TRIBUNAL REGIONAL ELEITORAL DE MINAS GERAIS
AV. PRUDENTE DE MORAIS, 320 - Bairro CIDADE JARDIM - CEP 30380000 - Belo Horizonte - MG

ESTUDOS TÉCNICOS PRELIMINARES

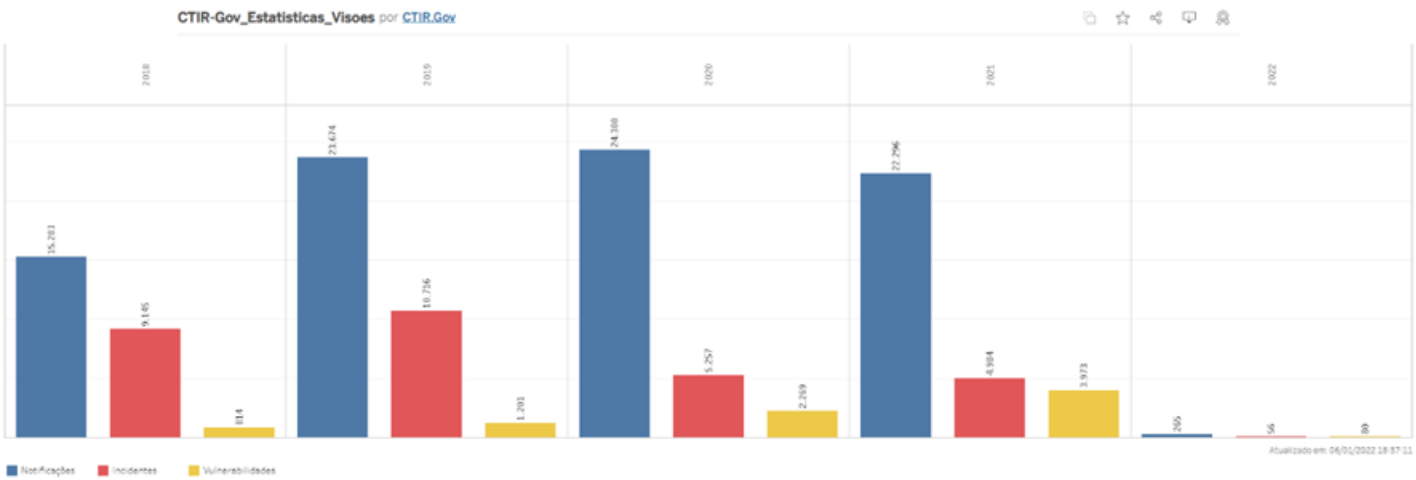
1. DESCRIÇÃO SUCINTA DA NECESSIDADE

Contratação de empresa para prestação de serviços relacionados à solução de Inteligência de Ameaças Cibernéticas (*Cyber Threat Intelligence - CTI*).
A ferramenta de mineração e prospecção de dados de código aberto (variedade de fontes publicamente disponíveis), baseado no conceito OSINT (*Open Source Intelligence*), deverá monitorar e coletar, de forma automatizada, potenciais ameaças na internet à Justiça Eleitoral, promovendo, de forma antecipada, medidas defensivas e preventivas, gerando alertas cibernéticos em tempo real, de acordo com as condições estabelecidas por este Regional, com emissão de relatórios contendo análise de inteligência de ameaças.
A solução deverá possuir mecanismo de captura automatizado de informações armazenadas na *surface web*, *deep web* e *dark web*, sites, fóruns, blogs, aplicativos de mensagens instantâneas (*Telegram*, *Snapchat*, *Whatsapp* e *Messenger* (*Facebook*)), mídias sociais (*Twitter*, *Facebook*, *Instagram* e *Linkedin*) e arquivos de logs, com acesso para gerenciamento via plataforma WEB.
Os alertas emitidos pela solução deverão atuar, no mínimo, nos seguintes contextos:
1. Intenções de ataques a vulnerabilidades que afetem os ambientes da Justiça Eleitoral;
2. Intenções de ataques que tenham como objetivo os recursos pesquisados ou o seu nicho de atuação;
3. Campanhas relevantes de "hacktivismo" eleitoral;
4. Atividades fraudulentas relacionadas aos recursos pesquisados;
5. Pessoas envolvidas em atividades contra a Justiça Eleitoral;
6. Códigos maliciosos (*malwares*) direcionados para os recursos pesquisados; e
7. Discussões online que divulguem ou acompanhem informações dos recursos monitorados com ênfase na Justiça Eleitoral.

2. JUSTIFICATIVA PARA A NECESSIDADE DOS SERVIÇOES E RESULTADOS PRETENDIDOS

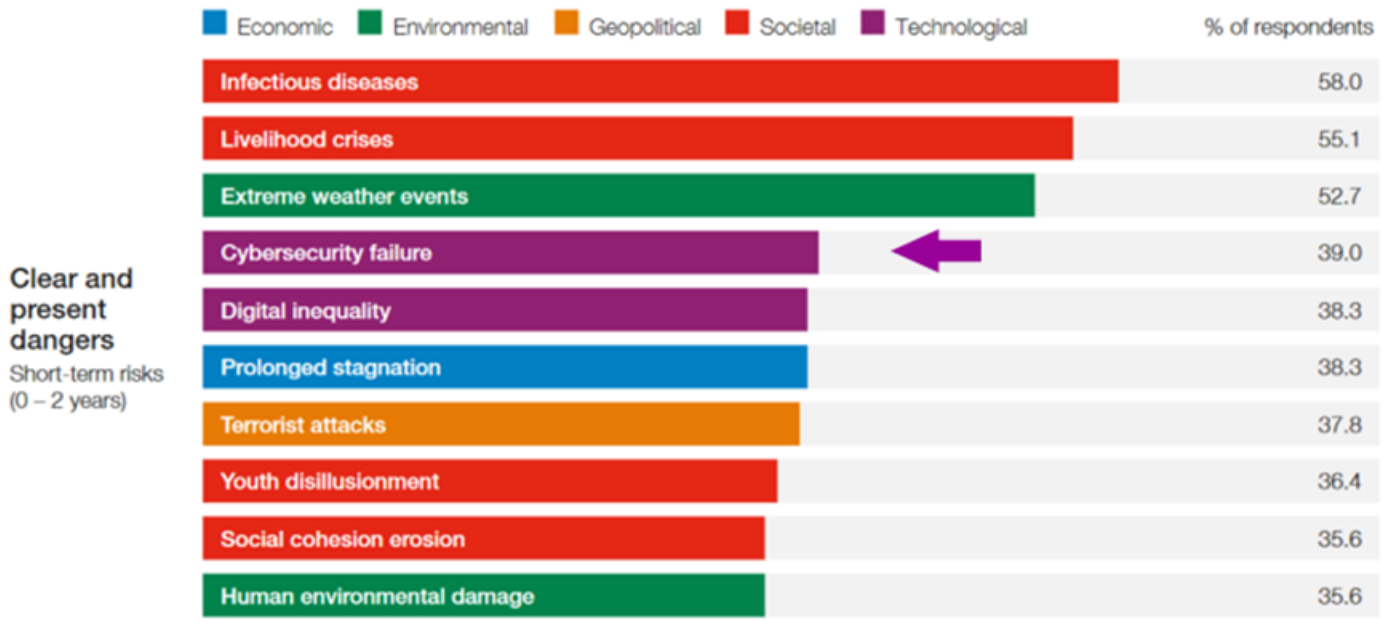
2.1 - Justificativa

A Secretaria de Tecnologia da Informação tem por atribuição o provimento de soluções informatizadas, que busquem prover de segurança quanto aos riscos e ameaças internas e externas.
O cenário de crimes cibernéticos vem passando por um processo de grande sofisticação, com uma escalada de ataques amplamente divulgados pela mídia, internet e redes sociais.
Esse ambiente evoluiu a partir de suas origens baseadas na disseminação de vírus de computador e, mais recentemente, os ataques mais sofisticados incluem Roubo de Identidades, *Ransomware*, Vazamento de Dados, Sequestro de Telefones, *Phishing* direcionado a pessoas chave ligadas à Instituição e Ameaças Avançadas Persistentes, que determinam um alvo e buscam todas as formas de invadi-lo até que tenham sucesso.
Grande parte dessas informações relacionadas a ataques cibernéticos tem sua origem ou são estruturadas na *deep web* e *dark web*, através de fóruns de discussão, blogs, aplicativos de mensagens instantâneas como o *Telegram*, *Snapchat*, *Whatsapp*, *Signal* e *Messenger* (*Facebook*) e/ou através das mídias sociais como *Twitter*, *Facebook*, *Instagram*, *Youtube* e *Linkedin*.
Com efeito, dados atualizados sobre o cenário das redes de computador de instituições do governo brasileiro (incluindo os poderes Executivo, Legislativo e Judiciário), disponibilizados pelo CTIR.Gov, confirmam a tendência de recrudescimento de ameaças no cenário cibernético, indicando um crescente na descoberta de vulnerabilidades a serem exploradas entre 2018 e 2021.



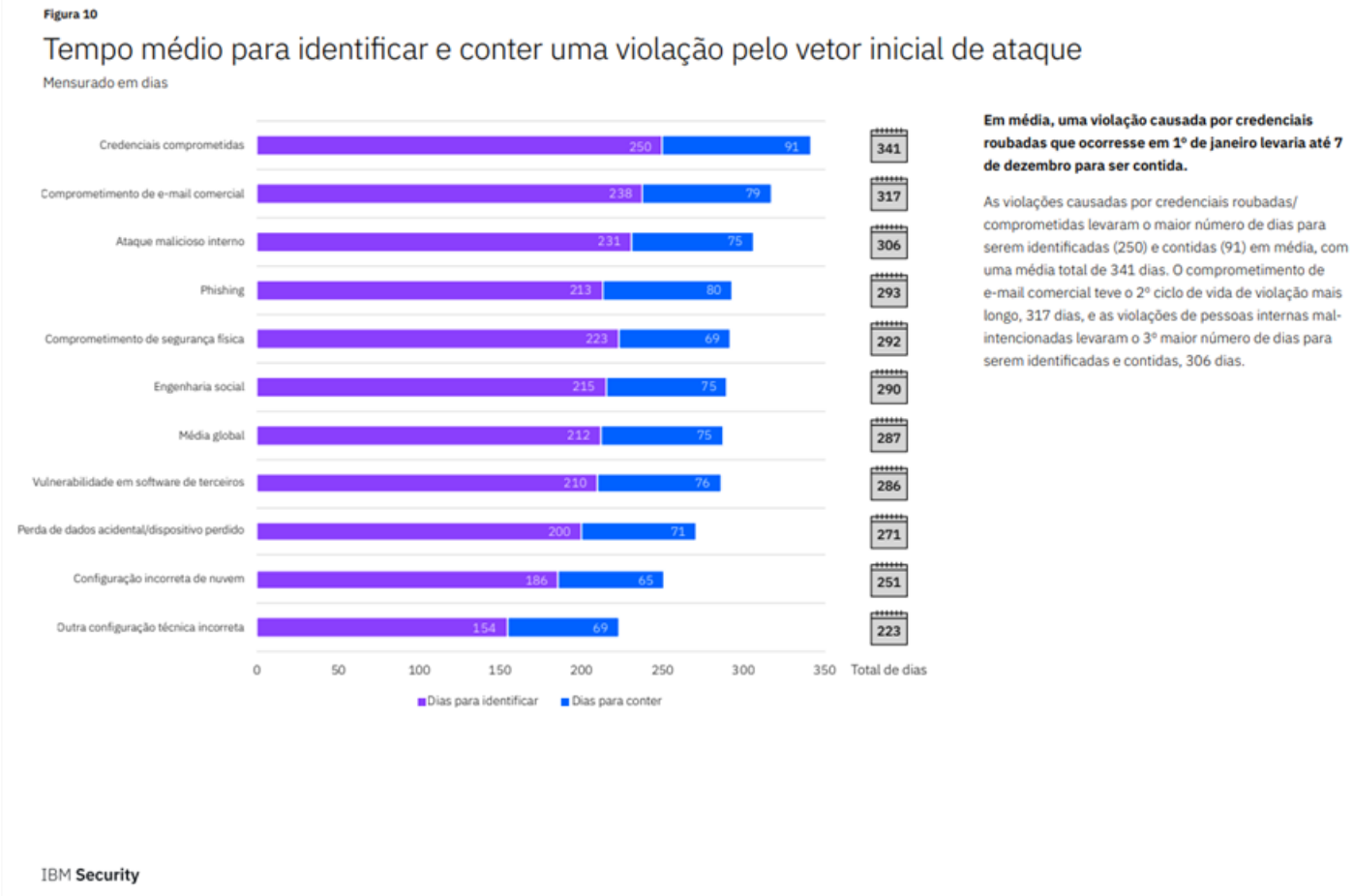
Fonte: CTIR-Gov_Estatisticas_Visoes | Tableau Public

Estudos realizados pelo Fórum Econômico Mundial, publicados no "Relatório Global de riscos de 2021", apontam que falhas em Cibersegurança (*Cibersecurity Failure*) ocupam o quarto lugar no ranking da percepção de riscos globais de curto prazo (0 a 2 anos).



Fonte: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

As soluções de segurança devem atuar nas fases de detecção, prevenção e resposta aos ataques para demonstrar o esforço e investimento na proteção dos dados sensíveis de usuários e, assim, cumprir os requisitos da legislação.
As novas gerações de ferramentas de segurança de antivírus, *firewall* e *antispam*, por exemplo, podem atuar de modo prospectivo, porém somente antes da contaminação real do ambiente.
Além disso, estruturas de SOC (*Security Operations Center*) e de Resposta a Incidentes normalmente utilizam, além de suas estruturas de monitoramento pró-ativas, relatórios de segurança estruturados na anatomia de um ataque cibernético, que são muito úteis, pois podem auxiliar a identificar padrões, porém são baseados em ocorrências passadas e padrões ou tendências. Não há inteligência aplicada sobre novas táticas, técnicas e atores mal-intencionados, que planejam empregar um ataque ou mesmo explorar a descoberta de uma vulnerabilidade que ainda não foi utilizada e que a organização possa estar exposta.
Continuamente, surgem novas ameaças, que estão em evolução constante. As plataformas de CTI são ferramentas de segurança que usam dados de segurança global para ajudar a identificar, mitigar e remediar ameaças à segurança de forma preventiva.
Embora os analistas de segurança saibam que a chave para ficar à frente dessas ameaças é analisar dados sobre eles, a real dificuldade está relacionada à forma e como coletar eficientemente grandes volumes de dados e, consequentemente, obter alertas adequados de forma a gerar relatórios que possibilitem frustrar antecipadamente ataques futuros.
Uma ferramenta de *Threat Intelligence* busca atuar, de forma antecipada, gerando medidas preventivas e protetivas através dos relatórios emitidos pela solução, antes mesmo que uma tentativa de ataque possa ocorrer.
Segundo o "Relatório do Custo de uma Violação de Dados 2021", elaborado pela Divisão de Segurança da IBM (*IBM Security*), os custos relacionados à violação de dados "subiram de US$ 3,86 milhões para US$ 4,24 milhões", maior aumento de custo em um único ano nos últimos 7 anos.
O referido relatório destaca ainda que "os custos foram significativamente inferiores para algumas das organizações com uma postura de segurança mais madura e superiores para as organizações que se atrasaram em áreas como IA (Inteligência Artificial) e automação de segurança, confiança zero e segurança de nuvem."
Outra informação relevante encontrada neste relatório é de que o número médio de dias para se identificar e conter uma violação ou vazamento de dados é de 287.
A título de exemplo, se uma violação ocorrida em 1º de janeiro de 2021 levasse 287 dias para ser identificada e contida, a violação não seria contida até 14 de outubro. O tempo médio para identificar e conter variou muito dependendo do tipo de violação de dados, do vetor de ataque, de fatores como o uso da IA e da automação de segurança e do estágio de modernização da nuvem.



Fonte: https://www.ibm.com/downloads/cas/RBJ6BJVN

O mesmo relatório da *IBM Security* aponta que "organizações com IA e automação de segurança totalmente implementadas tiveram custos de violação de US$ 2,90 milhões, em comparação a US$ 6,71 milhões em organizações sem IA e automação de segurança. A diferença de US$ 3,81 milhões, ou quase 80%, representa a maior diferença no estudo ao comparar violações com um fator de custo específico vs. sem um fator de custo específico. " "A IA e a automação de segurança foram associadas a um tempo mais rápido para identificar e conter a violação. "

Portanto, é possível depreender dessa análise que a atuação de forma preventiva pode abreviar o tempo médio para descobrir (e em alguns casos até evitar) um vazamento de dados, reduzido assim custos e impactos relacionados a esse tipo de incidente.

Existe uma grande variedade de ferramentas de mineração e prospecção de dados de código aberto (variedade de fontes publicamente disponíveis), baseado no conceito OSINT, porém, as soluções que se enquadram no conceito de CTI estão em um universo restrito. Rob McMillan e Khushbu Pratap do Gartner alertam, "nem todas as 'inteligências de ameaças' são iguais."

Importante salientar a diferença entre a contratação de um serviço de CTI e uma estrutura de SOC (Security Operation Center), que é uma instalação destinada a abrigar uma equipe de segurança da informação responsável por monitorar e analisar processos de uma organização continuamente. O objetivo da equipe SOC é detectar, analisar e responder a incidentes de segurança cibernética usando uma combinação de soluções de tecnologia e um forte conjunto de processos.

A equipe do SOC trabalha em estreita colaboração com equipes de resposta a incidentes organizacionais para garantir que os problemas de segurança sejam resolvidos rapidamente após a descoberta.

Os SOCs monitoram e analisam a atividade em redes, servidores, terminais, bancos de dados, aplicativos, sites e outros sistemas, procurando atividades anômalas que possam indicar um incidente ou comprometimento de segurança. Eles também são responsáveis por garantir que possíveis incidentes sejam corretamente identificados, analisados, defendidos, investigados e relatados.

Uma verdadeira solução de CTI é focada no adversário e voltado para o futuro, fornecendo dados contextuais, ricos sobre invasores e suas táticas, técnicas e procedimentos (TTPs). Pode, por exemplo, determinar a motivação e os alvos de uma nova variedade de cibercriminoso, as vulnerabilidades que eles visam, os domínios, *malware* e engenharia social; métodos que utilizam, a estrutura e evolução de suas campanhas e as técnicas que eles são susceptíveis de empregar para evitar a segurança atual. Por fim, o CTI pode ser customizado para cada cliente.

Ferramentas de CTI de alta qualidade pode franquear acesso direto aos seus analistas, para que os clientes possam receber esclarecimentos aprofundados sobre inteligência e enviar amostras de *malware* para análise detalhada.

Informações personalizadas dão às empresas um contexto extra para definir prioridades e otimizar decisões baseadas em suas necessidades e riscos específicos perfis, em vez de médias amplas da indústria.

Concluímos que não é apenas a ação de detectar mais ataques direcionados. Maior visibilidade das ameaças é claramente uma das vantagens do CTI, por isso é importante definir a abordagem de uso que se deseja implementar para que ocorra um alinhamento com a demanda proposta.

Com o uso adequado de uma ferramenta de *Threat Intelligence* e de suas informações coletadas, as autoridades responsáveis poderiam ser devidamente municiadas para, por exemplo, notificar os serviços de mensagens

instantâneas, redes sociais; solicitar o bloqueio de domínios e endereços na internet, preparando contramedidas ou ações de mitigação para os riscos e ameaças cibernéticos.

2.2 - Contextualização
Cabe ao Núcleo de Assessoria em Segurança de Tecnologia da Informação propor ações e iniciativas para aumentar o nível de segurança em tecnologia da informação, acompanhando o cenário mundial no contexto de segurança da tecnologia da informação.
Diante do cenário político em que o país se encontra e com a aproximação das eleições de 2022, a desinformação e os ataques à Justiça Eleitoral tendem a crescer. Nesse sentido, o NASTI propõe a contratação do serviço de *Cyber Threat Intelligence* (CTI), por um período mínimo de 12 (doze) meses, buscando identificar de modo preditivo ameaças e a mitigação de possíveis ocorrências ou incidentes cibernéticos que possam afetar reputação e a imagem deste Regional e, dessa forma, municiar as equipes técnicas e autoridades envolvidas com o processo eleitoral para a tomada de decisões no sentido de ampliar a proteção cibernética institucional.
Importante evidenciar a recente criação do Programa de Enfrentamento à Desinformação – PED, instituído em caráter permanente no âmbito deste Regional. Uma ferramenta de CTI poderá auxiliar na prevenção à desinformação sobre assuntos alusivos às eleições e à Justiça Eleitoral.

2.3 – Critérios de Sustentabilidade
O entendimento da equipe técnica é de que não se aplicam critérios de sustentabilidade para a contratação de serviço proposta, visto que o serviço trata-se de contratação de Software como Serviço (SaaS). Além disso, o uso de robôs e inteligência artificial resultam em economia e gestão mais eficaz de recursos relacionado ao serviço prestado.
Por se tratar de um software sendo executado em uma solução em nuvem, não há critérios de sustentabilidade aplicáveis. Tais critérios seriam exigíveis para aquisições com hardware com software embarcado.

3. ESTUDO DE CONTRATAÇÕES ANTERIORES
Não há contratações anteriores deste serviço no TRE-MG, no entanto, cabe informar que o TSE contratou esse tipo de serviço, utilizando a ferramenta BTTng, da empresa Apura.

4. DEMONSTRAÇÃO DO ALINHAMENTO ENTRE A CONTRATAÇÃO E O PLANEJAMENTO DO TRIBUNAL
Objetivo estratégico nº 07/PETRE 2021-2026 – Zelar pela integridade administrativa e pelo enfrentamento aos ilícitos eleitorais.
Objetivo estratégico nº 10/PETRE 2021-2026 - Fortalecer a estratégia de tic, de segurança da informação e de proteção de dados.
Objetivo estratégico nº 07/PDTIC 2021-2026 – Aprimorar a segurança da informação e gestão de dados.

5. IDENTIFICAÇÃO DAS SOLUÇÕES
Foram identificadas 03 (três) soluções com potencial para atender ao escopo de atuação definido para o serviço contratado.

1. BTTng (Empresa APURA)

O BTTng engloba um completo pacote de serviços que envolve desde ações de busca ativa de ameaças em fontes abertas, até configuração direcionada dos robôs de coleta, além de disponibilizar boletins frequentes sobre ameaças e incidentes em destaque no cenário de cibersegurança nacional e internacional.
O BTTng é hoje a solução de OSINT e CTI líder no Brasil e na América Latina e a Apura tem em sua carteira de clientes 8 dos 10 maiores bancos brasileiros, diversas Fintechs, grandes varejistas, gigantes da área de saúde, APPs, Governo, Forças da Lei, setor industrial, empresas de serviços, empresas líderes no setor de telecomunicações e tecnologia, dentre outros.
Possui mecanismos poderosos de coleta de informações em variadas fontes, tanto na surface web, quanto na deep web e dark web, possibilitando uma visibilidade ampla e dinâmica de possíveis ameaças presentes na rede.
Coleta de informações em fontes abertas (meios digitais) com coleta automatizada e correlacionamento dos eventos.
Visa proteção dos executivos, marcas e reputação; adequada à LGPD/GDPR: melhora na conformidade antevendo ameaças e traçando melhores estratégias de proteção e detecção de vazamentos, de incidentes de segurança e golpes;
Realiza monitoramento de fraudes, golpes, risco cibernético, problemas com segurança física, monitoramento de marca, campanhas de phishing, vazamento de credenciais e informações, hacktivismo, etc.
Possui ainda as seguintes características:

- Aplicação de técnicas de OCR e *machine learning* nos eventos coletados;
- Realiza a transcrição de áudio em mensagens e vídeos;
- Filtros de buscas;
- Sistema de ocorrências para eventos maliciosos identificados;
- Alertas automáticos via e-mail ou plataformas terceiras;
- API/SDK para outras integrações;
- Possui integração com MISP;
- Existe a possibilidade de segmentação de times e permissionamento de usuários.

Site: Apura – Cybersecurity Intelligence

2. ZeroFox (Empresa PROOF)

Solução proprietária, que protege contra invasão de contas, imitações de perfis ou produtos, *phishing*, *malware*, vazamento de informação, danos à reputação, atuando nas fases de identificação, proteção, análise e remediação.
Na identificação a solução conta com pontos de coleta de dados e monitoração em todas as camadas da internet, desde a surface, varrendo redes sociais, *marketplaces*, lojas de aplicativos, fóruns, blogs, site de *review*, *code sharing*, *dark* e *deep web*.
Na etapa de proteção, realiza a análise de domínios e endereços locais, pode proteger perfis de executivos e colaboradores, ativos intangíveis, como marcas e propriedade intelectual.
Na fase de análise ocorre a atuação de IA, de forma que é possível automatizar alertas e emissão de relatórios dos dados monitorados. Existe ainda a possibilidade de realizar a análise humana com a contratação do serviço PROOF SOC, que é comercializado à parte.
Na etapa de remediação, ocorre o *takedown*, bloqueio ou ocultação da informação considerada sensível.
Na produção de inteligência ocorre a partir da análise aprofundada de cenários específicos e do acompanhamento de tendências por fontes internacionalmente reconhecidas, sendo possível oferecer insumos que enriquecem ações e decisões de todos os agentes envolvidos na segurança.
A ferramenta entrega artefatos de inteligência que promovem a consciência em relação às ameaças e uma postura ativa frente aos riscos a partir da entrega de conteúdos relevantes de cibersegurança, como o resumo de acontecimentos recentes, falhas urgentes (através de relatórios de vulnerabilidades) e tendência externas que podem impactar direta ou indiretamente na organização.
Possui representante no Brasil, sendo um dos maiores players do mercado, no entanto não possui atuação no setor público. Sua base de clientes está distribuída na esfera privada.

Site: Home - PROOF | Segurança da Informação

3. AxurOne (Empresa AXUR)

O portfólio da solução AxurOne estrutura-se na proteção da presença digital de suas marcas e programas do cliente, com foco nos seguintes canais digitais: *surface web*, mídias sociais, *mobile apps* e *deep* & *dark web* .
A Axur possui as seguintes ofertas em seu portfólio:

- Fraudes Digitais
- Vendas Abusivas *on line*
- Presença digital da marca
- Vazamento de Dados
- Ameaças a Executivos
- *Threat Intelligence*
- Remoção de conteúdo infrator
- Análise de Riscos digitais

As ofertas são compostas por agrupamentos de casos de uso, com a finalidade de atender as dores de um determinado indivíduo ou instituição em uma ou mais situações específicas.
Os casos de uso cobertos pela Axur são:

- Uso indevido de marca;
- Uso indevido de marca em buscas pagas;
- Perfis e *fanpages* falsos em redes sociais;
- Aplicativos falsos;
- Nomes de domínios similares;
- Inserção de endereço falso em mapas;
- *Phishing* e *Smishing*;
- *Malware* (vírus);
- Cupons, vouchers e códigos promocionais falsos;
- Fraudes com Proxy, DNS e redirect;
- Vendas não autorizadas;
- Fraudes na *deep* e *dark web*;
- Vazamento de dados sensíveis;
- Vazamento de credenciais corporativas;
- Vazamento de credenciais de clientes;
- Vazamento de cartões de crédito;
- Compras fraudulentas com cartões vazados.

Site: Axur. Experiências digitais mais seguras

6. COMPARAÇÃO ENTRE AS SOLUÇÕES IDENTIFICADAS
Todas as soluções realizam a varredura e análise dos ambientes definidos no escopo, no entanto, foram identificadas as seguintes desvantagens da solução ZeroFox em relação ao BTTng e AxurOne:
- Não possui integração com o MISP. O projeto MISP *Threat Sharing* consiste em várias iniciativas, desde *software* para facilitar a análise e o compartilhamento de ameaças até informações estruturadas sobre ameaças cibernéticas e taxonomias de uso livre, portanto trata-se de base de dados colaborativa significativa para aumentar a eficiência dos serviços.
- Não possui contrato de prestação de serviços vigente com nenhum Órgão do Governo.
A solução BTTng possui o diferencial sobre as demais ferramentas de realizar a transcrição de áudios e vídeos de mensagens coletadas. Cumpre destacar que buscas em formato somente texto podem não ser suficientes, pois

muitas fraudes e campanhas de *phishing*, por exemplo, são trafegadas utilizando arquivos de áudio e vídeo.
A representante comercial da solução AxurOne informou que prevê disponibilização futura da funcionalidade de transcrição de áudio e vídeo de mensagens, no entanto, até a data em que a solução foi apresentada, essa tecnologia ainda não havia sido implementada.
Apesar de somente a solução da empresa Apura apresentar, até o momento, a funcionalidade de transcrição de áudio e vídeo, não é possível afirmar que não existam outras soluções de CTI no mercado que não atendam a todos os requisitos considerados necessários para a contratação em estudo, portanto, não podemos considerar que trata-se de característica exclusiva de um produto.

7. JUSTIFICATIVAS PARA ESCOLHA DA SOLUÇÃO OU FORMATO DA CONTRATAÇÃO
O NASTI, como corpo técnico responsável por apontar os requisitos mais adequados para uso de uma ferramenta de CTI, recomenda que a solução possua as seguintes caraterísticas detalhadas a seguir:

DESCRIÇÃO DETALHADA DOS SERVIÇOS:
Os serviços, que deverão ser entregues em um único item, podem ser relacionados da seguinte forma:

- Monitoramento e coleta automatizada;
- Geração de alertas em tempo real; e
- Emissão de relatórios com análise de inteligência de ameaças.

1. Monitorar e coletar, de forma automatizada, potenciais ameaças à Justiça Eleitoral, promovendo a antecipação de medidas defensivas preventivas.
1.1. O monitoramento deverá ser realizado pela contratada em regime de 24x7, durante toda a vigência contratual, mediante parâmetros e pesquisa indicados pelo TRE-MG.
1.2. O monitoramento deverá ser realizado por solução baseada em aplicação ou conjunto de aplicações apropriadas para esta finalidade, instaladas sobre ambiente da própria contratada, na modalidade de SaaS (Software as a Service), que possuam mecanismo de captura automatizado de informações armazenadas na surface web, deep web e dark web, sites, fóruns, blogs, aplicativos de mensagens instantâneas, mídias sociais, arquivos de logs;
1.3. A solução deverá ser disponibilizada em plataforma web, acessível via Internet, e possibilitar o acesso, sem falhas, ao menos pelos navegadores Google Chrome, Mozilla Firefox e Microsoft Edge, de forma a também possibilitar à equipe do TRE-MG possua acesso às consultas dos resultados obtidos;
1.4. Realizar o monitoramento na Internet (fontes abertas, redes sociais, aplicativos de mensagens instantâneas, fóruns, blogs, surface web, deep web e dark web), e deve ser capaz de realizar pesquisas automatizadas previamente cadastradas, periódicas, manuais, avulsas e conforme estabelecido no item 1.9 pelo TRE-MG;
1.5. Exibir os endereços ou IP nos resultados das pesquisas realizadas sobre qualquer site, inclusive os existentes na Deep Web e Dark Web;
1.6. Sobre o monitoramento de redes sociais:
1.6.1. Permitir a pesquisa de contas de usuários nas redes sociais por, no mínimo, nome do usuário, telefone, apelido e endereço de e-mail;
1.6.2. Possuir a busca automática de novas publicações das contas cadastradas conforme um agendamento pré-configurado;
1.6.3. Extrair metadados de cada publicação com, no mínimo: texto, endereço eletrônico, identificador e Timestamp;
1.6.4. Coletar todas as publicações já feitas pela conta, mesmo que estas sejam anteriores à primeira sincronização na ferramenta;
1.6.5. A solução deverá manter sincronia com as associações de contexto e pessoas já realizadas e com as novas buscas;
1.6.6. Publicações já coletadas pelas aplicações deverão ser mantidas em suas bases de dados e resultados de pesquisa caso sejam excluídas de suas fontes originais;
1.7. Relação mínima de fontes que devem ser monitoradas
1.7.1. Aplicativos de mensagens instantâneas: Telegram, Whatsapp e Messenger (Facebook);
1.7.2. Redes Sociais: Twitter, Facebook, Instagram, Snapchat e Linkedin
1.7.3. Sites de busca: Google, Bing, Yahoo! e DuckDuckGo
1.7.4. Serviços de vídeo: Youtube
1.7.5. Ransomware: Sites de ransomware shaming
1.7.6. Segurança cibernética: Shodan, BinaryEdge, Zone-H, Bases de CVE
1.7.7. Lojas de aplicativos Android e Apple
1.7.8. Outras fontes abertas: Pastebin, GhostBin, Paste24, GitHub, GitLab, Feeds RSS
1.8. Capaz de realizar a transcrição de áudios, imagens e vídeos capturados em aplicativos de mensagens instantâneas;
1.9. Sobre o uso de Avatares
1.9.1. As aplicações devem ser capazes de criar avatares por tipo de rede social, para, no mínimo: Twitter, Facebook, Instagram, Snapchat e Linkedin, bem como fóruns e blogs previamente definidos pelo TRE-MG, para a realização de pesquisas e coletas de dados;
1.10. Capaz de realizar pesquisa de informações nos seguintes contextos (Cada Ordem de Serviço especificará os contextos a serem efetivamente pesquisados):
1.10.1. Ameaças cibernéticas;
1.10.2. Resposta a Incidentes;
1.10.3. Prevenção de perdas de dados;
1.10.4. Proteção de Marca;
1.10.5. Fraudes;
1.10.6. Domínios Web;
1.10.7. Ameaças Internas;

1.10.8. Imagem e reputação de autoridades ligadas ao TRE-MG;
1.10.9. Imagem e reputação Institucionais.
1.10.10. Vazamento de dados sensíveis;
1.10.11. Vazamento de credenciais corporativas.
1.11. Não deve limitar quantidade de recursos pesquisados;
1.12. Sobre o monitoramento de domínios de internet:
1.12.1. Realizar a detecção de domínios recentemente registrados que possam oferecer, no mínimo:
1.12.1.1. Riscos de serem utilizados de forma maliciosa;
1.12.1.2. Variações comuns de nomes;
1.12.1.3. Permutações de caracteres;
1.12.1.4. Desvio de URL (typosquatting);
1.12.2. Informar anomalias nos registros "WhoIS" dos domínios monitorados;
1.12.3. Detectar as páginas internas (intranet) dos recursos pesquisados que estejam expostas na internet;
1.12.4. Identificar as vulnerabilidades dos domínios monitorados que tenham sido tornadas públicas;
1.13. Permitir a solicitação de pelo menos 72 (setenta e dois) takedowns durante o período de contratual.
1.13.1. As solicitações de takedowns poderão ocorrer a qualquer momento e em qualquer quantidade, limitado ao quantitativo especificado no item 1.13, sob demanda do TRE-MG.
1.14. Sobre a interface de consulta:
1.14.1. Os resultados das pesquisas devem conter, no mínimo, os seguintes campos: Contexto pesquisado, data, idioma, endereço web, conteúdo original completo;
1.14.2. Permitir que os resultados exibidos sejam ordenados conforme o interesse do usuário sendo, no mínimo, ordenáveis por data e hora, da ocorrência mais recente para a mais antiga;
1.14.3. Permitir a atualização do resultado das pesquisas realizadas anteriormente com a sinalização das atualizações;
1.14.4. Disponibilizar as informações das pesquisas por, no mínimo: intervalo de data, contexto, metadados e tipo da fonte;
1.14.5. Possuir interface de fácil visualização para demonstrar os resultados das buscas por cada tipo de fonte realizada, (fontes abertas, fóruns, blogs, redes sociais, aplicativos de mensagens instantâneas, deep web e dark web);
1.14.6. Permitir que o usuário veja o conteúdo em seu local original, por meio de um link atrelado ao resultado da pesquisa;
1.14.7. Exibir os relacionamentos de pessoas pesquisadas por um determinado contexto ou seleção feita;
1.14.8. Disponibilizar um ambiente para visualização das pesquisas realizadas e alertas cadastrados;
1.14.9. Permitir exportar qualquer pesquisa realizada de forma manual ou automática para os seguintes formatos: HTML, PDF, CSV, Planilha.
1.15. Relatórios e Gráficos
1.15.1. Permitir a emissão de relatórios e gráficos;
1.15.2. Possuir a capacidade de analisar dados coletados, fornecendo um painel de visualização que contemple, no mínimo, as seguintes funcionalidades: visualização de perfis relacionados a palavras-chave, realização de buscas nos dados incluindo buscas avançadas com critérios e entidades diferentes, vínculos com outros indivíduos;
1.15.3. Exibir todos os relatórios e gráficos em painel de bordo (dashboard);
1.15.4. Permitir exportar todos os relatórios e gráficos de forma manual ou automática para os seguintes formatos: HTML, PDF, CSV, Planilha eletrônica e Documento Texto;
1.16. Das credenciais de acesso ao sistema
1.16.1. A contratada deverá fornecer ao TRE-MG direitos de acesso (credenciais/contas) para a realização de consultas e geração de relatórios para no mínimo 06 (seis) colaboradores;
1.16.2. A autenticação para acesso ao sistema deverá contar com duplo fator de autenticação (2FA), oferecendo, no mínimo, as opções de SMS, Email e One Time Password (OTP).
1.16.2.1. A opção de duplo fator de autenticação por meio de SMS deverá ser completamente implementada pela Contratada, e o efetivo envio de mensagens deve ocorrer sem qualquer custo adicional para o TRE-MG.
1.16.2.2. Caso a opção de OTP não seja implementada por meio de uso de aplicação para smartphones ou computadores pessoais, a contratada deverá fornecer aos colaboradores do TRE-MG os equipamentos necessários para utilização dessa funcionalidade.
1.17. Da Confidencialidade, Integridade e Disponibilidade dos dados, a contratada deverá:
1.17.1. Implementar os controles necessários para que apenas os seus profissionais vinculados às Ordens de Serviço e os usuários e grupos criados pelo TRE-MG, tenham acesso às pesquisas realizadas e aos dados armazenados;
1.17.2. Permitir a guarda das informações coletadas por período a ser definido em cada Ordem de Serviço, por períodos de no mínimo 6 meses;
1.17.3. Realizar cópia de segurança dos dados coletados em razão das Ordens de Serviço formalizadas pelo TRE-MG, de forma a permitir ao menos a restauração do ambiente na situação equivalente à véspera da data de eventual solicitação formalizada pelo Tribunal;
1.17.4. Gerar e armazenar trilhas de auditoria que permitam o rastreamento de ações efetuadas em todos as contas de usuários. Os registros de logs devem conter, no mínimo, a data e hora do evento, origem de acesso, usuário, hostname do equipamento e ação/pesquisa efetuada.
2. Gerar alertas cibernéticos em tempo real, de acordo com as condições estabelecidas na respectiva Ordem de Serviço.
2.1. A Contratada deverá configurar na solução o envio de alertas relacionados aos monitoramentos realizados.
2.2. Os alertas deverão ser configurados, no mínimo, nos seguintes contextos:
2.2.1. Intenções de ataques a vulnerabilidades que afetem os ambientes da Justiça Eleitoral;
2.2.2. Intenções de ataques que tenham como objetivo os recursos pesquisados ou o seu nicho de atuação;
2.2.3. Campanhas relevantes de "hacktivismo" eleitoral;
2.2.4. Atividades fraudulentas relacionadas aos recursos pesquisados;

2.2.5. Pessoas envolvidas em atividades contra a Justiça Eleitoral;
2.2.6. Códigos maliciosos (malwares) direcionados para os recursos pesquisados;
2.2.7. Discussões online que divulguem ou acompanhem informações dos recursos monitorados com ênfase na Justiça Eleitoral.
2.3. A solução deve ser capaz de emitir alertas e relatórios de inteligência sobre ameaças iminentes e tendências em períodos de tempo pré-definidos, conforme listados abaixo:
2.3.1. Online
2.3.2. Diário
2.3.3. Semanal
2.3.4. Mensal
2.3.5. Anual
2.3.6. Determinado
2.4. Formas de envio dos Alertas
2.4.1. Os alertas devem ser emitidos por periodicidade ou por expressão de busca;
2.4.2. Os alertas devem ser enviados à equipe do TRE-MG por e-mail, SMS ou aplicativos de mensageria tais como Whatsapp ou Telegram;
2.4.3. Os alertas devem incluir, no mínimo: tipo da fonte, contexto procurado e o Timestamp do momento da geração do alerta;
2.4.4. A solução deve permitir a customização dos textos dos alertas;
2.4.5. A solução deve possibilitar o envio de e-mails criptografados, de acordo com os padrões de segurança a serem validados pelo TRE-MG.
3. Emissão de relatório com a análise de inteligência cibernética.
3.1. Além dos relatórios e gráficos automatizados disponibilizados pela própria solução, o TRE-MG poderá demandar relatório de análise de inteligência cibernética sobre os monitoramentos realizados, especificando o intervalo de monitoramento sobre o qual o relatório deverá ser elaborado.
3.2. A contratada deverá complementar os relatórios gerados pela própria solução, elaborando o documento final contendo os principais achados do monitoramento, indicando os principais riscos identificados e formas de mitigação de tais riscos.

8. REQUISITOS DE GARANTIA
Não se aplica, pois trata-se de prestação de serviços.

9. JUSTIFICATIVA DA QUANTIDADE SOLICITADA (COM MEMÓRIA DE CÁLCULO, SE POSSÍVEL)
O acesso à plataforma ocorre através de credenciais fornecidas pela CONTRATADA.
A solução da Axur, a precificação não depende do quantitativo de contas cadastradas.
Na solução da Apura, ocorre aumento de preço se o número de credenciais for superior a 06 (seis) credenciais.
A empresa Proof não se manifestou nesse sentido.
Devido ao critério de economicidade e considerando que a solução possui caráter estratégico, tático e operacional, sugere-se utilização de 06 credenciais, podendo ser distribuídas da seguinte forma:
- 01 (uma) credencial para a Corregedoria Eleitoral;
- 01 (uma) credencial para a Diretoria Geral;
- 01 (uma) credencial para a Secretária de Tecnologia da Informação;
- 01 (uma) credencial para a Coordenadoria de Comunicação Social;
- 01 (uma) credencial para o Núcleo de Segurança Institucional;
- 01 (uma) credencial para o Núcleo de Assessoria em Segurança de Tecnologia da Informação.

Em relação ao quantitativo de *takedowns*, cabe ressaltar que trata-se da primeira contratação de serviço com essa funcionalidade, portanto não existem parâmetros de contratações anteriores que possam sustentar de forma sólida a definição volumétrica.
O TSE possui contrato vigente com a empresa Apura e o número de takedowns contratado foi de 10 (dez) *takedowns* por mês, totalizando 120 *takedowns* ao ano.
O NASTI manifestou-se em Nov/2020 em pelo menos 08 (oito) situações, conforme os processos SEI 0014447-82.2020.6.13.8000, 0013914-26.2020.6.13.8000, 0013525-41.2020.6.13.8000, 0013120-05.2020.6.13.8000, 0012834-27.2020.6.13.8000, 0012641-12.2020.6.13.8000, 0012559-78.2020.6.13.8000 e 0012412-52.2020.6.13.8000, sendo que 06 (seis) processos eram passíveis de solicitações de *takedown*.
Considerando que trata-se de uma eleição geral em um cenário que tende a ser bastante conturbado, sugerimos pela manutenção da medida aferida no ano de 2020, ou seja, uma média de 06 (seis) *takedows* ao mês, perfazendo um total de 72 (setenta e dois) *takedowns* durante o período de vigência contratual.

10. ANÁLISE DO PARCELAMENTO DA CONTRATAÇÃO (AQUISIÇÃO POR LOTES OU POR ITENS)
A aquisição possui um único item, não havendo, portanto, o parcelamento para entrega do objeto.

11. ANÁLISE DA POSSIBILIDADE E CONVENIÊNCIA DE UTILIZAÇÃO DO INSTRUMENTO DE MEDIÇÃO DE RESULTADOS – IMR
Será adotado um Instrumento de Medição de Resultados – IMR – estruturado em um sistema de pontuação para um conjunto de indicadores previamente definidos de modo a possibilitar a realização de glosa em fatura do mês subsequente à prestação do serviço.
O fato de incorrer em desconto em fatura devido à inconformidade na prestação de serviço, não isentará a CONTRATADA de possíveis sansões previstas em lei.
A pontuação será apurada considerando 3 (três) níveis de graduação de impacto, conforme tabela 1:

TABELA 1	
Classificação	**Pontuação**

Baixo Impacto	4
Médio Impacto	8
Alto Impacto	20

O percentual de glosa na fatura será definido pelo somatório das pontuações referente ao período avaliado, conforme tabela 2:

TABELA 2	
Pontuação	**Desconto na fatura**
Até 20 pontos	Não haverá ajuste sobre o valor da fatura
21 a 30 pontos	1% sobre o valor da fatura
31 a 40 pontos	2% sobre o valor da fatura
41 a 50 pontos	3,5% sobre o valor da fatura
Acima de 51 pontos	5% sobre o valor da fatura

Os indicadores, considerados para apuração da pontuação, terão como referência a prestação dos serviços, conforme tabela 3:

TABELA 3	
Item	**INDICADOR**
01	Indisponibilidade de acesso à plataforma da solução por período superior a 24 horas.
02	Impossibilidade de uso de credenciais/contas por período superior à 48 horas.
03	Iniciar tratativas referente à de Ordem de Serviço em prazo superior à 2 horas.
04	Indisponibilidade de emissão de relatórios e gráficos através do dashboard da plataforma, com prazo superior à 72 horas.

OBS: Não será considerada indisponibilidade de serviço caso a CONTRATADA comunique com 48 (quarenta e oito) horas de antecedência a indisponibilidade de uso do serviço. Ex. Manutenção de serviços na nuvem aonde a plataforma está hospedada.
O pagamento será efetuado à CONTRATADA após apuração dos indicadores previstos na Tabela 3 acima.
As faturas mensais poderão sofrer ajustes de pagamento (glosa), considerando a pontuação atribuída às ocorrências previstas na tabela 4:

TABELA 4		
Indicadores	**Ocorrência**	**Impacto**
01 e 02	Prejuízo na prestação de serviço com dano no acompanhamento da equipe técnica sobre vulnerabilidades ou tentativas de ataques à Justiça Eleitoral.	Alto
03	Prejuízo na prestação de serviço e/ou dano no acompanhamento da equipe técnica.	Médio
04	Prejuízo ou dano na qualidade da prestação de serviço.	Baixo

Obs.: A apuração do IMR ocorrerá mensalmente em relatório/atestado específico, de acordo com os apontamentos do fiscal(is) responsável(is) pelo contrato.
O pagamento será realizado mensalmente, independentemente do número de ocorrência de requisições emitidas através de Ordens de Serviços e/ou acesso(s) à plataforma da solução da CONTRATADA, observando o relatório emitido pela fiscalização do contrato.

12. OBRIGAÇÕES DO CONTRATANTE

1. Fornecer à CONTRATADA todas as informações relacionadas com o objeto do contrato.
2. Realizar o pagamento conforme estabelecido no contrato.
3. Notificar, por escrito, a CONTRATADA a respeito de quaisquer irregularidades constatadas na prestação dos serviços.
4. Proporcionar as condições necessárias para que a CONTRATADA possa desempenhar seus serviços de acordo com as determinações do Termo de Referência.
5. Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com as cláusulas contratuais e os termos de sua proposta.
6. Exercer o acompanhamento e a fiscalização dos serviços por meio da designação de servidores (titular e suplente) do seu Quadro de Pessoal que deverão encaminhar os apontamentos à autoridade competente para as providências cabíveis.
7. Notificar a CONTRATADA por escrito da ocorrência de eventuais irregularidades constatadas no curso da execução dos serviços, fixando prazo para a sua correção.
8. Pagar à CONTRATADA o valor resultante da prestação do serviço, na forma do contrato.

13. OBRIGAÇÕES DA CONTRATADA

1. Executar, com observação dos prazos e exigências, todas as obrigações constantes deste Termo de Referência.
2. Responsabilizar-se pelas despesas decorrentes da execução dos serviços.
3. Informar, no momento da assinatura do contrato, nome do responsável (preposto), os contatos de telefone, e-mail ou outro meio hábil para comunicação com o TRE-MG, bem como manter os dados atualizados durante toda a fase de execução da contratação.
4. Toda a comunicação referente à execução do objeto será realizada através do e-mail informado pela CONTRATADA no momento da assinatura do contrato.

5. A comunicação será considerada recebida após a confirmação, pelo remetente por parte do tribunal, de entrega automática encaminhada pelo Sistema de Correio Eletrônico, independentemente de confirmação de recebimento por parte da contratada, ficando sob sua responsabilidade a consulta à caixa de e-mail.
6. A comunicação só será realizada de forma diversa quando a legislação exigir ou quando a contratada demonstrar ao fiscal os motivos que justifiquem a utilização de outra forma.
7. Acatar as recomendações efetuadas pelo fiscal do contrato.
8. Responsabilizar-se pelos danos causados diretamente à Administração ou a terceiros, decorrentes de culpa ou dolo na execução do objeto do Termo de Referência.
9. Fazer com que seus colaboradores se submetam aos regulamentos de segurança e disciplina durante o período de permanência nas dependências do TRE-MG, os quais devem estar devidamente identificados, não sendo permitido o acesso dos funcionários que estejam utilizando trajes sumários (por exemplo, bermudas, chinelos de dedo, camisetas regatas ou sem camisa).
10. Comunicar ao TRE-MG, por escrito, quando verificar condições inadequadas de execução do objeto ou a iminência de fatos que possam prejudicar a sua execução e prestar os esclarecimentos que forem solicitados pelos fiscais.
11. Manter o caráter confidencial dos dados e informações obtidos por qualquer meio ou prestados pelo TRE-MG, não os divulgando, copiando, fornecendo ou mencionando a terceiros e nem a quaisquer pessoas ligadas direta ou indiretamente à contratada, durante e após a vigência do contrato.
12. Tal exigência se dará de acordo com o Termo de Compromisso de Manutenção de Sigilo da Informação, a ser assinado pelos profissionais da contratada que executarão os serviços definidos neste Termo de Referência.
13. O Termo de Compromisso de Manutenção de Sigilo da Informação deverá ser assinado pelo profissional antes de sua participação na primeira Ordem de Serviço que for a ele designada, e terá validade durante todo o período da vigência contratual.
14. Manter, durante a execução do contrato, as condições de habilitação exigidas na licitação.
15. Verificadas irregularidades nas condições que ensejaram sua habilitação quanto à regularidade fiscal, a contratada terá o prazo de 30 (trinta) dias corridos, contados da notificação da fiscalização, para regularizar a situação, sob pena de aplicação das penalidades cabíveis, sem prejuízo da rescisão do contrato a critério da Administração.
16. Responsabilizar-se pelos encargos fiscais e comerciais resultantes da contratação.
17. A inadimplência da contratada com referência aos encargos suportados não transfere a responsabilidade por seu pagamento ao contratante, nem poderá onerar o objeto do contrato.

14. PENALIDADES ESPECÍFICAS (OU INFORMAR A UTILIZAÇÃO DO PADRÃO DO TRIBUNAL)

Pelo descumprimento dos prazos e condições determinados neste Termo de Referência, a empresa contratada estará sujeita às penalidades previstas na legislação vigente, bem como nos instrumentos convocatório e contratual, conforme o caso.

15. PRAZO DE VIGÊNCIA DA CONTRATAÇÃO E INFORMAÇÃO QUANTO À NATUREZA DOS SERVIÇOS (CONTÍNUOS OU NÃO)

O objetivo da contratação é buscar antecipar riscos ao processo eleitoral, ameaças a agentes e ativos da Justiça Eleitoral e às eleições de 2022, portanto a contratação da solução visa objetivamente atender ao período eleitoral e às eleições 2022.
Transcorridas as eleições, o serviço poderá ser utilizado também como ferramenta de apoio ao Programa de Enfrentamento à Desinformação – PED, instituído em caráter permanente no âmbito deste Regional.
Contudo, uma vez que se trata de solução inovadora no mercado, recomenda-se cautela em relação ao prazo de contratação, até que se possa conhecer e medir sua real eficácia e ganhos em relação aos objetivos a serem alcançados.
Devido à possibilidade de renovação da contratação do serviço, no interesse da administração, consideramos o serviço como de natureza contínua.
Pelos motivos expostos acima, sugerimos a contratação do serviço por um período de 12 (doze) meses.

16. FORNECEDORES IDENTIFICADOS (PELO MENOS TRÊS)

Identificam-se, pelo menos, os seguintes fornecedores potencial:
- BTTng
Site: Apura – Cybersecurity Intelligence
Contato: Yuri Bojarczuk <yuri.bojarczuk@apura.com.br>
- ZeroFox
Site: Home - PROOF | Segurança da Informação
Contato: João Stohler <joao.stohler@proof.com.br>
- AxurOne
Site: Axur. Experiências digitais mais seguras
Contato: Mari Zappa <mari.zappa@axur.com>

17. PROPOSTA COMERCIAL DE PELO MENOS DOIS FORNECEDORES (SERVIÇOS NÃO USUAIS)

As propostas comerciais enviadas pelas empresas Apura e Axur encontra-se nos documentos nºs 2653823 e 2744849, respectivamente.
Apesar de consultada, a empresa Proof não enviou proposta até o momento da conclusão deste artefato.

18. ANÁLISE DE RISCOS

A matriz de risco do processo de aquisições encontra-se no doc. SEI nº 2653758.

Assinaturas da Equipe de Planejamento da Contratação

Marcos de Almeida Alves
(NASTI/STI)
Integrante técnico - titular

Luciano Chapuis de Oliveira
(NASTI/STI)
Integrante técnico - suplente substituto

Belo Horizonte, 27 de maio de 2022.

ANEXO A – Lista de Potenciais Fornecedores

- BTTng
Site: Apura – Cybersecurity Intelligence
Contato: Yuri Bojarczuk <yuri.bojarczuk@apura.com.br>
- ZeroFox
Site: Home - PROOF | Segurança da Informação
Contato: João Stohler <joao.stohler@proof.com.br>
- AxurOne
Site: Axur. Experiências digitais mais seguras
Contato: Mari Zappa <mari.zappa@axur.com>

ANEXO B – Contratações Públicas Similares

Órgão	Termo de Referência (TR)
1-Banco do Brasil	Documento SEI nº 2966601
2-SERPRO	Documento SEI nº 2966629
3-TSE	Documento SEI nº 2966653

ANEXO C – Memória de Cálculo

Período estimado de vigência da contratação: de 01/07/2022 a 31/06/2023.
Valor de referência mensal: R$ 43.000,00

DESPESAS POR EXERCÍCIO		2022	2023
THREAT INTELLIGENCE E OPEN SOURCE INTELLIGENCE (OSINT)	Jul/22 a Dez/22 (6 meses)	R$ 258.000,00	
	Jan/23 a Jun/23 (6 meses)		R$ 258.000,00
SERVIÇO DE TAKEDOWN	Jul/22 a Jun/23 (12 meses)	R$ 11.520,00	

IMPACTO ORÇAMENTÁRIO ESTIMADO	2022	2023
	Entre R$ 258.000,00 a R$ 269.520	Entre R$ 258.000,00 a R$269.520,00

OBS.: Os valores informados neste anexo foram estimado na proposta com maior vantajosidade financeira, conforme proposta do doc. nº 2653823.

Belo Horizonte, 27 de maio de 2022.

Documento assinado eletronicamente por **LUCIANO CHAPUIS DE OLIVEIRA**, **Técnico Judiciário**, em 30/05/2022, às 14:35, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **GUSTAVO OLIVEIRA HEITMANN**, **Técnico Judiciário**, em 03/06/2022, às 14:50, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **ROBERTO DE CARTÉIA PRADO**, **Chefe de Seção**, em 03/06/2022, às 14:50, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **MARCOS DE ALMEIDA ALVES**, **Chefe do Núcleo**, em 03/06/2022, às 16:08, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **MOZART FERNANDES MOREIRA LIMA**, **Técnico Judiciário**, em 03/06/2022, às 16:17, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade deste documento pode ser conferida no site https://sei.tre-mg.jus.br/controlador_externo.php?acao=documento_conferir&acao_origem=documento_conferir&lang=pt_BR&id_orgao_acesso_externo=0, informando o código verificador **2977327** e o código CRC **FB68B674**.

0000500-87.2022.6.13.8000 2977327v28