funcionalidades de inteligência cibernética.

4.4.4. **EXTRAHOP:** O ExtraHop oferece Reveal(x) como uma solução de aparelhos de autoatendimento ou IaaS, ou como SaaS hospedado na nuvem**.** Reveal(x) sensores extraem metadados enriquecidos para alimentar múltiplos mecanismos de análise e construir eventos de segurança correlacionados.

4.4.4.1. O ExtraHop também oferece captura de pacote completo ou captura de pacotes acionados por eventos.

4.4.4.2. Os usuários podem detalhar os metadados sumários nos pacotes brutos, pois o Reveal(x) permite filtrar e baixar apenas a gama de pacotes necessários.

4.4.4.3. Reveal(x) pode descriptografar o tráfego TLS, se tiver acesso às chaves secretas do servidor ou à chave de sessão simétrica, e se baseia em impressões digitais JA3 e outras técnicas de análise de tráfego quando a descriptografia não é uma opção.

4.4.4.4. Os recursos de detecção do ExtraHop aproveitam uma combinação de técnicas, incluindo controles baseados em regras e reputação, mas também combinam aprendizado de máquina supervisionado e não supervisionado para detectar anomalias e desvio de comportamentos normais da rede.

4.4.4.5. O ExtraHop optou por se integrar com a bilheteria, SIEM e SOAR para orquestração automatizada e com firewalls ou soluções de proteção de ponto final para resposta automatizada.

4.4.4.6. Reveal(x) é precificado como um conjunto de assinaturas, que depende do número de pontos finais, e os chamados "ativos críticos" combinados com níveis de largura de banda. Recursos adicionais, como captura de pacotes completos e aparelhos físicos, têm preços separados.

4.4.4.7. Vantagens

4.4.4.7.1. Maior competitividade na licitação, possível redução de custo.

4.4.4.7.2. No contexto do estudo realizado pelo Gartner PeerInsights a solução recebeu nota 4,8 onde o máximo era 5,0, com 75 avaliações.

4.4.4.8. Desvantagens

4.4.4.8.1. A solução se prende a regras e reputação, criando condições limitadas de proteção para os casos de ameaças desconhecidas.

4.4.4.8.2. A solução não contempla funcionalidades de inteligência cibernética.

4.4.5. **DIGITAL – solução de inteligência cibernética -** Sua principal ferramenta se chama Digital Shadows SearchLights.

4.4.5.1. O Searchlight compreende quatro fases principais (coleta, análise, inteligência e implantação). Este é um processo iterativo e as organizações irão continuamente voltar para refinar ainda mais e adicionar aos seus principais ativos. Crucialmente, em cada fase, atua como uma extensão da equipe para ajudar a configurar o Searchlight, coletar de fontes difíceis de alcançar, adicionar análise de inteligência de ameaça, e fornecer playbooks para remediar o risco.

4.4.5.2. Vantagens:

4.4.5.2.1. Monitoramento de fontes abertas publicamente disponíveis;

4.4.5.2.2. Coleta de dados de fontes relacionadas ao ciberespaço (por exemplo, CERTs, CVE DBs);

4.4.5.2.3. Integração com soluções de segurança existentes (Por exemplo, firewall's)

4.4.5.3. Desvantagens:

4.4.5.3.1. Não possui integração de repositórios únicos e indisponíveis

4.4.5.3.2. Não possui opção de implantação na infraestrutura do órgão, somente em ambiente cloud;

4.4.6. **INTSIGHTS** – solução de inteligência cibernética

4.4.6.1. São compostas de duas ferramentas: Threat Command e Threat Intelligence Platform.

4.4.6.1.1. O Intsights Threat Command retira a complexidade da inteligência de ameaças e oferece valor instantâneo sem o pesado aumento das soluções tradicionais de inteligência de ameaças, descobrindo continuamente as ameaças críticas direcionadas à sua empresa, e mapear essa inteligência para seus ativos digitais e vulnerabilidades exclusivos. Você se beneficiará de informações de ameaça adequadas e relevantes que minimizam a exposição à sua marca, reduzindo significativamente a carga de trabalho em suas equipes de segurança.

4.4.6.1.2. Com a Plataforma de Inteligência de Ameaças Intsights (TIP), você pode automatizar todo o seu ciclo de vida de inteligência de ameaças - desde coleta de dados, processamento, análise e enriquecimento até a colaboração e disseminação. Ao centralizar a coleta, o gerenciamento e a integração de dezenas de fontes de inteligência de ameaças no ambiente operacional, suas equipes de segurança podem simplificar a investigação e bloquear proativamente as ameaças.

4.4.6.2. Vantagens:

4.4.6.2.1. Monitoramento de fontes abertas publicamente disponíveis;

4.4.6.2.2. Identificação e análise de agentes de ameaças;

4.4.6.2.3. Remoção de sites ilegítimos e contas de mídia social;

4.4.6.3. Desvantagens:

4.4.6.3.1. Não apura dados de IOC (indicadores de comprometimento), indicadores técnicos e análise de malware;

4.4.6.3.2. Não possui integração de inteligência de ameaças com dados históricos;

4.4.6.3.3. Não possui opção de implantação na infraestrutura interna do Tribunal, somente em ambiente cloud;

4.4.7. **KELA** – solução de inteligência cibernética

4.4.7.1.1. Sua principal ferramenta se chama DarkBeast - fornece respostas a incidentes, caçadores de ameaças, investigadores e analistas de inteligência com uma tecnologia robusta para mergulhar no submundo do crime cibernético e investigar através do Data Lake DarkWeb da KELA, com visibilidade das operações obscuras e ficando à frente dos atacantes, mantendo o anonimato e cumprindo quaisquer restrições de segurança.

4.4.7.2. Vantagens:

4.4.7.2.1. Painel personalizado com cenário de ameaças no Tribunal;

4.4.7.2.2. Relatórios e alertas de inteligência direcionados e específicos para o Tribunal;

4.4.7.2.3. Fornecimento de dados de ameaças no formulário STIX/TAXII;

4.4.7.3. Desvantagens:

4.4.7.3.1. Não possui monitoramento de fontes abertas publicamente disponíveis;

4.4.7.3.2. Não realiza coleta de dados de fontes relacionadas ao ciberespaço (por exemplo, CERTs, CVE DBs);

4.4.7.3.3. Remoção de sites ilegítimos e contas de mídia social.

4.4.8. A análise de viabilidade da contratação foi realizada pela equipe técnica do TRE-DF, que esteve reunida com os principais fabricantes das soluções analisadas (CISCO, TREND Micro, HILLSTONE, DARKTRACE), com o objetivo de os fabricantes apresentarem suas necessidades retratadas nesta análise, bem como apresentação de críticas da solução ora proposta. Restou claro para equipe de planejamento da contratação que todos os fabricantes presentes estão plenamente cientes quanto aos requisitos estabelecidos e ao pleno atendimento deles, bem como estão cientes também da necessidade de composições tecnológicas, que deverão adotar junto a seus parceiros, com base nas estratégicas comerciais a serem definidas por cada um deles.

4.4.8.1. Durante as reuniões também foi solicitado a todos os fabricantes que apresentassem considerações às especificações técnicas definidas, e até o momento da finalização da versão desta análise, somente o fabricante CISCO apresentou suas considerações, que foram plenamente analisadas e apresentadas aos representantes da fabricante, em outra agenda, e destas considerações, várias foram apreciadas.

4.4.8.2. Outra solicitação feita nas reuniões foi a indicação das empresas parceiras, para que pudéssemos consultá-las para estimativa de custos, e até o momento da finalização da versão desta análise, as fabricantes CISCO, TRENDMICRO e DARKTRACE enviaram essas informações.

5. INDICAÇÃO DA STIC ESCOLHIDA

5.1. DESCRIÇÃO DA SOLUÇÃO

5.1.1. Contratação de solução de segurança cibernética incluindo licenças de uso de software, equipamentos, garantia e manutenção, instalação, treinamento e suporte técnico especializado, nos termos dos requisitos listados no item 1.2 deste Estudo Preliminar.
5.1.2. Todos os itens abaixo irão compor o objeto e deverão atender às especificações definidas nos requisitos técnicos deste Estudo Preliminar, de acordo com os quantitativos abaixo:

Grupo	Item	Descrição	Unidade	Qtde
1	1	Solução – Licenças de uso de software e hardware, no formato de subscrição, com garantia técnica e manutenção de 24 (vinte e quatro) meses	Unidade	01
	2	Instalação da solução	Unidade	01
	3	Serviço de Operação Assistida em bloco de 4 horas	Bloco	50
	4	Treinamento	Pessoas	05

5.1.3. Para o correto dimensionamento da solução está sendo considerada a seguinte infraestrutura do TRE-ES:

TRIBUNAL REGIONAL ELEITORAL DO ESPÍRITO SANTO	
Ativo	Quantic
Dispositivos de rede: LAN, WAN, WI-FI, Firewalls, IPS, Balanceadores de Carga, Antispam	140
Servidores: hipervisor Acropolis/Nutanix, VMs, Windows e Linux	160
Instâncias de banco de dados Oracle, PostgreSQL	17
Instâncias de aplicações/serviços corporativos/senhas hardcode	70
Desktops	1337
Total	1724

5.2. JUSTIFICATIVA/MOTIVAÇÃO DA ESCOLHA

5.2.1. Conforme explicado no item 4.1.6, as soluções citadas tanto no item 4.1.1.1 quanto no item 4.1.1.2 apresentam contratações realizadas no âmbito da Administração Pública Federal identificadas durante a pesquisa nos portais de compras públicas, com características e condições comerciais diversas.

5.2.1.1. A melhor solução é uma contratação envolvendo tanto segurança cibernética para rede interna e externa, com uso de inteligência artificial, respostas autônomas e *machine learning* não supervisionado, integrados com recursos de inteligência cibernética. Isso reduz a necessidade de contratação de mão de obra, e oferece uma solução robusta e autônoma para auxiliar na identificação e tratamento de ameaças cibernéticas.

5.2.1.2. Considerando o reduzido tamanho da unidade responsável pela segurança cibernética do TRE-ES, a contratação de uma ferramenta que auxilie na identificação de ameaças, sem implicar em diversos alertas de falsos positivos a serem tratados pelas pessoas da unidade, permite maior eficiência e eficácia na identificação e tratamento de ameaças à segurança cibernética.

5.3. ESTIMATIVA DE CUSTO

5.3.1. Com base nos exemplos de contratação similares, constam junto a cada contratação o valor contratado, que servirão como apoio para estimativa dos preços.

Item	Descrição	Unidade	Quantidade	Valor Unitário	Valor Total
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	R$ 3.590.000,00	R$ 3.590.000,00
2	Serviço de Ativação da Solução	Unidade	**1**	R$ 74.000,00	R$ 74.000,00
3	Serviço de Operação Assistida	Blocos de 4h	**50**	R$590,00	R$ 29.500,00
4	Treinamento (por pessoa)	Alunos	**5**	R$22.520,00	R$ 112.600,00
VALOR TOTAL					R$ 3.806.100,00

Fonte: Pregão eletrônico 08/2023, TRE-DF.

5.4. ADERÊNCIA AOS REQUISITOS

5.4.1. Esta contratação está em consonância com os seguintes instrumentos:

5.4.1.1. PLANEJAMENTO ESTRATÉGICO DO PODER JUDICIÁRIO – ENTIC / JUD 2021 A 2026:

5.4.1.1.1. Dentre os objetivos da Resolução 370/2021 CNJ, pode-se destacar:

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

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

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

5.4.1.2.1. Para elevar o nível de segurança das infraestruturas críticas, deve-se (Art.11):

I – Estabelecer todas as ações que possibilitem maior eficiência, ou seja, capacidade de responder de forma satisfatória a incidentes de segurança, permitindo a contínua prestação dos serviços essenciais a cada órgão;

...

IV – Utilizar tecnologia que possibilite a análise consolidada dos registros de auditorias coletados em diversas fontes de ativos de informação e de ações de usuários, permitindo automatizar ações de segurança e oferecer inteligência à análise de eventos de segurança; V – Utilizar tecnologia que permita a inteligência em ameaças cibernéticas em redes de informação; especialmente em fóruns, inclusive da iniciativa privada e comunidades virtuais da internet;

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

5.4.1.3.1. Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ), onde podemos destacar a aderência deste estudo preliminar 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.

5.4.1.3.2. Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário (PGCRC-PJ); e

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

5.4.1.3.4. Manual de Proteção de Infraestruturas Críticas de TIC;

5.4.1.3.5. Manual de Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital;

5.4.1.4. PLANEJAMENTO ESTRATÉGICO DO TRIBUNAL SUPERIOR ELEITORAL 2021-2026

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

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

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

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

5.4.1.5. PLANEJAMENTO ESTRATÉGICO INSTITUCIONAL DO TRE-ES (PEI):

5.4.1.5.1. MD 9: Fortalecimento da Estratégica Nacional de TIC e de Proteção dos Dados.

5.4.1.6. PLANO DIRETOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO – 2021/2026:

5.4.1.6.1. P6: Garantia da Segurança em TIC.

5.4.1.6.2. P7: Garantia da Melhoria Contínua da infraestrutura de TIC.

5.4.1.6.3. P6: D3: Garantir a disponibilidade, integridade e confidencialidade da informação.

5.4.1.6.4. P6: D5: Promover a melhoria dos sistemas de informação.

5.5. RELAÇÃO ENTRE DEMANDA PREVISTA E A STIC

5.5.1. A solução contratada deverá atender aos parâmetros listados abaixo e representa exatamente o quantitativo que se pretende contratar:

Grupo	Item	Descrição	Unidade	Qtde
1	1	Solução – Licenças de uso de software e hardware, no formato de subscrição, com garantia técnica e manutenção de 24 (vinte e quatro) meses	Mês	24
	2	Instalação da solução	Unidade	01
	3	Serviço de Operação Assistida em bloco de 4 horas	Bloco	50
	4	Treinamento	Turma	01

5.5.2. As licenças de uso de softwares e suas funcionalidades, bem como os equipamentos que compõem a subscrição da solução deverão ser dimensionados para atender ao que está determinado nos itens 3.1, 3.2, 3.3, 3.4 e 3.5 deste estudo preliminar, contemplando garantia e manutenção e instalação e configuração;

5.5.3. Serviço de Operação Assistida, sob demanda, durante a vigência contratual, como descrito no item 2.7 deste estudo preliminar.

5.5.4. Treinamento para servidores do TRE-ES, conforme descrito no item 2.2.1 deste estudo preliminar.

5.6 COMPOSIÇÃO DE BENS/SERVIÇOS DA SOLUÇÃO

Serviço. Software como serviço. Licenças de uso por período determinado, na infraestrutura local ou na nuvem.

6. PARCELAMENTO DO OBJETO

6.1. No contexto da solução apontada pela equipe de planejamento da contratação e de acordo com as necessidades e requisitos levantados no item 1.1 deste Estudo Preliminar, recomenda-se que o objeto seja dividido nos itens a seguir:

Grupo	Item	Descrição	Unidade	Quantidade
1	1	Solução – Licenças de uso de software e hardware, no formato de subscrição, com garantia técnica e manutenção de 24 (vinte e quatro) meses	Mês	24
	2	Serviço de Ativação da Solução	Unidade	01
	3	Serviço de Operação Assistida em bloco de 4 horas	Blocos	50
	4	Treinamento	Turma	01

6.2. Assim, fica clara a correspondência dos itens do objeto com as necessidades e requisitos listados no tópico 2 deste Estudo Preliminar. Cabe ressaltar, ainda, 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.

6.3 O Tribunal Regional Eleitoral do Espírito Santo optou por agrupar os serviços em lote único, para fins de licitação, uma vez que as melhores práticas de gestão em TI se baseiam na integração desses serviços e softwares, que são indissociáveis e apresentam inter-relação entre si, de forma que assegurem o alinhamento e a coerência em termos de qualidade técnica, resultando assim, no perfeito atendimento aos princípios da celeridade, economicidade e eficiência.

6.4. Somente a execução de forma integrada dos serviços licitados garantem a disponibilidade, segurança e a preservação dos dados de execução, evitando transferência de responsabilidades, nos casos de eventuais problemas/invasões ou paralisação dos sistemas causados por serviços prestados por mais de uma empresa contratada.

6.5. O agrupamento do objeto em lote único se torna viável, pelos seguintes aspectos:

6.5.1. Modelo amplamente utilizado para as contratações de objeto análogo;

6.5.2. A simplificação da condução das atividades de gestão, fiscalização e controle do contrato;

6.5.3. A minimização de potenciais conflitos internos entre diferentes prestadores de serviços; e

6.5.4. O atingimento de níveis de desempenho em razão da continuidade da prestação que garantam de forma global a qualidade dos serviços executados, o que não se verifica na divisão dessas atividades.

6.6. É importante também, se observar o posicionamento do Egrégio Tribunal de Contas da União sob a matéria:

6.6.1. 15. Acerca da alegada possibilidade de fragmentação do objeto, vale notar que nos termos do art. 23, § 1º, da Lei n. 8.666/1993, exige-se o parcelamento do objeto licitado sempre que isso se mostre técnica e economicamente viável. A respeito da matéria, esta Corte de Contas já editou a Súmula n. 247/2004, verbis: "É obrigatória a admissão da adjudicação por item e não por preço global, nos editais das licitações para a contratação de obras, serviços,

compras e alienações, cujo objeto seja divisível, desde que não haja prejuízo para o conjunto ou complexo ou perda de economia de escala, tendo em vista o objetivo de propiciar a ampla participação de licitantes...” (grifos não constam do original).

6.6.2. 16. Depreende-se, portanto, que a divisão do objeto deverá ser implementada sempre que houver viabilidade técnica e econômica para a sua adoção.

6.6.3. 17. Nesse ponto, calha trazer à baila o escólio de Marçal Justen Filho: “O fracionamento em lotes deve respeitar a integridade qualitativa do objeto a ser executado. Não é possível desnaturar um certo objeto, fragmentando-o em contratações diversas e que importam o risco de impossibilidade de execução satisfatória.” (Comentários à Lei de Licitações e Contratos Administrativos. 10. ed. São Paulo: Dialética, 2004. p. 209).

6.4. Portanto, em virtude da singularidade do objeto deste Estudo Preliminar, pode-se afirmar ser tecnicamente inadequado o seu desmembramento, sob pena de não se atender o objetivo buscado pelo TRE-ES no sentido de fortalecer a gestão da segurança dos ativos de TI do Tribunal contra ataques e desordens cibernéticas de toda ordem interna e externa. Sob o ponto de vista econômico, não há elementos nos autos que permitam concluir que a adoção do parcelamento do objeto, seria, no caso concreto, mais vantajosa para o TRE-ES.

7. INDICAÇÃO DA NECESSIDADE DE ADEQUAÇÃO AMBIENTAL

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

ANÁLISE DE RISCOS

8. IDENTIFICAÇÃO DOS RISCOS

8.1. IDENTIFICAÇÃO DOS RISCOS DE DEPENDÊNCIA TECNOLOGICA

8.1.1. Os serviços objeto desta contratação são considerados essenciais e de natureza contínua, pois devem ser realizados ininterruptamente, e sua paralisação acarretará suspensão ou o comprometimento das atividades prestadas pelos servidores e colaboradores do TRE-ES.

8.1.2. A descontinuidade da prestação do serviço poderá afetar a disponibilização de sistemas providos pelo TRE-ES como uma insegurança em relação a rede da justiça eleitoral.

8.1.3. Havendo uma descontinuidade e em momento crítico, o TRE-ES poderá proceder contratação imediata nos moldes permitidos nas Leis nº 8.666/93 e 14.133/2021.

9. RELAÇÃO DOS RISCOS E AÇÕES DE MITIGAÇÃO

9.1. ANÁLISE DOS RISCOS

1. Probabilidade e impacto, ações de prevenção/contingência, responsáveis. Incluídos nas tabelas abaixo.

RISCO 1	Contratada falha com a execução, implicando inexecução parcial ou total	
Probabilidade (Alta, média ou baixa)	BAixa	
	Efeito (Dano)	*Impacto
1	Não realização das atividades de monitoramento e investigação cibernética	Alto
2		
3		
	Ações de Mitigação e Contingência	Responsável
1	Realizar nova contratação	Equipe de Planejamento da Contratação
2	Aplicação de Sanções	Equipe de Fiscalização da Contratação
3		

*Impacto (Baixo, Médio ou Alto)

RISCO 2	Má qualidade na prestação do serviço de suporte técnico	
Probabilidade (Alta, média ou baixa)	Medio	
	Efeito (Dano)	*Impacto
1	CONTRATADA não atende os chamados de suporte técnico de acordo com o especificado	Medio
2		
3		
	Ações de Mitigação e Contingência	Responsável
1	Reunião com empresa e controle das ações, conforme o contrato	Equipe de Fiscalização da Contratação
2	Aplicação de Sanções	Equipe de Fiscalização da Contratação
3		

*Impacto (Baixo, Médio ou Alto)

RISCO 3	Falta de recursos orçamentários para a concretização da licitação	
Probabilidade (Alta, média ou baixa)	Baixo	
	Efeito (Dano)	*Impacto
1	Não realização das atividades de monitoramento e investigação cibernética	Alto
2		
3		
	Ações de Mitigação e Contingência	Responsável
1	Atuar junto aos setores técnicos responsáveis pela gestão orçamentária ressaltando a importância da contratação	Equipe de Planejamento da Contratação
2	Realizar pregão no próximo período orçamentário	SAO
3		

*Impacto (Baixo, Médio ou Alto)

RISCO 4	Não concretização da licitação por impugnação ao edita	
Probabilidade (Alta, média ou baixa)	Baixo	
	Efeito (Dano)	*Impacto
1	Não realização das atividades de monitoramento e investigação cibernética	Alto
2		
3		
	Ações de Mitigação e Contingência	Responsável
1	Realizar as correções no Termo de Referência	Equipe de Planejamento da Contratação
2	Realizar novo pregão	SAO
3		

*Impacto (Baixo, Médio ou Alto)

RISCO 5	Incapacidade de execução do contrato	
Probabilidade (Alta, média ou baixa)	Baixo	
	Efeito (Dano)	*Impacto
1	Equipamentos com falha ou com necessidade de adaptações de hardware	Alto
2	Descumprimento sistemático do contrato.	Alto
3	Equipamentos com qualidade inferior à exigida ou não compatíveis com o legado do TREES	Alto
	Ações de Mitigação e Contingência	Responsável
1	Verificar se a empresa apresentou alguma inexecução em outros órgãos governamentais.	Equipe de Planejamento da Contratação
2	Acompanhamento e verificação de qualidade dos equipamentos, instalação e disponibilização	Equipe de Fiscalização da Contratação
3	Aplicação das sanções cabíveis.	Equipe de Fiscalização da Contratação

*Impacto (Baixo, Médio ou Alto)

RISCO 6	Tempo para atendimento de resolução de problemas insatisfatório.	
Probabilidade (Alta, média ou baixa)	Média	
	Efeito (Dano)	*Impacto
1	Comprometimento dos serviços prestados pelo TRE-ES aos usuários.	Médio
2		
3		
	Ações de Mitigação e Contingência	Responsável
1	Acompanhamento a execução do contrato e atuação proativa dos fiscais.	Equipe de Fiscalização da Contratação
2	Aplicar sanções previstas no contrato. Fazer reuniões com a empresa fornecedora do serviço	Equipe de Fiscalização da Contratação
3		

*Impacto (Baixo, Médio ou Alto)

ANÁLISE DE SUSTENTAÇÃO DO CONTRATO

10. RECURSOS MATERIAIS E HUMANOS

10.1. Em relação aos recursos humanos, o objeto a ser contratado não impõe necessidades especiais de pessoal, além dos já disponíveis no TRE-ES.

10.2. Os recursos materiais necessários para o pleno funcionamento da solução pretendida deverão ser fornecidos pela CONTRATADA, conforme item 3.5 deste Estudo Preliminar

11. DESCONTINUIDADE DO FORNECIMENTO

11.1. Os serviços objeto desta contratação são considerados essenciais e de natureza contínua, pois devem ser realizados ininterruptamente, e sua paralisação acarretará suspensão ou o comprometimento das atividades prestadas pelos servidores e colaboradores do TRE-ES.

11.2. A descontinuidade da prestação do serviço poderá afetar a disponibilização de sistemas providos pelo TRE-ES como uma insegurança em relação a rede da justiça eleitoral.

11.3. Havendo uma descontinuidade e em momento crítico, o TRE-ES poderá proceder contratação imediata nos moldes permitidos nas Leis nº 8.666/93 e 14.133/2021.

11.4. TRANSIÇÃO CONTRATUAL

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

11.4.2. Ao final do contrato de prestação dos serviços, a empresa contratada deverá fornecer, pelo período de 60 (sessenta) dias corridos, todas as informações necessárias à transição para a empresa sucessora à prestação dos serviços, além de elaborar e atualizar toda a documentação que por ventura não tenha sido devidamente gerada ou atualizada durante o período de vigência do contrato.

11.4.3. A empresa contratada deverá responsabilizar-se pela transição inicial e final dos serviços, absorvendo as atividades de forma a documentá-las minuciosamente para que os repasses de informações, conhecimentos e procedimentos, no final dos contratos, aconteçam de forma precisa e responsável.

12. CONTRATAÇÕES SIMILARES

EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO (Portaria DG nº151, 0935680)

Integrante Demandante: SANDRO MERÇON DA SILVA (substituto: OLGA BAYERL VITA)

Integrante Técnico: OLGA BAYERL VITA (substituto: LUCAS RIBEIRO CARLIN)

Integrante Administrativo: MARCOS VENTUROTT FERREIRA (substituto: CARLOS ALBERTO DA ROCHA PADUA FILHO)

Vitória, 19 de abril de 2023.

Documento assinado eletronicamente por **MARCOS VENTUROTT FERREIRA**, **Integrante Administrativo**, em 19/12/2023, às 17:06, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **OLGA BAYERL VITA**, **Integrante Técnico**, em 19/12/2023, às 17:09, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.tre-es.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0941688** e o código CRC **13F526F2**.