TRIBUNAL SUPERIOR ELEITORAL

ANEXO I DO EDITAL - TERMO DE REFERÊNCIA

PREGÃO ELETRÔNICO Nº 90006/2025

1. OBJETO

1.1. Fornecimento sob demanda de subscrições de solução correlação de eventos de segurança da informação (Security Information and Event Management - SIEM) devendo ter a capacidade de processar efetivamente 30.000 (trinta mil) eventos por segundo, incluindo infraestrutura computacional, implantação, garantia e serviço de suporte técnico especializado, pelo período de 30 (trinta) meses, prorrogáveis nos termos da lei, consoante especificações, exigências e prazos constantes neste Termo de Referência.

2. JUSTIFICATIVA

2.1. A fundamentação da presente contratação e de seus quantitativos, assim como a descrição da solução como um todo, encontram-se pormenorizadas no Estudo Técnico Preliminar (ETP) 3057387.

3. ESPECIFICAÇÃO E FORMA DE EXECUÇÃO DO OBJETO

3.1. TABELA DE ITENS

Grupo	Item	Descrição	Unidade de Medida	Quantidade
1	1	Subscrição de solução de gerenciamento e correlação de eventos de segurança da informação (SIEM – Security Information and Event Management) com tecnologia Security Analytics e UEBA (User and Entity Behavior Analytics) ou UBA (User Behavior Analytics) para 20 usuários simultâneos, com garantia de 30 meses, dimensionado para 6.000 eventos por segundo (EPS)	Un.	5
	2	Fornecimento de infraestrutura de processamento, conectividade e armazenamento (instalação, manutenção e suporte de peças) de dados necessária e suficiente às operações da solução de gerenciamento e correlação de eventos de segurança da informação – SIEM (a ser instalado nas dependências do Contratante), composto por cluster de hardware em alta disponibilidade, incluindo equipamento de gerência e equipamento de tratamento de logs e evidências, com garantia de 30 meses, dimensionado para 30.000 eventos por segundo (EPS)	Un.	1

Grupo	Item	Descrição	Unidade de Medida	Quantidade
	3	Subscrição, com licenciamento somente para o TSE, para simulação de ataque e verificação de brechas de segurança do ambiente de rede corporativa, incluindo serviço de diretório e firewall de aplicações, com garantia de 30 meses.	Un.	1
	4	Serviço de operação assistida em regime de consultoria especializada para suporte e parametrização da solução do Grupo 1, com foco no gerenciamento e correlação de eventos de segurança da informação – SIEM, por 30 meses.	Un.	30
	5	240 (duzentas e quarenta) horas, durante a vigência do contrato, de suporte técnico especializado realizado exclusivamente pelo fabricante, sob demanda, em horas.	Un.	240
-	6	Subscrição de solução de lista de reputação de endereços IP que cubram a proteção de serviços maliciosos de VPN, Proxy, Proxy Residencial, Proxy Malware ou redes de Bots, bem como a visibilidade de tráfego malicioso no ambiente da Contratante (internet e rede local), com garantia de 30 meses.	Un.	1

Tabela 01- Descrição sucinta dos itens

3.2. DESCRIÇÃO GERAL

3.2.1. O(s) serviço(s) objeto desta contratação são caracterizados como comum(ns), conforme justificativa constante do Estudo Técnico Preliminar.

3.2.2. O **Item 1 do Grupo 1** diz respeito a subscrição de licenças de softwares, com obrigação acessória de implantação destas no ambiente do TSE e garantia de 30 meses.

3.2.3. O **Item 2 do Grupo 1** diz respeito a fornecimento de infraestrutura, composta de hardwares e softwares (a exemplo dos sistemas operacionais dos hardwares), com obrigação acessória de implantação destes no ambiente do TSE e garantia de 30 meses.

3.2.4. O **Item 3 do Grupo 1** diz respeito a subscrição de software, com obrigação acessória de implantação destes no ambiente do TSE e garantia de 30 meses.

3.2.5. O **Item 4 do Grupo 1** diz respeito a serviço de operação assistida da solução que compõe o Grupo 1, com foco no gerenciamento e correlação de eventos de segurança da informação – SIEM, por 30 meses.

3.2.6. O **Item 5 do Grupo 1** diz respeito a serviços a serem prestados por consultor do fabricante dos softwares do item 1 do Grupo 1, com foco em questões associadas à arquitetura da solução.

3.2.7. O **Item 6** diz respeito a subscrição de software, com obrigação acessória de implantação destes no ambiente do TSE e garantia de 30 meses.

3.2.8. As características e detalhamentos técnicos dos serviços descritos na Tabela 01 encontram-se descritos no **Anexo I-VI.**

3.3. CONSIDERAÇÕES GERAIS

3.3.1. Quanto aos **Itens 1 e 3 do Grupo 1 e Item 6**, a solução deve ser fornecida, instalada e implantada de forma completa de acordo com as condições e prazos previstos neste TR e seus anexos.

3.3.1.1. Não serão aceitas, como solução de SIEM, sistemas baseados em software *opensource* de uso genérico, softwares disponibilizados gratuitamente ou sistemas baseados em software ou sistema operacional diferentes daqueles oferecidos pelos fabricantes do mercado em geral.

3.3.1.2. No momento da apresentação das propostas a(s) licitante(s) deverá(ão):

a) Comprovar que todos os sistemas operacionais e softwares/licenças (integrados na solução) devem estar em linha de produção do fabricante. Não serão aceitas soluções com previsão de descontinuidade, *end-of-support* ou *end-of-life*.

a.1) A comprovação da obrigação estabelecida no item 3.3.1.2. deste TR deverá ser realizada por meio da apresentação de relação de *links* oficiais dos sites do fabricantes ou documentos probatórios oficiais que atestem o atendimento ao requisito definido.

b) Apresentar os catálogos técnicos dos produtos componentes da solução (itens 1 e 2 do grupo 1 deste TR) para que se possa certificar que o bem/serviço proposto pela proponente atende a todas as condições e especificações técnicas exigidas no TR.

c) Apresentar lista com as marcas e modelos dos componentes da solução dos itens 1 e 2 do grupo 1 deste TR para análise de qualidade.

d) Apresentar a planilha auxiliar do Anexo I-I deste TR de composição de custos devidamente preenchida com os detalhamentos dos componentes dos itens a serem contratados (fabricante, modelo, part number/código do produto, descrição técnica, quantidade e preço unitário),

e) Apresentar documento que descreva ponto-a-ponto a comprovação às exigências técnicas das subscrições/softwares e detalhamento da formação dos preços dos serviços ofertados, contendo discriminação de todos os insumos e custos unitários em conformidade com o Acórdão TCU nº 1432/2024 – Plenário.

3.3.1.2.1. As especificações das características técnicas da solução de segurança ofertada deverão estar descritas de forma clara e detalhada.

3.3.1.3. Quaisquer componentes adicionais, além dos previstos no Anexo I - VI, que se fizerem necessários para que sejam atendidas todas as características previstas neste TR e seus anexos durante a vigência contratual, deverão ser providos pela Contratada, sem ônus adicional ao Contratante.

3.3.2. Quanto ao **Item 2 do Grupo 1**, cabe à licitante realizar o correto dimensionamento da infraestrutura a ser fornecida para que os softwares que compõem a solução funcionem em perfeito alinhamento com a performance exigida neste Termo de Referência

3.3.2.1. Não será realizado dimensionamento prévio por parte da contratante, uma vez que a necessidade de hardware para processamento de 30.000 EPS depende da solução de SIEM que será fornecida.

3.3.2.2. A carga média da infraestrutura fornecida não deverá ultrapassar 80%.

3.3.2.3. Os serviços especificamente prestados por intermédio do item 2 da Tabela deste TR deverão ter sua atualização/upgrade realizado de forma imediata sempre que os componentes de hardware alcançarem 80% de uso dos recursos, sob pena de multa, bem como o atendimento a outras obrigações definidas no Anexo - I - VI.

3.3.3. Os serviços do **Item 4 do Grupo 1** deverão ser realizados por profissional(is) da contratada.

3.3.3.1. Os serviços não serão caracterizados como alocação de profissionais com exclusividade nas dependências do Contratante.

3.3.3.2. O TSE não terá gestão sobre os profissionais da contratada.

3.3.3.3. Os serviços serão realizados preferencialmente na forma remota (teletrabalho). Excetuam-se dessa regra geral a situação descrita a seguir, na qual os serviços deverão ser realizados presencialmente, isto é, na sede do TSE em Brasília:

3.3.3.3.1. Durante o período compreendido entre a segunda-feira

anterior ao primeiro e segundo turnos das eleições ordinárias e a terça-feira após o primeiro e segundo turnos das eleições ordinárias. Nesse período, os sábados (véspera de 1º e 2º turno das eleições ordinárias) e os domingos (1º e 2º turnos das eleições ordinárias), o horário de trabalho será das 07:00 às 22:00, nos demais dias o horário de trabalho será das 09:00 às 19:00.

3.3.3.4. Por se tratar de serviços associados a sistemas críticos de segurança da informação, a contratada deverá apresentar previamente ao TSE a indicação dos profissionais que realizarão os serviços.

3.3.3.5. Será realizada pesquisa de vida pregressa dos profissionais indicados pela contratada. Somente profissionais aprovados pelo TSE poderão atuar no contrato.

3.3.3.6. A contratada terá que assinar o Termo de Confidencialidade disponível no Anexo I-X e os profissionais indicados terão que assinar Termo de Ciência, conforme modelo disponível no Anexo I-IX.

3.3.3.7. É desejável que a contratada preserve a equipe de profissionais, mitigando alta rotatividade destes, haja vista a curva de aprendizado e a restrição de informações de segurança da informação a um grupo limitado de profissionais.

3.3.4. Os serviços do **Item 5 do Grupo 1** deverão ser realizados de forma remota, por profissionais do fabricante da solução do Item 1 do Grupo 1.

3.3.4.1. Consistem de serviços de consultoria e engenharia prestados por profissionais do fabricante do Item 1 do Grupo 1.

3.3.4.2. Serão demandados por meio da emissão de Ordens de Serviço, endereçadas à contratada.

3.3.5. O objeto a ser contratado não consta do catálogo eletrônico de padronização de compras, serviços e obras do Portal Nacional de Contratações Públicas - PNCP.

3.4. PRAZO E LOCAL DE EXECUÇÃO DOS SERVIÇOS

3.4.1. Os prazos para a execução dos serviços e entrega das licenças estão descritos no **CRONOGRAMA DE EXECUÇÃO** conforme item 3.5 deste TR.

3.4.2. Os equipamentos, softwares e serviços descritos neste Termo de Referência, deverão ser entregues e terão sua execução nas dependências do TSE localizado no Setor de Administração Federal Sul (SAFS) Quadra 7, Lotes 1/2, Brasília - DF CEP: 70095-901.

3.4.3. Os serviços serão prestados nos locais e horários definidos pelo Anexo - I-VI.

3.5. CRONOGRAMA DE EXECUÇÃO

3.5.1. A Contratada deverá cumprir os eventos conforme Cronograma de execução do objeto, a seguir, respeitando os prazos máximos estabelecidos, os quais poderão ser antecipados sempre que as circunstâncias assim o permitam, observando-se os dias úteis do calendário forense do TSE.

3.5.2. A contratada deverá realizar **Reunião Inaugural de Planejamento** em 5 (cinco) dias úteis após o Início da vigência contratual.

3.5.3. Prazos de entrega e de início de execução:

3.5.3.1. Para as subscrições dos itens 1 e 3 do Grupo 1 e item 6: As subscrições deverão ser entregues em, no máximo, 24 (vinte e quatro) dias úteis, contados do recebimento da ordem de fornecimento para entrega do licenciamento.

3.5.2.1.1. A ordem de fornecimento deverá ser emitida pelo contratante em, no máximo, 10 (dez) dias úteis da vigência do contrato.

3.5.2.1.2. Para o item 1 do Grupo 1, será emitida uma ordem de fornecimento distinta para cada uma das cinco subscrições de 6.000 EPS.

3.5.2.1.3. As ordens de fornecimento para os demais lotes de 6.000 EPS serão emitidas sob demanda, de acordo com a necessidade de se processar mais Eventos por Segundo (EPS).

3.5.3.2. Para os hardwares e softwares do Item 2 do Grupo 1: A infraestrutura deverá ser entregue em, no máximo, 77 (setenta e sete) dias úteis contados do recebimento da ordem de fornecimento para entrega dos hardwares e softwares.

3.5.2.2.1. A ordem de fornecimento deverá ser emitida pelo contratante em, no máximo, 10 (dez) dias úteis da vigência do

contrato.

3.5.2.2.2. A implantação de hardwares e softwares deverá ocorrer em até 10 (dez) dias úteis contados do recebimento provisório dos hardwares e softwares.

3.5.3.3. **Para as subscrições do Item 3 do Grupo 1**: A subscrição da ferramenta de simulação de ataque e verificação de brechas deverá ser entregue em, no máximo, 24 (vinte e quatro) dias úteis, contados do recebimento da ordem de fornecimento para entrega do licenciamento.

3.4.2.3.1. A ordem de fornecimento deverá ser emitida pelo contratante em, no máximo, 10 (dez) dias úteis da vigência do contrato.

3.5.3.4. **Grupo 1 - Item 04**: O serviço de operação assistida, terá início mediante emissão da ordem de início do serviço, seguindo-se o rito abaixo:

3.5.2.4.1. O contratante emitirá ordem de início do serviço em até 3 (três) dias úteis após o recebimento provisório das licenças do item 1 do Grupo 1.

3.5.2.4.2. A contratada terá 5 (cinco) dias úteis para indicar ao contratante a relação do(s) profissional(is) que realizarão os serviços.

3.5.2.4.3. O contratante terá 10 (dez) dias úteis para realizar análise de vida pregressa do(s) profissional(is) que realizarão os serviços e encaminhar à contratada a relação dos profissionais habilitados a realizar os serviços junto ao contratante, os quais deverão assinar termo de sigilo antes de iniciar suas atividades.

3.5.2.4.4. Caso nenhum profissional seja habilitado pelo TSE, a contratada terá prazo de indicação de profissionais reiniciado, nos termos do item 3.5.2.4.2.

3.5.3.5. **Grupo 1 - Item 05**: A execução das horas de suporte técnico especializada está condicionada a abertura de Ordem de Serviço específica.

3.5.2.5.1. Os trabalhos deverão ser iniciados por profissional do fabricante em até 5 (cinco) dias úteis após o recebimento da Ordem de Serviço pela contratada.

3.5.3.6. **Item 06:** A subscrição da lista de reputação de endereços IP deverá ser entregue em, no máximo, 24 (vinte e quatro) dias úteis contados do início da vigência contratual.

3.4.2.6.1. A ordem de fornecimento deverá ser emitida pelo contratante em, no máximo, 10 (dez) dias úteis da vigência do contrato.

3.5.4. Os prazos de adimplemento dos eventos listados acima, de responsabilidade da contratada, admitem prorrogação, em caráter excepcional, sem efeito suspensivo, devendo a solicitação ser encaminhada por escrito, com antecedência mínima de 5 (cinco) dias úteis do seu vencimento, anexando-se documento comprobatório do alegado pela contratada, ficando a aceitação da justificativa a critério do TSE e sem prejuízo da aplicação das sanções previstas neste Termo de Referência, caso convier, ressalvadas situações de caso fortuito e força maior.

3.5.5. O pedido de prorrogação deverá conter ao menos:

3.5.5.1. O motivo para não cumprimento do prazo, devidamente comprovado, e o novo prazo previsto para entrega.

3.5.5.2. A comprovação de que trata este tópico deverá ser promovida não apenas pela alegação da empresa Contratada, mas por meio de documentos que relatem e justifiquem a ocorrência dos fatos que ensejarão o descumprimento de prazo, tais como: carta do fabricante/fornecedor, laudo técnico de terceiros, Boletim de Ocorrência de Sinistro, ou outro equivalente.

3.6. GARANTIA TÉCNICA

3.6.1. As garantias deverão ser prestadas com vistas a manter os bens/serviços alocados e as licenças disponibilizadas, objeto da contratação, em perfeitas condições de uso, sem qualquer ônus ou custo adicional ao Contratante e deverão ser contadas a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto, conforme a seguir:

3.6.1.1. A Contratada estará obrigada a garantir todos os serviços por ela realizados pelo período de vigência contratual.

3.6.1.2. O prazo para refazer os serviços que apresentarem defeito dentro do prazo de garantia deverá ser de até 05 (cinco) dias úteis, contados do recebimento da notificação do Contratante.

3.6.1.3. A garantia dos equipamentos/hardwares fornecidos pela contratada deverá ter vigência de 30 (trinta) meses.

3.6.2. A garantia dos softwares deverá cobrir o fornecimento de atualizações e correções dos softwares.

3.6.3. Quanto aos serviços prestados:

3.6.3.1. As garantias deverão corrigir todos e quaisquer defeitos nos serviços prestados pela Contratada que compreendem, dentre outros: os erros e falhas, funcionais ou não funcionais, causados por ações ou omissões da Contratada; as imperfeições percebidas; a ausência de artefatos ou de documentação obrigatória; e qualquer outra ocorrência que impeça o funcionamento normal dos serviços contratados e adjacentes ou que não se apresentem dentro dos padrões e níveis de mercado.

3.6.4. A garantia deverá cobrir o direito de o TSE abrir chamados de suporte junto aos respectivos fabricantes dos softwares e hardwares fornecidos.

3.6.4.1. Os chamados registrados deverão obedecer aos seguintes níveis de severidade:

Severidade	**Descrição**
SEVERIDADE 1	Situação emergencial ou problema crítico que cause a indisponibilidade de sistema. A solução não está operante e não é possível nenhuma solução de contorno viável.
SEVERIDADE 2	Um ou mais componentes da solução parcialmente indisponíveis, causando indisponibilidade de funcionalidades.
SEVERIDADE 3	Um ou mais componentes da solução apresentam erros ou alertas que não causam indisponibilidade das suas funcionalidades.

3.6.4.2. Prazos de atendimentos

Severidade	**Prazo de solução**
SEVERIDADE 1	Até 24 horas, contadas da abertura do chamado.
SEVERIDADE 2	Até 48 horas, contadas da abertura do chamado.
SEVERIDADE 3	Até 72horas, contadas da abertura do chamado.

3.6.4.3. Aplicação de glosas

1	Não atender ao percentual mínimo de 95% de atendimento no prazo previsto no item 3.6.4.2. para Severidade 1 no período de um mês.	Desconto 1% (um por cento) a cada hora de atraso, sobre o valor da parcela mensal do item 4 da Tabela 01 deste Termo de Referência, limitada sua aplicação até o máximo de 10 (dez) horas.
2	Não atender ao percentual mínimo de 95% de atendimento no prazo previsto no item 3.6.4.2 para Severidade 2 no período de um mês.	Desconto 0,5% (meio por cento) a cada hora de atraso, sobre o valor da parcela mensal do item 4 da Tabela 01 deste Termo de Referência, limitada sua aplicação até o máximo de 20 (vinte) horas.
3	Não atender ao percentual mínimo de 95% de atendimento no prazo previsto no item 3.6.4.2 para Severidade 3 no período de um mês.	Desconto de 0,25% (vinte e cinco centésimo por cento) a cada hora de atraso, sobre o valor da parcela mensal do item 4 da Tabela 01 deste Termo de Referência, limitada sua aplicação até o máximo de 48 (quarenta e oito) horas.

3.7. NÍVEIS MÍNIMOS DE SERVIÇO (NMS)

3.7.1. Serão aplicáveis os seguintes Níveis Mínimos de Serviço.

3.7.1.1. **Indicador "A":** Disponibilidade dos serviços

ITEM	**DESCRIÇÃO**
Definição:	Garantir a disponibilidade do serviço SIEM (aplicável ao Item 4 do Grupo 1)

ITEM	DESCRIÇÃO
Finalidade:	Assegurar que a contratada atue proativamente para prover alta disponibilidade para o SIEM
Meta a Cumprir (nível mínimo de serviço):	Disponibilidade mensal de 99,9%, ou seja, pode ficar indisponível por cerca de 43 min. no mês (considerando-se a existência de 43.200 minutos em um mês comercial de 30 dias).
Instrumento de Medição:	Percentual de disponibilidade do sistema mensurado por meio de sistema Nagios ou similar.
Responsável:	Fiscalização técnica do contrato.
Periodicidade:	Mensal.
Mecanismos de Cálculo:	DISP = 1-(Total de minutos de indisponibilidade/43.200) x 100%
Início da Vigência:	A partir do início da execução dos serviços.
Ajustes no Pagamento:	Se DISP < 99,9%, então será aplicado desconto proporcional ao triplo do tempo em que o software ficou indisponível além da tolerância de 43 minutos: DESC= [3 x (Total de minutos de indisponibilidade - 43) x 100%]/43200 O valor do desconto está limitado a 20% do valor mensal do serviço do Item 4 do Grupo 1. Ultrapassado o valor limite estabelecido, será cobrada multa nos termos da tabela do Anexo I-IV – Penalidades, deste Termo de Referência. **Exemplo:** O sistema ficou fora do ar por 6 horas (360 minutos) DISP = 1-(360/43.200) DISP = 99,1666% DESC = [3 x (360-43) x 100%]/43.200 DESC = [951 x 100%]/43.200 DESC = [95.100%]/43.200 **DESC = 2,2%**

Obs: Não será considerado descumprimento de nível de serviço a ocorrência de indisponibilidade nas seguintes situações:

a) Interrupções programadas para manutenções preventivas e configurações (upgrade de hardware, correção de desvios, adequação tecnológica em atendimento às necessidades do Contratante), de iniciativa do Contratante ou Contratada, previamente acordadas com o Contratante;

b) Períodos de manutenção de interesse comum entre as partes;

c) Incidentes que, após análise, foram descaracterizados como indisponibilidade, desde que devidamente comprovado pelo Contratante;

d) Problemas de infraestrutura de responsabilidade do Contratante; e

e) Motivos de calamidade pública, desastres naturais e força maior, de acordo com a conceituação prevista em regulamentação legal.

f) Incidentes iniciados fora do horário de expediente, em finais de semana ou feriados.

3.7.1.2. Indicador "B": Entrega de produtos de serviços

ITEM	DESCRIÇÃO
Definição:	Entrega de produtos de serviços (aplicável aos itens 4 e 5 do Grupo 1)
Finalidade:	Garantir entrega de artefatos a cada período de realização de serviços ou OS.

ITEM	DESCRIÇÃO
Meta a Cumprir (nível mínimo de serviço:	Entregar, até o quinto dia útil subsequente ao término da OS ou do mês de exercício, os relatórios de execução de serviços do mês anterior
Instrumento de Medição:	Termo de recebimento provisório dos serviços
Responsável:	Fiscalização técnica do contrato.
Periodicidade:	Nos momentos de entrega de produtos e serviços.
Mecanismos de Cálculo:	I. Para cada entrega durante o período de apuração, será identificado se foi atendida no prazo. No caso do não cumprimento do prazo acordado, deverá ser apurada a quantidade de dias em atraso para entrega da demanda. II. Será computada a quantidade de dias úteis em atraso. III. Não serão computadas como atraso a indisponibilidade do Contratante para homologar a entrega. Fórmula para aferição: QT = [DTE – DTA]. Onde: QT = Quantidade de dias em atraso: DTE = Data da entrega: DTA = Data acordada para entrega
Início da Vigência:	A partir do início da execução dos serviços.
Ajustes no Pagamento:	Desc = QT (Vs x 0,0025), onde: Desc = Valor do desconto; QT = Quantidade de dias em atraso; Vs = Valor do serviço. 0,0025 = Valor fixo que representa o percentual diário de 0,25% para subtração do valor do serviço. O valor do desconto está limitado a 15 dias de atraso. Ultrapassado o valor limite estabelecido, será cobrada multa nos termos da tabela do Anexo I-IV – Penalidades, deste Termo de Referência.

3.8. FORMAS DE COMUNICAÇÃO E ACOMPANHAMENTO DA EXECUÇÃO DO CONTRATO

3.8.1. A comunicação entre o TSE e a Contratada durante a execução do contrato, far-se-á, preferencialmente, por meio do preposto designado pela contratada.

3.8.2. Poderão ser utilizados para a comunicação:

3.8.2.1. Ofícios;

3.8.2.2. Ordens de Serviço;

3.8.2.3. Mensagens escritas;

3.8.2.4. Relatórios de Medição e Relatórios em geral;

3.8.2.5. Termos de Recebimento;

3.8.2.6. Correspondência física ou eletrônica; e

3.8.2.7. Demais documentos previstos em contrato ou neste Termo de Referência.

3.8.3. Sem prejuízo da necessidade de realização de reuniões periódicas, as comunicações devem se dar, preferencialmente, da seguinte maneira:

3.8.3.1. Questões administrativas durante a execução do contrato, que exijam comunicação formal:

1. Meio de Comunicação: correspondência física ou eletrônica, com aviso e/ou confirmação de recebimento, por correio, ou por sistema informatizado de correio eletrônico;
2. Periodicidade: eventual ou conforme prazos previstos em contrato ou neste Termo de Referência.

3.8.3.2. Questões técnicas e/ou administrativas cotidianas, durante a execução do contrato:

1. Meio de Comunicação: correspondência eletrônica, telefone, sistemas ou qualquer outra forma acordada entre as partes, definidas na reunião inaugural;

2. Periodicidade: sempre disponível, em dias úteis, entre 8h e 20h.

3.8.3.3. Suporte Técnico e/ou Chamados de Manutenção.

Meio de Comunicação: página web, sistema informatizado, correspondência eletrônica, telefone (0800 ou Discagem Local);

Periodicidade: conforme discriminado no Anexo I - VI deste TR.

4. RECEBIMENTO E PAGAMENTO

4.1. RECEBIMENTO

4.1.1. O recebimento do **Item 1 do Grupo 1** será realizado mediante emissão de um Termo de Recebimento Provisório - TRP e um Termo de Recebimento Definitivo - TRD - Anexo I-II deste Termo de Referência, para cada uma das cinco subscrições de 6.000 EPS contratadas. O TRD somente será emitido após efetivamente ativado o licenciamento a que se refere.

4.1.2. O recebimento do **Item 2 do Grupo 1** será realizado mediante emissão de um Termo de Recebimento Provisório - TRP e um Termo de Recebimento Definitivo - TRD - Anexo I-II deste Termo de Referência. O TRD somente será emitido após a efetiva instalação de hardwares e softwares que compõem o item.

4.1.3. O recebimento do **Item 3 do Grupo 1** e do I**tem 6** será mediante emissão de um Termo de Recebimento Provisório - TRP e um Termo de Recebimento Definitivo - TRD - Anexo I-II deste Termo de Referência. O TRD somente será emitido após efetivamente ativado o licenciamento a que se refere.

4.1.4. O recebimento do **Item 4 do Grupo 1** será realizado mensalmente, mediante emissão de um Termo de Recebimento Provisório - TRP e um Termo de Recebimento Definitivo - TRD - Anexo I-II deste Termo de Referência. O TRD somente será emitido após a anuência da fiscalização técnica quanto ao recebimento de serviços ou artefatos produzidos no período.

4.1.5. O recebimento do **Item 5 do Grupo 1** será realizado mediante emissão de um Termo de Recebimento Provisório - TRP e um Termo de Recebimento Definitivo - TRD - Anexo I-II deste Termo de Referência, para cada Ordem de Serviço aberta. O TRD somente será emitido após anuência da fiscalização técnica quanto ao recebimento de serviços ou artefatos produzidos no período.

4.1.6. Os TRD deverão ser emitidos em até 5 (cinco) dias úteis após a entrega do objeto a que se referem.

4.1.6.1. Ficará suspenso o prazo para emissão dos Termos de Recebimento nos casos em que a Contratada for notificada a apresentar esclarecimentos e documentos.

4.1.7. A contratada deverá entregar à Fiscalização Técnica todos os documentos necessários para recebimento dos serviços prestados, previstos neste Termo de Referência e em seu Anexo I - VI, conjuntamente com a entrega do objeto.

4.1.8. A Contratada deverá reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, os serviços em que se verificarem vícios, defeitos ou incorreções resultantes de sua execução ou de materiais empregados, além de cumprir quaisquer obrigações pendentes apontadas pela Fiscalização Técnica, em até 05 (cinco) dias úteis, contados da notificação.

4.1.8.1. Decorrido o prazo ou sanada a(s) incorreção(ões) apontada(s) pela fiscalização, referente aos itens acima, será reiniciado o prazo para emissão do TRD.

4.1.9. O TRD contemplará também:

a) todas as evidências de descumprimento das obrigações assumidas pela Contratada, no todo ou em parte, **inclusive quanto a adequação do pagamento considerando eventuais reduções decorrente do não cumprimento dos níveis mínimos de serviço preestabelecidos neste Termo de Referência, se aplicável, conforme itens 3.6.4.3 e 3.7 deste Termo de Referência.**

a.1) no caso de controvérsia sobre a execução do objeto quanto à dimensão, qualidade e/ou quantidade, deverá estar indicada no TRD a parcela incontroversa, a qual deve ser liberada para pagamento, nos termos do art. 143 da Lei nº 14.133/2021, sem prejuízo da aplicação das sanções previstas neste Termo de Referência.

b) emissão de termo circunstanciado para efeito de recebimento definitivo dos serviços prestados, com base em relatórios e documentação apresentados; e

c) comunicação à empresa para que emita a nota fiscal ou fatura com o valor exato dimensionado pela fiscalização.

4.1.10. A Contratada deverá entregar o faturamento com toda documentação exigida em contrato para liquidação e pagamento em 08 (oito) dias úteis, contados da emissão do TRD.

4.1.11. A Contratada será responsável pelos danos causados diretamente à Administração ou a terceiros em razão da execução do contrato, e não excluirá nem reduzirá essa responsabilidade a fiscalização ou o acompanhamento pelo contratante, em conformidade com o art. 120 da Lei nº 14.133/21.

4.1.12. O recebimento provisório ou definitivo não excluirá da Contratada a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.

4.2. PAGAMENTO

4.2.1. Para o **Item 1 do Grupo 1**, o pagamento será realizado em uma parcela para cada lote de 6.000 EPS efetivamente recebido pelo TSE.

4.2.2. Para os **Itens 2 e 3 do Grupo 1 e Item 6**, será realizado em parcela única.

4.2.3. Para o **Item 4 do Grupo 1**, será realizado mensalmente.

4.2.4. Para o **Item 5 do Grupo 1**, será realizado por demanda, conforme item 4.1.5 deste TR.

4.2.5. O pagamento será efetuado até o 10º (décimo) dia útil, conforme atendimento das demandas de ordens de serviço para os itens 5 deste TR, após do atesto da nota fiscal/fatura pelo servidor responsável, com a emissão de ordem bancária para o crédito em conta corrente da contratada, observada a ordem cronológica estabelecida no art. 141 da Lei nº 14.133/21.

4.2.5.1. O atesto do **objeto contratual executado** se dará pelo fiscal administrativo, designado pela autoridade competente, por meio da emissão de Nota Técnica de Atesto (NTA). O fiscal administrativo terá o prazo de 4 (quatro) dias úteis para emitir a NTA e remeter o processo à unidade técnica responsável pelo pagamento, a partir do recebimento do documento fiscal, do Termo de Recebimento Definitivo - TRD e dos demais documentos exigidos em contrato para liquidação e pagamento da despesa.

4.2.5.1.1. A NTA deverá observar, no mínimo, os seguintes aspectos:

a) exigências previstas em normativo do TSE que disponha sobre os processos de contratação no âmbito do Tribunal.

b) análise dos relatórios e de toda a documentação apresentada conjuntamente com TRD e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando à Contratada, por escrito, as respectivas correções; e

c) verificação da necessidade de adequação do pagamento considerando eventuais reduções ou glosas decorrente do não cumprimento de indicadores e metas mínimos preestabelecidos neste Termo de Referência, conforme TRD.

4.2.5.2. Ficará suspenso o prazo para emissão da NTA, pelo período definido pela fiscalização, nos casos em que a Contratada for notificada a apresentar esclarecimentos e documentos. Após o prazo estabelecido, caso a contratada não sane as pendências, a fiscalização administrativa indicará a correspondente ressalva na NTA, e a liquidação poderá seguir com possibilidade de aplicação de glosas/sobrestamentos, até que haja os devidos esclarecimentos/comprovações.

4.2.5.3. O pagamento a ser efetuado em favor da **CONTRATADA**, em conta corrente previamente informada, estará sujeito à retenção na fonte de tributos e contribuições sociais de acordo com os normativos legais.

4.2.5.4. Na fase de liquidação e pagamento da despesa, a unidade de execução orçamentária e financeira realizará consulta *on-line* ao Sistema de Cadastramento Unificado de Fornecedores – SICAF, ou nos sítios de cada órgão regulador, com fins de verificar a regularidade da contratada perante a Seguridade Social e a Fazenda Federal, o Fundo de Garantia por Tempo de Serviço e a Justiça Trabalhista.

4.2.5.5. Quando houver ressalva no ateste dos serviços pela Fiscalização, no que concerne à execução do objeto do contrato, em relação às demais obrigações contratuais, ocorrerá à interrupção da contagem do prazo para pagamento, a partir da comunicação do fato à Contratada, até que sejam escoimados os vícios detectados.

4.2.5.6. As notas fiscais e os documentos exigidos nesse Termo de Referência, para fins de liquidação e pagamento das despesas, deverão ser entregues exclusivamente para o servidor responsável pela fiscalização do contrato.

4.2.5.7. O CNPJ constante da nota fiscal/fatura deverá ser o mesmo indicado na proposta e nota de empenho.

4.2.5.8. As notas fiscais apresentadas em desacordo com o estabelecido nesse tópico serão devolvidas à Contratada, não correndo, neste caso, o prazo para atesto da nota fiscal pelo fiscal responsável, o qual inicia-se somente a partir da completa regularização.

4.2.5.9. Sobre faturamentos complementares ou não emitidos no momento previsto, entregues posteriormente, não se aplica o prazo limite estabelecido neste item, sendo tratados junto com a liquidação de despesa do faturamento mensal seguinte.

4.2.6. Os pagamentos serão realizados a cada emissão de um termo de recebimento definitivo listados nos itens 4.1.1 a 4.1.5, conforme sua respectiva nota técnica de ateste.

5. OBRIGAÇÕES

5.1. OBRIGAÇÕES DA CONTRATADA

5.1.1. Executar, com observação dos prazos e exigências, todas as obrigações constantes deste TR.

5.1.2. Responsabilizar-se pelas despesas decorrentes da execução dos serviços objetos deste TR.

5.1.3. Informar, no momento da formalização da contratação, o nome do responsável (preposto), os contatos de telefone, e-mail ou outro meio hábil para comunicação com o TSE, conforme Anexo I-III deste Termo e observado o disposto no item 3.8 deste Termo de Referência.

5.1.4. Acatar as recomendações efetuadas pela fiscalização do contrato.

5.1.5. Responsabilizar-se pelos danos causados diretamente à Administração ou a terceiros, decorrentes de culpa ou dolo na execução do objeto do TR.

5.1.6. Fornecer à fiscalização do contrato relação nominal, com os respectivos números de documento de identidade e comprovações exigidas neste TR de todo o pessoal envolvido diretamente na execução dos serviços, em até 12 (doze) dias úteis após o início da vigência do contrato, bem como informar durante toda a vigência qualquer alteração que venha a ocorrer na referida relação.

5.1.7. Fazer com que seus empregados se submetam aos regulamentos de segurança e disciplina durante o período de permanência nas dependências do TSE, não sendo permitido o acesso dos funcionários que estejam utilizando trajes sumários (shorts, chinelos de dedo, camisetas regatas ou sem camisa).

5.1.8. Comunicar ao TSE, imediatamente, 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.

5.1.9. Manter o caráter confidencial dos dados e informações obtidos por qualquer meio ou prestados pelo TSE, 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, **observados ainda, no que couber, as diretrizes vigentes adstritas à LGPD (Lei Geral de Proteção de Dados)** e a Resolução CD/ANPD nº 2/2022, conforme disposto na cláusula - DA PROTEÇÃO DE DADOS do instrumento de contrato.

5.1.10. Fornecer aos seus funcionários EPIs, adequados à execução dos serviços e responsabilizar-se por seu uso obrigatório, durante todo período de execução do objeto, bem como as ferramentas e os equipamentos necessários para a execução de todos os serviços previstos nesse Termo.

5.1.11. Recompor, reconstituir ou consertar todo e qualquer elemento construtivo, instalação ou equipamento que venha a avariar no decorrer da execução dos serviços no prazo de até 5 (cinco) dias corridos, contados da notificação. Na impossibilidade de atendimento desse prazo, o mesmo poderá ser prorrogado, a critério da Administração, mediante aprovação de justificativa a ser apresentada pela CONTRATADA, dentro desse prazo

5.1.12. Manter, durante a execução do contrato as condições de habilitação e qualificação exigidas na licitação.

5.1.12.1. Verificadas irregularidades nas condições que ensejaram sua habilitação, 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.

5.1.13. Responsabilizar-se pelos encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução do contrato.

5.1.13.1. A inadimplência da contratada em relação aos encargos suportados não transferirá à Administração a responsabilidade pelo seu pagamento e não poderá onerar o objeto do contrato.

5.1.14. Orientar seus funcionários acerca da necessidade de observar protocolos sanitários definido pelo Contratante.

5.1.15. Fornecer máscaras N95 aos seus funcionários, em quantidade suficiente, para ingresso e permanência nas dependências do TSE, **quando houver a exigência do uso por parte do Tribunal.**

5.1.16. Afastar os funcionários que apresentarem sintomas de doenças infectocontagiosas, sem prejuízo da prestação dos serviços.

5.1.17. Exigir do AUTOR/CONTRATADA dos projetos, previstos no cronograma e neste TR, a cessão dos direitos patrimoniais a eles relativo para a Administração Pública, nos termos do art. 93 da Lei nº 14.133/2021.

5.1.18. Assinar o Termo de Confidencialidade, disponível no Anexo I-X deste Termo de Referência.

5.1.19. Apresentar ao TSE, o Termo de Ciência, disponível no Anexo I-IX deste Termo de Referência para cada profissional alocado para realizar serviços previstos no Item 4 do Grupo 1 junto ao TSE.

5.1.20. Durante a vigência da contratação, apresentar, sempre que solicitado, declaração de que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

5.2. OBRIGAÇÕES DO CONTRATANTE

5.2.1. Prestar as informações e os esclarecimentos que venham a ser solicitados pela contratada.

5.2.2. Designar comissão de servidores para fiscalizar a execução técnica do objeto contratual.

5.2.3. Acompanhar, fiscalizar, receber e atestar a execução contratual, bem como indicar as ocorrências verificadas, nos termos de normativo do TSE que disponha sobre os processos de contratação no âmbito do Tribunal.

5.2.4. Permitir que os funcionários da contratada, desde que devidamente identificados, tenham acesso aos locais de execução dos serviços.

5.2.5. Recusar qualquer serviço entregue em desacordo com as especificações constantes desse Termo de Referência ou com defeito.

5.2.6. Realizar reunião inaugural antes do início efetivo da prestação dos serviços entre a fiscalização e a contratada.

5.2.7. Efetuar o pagamento à contratada, segundo as condições estabelecidas nesse Termo de Referência.

i

6. DISPOSIÇÕES GERAIS

6.1. PRAZOS DE VIGÊNCIA

6.1.1. O contrato terá vigência a partir de _____/_____/_____ e duração de 30 (trinta) meses, prorrogáveis nos termos da lei.

6.1.2. A contratante terá a opção de extinguir o contrato, sem ônus, quando não dispuser de créditos orçamentários para sua continuidade ou quando entender que o contrato não mais lhe oferece vantagem.

6.1.3. A extinção mencionada no item 6.1.2 desse Termo de Referência ocorrerá apenas na próxima data de aniversário do contrato e não poderá ocorrer em prazo inferior a 2 (dois) meses, contado da referida data.

6.2. CRITÉRIOS DE SUSTENTABILIDADE

6.2.1. Comprovar, como condição para participação na licitação, não possuir inscrição no cadastro de empregadores que tenham submetido trabalhadores a condições análogas à de escravo (Portaria Interministerial MTPS/MM/IRDH nº 4/2016).

6.2.1.1. A comprovação desse critério será efetuada a partir da consulta ao Cadastro acima mencionado, no sítio eletrônico (https://www.gov.br/trabalho-e-emprego/pt-br/assuntos/inspecao-do-trabalho/areas-de-atuacao/cadastro_de_empregadores.pdf), no qual consta lista emitida pelo Ministério do Trabalho e Emprego.

6.2.2. Comprovar, como condição para contratação, não ter sido condenada, a adjudicatária e seus dirigentes, por infringir as leis de combate à discriminação de raça ou de gênero, ao trabalho infantil e ao trabalho escravo, em afronta ao previsto nos arts. 1º e 170 da Constituição Federal de 1988; no art. 149 do Código Penal; no Decreto nº 5.017/2004 (promulga o Protocolo de Palermo) e nas Convenções nºs 29 e 105 da Organização Internacional do Trabalho.

6.2.2.1. Deverá ser apresentada Certidão Judicial de Distribuição ("nada consta" ou "certidão negativa"), **da esfera criminal, da Justiça Comum, Federal e Estadual,** da

adjudicatária e de seus dirigentes.

6.2.3. Comprovar, como condição para participação na licitação, caso a empresa possua 100 (cem) ou mais empregados, atender ao disposto no art. 93 da Lei nº 8.213/91, que determina a obrigatoriedade do preenchimento de 2 a 5% dos seus cargos com beneficiários reabilitados ou com pessoas com deficiência habilitadas, na seguinte proporção:

I - até 200 empregados: 2%;

II - de 201 a 500: 3%;

III - de 501 a 1.000: 4%; e

IV - de 1.001 em diante: 5%.

6.2.3.1. A comprovação será feita mediante declaração de que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas, nos termos do Inciso IV do Art. 63 da Lei 14.133/2021.

6.2.3.2. Sempre que solicitado pela Administração, a contratada deverá comprovar o cumprimento da reserva de cargos a que se refere o item 6.2.3, com a indicação dos empregados que preencherem as referidas vagas, no prazo de até 10 (dez) dias úteis contados da solicitação, sob pena de notificação aos órgãos competentes pela fiscalização.

6.2.4. Tendo em vista as particularidades técnicas dos serviços a serem contratados, a Contratada, sempre que possível, está desobrigada de apresentar ou comprovar a entrega dos produtos e execuções de serviços de forma impressa. Dessa maneira, sempre que possível, os documentos resultantes da contratação serão apresentados em formato eletrônico.

6.3. SUBCONTRATAÇÃO

6.3.1. É vedado transferir a outrem, no todo ou em parte, o objeto da presente contratação.

6.4. VISTORIA

6.4.1. O TSE facultará a realização de vistoria, nos locais de execução dos serviços constantes deste TR, às empresas interessadas em concorrer, com fins de análise e elaboração de suas propostas.

6.4.1.1. A Licitante que entender por imprescindível a vistoria prévia no local de execução do serviço, mormente para o conhecimento pleno das condições e peculiaridades técnicas de recepção da infraestrutura do item 2 da Tabela 01 deste TR.

6.4.1.2. Antes de iniciar a vistoria técnica, o profissional designado da licitante deverá assinar Termo de Confidencialidade específico (Anexo I - VIII deste TR) quanto às informações repassadas;

6.4.2. Caso o Licitante opte por não realizar a vistoria, ele terá de atestar o conhecimento pleno das condições e peculiaridades da contratação, mediante declaração formal do seu responsável técnico (art. 63, §3º, da Lei 14.133/2021).

6.4.3. Caso o Licitante realize a vistoria, deverá apresentar atestado próprio dessa vistoria, sem ônus ao Contratante, informando dia, hora e o responsável técnico da empresa participante desse evento, sendo a validade deste documento verificada no momento da habilitação técnica.

6.4.4. A vistoria poderá ser realizada pela empresa, em dias úteis, das 12h às 19h e agendada com antecedência mínima de 24 horas pelo telefone (61) 3030-8971 - Seção de Defesa Cibernética ou pelo e-mail sdciber@tse.jus.br, podendo ser realizada até a data de abertura das propostas.

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

6.4.6. A não realização da vistoria não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes dos locais da prestação dos serviços, devendo o contratado assumir os ônus dos serviços decorrentes.

ANEXO I-I - MODELO DE PROPOSTA

Razão Social:		E-mail:	CNPJ:
Endereço:	Cidade:	CEP:	Tel:

Tabela - Contratação por grupo						
Grupo	**item**	**Descrição Sucinta do Serviço**	**Unidade de Medida**	**Quantidade**	**Valor Unitário (R$)**	**Valor Total (R$)**

Tabela - Contratação por grupo						
	1	Subscrição de solução de gerenciamento e correlação de eventos de segurança da informação (SIEM – Security Information and Event Management) com tecnologia Security Analytics e UEBA (User and Entity Behavior Analytics) ou UBA (User Behavior Analytics) para 20 usuários simultâneos, com garantia de 30 meses, dimensionado para 6.000 eventos por segundo (EPS) Obs: A licitante deverá apontar marca, modelo e partnumber de cada produto ofertado.	Un.	5		

	Tabela - Contratação por grupo					
1	2	Fornecimento de infraestrutura de processamento, conectividade e armazenamento (instalação, manutenção e suporte de peças) de dados necessária e suficiente às operações da solução de gerenciamento e correlação de eventos de segurança da informação – SIEM (a ser instalado nas dependências do Contratante), composto por cluster de hardware em alta disponibilidade, incluindo equipamento de gerência e equipamento de tratamento de logs e evidências, com garantia de 30 meses, dimensionado para 30.000 eventos por segundo (EPS). Obs: A licitante deverá apontar marca, modelo e partnumber de cada produto ofertado.	Un.	1		
	3	Subscrição, com licenciamento somente para o TSE, para simulação de ataque e verificação de brechas de segurança do ambiente de rede corporativa, incluindo serviço de diretório e firewall de aplicações Obs: A licitante deverá apontar marca, modelo e partnumber de cada produto ofertado.	Un.	1		

	Tabela - Contratação por grupo					
	4	Serviço de operação assistida em regime de consultoria especializada para suporte e parametrização da solução do Grupo 1, com foco no gerenciamento e correlação de eventos de segurança da informação – SIEM, por 30 meses. Obs: a licitante deverá detalhar a formação de custo dos serviços	Un.	30		
	5	240 (duzentas e quarenta) horas, durante a vigência do contrato, de suporte técnico especializado realizado exclusivamente pelo fabricante, sob demanda, em horas. Obs: a licitante deverá detalhar a formação de custo dos serviços.	Un.	240		
-	6	Subscrição de fornecimento de lista de reputação de endereços IP que cubram a proteção de serviços maliciosos de VPN, Proxy, Proxy Residencial, Proxy Malware ou redes de Bots, bem como a visibilidade de tráfego malicioso no ambiente da Contratante (internet e rede local). Obs: A licitante deverá apontar marca, modelo e partnumber de cada produto ofertado.	Un.	1		
					VALOR TOTAL DO CONTRATO (R$):	

Deverá ser atendida, juntamente com a proposta, a exigência prevista no item 3.3.1.2. deste TR.
Declarações: i) Esta empresa declara que tem pleno conhecimento das condições necessárias para a prestação dos serviços e peculiaridades da contratação. ii) Esta empresa atesta que conhece o local e as condições de realização do serviço. iii) Esta empresa declara que nos preços propostos acima estão incluídas todas as despesas, frete, tributos e demais encargos de qualquer natureza incidentes sobre o objeto desta contratação, inclusive compreendem a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes. iv) Esta empresa declara estar ciente de que a apresentação da presente proposta implica na plena aceitação das condições estabelecidas **no Edital e seus Anexos**. v) Esta empresa declara estar ciente da necessidade de apresentação dos documentos de habilitação exigidos, bem como dos critérios de sustentabilidades a serem comprovados e dos demais documentos previstos **no Edital e seus Anexos.**
Validade da Proposta: O prazo de validade desta proposta é de 60 (sessenta) dias corridos, contados da data de abertura do Pregão.
Local e data. _____ Nome do Responsável Legal Cargo/Função

Observações para o Preenchimento da Proposta pelas Empresas:

1) A tabela da proposta deverá ser ajustada, preenchendo-se as linhas e colunas de acordo com os itens e/ou grupos para os quais a empresa tenha ofertado a melhor proposta, com o detalhamento do objeto a ser fornecido, observadas as especificações contidas no Termo de Referência.

Planilha auxiliar do Modelo de proposta (Anexo I - I)

Grupo	Item	Descrição do item	Descrição dos componentes (conforme solução ofertada)	Fabricante	Modelo	Part number/Código do produto	Quantidade	Preço unitário
	1	Licença de subscrição para solução de gerenciamento e correlação de eventos de segurança da informação (SIEM – Security Information and Event Management) com tecnologia Security Analytics e UEBA (User and Entity Behavior Analytics) ou UBA (User Behavior Analytics) para 20 usuários simultâneos	Licença de subscrição:					
			Garantia:					
			Outros componentes:					
			Equipamentos de hardware em alta disponibilidade: Equipamento 1 - Equipamento 2 - Equipamento n -					

1	2	Fornecimento de Infraestrutura de processamento, conectividade e armazenamento (instalação, manutenção e suporte de peças) de dados necessária e suficiente às operações da solução de gerenciamento e correlação de eventos de segurança da informação – SIEM (a ser instalado nas dependências do Contratante), composto por cluster de hardware em alta disponibilidade, incluindo equipamento de gerência e equipamento de tratamento de logs e evidências.	Softwares relacionados aos hardwares em alta disponibilidade: Software 1 - Software 2 - Software n -					
			Equipamentos de gerência: Equipamento 1 - Equipamento 2 - Equipamento n -					
			Softwares relacionados aos equipamentos de gerência: Software 1 - Software 2 - Software n -					
			Equipamentos de tratamento de log e evidências: Equipamento 1 - Equipamento 2 - Equipamento n -					
			Softwares relacionados aos equipamentos de tratamento de log e evidências: Software 1 - Software 2 - Software n -					
			Equipamentos de conectividade: Equipamento 1 - Equipamento 2 - Equipamento n -					
			Softwares relacionados aos equipamentos de conectividade: Software 1 - Software 2 - Software n -					
			Equipamento de armazenamento: Equipamento 1 - Equipamento 2 - Equipamento n -					
			Softwares relacionados aos equipamentos de armazenamento: Software 1 - Software 2 - Software n -					
			Suporte de peças:					
			Características exclusivas dos serviços (custo e formação de preços)	Perfil profissional do executante do serviço	Quantidade de profissionais	Valor unitário da hora por profissional	Quantidade de horas estimadas para execução do serviço	Custo total do serviço
			Descrição sucinta do serviço de Instalação:					
			Descrição sucinta do serviço de manutenção:					

	3	Subscrição, com licenciamento somente para o TSE, para simulação de ataque e verificação de brechas de segurança do ambiente de rede corporativa, incluindo serviço de diretório e firewall de aplicações.	Licença de subscrição:					
			Serviço de diretório:					
			Serviço de firewall:					
	4	180 (cento e oitenta) horas mensais de Serviço de operação assistida onsite em regime de consultoria especializada para suporte e parametrização da solução de gerenciamento e correlação de eventos de segurança da informação – SIEM.	Descrição dos serviços de operação assistida:				180	
	5	240 (duzentos e quarenta) horas, durante a vigência do contrato, de suporte técnico especializado realizado exclusivamente pelo fabricante, sob demanda.	Descrição dos serviços de suporte técnico especializado do fabricante:				240	
			Descrição dos componentes *	**Fabricante**	**Modelo**	**Part number/Código do produto**	**Quantidade**	**Preço unitário**
	6	Subscrição de fornecimento de lista de reputação de endereços IP que cubram a proteção de serviços maliciosos de VPN, Proxy, Proxy Residencial, Proxy Malware ou redes de Bots, bem como a visibilidade de tráfego malicioso no ambiente da Contratante (internet e rede local).	Licença de subscrição:					

ANEXO I-II - LISTAS DE VERIFICAÇÃO

TERMO DE RECEBIMENTO PROVISÓRIO - PARA OS ITENS 1, 2 E 3 DO GRUPO 1 E ITEM 6 DO OBJETO			
Processo SEI Relacionado: **Contratada:** **CNPJ nº:** **Contrato TSE nº:** **Objeto:** **Vigência:**			
Fiscalização: Memorando nº (SEI nº) **Fiscal Técnico Titular:** **Fiscal Técnico Substituto:**			
LISTA DE VERIFICAÇÃO			
ITEM	**ANÁLISE DOS ASPECTOS DE EXECUÇÃO E ENTREGA:**	**SIM**	**NÃO**
1	A CONTRATADA iniciou os serviços no prazo previsto?		
2	A CONTRATADA entregou licenças e subscrições no prazo previsto?		
3	Os serviços foram entregues dentro do prazo previsto?		
RELATÓRIO DE OCORRÊNCIAS			
RECEBIMENTO PROVISÓRIO DO OBJETO			
Diante da entrega dos serviços pela CONTRATADA e observada a posterior avaliação detalhada dos aspectos quantitativos e qualitativos a ser efetuada durante o Recebimento Definitivo, essa fiscalização decide por:			
	R E C E B E R PROVISORIAMENTE O OBJETO, **RESSALVADAS EVENTUAIS OCORRÊNCIAS DESCRITAS NESTE DOCUMENTO.**		
	NÃO RECEBER PROVISORIAMENTE O OBJETO.		

TERMO DE RECEBIMENTO DEFINITIVO - PARA OS ITENS 1, 2 E 3 DO GRUPO 1 E ITEM 6 DO OBJETO				
Processo SEI Relacionado: **Edital de Licitação TSE nº:** **Contratada:** **CNPJ nº:** **Contrato TSE nº:** **Objeto:** **Vigência:**				
Fiscalização: Memorando nº (SEI nº) **Fiscal Técnico Titular:** **Fiscal Técnico Substituto:**				
ITEM	**CRITÉRIO DE CONFERÊNCIA**	**SIM**	**NÃO**	**N/A**
1	**ASPECTOS QUANTITATIVOS DO SERVIÇO:**			
1.1	As licenças e subscrições estão de acordo com os requisitos qualitativos e quantitativos estabelecidas no TR?			
1.2	A infraestrutura de TI foi entregue em quantitativo e requisitos qualitativos proporcional ao que foi estabelecido no TR, incluindo aspectos de capacidade e desempenho?			
2	**ASPECTOS QUALITATIVOS DO SERVIÇO**:			
2.1	Os níveis mínimos de serviço previstos no Instrumento de Medição de Resultado (IMR) foram aferidos e contabilizados os requisitos qualitativos para apresentação à contratada e ajustes no pagamento?			
2.2	O ambiente de TI disponibilizado atendeu aos critérios estabelecidos no TR, incluindo aspectos de capacidade e desempenho?			
2.3	A lista de reputação de endereços IP que cubram a proteção de serviços maliciosos foi atualizada conforme estabelecidos no TR?			
3	**OUTRAS OBRIGAÇÕES CONTRATUAIS**:			
3.1	As documentações que exigem periodicidade de entrega foram entregues conforme estabelecidos no TR, incluindo aspectos de capacidade e desempenho?			

TERMO DE RECEBIMENTO DEFINITIVO - PARA OS ITENS 1, 2 E 3 DO GRUPO 1 E ITEM 6 DO OBJETO	
	HOUVE ABERTURA DE PROCESSO ADMINISTRATIVO PARA APLICAÇÃO DE PENALIDADES? **SEI nº:**
RELATÓRIO DE OCORRÊNCIAS	
RECEBIMENTO DEFINITIVO DO OBJETO	
Efetuada a análise de conformidade do objeto com as especificações do Termo de Referência e do instrumento contratual, quanto aos aspectos quantitativos, qualitativos e de obrigações contratuais, a fiscalização decide, ressalvadas eventuais observações contidas no Relatório de Ocorrências, por:	
	RECEBER DEFINITIVAMENTE O OBJETO
	NÃO RECEBER DEFINITIVAMENTE O OBJETO

TERMO DE RECEBIMENTO PROVISÓRIO - PARA OS ITENS 4 e 5 DO GRUPO 1 DO OBJETO	
Processo SEI Relacionado: **Contratada:** **CNPJ nº:** **Contrato TSE nº:** **Objeto:** Prestação de serviço de **Vigência:**	
Fiscalização: Memorando nº (SEI nº) **Fiscal Técnico Titular:** **Fiscal Técnico Substituto:**	
LISTA DE VERIFICAÇÃO	
ITEM	**ANÁLISE DOS ASPECTOS DE EXECUÇÃO E ENTREGA:**
1	A CONTRATADA iniciou os serviços no prazo previsto na ordem de serviço, inclusive aspectos de capacidade e desempenho?
2	As exigências de qualificação técnica dos profissionais foram cumpridas?
3	A CONTRATADA finalizou os serviços no prazo previsto na ordem de serviço?
RELATÓRIO DE OCORRÊNCIAS	
RECEBIMENTO PROVISÓRIO DO OBJETO	
Diante da entrega dos serviços pela CONTRATADA e observada a posterior avaliação detalhada dos aspectos quantitativos e qualitativos a ser efetuada durante o Recebimento Definitivo, essa fiscalização decide por:	
	R E C E B E R PROVISORIAMENTE O OBJETO, **RESSALVADAS EVENTUAIS OCORRÊNCIAS DESCRITAS NESTE DOCUMENTO.**
	NÃO RECEBER PROVISORIAMENTE O OBJETO.

TERMO DE RECEBIMENTO DEFINITIVO - PARA OS ITENS 4 E 5 DO GRUPO 1 DO OBJETO	
Processo SEI Relacionado: **Edital de Licitação TSE nº:** **Contratada:** **CNPJ nº:** **Contrato TSE nº:** **Objeto:** Prestação de serviço de **Vigência:**	
Fiscalização: Memorando nº (SEI nº) **Fiscal Técnico Titular:** **Fiscal Técnico Substituto:**	
ITEM	**CRITÉRIO DE CONFERÊNCIA**
1	**ASPECTOS QUANTITATIVOS DO SERVIÇO:**
1	Todas as demandas da ordem de serviço foram atendidas conforme nela estabelecido?
2	**ASPECTOS QUALITATIVOS DO SERVIÇO**:
2.1	Os serviços executados na ordem de serviço atenderam aos critérios estabelecidos neste TR e em seus anexos?
2.2	Houve postergação de demandas da ordem de serviço em decorrência de fatos supervenientes ou a critério do Contratante?
3	**OUTRAS OBRIGAÇÕES CONTRATUAIS**:
3.1	As documentações que foram exigidas na ordem de serviço foram entregues?
	HOUVE ABERTURA DE PROCESSO ADMINISTRATIVO PARA APLICAÇÃO DE PENALIDADES? **SEI nº:**
RELATÓRIO DE OCORRÊNCIAS	
RECEBIMENTO DEFINITIVO DO OBJETO	
Efetuada a análise de conformidade do objeto com as especificações do Termo de Referência e do instrumento contratual, quanto aos aspectos quantitativos, qualitativos e de obrigações contratuais, a fiscalização decide, ressalvadas eventuais observações contidas no Relatório de Ocorrências, por:	
	RECEBER DEFINITIVAMENTE O OBJETO
	NÃO RECEBER DEFINITIVAMENTE O OBJETO

ANEXO I-III - DESIGNAÇÃO DE PREPOSTO

DESIGNAÇÃO DE PREPOSTO	
A empresa **Nome da Empresa**, com sede na **Endereço da empresa**, na cidade de **Cidade**, (**UF**), CNPJ nº **000.000.000/0000-0**, neste ato representada pelo seu **Cargo do Representante**, Senhor(a) **Nome do Representante** portador(a) da Carteira de Identidade nº **Identidade do Representante**, CPF nº **CPF do Representante**, em atenção ao art. 44 da IN MPDG nº 5/2017, DESIGNA, o(a) Senhor(a) **Nome do Colaborador**, portador(a) da Carteira de Identidade nº **Identidade do Colaborado**, CPF nº **CPF do Colaborador**, para atuar como preposto no âmbito do **Contrato TSE nº xx/xxxx**.	
2. O preposto designado representará a empresa perante o Tribunal Superior Eleitoral, zelará pela boa execução do objeto contratual, exercendo os seguintes poderes e deveres:	
a)	Ser acessível ao Contratante, por intermédio do email e dos números de telefone fixo e celular informados neste formulário.
b)	Acatar as recomendações efetuadas pelo fiscal do contrato.
c)	Verificar se os funcionários da contratada encontram-se devidamente uniformizados, utilizando EPI, se for caso, e com apresentação compatível com o serviço.
d)	Manter a ordem, a disciplina e o respeito, junto a todo o pessoal da Contratada, orientando e instruindo os empregados quanto à forma de agir com vistas a proporcionar ambiente de trabalho harmonioso.

3. A comunicação entre o preposto e o Tribunal Superior Eleitoral será efetuada por meio dos telefones fixo **(DDD) 00000-0000** e celular **(DDD) 00000-0000** ou do e-mail **email@email.com.br**.
4. A **Nome da Empresa** compromete-se a manter atualizados, durante toda fase de execução da contratação, os contatos de telefone e e-mail para comunicação com o Tribunal Superior Eleitoral.

ANEXO I-IV - PENALIDADES

1. Nos termos do art. 155 da Lei 14.133/2021, o licitante ou contratado será responsabilizado administrativamente pelas seguintes infrações:

1.1. dar causa à inexecução parcial do contrato;

1.2. dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

1.3. dar causa à inexecução total do contrato;

1.4. deixar de entregar a documentação exigida para o certame;

1.5. não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

1.6. não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

1.7. ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

1.8. apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato;

1.9. fraudar a licitação ou praticar ato fraudulento na execução do contrato;

1.10. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

1.11. praticar atos ilícitos com vistas a frustrar os objetivos da licitação;

1.12. praticar ato lesivo previsto no art. 5º da Lei nº 12.846/2013.

2. Ao responsável pela prática de quaisquer dos atos tipificados como infração administrativa, será aplicada sanção de:

2.1. advertência, na ocorrência de causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave;

2.2. multa, na ocorrência de quaisquer das infrações administrativas previstas no item 1 desta Cláusula.

2.3. impedimento de licitar e contratar, na ocorrência das condutas previstas nos itens 1.2, 1.3, 1.4, 1.5, 1.6 e 1.7 deste Anexo, sempre que não se justificar a imposição de penalidade mais grave.

2.3.1. nesta hipótese, o responsável será impedido de licitar ou contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo de até 3 (três) anos;

2.4. declaração de inidoneidade para licitar ou contratar, na ocorrência das condutas previstas nos itens 1.8, 1.9, 1.10, 1.11 e 1.12, bem como nos itens 1.2, 1.3, 1.4, 1.5, 1.6 e 1.7 desta Cláusula, que justifiquem a imposição de penalidade mais grave.

2.4.1. nesta hipótese, o responsável será impedido de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos.

3. Para efeito de aplicação de advertência e multa, às infrações são atribuídas regras, conforme a tabela a seguir:

Item	Descrição	Incidência	Ação administrativa sobre a incidência da infração	Inexecução parcial do contrato
INFRAÇÕES DE IMPACTO MÉDIO				
1	Deixar de apresentar documentação prevista no Termo de Referência.	1ª ocorrência para os itens de 1 a 3 deste quadro.	Advertência	Não se aplica
2	Deixar de cumprir determinação formal ou orientação da fiscalização prevista no Termo de Referência.	Da 2ª a 4ª ocorrência para os itens de 1 a 3 deste quadro.	Multa de 0,5% sobre o valor do contrato.	Não se aplica
3	Descumprimento de outras obrigações previstas no Termo de Referência.	Da 5ª a 8ª ocorrência para os itens de 1 a 3 deste quadro.	Multa de 0,6% sobre o valor do contrato.	A partir da 9ª ocorrência (para os itens de 1 a 3 deste quadro) será caracterizada a inexecução parcial do contrato.
4	Deixar de prestar quaisquer informações solicitadas no prazo estipulado ou prestar informações inverídicas.	1ª ocorrência para os itens 4 a 6 deste quadro.	Advertência	Não se aplica.
5	Não cumprir os requisitos qualitativos e quantitativos, de desempenho, eficiência e produtividade das entregas técnicas, conforme previsto em ordem de serviço, estudo técnico preliminar e termo de referência, durante toda a fase de execução contratual.	Da 2ª a 4ª ocorrência para os itens 4 a 6 deste quadro.	Multa de 0,7% sobre o valor do contrato	A partir da 5ª ocorrência para os itens 4 a 6 deste quadro será caracterizada a inexecução parcial do contrato.
6	Não substituir, no prazo determinado pela fiscalização, o profissional que apresente atitude incompatível, falta de urbanidade ou cometa transgressão das normas disciplinares do Contratante.			
INFRAÇÕES DE IMPACTO GRAVE				
7	Infringir os critérios definidos no Termo de Confidencialidade e no Termo de Responsabilidade e Compromisso de Manutenção de Sigilo, anexos do Termo de Referência.	Da 1ª a 3ª ocorrência para os itens 7 a 14 deste quadro.	Multa de 0,8% sobre o valor do contrato	Não se aplica.
8	Prestar serviço em desconformidade ao estabelecido no objeto da contratação.			

9	Não designar o preposto conforme previsto no Termo de Referência			
10	Não atender no prazo previsto a regularização dos serviços executados fora dos requisitos exigidos no Termo de Referência.			
11	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços contratuais.			
12	Não atender a determinação prevista nos itens 2.1 e 2.2 do Anexo I-IV do Termo de Referência.			
13	Deixar de executar o contrato, salvo por motivo de força maior ou caso fortuito, por qualquer tempo.			
14	Não regularizar, no prazo previsto no Termo de Referência as condições que ensejaram a habilitação da empresa quanto àregularidade fiscal e trabalhista.	Da 4ª a 5ª ocorrência para os itens 7 a 14 deste quadro.	Multa de 0,9% sobre o valor do contrato	A partir da 6ª ocorrência para itens 7 a 14 deste quadro serácaracterizada a inexecução parcial do contrato.
15	Exceder em até 50% (cinquenta por cento) ao limite máximo de horas no descumprimento do nível de serviço estabelecido para os chamados de qualquer severidade do item 3.6.4.3. deste Termo de Referência.	Ocorrência única a qualquer nível de severidade.	Multa de 0,9% sobre o valor do contrato.	Não se aplica.
INFRAÇÕES DE IMPACTO MUITO GRAVE				
16	Atrasar a entrega de bens e serviços após a formalização da demanda ou prazos prefixados, iniciando-se a contagem, para fins desta infração no 10º dia corrido.	Do 11º dia ao 30º dia corrido de atraso para o item 16 deste quadro.	Multa de 1%sobre o valor do contrato	A partir do 31º dia de atraso para o item 16 deste quadro será caracterizada a inexecução parcial do contrato.
17	Causar danos ou não zelar pelas instalações ou patrimônio do Contratante	1ª ocorrência para os itens 17 e 18 deste quadro.	Multa de 1,1%sobre o valor do contrato.	Não se aplica.

18	Utilizar quaisquer produtos (metodologias, políticas, normas, procedimentos, softwares etc.) sem a autorização expressa do proprietário do produto e do Contratante, sem prejuízo de responsabilização por danos causados a terceiros.	2ª ocorrência para os itens 17 e 18 deste quadro.	Multa de 1,2%sobre o valor do contrato.	A partir da 3ª ocorrência para os itens 17 e 18 deste quadro serácaracterizada a inexecuçãoparcial do contrato.
19	Permitir situação que crie a possibilidade de causar dano físico a terceiros, lesão corporal ou consequências letais.	Ocorrência única para o item 16 deste quadro.	-	A 1ª ocorrênciacaracterizará inexecução parcialpara o item 19 deste quadro.

4. Ultrapassado o limite máximo de aplicação da penalidade previsto na tabela de infração, a Administração poderá optar uma das seguintes hipóteses:

4.1. Presente o interesse público, aceitar a continuidade da prestação do serviço mediante justificativa com aplicação apenas da multa de mora e/ou convencional. A continuidade da prestação do serviço só será possível mediante demonstração nos autos de que sua recusa causará prejuízo à Administração.

4.2. Caso os serviços ainda não tenham sido recebidos pelo Contratante, no todo ou em parte, recusar o objeto e rescindir o contrato, configurando sua inexecução total, com aplicação de multa compensatória de 20% (vinte por cento) do valor total contratado, sem prejuízo das demais consequências previstas em lei e no instrumento contratual.

4.2.1 Se a parte recebida do serviço não apresentar serventia à Administração em virtude de ser o serviço indivisível ou interdependentes suas partes, configurar-se-á a inexecução total do contrato, com eventual devolução de valores recebidos pela Contratada, sem prejuízo da aplicação das sanções incidentes ao descumprimento contratual.

4.3. Caso o todo ou parte dos serviços já tenham sido recebidos pelo Contratante, rescindir o contrato e recusar o restante do objeto, se aplicável, configurando sua inexecução parcial, com a aplicação de multa compensatória de 15% (quinze por cento) do valor total contratado, sem prejuízo das demais consequências previstas em lei e no instrumento contratual.

4.4. As multas de mora ou convencional não serão cumuladas com a multa compensatória proveniente de inexecução contratual pela mesma infração. A multa de mora ou convencional que já tiver sido quitada poderá ter seu valor abatido do montante apurado da multa compensatória, desde que decorrentes da mesma infração/ocorrência.

5. Na aplicação das penalidades, a Autoridade Competente poderá considerar, além das previsões legais, contratuais e dos Princípios da Administração Pública, as seguintes circunstâncias:

5.1. a natureza e a gravidade da infração;

5.2. as peculiaridades do caso concreto;

5.3. as circunstâncias agravantes ou atenuantes;

5.4. os danos que dela provierem para a Administração Pública;

5.5. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle;

5.6. a vantagem auferida em virtude da infração; e

5.7. os antecedentes.

6. Os prazos de adimplemento das obrigações Contratadas admitem prorrogação, em caráter excepcional, sem efeito suspensivo, devendo a solicitação ser encaminhada por escrito, com antecedência mínima de 5 (cinco) dias úteis do seu vencimento, anexando-se documento comprobatório do alegado pela Contratada, ficando a aceitação da justificativa a critério do TSE, ressalvadas as situações de caso fortuito e força maior.

7. A recusa da licitante vencedora em assinar o contrato ou aceitar a nota de empenho no prazo

estabelecido pela Administração será considerada como inexecução total da obrigação assumida, ensejando a aplicação das sanções previstas em lei e no Edital da Licitação e a imediata perda da garantia de proposta em favor do TSE, quando for o caso.

8. As sanções serão registradas e publicadas no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo federal, no prazo máximo de 15 (quinze) dias úteis, contado da data de aplicação da sanção, nos termos do art. 161 da Lei nº 14.133/2021.

9. As sanções serão registradas e publicadas no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis), no Cadastro Nacional de Empresas Punidas (Cnep) e no Sistema de Cadastramento Unificado de Fornecedores (SICAF), instituídos no âmbito do Poder Executivo federal, no prazo máximo de 15 (quinze) dias úteis, contado da data de aplicação da sanção, nos termos dos arts. 78, V e 161 da Lei nº 14.133/2021.

10. As multas de mora e por inexecução parcial, quando aplicadas em razão de descumprimento contratual, não ultrapassarão o limite de 20% (vinte por cento) do valor total do contrato, considerando-se para esse fim cada item como um contrato em apartado, salvo no caso de agrupamento de itens em lote.

11. Antes da aplicação da sanção de multa, será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

12. Se a Contratada não recolher o valor da multa que lhe for aplicada, dentro de 5 (cinco) dias úteis a contar da data da intimação para o pagamento, a importância será descontada automaticamente do valor devido pela Administração à CONTRATADA, ou ajuizada a dívida, consoante art. 156, §8º, da Lei nº 14.133/2021, acrescida de juros moratórios de 0,5% (meio por cento) ao mês.

13. Antes da aplicação das sanções de impedimento de licitar e contratar ou declaração de inidoneidade para licitar ou contratar, a comissão responsável pela apuração da infração intimará o licitante ou a Contratada para, no prazo de 15 (quinze) dias úteis, contado da data de intimação, apresentar defesa escrita e especificar as provas que pretenda produzir, observado o disposto no art. 158 da Lei nº 14.133/2021.

14. Na hipótese de deferimento de pedido de produção de novas provas ou de juntada de provas julgadas indispensáveis pela comissão, o licitante ou a Contratada poderá apresentar alegações finais no prazo de 15 (quinze) dias úteis, contado da data da intimação.

15. Os atos previstos como infrações administrativas na Lei nº 14.133/2021 ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846/2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e a autoridade competente definidos na referida Lei.

16. A personalidade jurídica poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos na Lei nº 14.133/2021 ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, a pessoa jurídica sucessora ou a empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o sancionado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia.

17. É admitida a reabilitação do licitante ou contratado perante a própria autoridade que aplicou a penalidade, nos termos do art. 163 da Lei nº 14.133/2021.

18. Da aplicação das sanções de advertência, multa ou impedimento de licitar ou contratar caberá recurso no prazo de 15 (quinze) dias úteis, contado da data da intimação.

19. O recurso deverá ser dirigido à autoridade que tiver proferido a decisão recorrida, que, se não a reconsiderar no prazo de 5 (cinco) dias úteis, encaminhará o recurso com sua motivação à autoridade superior, a qual deverá proferir sua decisão no prazo máximo de 20 (vinte) dias úteis, contado do recebimento dos autos, conforme parágrafo único do artigo 166 da Lei nº 14.133/2021.

20. Da aplicação da sanção de declaração de inidoneidade para licitar ou contratar caberá apenas pedido de reconsideração, que deverá ser apresentado no prazo de 15 (quinze) dias úteis, contado da data da intimação, e decidido no prazo máximo de 20 (vinte) dias úteis, contado do seu recebimento.

21. Fica estabelecido que as situações omissas serão resolvidas entre as partes Contratantes, respeitados o objeto do contrato, a legislação e as demais normas reguladoras da matéria, em especial a Lei nº 14.133/2021, aplicando-lhe, quando for o caso, supletivamente, os princípios da Teoria Geral dos Contratos e as disposições do Direito Privado.

ANEXO I-V - Exigências para Avaliação da Habilitação Técnica

1. A licitante classificada em primeiro lugar deverá apresentar:

1.1. Atestado(s) ou declaração(ões) de capacidade técnica operacional em seu nome, expedido(s) por pessoa(s) jurídica(s) de direito público ou privado, que comprove(m) que a(s) licitante(s) executou(ram) a contento serviço compatível**,** conforme subitem a seguir:

1.1.1. Será considerada compatível a execução de:

Item do objeto	**Descrição do item**	**Compatibilidade mínima**
		Apresentação de atestado(s) ou declaração(ões) de capacidade técnica, expedido(s) por pessoa jurídica de direito público ou privado que comprove(m) que a licitante forneceu por meio de contrato:
1	Fornecimento de licença de subscrição para solução de gerenciamento e correlação de eventos de segurança da informação (SIEM – Security Information and Event Management) com tecnologia Security Analytics e UEBA (User and Entity Behavior Analytics).	Solução/serviços para o monitoramento de ambiente corporativo, utilizando soluções de segurança cibernética com eventos centralizados para ao menos 9.000 ativos/usuários.
2	Fornecimento de infraestrutura de processamento, conectividade e armazenamento (instalação, manutenção e suporte de peças) de dados necessária e suficiente às operações da solução de gerenciamento e correlação de eventos de segurança da informação – SIEM (a ser instalado nas dependências do Contratante), composto por cluster de hardware em alta disponibilidade, incluindo equipamento de gerência e equipamento de tratamento de logs e evidências, com garantia de 30 meses.	Infraestrutura de processamento, do tipo equipamento servidor ou appliance de funções específicas de TI.
3	Subscrição para simulação de ataque e verificação de brechas de segurança do ambiente de rede corporativa, incluindo serviço de diretório e firewall de aplicações, com garantia de 30 meses.	01 (uma) subscrição de solução de segurança da informação.
4	Serviço de operação assistida em regime de consultoria especializada para suporte e parametrização da solução do Grupo 1, com foco no gerenciamento e correlação de eventos de segurança da informação – SIEM, por 30 meses.	Serviço de operação assistida em tecnologia da informação, por 12 meses.
5	240 (duzentas e quarenta) horas, durante a vigência do contrato, de suporte técnico especializado realizado exclusivamente pelo fabricante, sob demanda.	100 (cem) horas de suporte técnico especializado em tecnologia da informação.
6	Subscrição de solução de lista de reputação de endereços IP que cubram a proteção de serviços maliciosos de VPN, Proxy, Proxy Residencial, Proxy Malware ou redes de Bots, bem como a visibilidade de tráfego malicioso no ambiente da Contratante (internet e rede local), com garantia de 30 meses.	01 (uma) subscrição de solução de segurança da informação.

1.1.2. Será admitido o somatório de atestados.

1.1.3. Somente serão aceitos atestados expedidos após a conclusão do contrato ou se decorrido, pelo menos, um ano do início de sua execução.

DESCRIÇÃO DO SERVIÇO A SER EXECUTADO

1. Item 1 do Grupo 1 - Licença de subscrição para solução de gerenciamento e correlação de eventos de segurança da informação (SIEM – Security Information and Event Management) com tecnologia Security Analytics e UEBA (User and Entity Behavior Analytics) ou UBA (User Behavior Analytics).

1.1. Características Gerais

1.1.1. Serão contratadas licenças para coletar, armazenar e correlacionar 30.000 (trinta mil) EPS (1,65 TB/dia) de média, considerando-se a seguinte memória de cálculo:

1.1.1.1. Eventos por segundo: 30.000

- Total de eventos por dia:
- eventos/segundo × 86.400 segundos/dia = 2.592.000.000 eventos/dia
- 30.000 eventos/segundo×86.400 segundos/dia=2.592.000.000 eventos/dia
- Volume total de dados por dia: 2.592.000.000 eventos/dia × 700 bytes/evento = 1.814.400.000.000 bytes/dia

1.1.1.2 Para converter bytes em terabytes (TB), utilizamos o fator de conversão de que 1 terabyte equivale a 1×10^{12} bytes. Portanto, para converter 1.814.400.000.000 bytes em terabytes, dividimos esse número por 1×10^{12} considerando:

- $1.814.400.000.000 \text{ bytes/dia} \div (1024)^4 \text{ bytes/TB} = 1,65 \text{ TB/dia}$

1.1.1.3 Para mensuração dos eventos por segundo devem ser considerados apenas os eventos processados na

1.1.1.4 Será aceito, para fins de atendimento do volume de licenciamento, que a licitante oferte, para cada unidade do item 1 do grupo 1, conjunto de licenças que alcancem 6mil eventos por segundo.

1.1.2. As taxas de eventos por segundo (EPS) consideradas neste anexo se referem a média diária de eventos por segundo que a solução deverá estar dimensionada para coletar, armazenar e correlacionar.

1.1.3. O serviço de suporte técnico avançado e a transferência de conhecimento serão utilizados sob demanda, conforme necessidade da Tribunal Superior Eleitoral e especificações constantes neste documento e demais anexos.

1.1.4. Todos os componentes da solução devem ser homologados pelo fabricante, e suportada pela CONTRATADA de maneira a garantir a padronização e interoperabilidade entre todos os componentes.

1.1.5. Todos os componentes da solução, sistemas operacionais (se integrados pela solução) e softwares devem estar em linha de produção do fabricante. Não serão aceitas soluções com previsão de descontinuidade, end-of-support ou end-of-life.

1.1.6. Caso os componentes da solução, programas e/ou sistemas operacionais sofram atualizações tecnológicas pelo fabricante, essas deverão ser disponibilizadas para a Tribunal Superior Eleitoral sem qualquer ônus adicional durante a vigência do contrato e/ou da garantia de 24 (vinte e quatro) meses e devem estar em linha de produção do fabricante.

1.1.7. Não serão aceitos sistemas baseados em software opensource de uso genérico, softwares disponibilizados gratuitamente ou sistemas baseados em software e sistema operacional diferentes daqueles oferecidos pelo fabricante para o mercado em geral.

1.1.8. A solução deverá ser fornecida na forma Appliance Virtual ou software sendo executado em sistemas operacionais x64.

1.1.9. Os Appliances devem ser executados em sistemas operacionais x64.

1.1.10. Os softwares a serem utilizados devem ser homologados pelo fabricante, o que deverá ser comprovado através de documentação.

1.1.11. A solução deve ser fornecida, instalada e implantada de forma completa de acordo com as condições e prazos previstos neste documento e demais anexos.

1.1.12. A solução deve permitir a operação em alta disponibilidade, utilizando equipamentos com conectividade entre si, sem qualquer dependência de ativo/dispositivo disponível no ambiente da Tribunal Superior Eleitoral.

1.1.13. A solução deve possuir a funcionalidade de envio de e-mails automáticos, SYSLOG e trap-snmp.

1.1.14. As funcionalidades citadas devem ser suportadas nativamente pela solução ou através de customização executada pela CONTRATADA, sem custos adicionais para a

Tribunal Superior Eleitoral.

1.1.15. A solução de SIEM deverá ser fornecida para instalação e uso nos idiomas português Brasil (pt_br) ou em inglês ("en-US"/"en-GB").

1.1.16. A solução deve possuir um mecanismo de correlação avançada para processar e comparar informações de logs de diferentes fontes e fluxos de rede.

1.1.17. A solução deve incluir regras pré-programadas (out-of-the-box), bem como permitir que a CONTRATANTE escreva suas próprias regras.

1.1.18. A solução deve poder coletar dados de feeds externos

1.1.19. Quaisquer componentes adicionais que se fizerem necessários para que os produtos descritos ofereçam todas as características deste anexo, bem como para a correta instalação e utilização dos produtos, serão providos pela CONTRATADA, sem ônus adicional ao Tribunal Superior Eleitoral.

1.1.20. A caracterização detalhada do objeto contratado, os requisitos técnicos e as condições de fornecimento, bem como as obrigações e responsabilidades estão indicadas nos artefatos que compõem o Edital de Licitação.

1.2. Licenciamento e garantia para 30.000 (trinta mil) EPS (Eventos por segundo) ou, aproximadamente, 1,65 TB/dia**.**

1.2.1. A modalidade de licenciamento por subscrição deverá permitir o uso e suporte a solução, especificada neste documento e demais anexos.

1.2.2. A solução deve ter garantia de atualizações, correções, suporte técnico e suporte técnico especializado, durante toda a vigência do contrato, a partir da data de instalação.

1.2.3. Todas as licenças de software necessárias ao pleno funcionamento da solução deverão ser fornecidas pela CONTRATADA.

1.2.4. A solução deve prover toda configuração de virtualização, software e componentes necessários ao seu funcionamento, bem como ter as respectivas licenças, sistema gerenciador de banco de dados, exceto quando houver ressalvas por parte da Tribunal Superior Eleitoral, licença para os coletores/agentes independentemente do número de ativos instalados. Todas essas licenças devem ser do tipo subscrição, com direito de atualização de versões, durante o prazo de vigência contratual.

1.3. Composição e funcionalidades da solução para 30.000 (trinta mil) EPS (Eventos por segundo) ou, aproximadamente, 1,65 TB/dia**.**

1.3.1. Deverá ser dado suporte pela CONTRATADA na instalação dos coletores em ambiente operacional fornecido pelos 27 (vinte e sete) Regionais Eleitorais e TSE em quantidade necessária e suficiente para atender a demanda, conforme parâmetros já presentes neste documento.

1.3.2. Os logs deverão receber uma pré-filtragem de modo a otimizar o envio ao SIEM de logs relevantes aos casos de uso especificados.

1.3.3. Agentes responsáveis pela coleta de eventos (LOG) ou solução similar (se necessário, quando não há forma nativa de conexão, de acordo com o ambiente corporativo e solução ofertada);

1.3.4. Armazenador de eventos e registros processados;

1.3.5. Correlacionador de eventos;

1.3.6. Módulo de UEBA (User and Entity Behavior Analytics) ou UBA (User Behavior Analytics)

1.3.7. Consoles de administração, operação, monitoramento e pesquisa da solução.

1.3.8. Todos os componentes núcleo da solução deve ser do mesmo fabricante, caso haja componentes de terceiros devem estar incluídos no pacote como responsabilidade do fornecedor para instalação e suporte, e sem ônus para a Tribunal Superior Eleitoral.

1.3.9. Todos os componentes da solução devem ser instalados em ambiente arquitetura x64 provido pela CONTRATADA em operação modo cluster de alta disponibilidade do tipo failover. Todos os equipamentos da solução devem ter seus discos operando minimamente em RAID 5 com mais 1(um) disco em hotspare para ser substituído em caso de falha de, no mínimo, 2(dois) discos em funcionamento, utilizando discos NVME.

1.3.10. Todos os componentes que fazem parte da estrutura da solução, devem suportar redundância em um conjunto de, no mínimo, 2 (dois) componentes. No caso de falha de um dos componentes do conjunto, o outro deve ser capaz de assumir as todas as operações e funcionalidades com interrupção dos serviços de até 10(dez) minutos.

1.3.11. Todos os equipamentos que compuserem o **Item 2 do Grupo 1** da solução devem ser dimensionados para operar com carga de qualquer componente com no máximo 70% cada. Será calculada a média no intervalo de 5 minutos, em uma janela de 24 horas para aferir o indicador. Caso seja identificado, durante a execução do contrato,

um equipamento com operação de hardware acima deste limite, este deverá ser substituído ou atualizado, sem ônus adicional para o CONTRATANTE, num prazo máximo de até 60 (sessenta) dias úteis, a partir da notificação à contratada, sob pena de multa.

1.3.12. Deverá haver a atualização/upgrade dos componentes de hardware quando ultrapassarem 80% (oitenta) porcento de uso dos recursos, caso o hardware não seja capaz de processar os 30.000 (trinta mil) EPS até esse limiar de uso de recursos do hardware, sob pena de multa.

1.3.13. Os componentes da solução que, de modo conjunto ou individual, apresentarem gargalo de desempenho deverão ser substituídos ou atualizados de modo a manter a saúde operacional da solução.

1.3.14. Os equipamentos que compuserem a solução fornecida pela CONTRATADA deverão ser dimensionados de forma a garantir o desempenho e os níveis de serviço requeridos para o exigido.

1.3.15. É de responsabilidade da CONTRATADA informar ao TSE sobre novas versões de sistemas operacionais e/ou “firmware” e fornecer os manuais no prazo de até 30 (trinta) dias da data de atualização pelo fabricante.

1.3.16. Sempre que houver lançamento de uma nova versão de sistema operacional e/ou “firmware” que faça correções de segurança ou dos serviços prestados, poderá ser solicitada formalmente pelo TSE a CONTRATADA a atualização do sistema operacional e/ou “firmware” dos equipamentos instalados em até 60 (sessenta) dias a contar da solicitação por parte do TSE. Para execução da atualização do firmware, a contratada deverá utilizar-se de ambiente de hardware do cluster já fornecido, sem parar o ambiente.

1.3.17. A CONTRATADA deverá fornecer ao CONTRATANTE as senhas de acesso, via portas de console e remota, para cada um dos equipamentos instalados nas dependências do TSE, com privilégios para operações de leitura, bem como fornecer acesso de leitura às estatísticas de SNMP (comunidade de leitura ou usuário/senha). Além disso, a CONTRATADA deverá realizar configurações para geração de logs (Syslog – RFC 3164) ou traps SNMP para um ou mais endereços IPs a serem definidos pelo TSE quando ele julgar necessário.

1.3.18. As senhas de leitura serão compartilhadas entre o TSE e a CONTRATADA.

1.3.19. A CONTRATADA deverá fornecer as credenciais de acesso a gerência de todo o ambiente provido ao TSE.

1.3.20. Os equipamentos instalados no TSE deverão estar configurados para permitir acesso remoto somente através de SSH v2 ou protocolo análogo, ficando por conta da CONTRATADA o fornecimento de todos os recursos necessários à configuração remota, sem ônus adicional ao TSE.

1.3.21. Para início dos trabalhos, a CONTRATADA poderá utilizar hardware e software fornecido pelo TSE para início de testes e validação funcional da solução, até os equipamentos que compõem a solução serem entregues.

1.3.22. A utilização do hardware e software fornecido pelo TSE não exime nem abona a CONTRATADA de cumprir os prazos previstos neste TR para entrega dos componentes da solução.

1.4. Capacidade das soluções para 30.000 (trinta mil) EPS (Eventos por segundo) ou, aproximadamente, 1,65 TB/dia**.**

1.4.1. A solução deve ter capacidade para coletar, armazenar e correlacionar no mínimo 30.000 (trinta mil) EPS (1,65 TB/dia) de média diária de forma nativa, considerando que cada evento tenha em média 700 bytes, conforme Informação 7 (2806943).

1.4.2. A solução deve permitir a expansão futura através de licenciamento (acréscimo de licenças), para, no mínimo, 90.000 (noventa mil) EPS, aproximadamente, (5,443 TB/dia) de média de forma sustentada. Não será necessário fornecer licenciamento para expansão futura de EPS neste momento.

1.4.3. A solução deve ter a capacidade de ler, interpretar, normalizar e correlacionar o tráfego (flow) que flui através de ativos de rede no mínimo NetFlow v5 e v9, IPFIX e S-Flow, permitindo-se a utilização de componentes de terceiros desde que homologados pelo fabricante e totalmente integrados com a solução.

1.4.4. A solução deve ter capacidade e ser licenciada para coletar e processar no mínimo 2.000.000 (dois milhões) FPM (flows por minuto) de média diária, de forma nativa. Cada flow a ser processado deve ser considerado como 100 (cem) bytes. O custo com processamento de flows deve estar contido nos eventos por segundo da solução, na proporção de 400.000 FPM a cada bloco de licenciamento de 6.000 EPS.

1.4.5. A solução deve permitir a adição de novos componentes, inclusive referentes ao banco de dados, sem provocar interrupções no funcionamento do ambiente de produção da solução.

1.4.6. Deve estar licenciada de forma a permitir criar quantidades ilimitadas de regras de correlação, bem como a customização das regras existentes.

1.4.7. Os módulos deverão permitir a integração com soluções de armazenamento SAN/NAS/Ethernet (Storage Area Network) de terceiros para permitir maior escalabilidade e crescimento.

1.4.8.Toda comunicação entre os componentes deverá ser criptografada com os protocolos SSL, TLS ou SSH.

1.4.9.A solução deverá suportar o uso de IPv4 e IPv6.

1.4.10. O armazenamento e a correlação dos logs/eventos devem ser realizados em processos paralelos.

1.4.11. A solução deve ser capaz de executar regras avançadas que ligam eventos díspares e gerar incidentes se houver uma anomalia.

1.4.12. Deve ser capaz de integrar, de forma nativa ou customizada, com soluções dos seguintes fabricantes: NMAP, Open VAS, Varonis, Veeam, Kibana, Vmware, Nagios, F5 BigIP, Checkpoint, TrendMicro ou outra solução de EDR, conforme a seguir:

1.4.12.1. NMAP: A integração pode permitir que o SIEM colete dados de varredura de rede para identificar dispositivos ativos e suas vulnerabilidades, melhorando a visibilidade da rede.

1.4.12.2.Varonis: Integrando com um SIEM, deve-se obter visibilidade sobre atividades de dados anormais ou potencialmente maliciosas, ajudando a detectar ameaças internas e externas.

1.4.12.3. Veeam: A integração com o SIEM deve permitir monitorar eventos relacionados a backups, garantindo que as atividades de backup sejam concluídas com sucesso e alertando sobre possíveis falhas ou vulnerabilidades.

1.4.12.4. Kibana: Integrando com o SIEM, Kibana deve ser usado para criar painéis personalizados que apresentam insights e análises de segurança em tempo real, facilitando a interpretação de dados.

1.4.12.5. VMware: A integração deve permitir ao SIEM monitorar eventos e logs de máquinas virtuais e infraestrutura de nuvem, identificando comportamentos suspeitos e ameaças potenciais.

1.4.12.6. F5 BigIP: A integração com o SIEM deve ajudar a monitorar o tráfego de rede, ataques de aplicativos web e atividades de autenticação, contribuindo para a defesa contra ataques e ameaças.

1.4.12.7. Checkpoint: Integrando-se com o SIEM, deve-se analisar logs de segurança e eventos de tráfego de rede para detectar padrões de ataque e atividades suspeitas.

1.4.12.8. TrendMicro ou outra solução de EDR: A integração deve permitir que o SIEM utilize dados de ameaças e segurança de endpoints, email e redes da fabricante para melhorar a detecção de ameaças e a resposta a incidentes.

1.4.13. Deve permitir a integração com ferramenta profissional e especializada em gerenciamento de incidentes de segurança fornecida pelo SOC. Ferramentas referência: The Hive; Strangebee; ServiceNow Security Operations; IBM Resilient.

1.4.14. Deve ter capacidade de reativar informações já arquivadas no banco de dados de forma automática e/ou manual, desde que ação seja efetuada via console da aplicação.

1.4.15. A solução deve possuir a capacidade de prover contextualização dos dados de alertas de fontes diversas (ativos de rede e/ou segurança, servidores, aplicações, etc.) em uma única console, otimizando a capacidade e prazos de análise no processo de resposta a incidentes de segurança.

1.4.16. A solução deve ser capaz de inserir nos eventos normalizados metadados sobre georreferencia deles.

1.4.17. Os dados de georreferenciamento devem ser fornecidos pela solução, de forma nativa.

1.4.18. A solução também deve ser capaz de receber dados de georreferenciamento de sistemas internos da Tribunal Superior Eleitoral.

1.4.19. A solução não poderá descartar logs e/ou interromper o funcionamento em caso de aumento pontual na quantidade de EPS (GB/dia) processados, mesmo que o volume exceda o limite contratado.

1.4.20. A solução deverá informar que a média diária de EPS está superior ao contratado para que os ajustes necessários sejam efetuados pela Tribunal Superior Eleitoral.

1.4.21. A solução será contratada com licenciamento em grupos de 6.000 EPS. Caso a média diária de EPS seja superior ao já habilitado, o contratante solicitará, por meio de OS específica, novo grupo de licenciamento.

1.5. Características da solução para 30.000 (trinta mil) EPS (Eventos por segundo) ou, aproximadamente, 1,65 TB/dia**.**

1.5.1. Ser capaz de coletar e aplicar parsing nos dados dos dispositivos monitorados em tempo próximo ao real (near-real-time).

1.5.2. Ser capaz de normalizar e categorizar logs e flows de rede.

1.5.3. Ser capaz de ler dados externos, backup frio da própria ferramenta – por 5 (cinco) anos, mantendo toda a operação do ambiente de SIEM em funcionamento.

1.5.4. Ser capaz de tratar os logs antes de enviar para o SIEM, utilizando técnicas para otimização, tratamento e pré filtragem.

1.5.5. Possuir a capacidade de exibir o perfil do tráfego normalizado em tempo real e traçar o comportamento padrão (baseline) do tráfego de cada ativo de rede capturado, fornecendo alertas sempre que ocorrer algum evento fora do comportamento normal.

1.5.6. Ser capaz de realizar análise avançada sobre o comportamento do fluxo de rede, expondo as alterações quando houver.

1.5.6.1. Realizar uma análise avançada automatizada sobre todos os logs e flows capturados envolvendo a aplicação de técnicas de processamento de dados e análise estatística e/ou inteligência artificial para identificar padrões, anomalias e potenciais ameaças de segurança em tempo real. Não será necessário fornecer licenciamento para inteligência artificial neste momento.

1.5.7. Detectar ataques de negação de serviço (DoS) e de negação de serviço distribuído (DDoS).

1.5.8. Ser capaz de apresentar informações do fluxo de rede por período de tempo selecionado e por regiões geográficas.

1.5.9. Filtrar e selecionar os eventos que serão tratados pela equipe de segurança tecnológica no caso de incidentes evidenciados.

1.5.10. Ser capaz de mesclar (Merge) eventos com as mesmas características (agregação).

1.5.11. Possuir suporte aos protocolos de gerenciamento SNMPv1, SNMPv2 e SNMPv3.

1.5.12. Correlacionar os eventos coletados de forma a evidenciar incidentes que caracterizem um ataque.

1.5.13. Realizar análise avançada automatizada sobre todos os logs e flows capturados.

1.5.14. Deve permitir a criação de regras que identifiquem mudanças de comportamento, como surto ou ausência de eventos e/ou tráfego, quando comparados a outros períodos similares.

1.5.14. Deve permitir a criação de regras que identifiquem desvios, em qualquer metadado, de limites pré-estabelecidos.

1.5.16. A solução deverá identificar o endereçamento da rede habitual do usuário e alertar caso a autenticação do usuário ocorra a partir de endereço IP ou rede diferente do usual.

1.5.17. Permitir a configuração de ações automatizadas como resposta a incidentes detectadas pela solução.

1.5.18. Identificar automaticamente e mostrar em destaque incidentes de alta prioridade.

1.5.19. Fornecer a funcionalidade de geração de alertas (sonoros e/ou visuais) via dashboard ou e-mail para incidentes de alta criticidade detectados no correlacionamento de eventos.

1.5.20. Fornecer a funcionalidade de verificação de conformidade com as políticas, controles e normas internas e externas.

1.5.21. A solução deve possuir ferramenta de geração e tratamento de incidentes própria.

1.5.22. Possuir a funcionalidade de definição de prioridade para os eventos, alerta e incidente.

1.5.23. Possuir a capacidade de tratar eventos em formato compactado (zip, gz, tar.gz e similares), sem a necessidade de descompressão manual.

1.5.24. Armazenar os alertas, incidentes e os eventos, inclusive os normalizados, de forma indexada. Os eventos e flows devem ser sempre armazenados de forma comprimida.

1.5.25. Possuir a funcionalidade de apresentação de relatórios de eventos, alertas e incidentes em nível técnico e gerencial, os quais devem ter a possibilidade de customização e de serem gerados em PDF e HTML de forma automática e manual.

1.5.26. Permitir o agendamento de geração de relatórios periódicos e enviar automaticamente os relatórios gerados;

1.5.27. A solução deve permitir que os relatórios sejam executados periodicamente

(diário, semanal, quinzenal, mensal, etc.) ou sob demanda;

1.5.28. A solução deve fornecer, no mínimo, relatórios em conformidade com ISO 27001 e/ou ISO27002;

1.5.29. A solução deve permitir a geração de relatórios baseados em queries personalizadas e modelos predefinidos;

1.5.30. A solução deve ser capaz de gerar relatórios inibindo a exibição de campos sensíveis dos eventos (senhas, números de cartões de crédito, importâncias monetárias e outros similares);

1.5.31. Apresentar painéis de controles gráficos (dashboards) que mostrem o status do ambiente, dos logs de eventos, comportamento dos usuários, comportamento de outras entidades (entity), incidentes e alertas gerados, fluxos de rede, além de permitir a customização com consultas ad-hoc, quando se fizerem necessárias.

1.5.32. Permitir a pesquisa no histórico de eventos, fornecendo capacidade de drill down, ou seja, visualizar os detalhes dos eventos, inclusive o raw event (dado cru), quando aplicável, para análise forense e investigação de incidentes.

1.5.33. Mostrar a informação sobre os eventos que compõem um alerta e/ou incidente de segurança, identificado pelas regras de correlação da solução, referenciando tais eventos básicos a partir do evento alerta/incidente.

1.5.34. Permitir a autenticação dos usuários à solução por meio de serviço de diretório como Microsoft Active Directory (AD) e/ou LDAP.

1.5.35. Também deve suportar o controle de acesso/autorização baseado na validação de atributo do grupo que o usuário faça parte, associando os perfis de acesso aos dados e funcionalidades do SIEM com grupos do serviço de diretório;

1.5.36. A solução deve permitir configuração de múltiplos perfis de usuários.

1.6. Ser capaz de coletar, armazenar e correlacionar os logs de sistemas e ativos, sendo, no mínimo, 80% de forma nativa. Os demais logs dos sistemas e ativos que não sejam nativamente suportados deverão ser customizados na ferramenta durante a implantação, bem como durante o período contratado para suporte pela CONTRATADA, conforme os prazos dispostos neste contrato, sem custo adicional.

1.6.1. A característica acima deve ser aplicável aos seguintes sistemas e ativos:

1.6.1.1. A10-AX

1.6.1.2. Apache Tomcat

1.6.1.3. Apache Web Server

1.6.1.4. NGINX

1.6.1.5. Arbor – PeakFlow

1.6.1.6. Check Point - Firewall

1.6.1.7. Cisco-Firewall (Firepower)

1.6.1.8. Cisco-Catalyst

1.6.1.9. Cisco-IOS

1.6.1.10. FortiGuard - Antispam, Fortinet, Palo Alto, SonicWall

1.6.1.11. Cisco - Sourcefire Defense Center

1.6.1.12. CITRIX - NETSCALER

1.6.1.13. CITRIX - Virtual Desktop Interface (VDI)

1.6.1.14. F5 – BIG IP/Firewall/WAF

1.6.1.14. Huawei - Router

1.6.1.16. TrendMicro XDR; SentinelONE; Palo Alto (CORTEX); Microsoft Defender for Endpoint; Crowdstrike; Darktrace; Qualis, AWS - Amazon; Google Cloud; Azure; Netskope; Zscaller

1.6.1.17. IBM WebSphere

1.6.1.18. Varonis

1.6.1.19. JBOSS server

1.6.1.20. LDAP/Open Ldap

1.6.1.21. Linux, *NIX e FreeBSD, independente de versão

1.6.1.22. Microsoft Active Directory (AD)

1.6.1.23. Microsoft DNS

1.6.1.24. Microsoft Exchange

1.6.1.25. Microsoft Internet Information Services (IIS)

1.6.1.26. Microsoft SQL Server

1.6.1.27. Microsoft System Center Opeations e Configuration

1.6.1.28. Nagios

1.6.1.29. Microsoft Windows, versões - Vista/7/8,10, 11 2003, 2008 R2 Server, 2012 server, 2016 server e demais atualizações.

1.6.1.30. MySQL

1.6.1.31. Oracle Database, independente de versão

1.6.1.32. Postfix

1.6.1.33. Postgresql Database

1.6.1.34. Snort

1.6.1.35. VMware

1.6.2. A solução deverá suportar a coleta e correlacionamento dos logs de outros sistemas e ativos que venham a ser incorporados pela Tribunal Superior Eleitoral durante a vigência do contrato, mesmo que não conste listado neste Termo de Referência.

1.6.3. Prover mecanismo de coleta de logs de dispositivos não suportados nativamente, através de personalização de coletores, ou solução similar, sem linguagem de programação ou kits de desenvolvimento.

1.6.4. Prover mecanismo de coleta de logs de dispositivos não suportados nativamente, através de customização de coletores, ou solução similar, por meio de linguagem de programação. Tal mecanismo de coleta deverá ocorrer de modo transparente ao operador da ferramenta, ou seja, o usuário da ferramenta não deverá ter que interagir com linguagem de programação para seu trabalho no dia a dia. O operador ou usuário da ferramenta não se confunde com o professional/engineer/arquiteto que mantém a solução em funcionamento.

1.6.5. A customização de coletores ou solução similar deverá ser desenvolvida pela CONTRATADA, conforme os prazos dispostos neste contrato, sem custo adicional.

1.7. A solução deve ser capaz de tratar, no mínimo, os seguintes formatos, protocolos e fontes:

1.7.1. Bases de reputação de endereço IP e URL’s disponibilizadas pela CONTRATADA, conforme especificado neste documento e demais anexos, sem custos adicionais para a Tribunal Superior Eleitoral;

1.7.2. SYSLOG, SYSLOG-NG, SYSLOG com TLS, SNMP (V1, V2 e V3), Microsoft Windows Event Logging API, Microsoft Windows RPC, LOG SMF, FTP, arquivos de logs em texto formatado (vírgula/tabulação/delimitado) e logs em texto não formatado, JDBC e ODBC.

1.7.3. A solução deve possuir a capacidade de gerenciar o armazenamento de longo prazo dos dados e logs coletados, processados e correlacionados em um repositório central por, no mínimo, 180 (cento e oitenta) dias (HOT) staging,

1.7.4. A solução deve notificar e associar comportamentos anômalos baseados em múltiplos eventos que ocorrerem em um determinado período de tempo.

1.7.5. A comunicação entre os componentes da solução deve ser feita através de criptografia, com uso de algoritmos RSA 2048, AES (128 bits ou superior) e/ou 3DES (192 bits ou superior), garantindo a autenticidade, confidencialidade e integridade dos dados, utilizando o protocolo TCP/IP.

1.7.6. Deve utilizar algoritmos para verificação de integridade e autenticidade dos eventos armazenados para fins de auditoria (Ex.: SHA2, HMAC), devidamente reconhecidos como seguros.

1.7.7.A solução deve ser capaz de notificar o(s) administrador(es) ou usuários cadastrados, caso algum dispositivo monitorado pare de enviar eventos.

1.7.8.A solução deve possibilitar o envio de notificações ou alertas baseados no fator de importância e criticidade do ativo/dispositivo perante ao negócio.

1.7.9.As notificações e/ou alertas devem ser enviados via e-mail, além da notificação via dashboard.

1.7.10. A solução deverá possuir funcionalidade de análise visual avançada (visual analytics), permitindo a identificação gráfica de padrões entre eventos selecionados.

1.7.11. A solução deve ser capaz de apresentar os vínculos entre os dispositivos e usuários de origem, ação identificada e os dispositivos e usuários de destino, com base na seleção de eventos.

1.7.12. Deve possuir análise avançada de dispositivos (asset analytics), sendo capaz de atribuir a severidade de um evento baseado na criticidade do dispositivo alvo.

1.7.13. Deve ser capaz de implementar análise estatística avançada (statistical analytics), calculando a estatística (média e desvio padrão) de eventos específicos a cada minuto e alertar caso a estatística desses eventos varie em relação aos limites estabelecidos pela Tribunal Superior Eleitoral.

1.7.14. A solução deve suportar a captura, a normalização e o tratamento de eventos em tempo próximo ao real (near real-time) ou real-time.

1.7.15. A solução deve ser compatível com o ambiente monitorado da Tribunal Superior Eleitoral e sua atualização não poderá agregar novas características que a tornem incompatível com o ambiente.

1.7.16. A solução deve ser implementada de forma que não afete a confiabilidade dos demais sistemas e serviços da Tribunal Superior Eleitoral. Tais sistemas e serviços devem permanecer em funcionamento, mesmo que a solução de SIEM esteja fora de operação.

1.8. Software executado em sistemas operacionais X64

1.8.1.A CONTRATADA deverá licenciar todos os softwares e sistemas operacionais utilizados por sua solução na infraestrutura tecnológica da Tribunal Superior Eleitoral.

1.8.2. Deverão ser utilizados softwares e sistemas operacionais em suas versões 64 bits.

1.8.3. Deve permitir a instalação de patches e correções quando disponibilizado pelo fabricante do sistema operacional, bem como de atualizações de versões do próprio sistema operacional.

1.9. Requisitos dos agentes e coletores de eventos

1.9.1. Quando não puder realizar de forma nativa, a solução deve ser composta de agentes, ou solução similar (software), que têm como função básica fazer a interface com o dispositivo monitorado, recebendo ou buscando eventos relevantes que serão inseridos na solução.

1.9.2. A adoção de agentes ou solução similar deverá ser compatível com os padrões de instalações utilizados pela Tribunal Superior Eleitoral.

1.9.3. Os coletores devem possuir configuração para armazenamento de, no mínimo, 24 (vinte e quatro) horas de dados em disco, em caso de falha de comunicação com o console de administração.

1.9.4. A solução deve ser capaz de filtrar e selecionar os eventos que serão inseridos na solução.

1.9.5. Deve permitir a criação e alteração de filtros.

1.9.6. A solução deve ser capaz de coletar logs e eventos de quaisquer dispositivos e aplicações IP que suportem nativamente SYSLOG.

1.9.7. Caso sejam oferecidos componentes separados para coleta e para o correlacionamento, o coletor da solução deverá ser capaz de armazenar os dados localmente (cache) em caso de indisponibilidade do componente correlacionador.

1.9.8. Deve permitir a configuração do tamanho do cache;

1.9.9. O envio dos dados em cache deve ocorrer automaticamente e imediatamente após a disponibilização dos correlacionadores.

1.9.10. A solução deve ser capaz de enviar o evento bruto (raw) para o armazenamento e consulta futura.

1.9.11. Deve permitir acrescentar o horário (timestamp) correto da recepção do evento/log na solução, preservando o horário original do evento. O horário deverá ser obtido pelo sistema através de sincronização com servidores NTP previamente definidos e sincronizados entre todos os componentes da solução.

1.9.12. A solução deve ser capaz de marcar (através de tag, label ou similar) os eventos com base em unidade organizacional: departamento, setor, unidade ou similar. Essa marcação pode ser feita por atributos da própria mensagem, da origem do log, ou do endereço de origem do evento.

1.9.13. A solução deverá enviar os eventos coletados para o correlacionador e permitir enviar os logs e flows normalizados, inclusive dados “raw”, para outros destinos em tempo próximo ao real.

1.9.14. Os coletores serão instalados em máquinas virtuais fornecida pelos Tribunais Eleitorais e poderão rodar e sistema unix like em virtualizadores de mercado vmware, simplivity, kvm, acropoles, outros.

1.10. Requisitos do módulo de UBA/UEBA

1.10.1. Componentes da solução responsável pela análise avançada dos

comportamentos e atividades dos usuários e outras entidades (hosts, dispositivos, etc.).

1.10.2. Esse componente pode ser nativo da solução ou um módulo apartado, contanto que seja totalmente integrado a resto da solução.

1.10.3. O módulo de User and Entity Behavior Analytics (UEBA) ou UBA (User Behavior Analytics) deve ser licenciado para processar e analisar a mesma volumetria solicitada para os outros componentes do SIEM, quando aplicável, ou deve considerar o total de contas monitoradas (conta de usuários e contas de serviços) de no mínimo 17.000 (dezessete mil) contas e no mínimo 17.000 (dezessete mil) dispositivos (estações de trabalho, servidores, notebooks e outros).

1.10.4. Deve possuir integração nativa com os demais componentes da solução e ser capaz de coletar os dados de usuário e ações executadas dos eventos coletados para geração de score de risco.

1.10.5. Ser capaz de vincular dinamicamente identidades de usuários a endereços IP e a registros de atividades.

1.10.6. Deve ser capaz de importar dados e grupos de usuários em bases LDAP, Microsoft Active Directory, para identificação do usuário associado a contas dos sistemas monitorados e permitir selecionar quais os atributos devem ser importados.

1.10.7. As importações podem ser feitas de forma nativa e/ou por script e/ou API, sem custos adicionais para a Tribunal Superior Eleitoral.

1.10.8. Permitir a criação de listas de observação (watchlist).

1.10.9. Ser capaz de rastrear usuários por lista de observação.

1.10.10. Deve permitir a criação de lista de observações a partir de múltiplas fontes externas.

1.10.11. Deve ser capaz de criar um perfil dinâmico de cada usuário.

1.10.12. Deve permitir ajustar os critérios e pontuação de riscos já existentes na ferramenta e também criar novas regras de negócio que contribuam para a análise e pontuação de risco para atividades consideradas suspeitas ou que precisam ser monitoradas.

1.10.13. Deve possuir dashboards dos usuários com maior pontuação de risco e realizar drill down para detalhar quais as categorias de risco e as ações que contribuíram para o score atual.

1.10.14. Deve permitir a isenção de determinados usuários do processo de score de risco. Esses usuários não teriam riscos computados relacionados as suas atividades.

1.10.15. Deve possuir a capacidade de identificar as anomalias nos comportamentos relacionadas ao tempo, ao volume de transferência de dados, a fontes dos eventos, aos destinos dos eventos e a localização geográfica.

1.10.16. Deve permitir a inclusão de anotações dentro da monitoração de cada entidade, com o objetivo de melhorar o gerenciamento do risco e do histórico das ações tomadas.

1.10.17. Deve ser capaz de realizar analises avançadas sobre usuários, contas, dispositivos, endereços IP e outras entidades.

1.10.18. Deve ser capaz de realizar marcações de risco por entidade (usuário).

1.10.19. Deve ser capaz de aprender de forma supervisionada e/ou não supervisionada os padrões de cada usuário e outras entidades.

1.10.20. Deve identificar rapidamente os desvios de comportamento dos usuários e gerar eventos de alerta no dashboard.

1.10.21. Deve ser capaz de detectar no mínimo os seguintes desvios de comportamentos do usuário:

1.10.21.1. Tentativa de acesso a contas suspensas e bloqueadas;

1.10.21.2. Usuário acessando a rede a partir de uma localidade atípica, inclusive via VPN;

1.10.21.3. Usuário acessando a rede a partir de horários e dias atípicos, inclusive via VPN;

1.10.21.4. Tentativas seguidas de acesso a um recurso;

1.10.21.5. Usuários com grande fluxo de uploads e downloads na internet;

1.10.21.6. Ações repetitivas em curto espaço de tempo;

1.10.21.7. Tentativas de acesso a arquivos sensíveis;

1.10.21.8. Logon simultâneo em localidades ou recursos diferentes;

1.10.21.9. Identificação do uso indevido de contas de serviço;

1.10.21.10. Conta utilizada numa quantidade atípica de atividades;

1.10.21.11. Primeiro uso de um recurso importante por um usuário;

1.10.21.12. Acesso a endereços considerados suspeitos (Threat feed e IP Reputation);

1.10.21.13. Usuário executando um comando que está em blacklist;

1.10.21.14. Acesso incomum a sistemas e dados.

1.11. Requisitos do correlacionador

1.11.1. Componentes da solução responsável pelo correlacionamento dos eventos coletados.

1.11.2. O componente correlacionador deve possuir configuração para armazenamento de, no mínimo, 180 (cento e oitenta) dias de informação de eventos em disco, sem comprometer os requisitos de desempenho e sem a necessidade de arquivamento em backup, incluindo log bruto (raw).

1.11.3. Deve ser capaz de receber eventos dos agentes, coletores e de outros correlacionadores.

1.11.4. Deve efetuar a análise dos eventos em near real-time.

1.11.5. Deve permitir ao administrador a criação de novas regras e a edição das existentes.

1.11.6. O correlacionador deve identificar anomalias baseadas em eventos e em dados históricos conforme período a ser definido pela Tribunal Superior Eleitoral.

1.11.7. Deve possuir a capacidade de detectar automaticamente padrões de ataques especializados que acontecem ao longo do tempo e que não foram previstos ou observados anteriormente.

1.11.8. Deve permitir o correlacionamento de eventos e alertas com dados existentes em listas de observação (watchlist). Deve permitir também a criação de novas listas e a personalização das existentes.

1.11.9. O correlacionador deve permitir a execução das regras agendadas em eventos armazenados para análise histórica de atividades suspeitas.

1.11.10. Deve ter a capacidade de correlacionar eventos oriundos de: Diferentes ativos do mesmo tipo (por exemplo, Firewall A e Firewall B); Ativos de diferentes tipos (por exemplo, Firewall A e IPS B e Proxy C).

1.11.11. Deve ser capaz de inserir os alertas e incidentes gerados no próprio fluxo de correlacionamento ou no fluxo de eventos, possibilitando a detecção de padrões mais complexos de ameaças ou violações de conformidade.

1.11.12. O correlacionador deve priorizar os eventos e alertas com base, pelo menos, nos seguintes critérios: Severidade do evento (estabelecido pela Tribunal Superior Eleitoral); Criticidade do ativo (estabelecido pela Tribunal Superior Eleitoral); Existência de vulnerabilidade no ativo.

1.11.13. Deve ser capaz de executar ações automáticas como: enviar e-mail, enviar mensagens para o usuário conectado à console, como resultado da aplicação de regras.

1.11.14. O correlacionador deve permitir o armazenamento dos eventos, alertas e incidentes na base de dados da solução.

1.11.15. A solução deve fazer a agregação de eventos semelhantes que ocorrem dentro de um limite de tempo ou quantidade de eventos específicos.

1.12. Requisitos das consoles

1.12.1. De modo a garantir a eficiência e economicidade da solução, a console de gerência deverá ter a capacidade de gerenciar toda a solução, já na primeira contratação, ou seja, no mínimo, 30.000 (trinta mil) EPS, aproximadamente, (1,65 TB/dia).

1.12.2. As funções de manutenção, operação, pesquisa e administração da solução devem estar integradas na mesma console.

1.12.3. Possuir acesso seguro e criptografado de forma a garantir a autenticidade, confidencialidade e integridade dos dados.

1.12.4. Permitir a instalação de certificado digital de AC escolhida pela Tribunal Superior Eleitoral para prover o acesso seguro, e configurar o repositório de certificados confiáveis.

1.12.5. Manter seu próprio log de auditoria.

1.12.6. Fornecer visualização e ações diferenciadas por perfis de acesso.

1.12.7. Permitir que as visualizações e ações sejam personalizadas por grupos de usuários.

1.12.8. Permitir a utilização de ACLs (Listas de Controle de Acesso) ou configuração via

interface gráfica para limitar os recursos da solução aos grupos de usuários, conforme critério definido pela Tribunal Superior Eleitoral

1.12.9. Possuir a capacidade de efetuar a segregação de funções dos usuários da solução.

1.12.10. Deve ser capaz de segregar automaticamente os dados/logs dos eventos visualizados, dos dashboards e relatórios gerados conforme perfil e/ou grupos do usuário (por exemplo, numa mesma visualização, dashboard ou relatório, um usuário do grupo Firewall Administrators só poderá visualizar os eventos e dados de firewall e um usuário de grupo IPS Administrators, só poderá visualizar os eventos e dados de IPS, sem necessidade de criar uma visualização, dashboard ou relatório específico para cada grupo).

1.12.11. Ter a funcionalidade de visualização de eventos, alertas e incidentes de segurança em tempo real.

1.12.12. Ser capaz de criação de novas regras e alteração das existentes.

1.12.13. Permitir que sejam testadas as regras com eventos reais capturados anteriormente e mantidos na base de dados da solução, sem afetar a execução das regras em produção.

1.12.14. Permitir a pesquisa nos eventos históricos, fornecendo capacidade de drill down, ou seja, visualizar os detalhes dos eventos, inclusive dados “raw”, quando aplicável, para análise forense e investigação de incidentes.

1.12.14. Exibir os eventos que compõem um alerta e/ou incidente de segurança identificado pelas regras de correlação da solução.

1.12.16. Permitir a criação de novos painéis gráficos (dashboards) e alteração dos existentes.

1.12.17. Permitir a criação de novos relatórios e alteração dos existentes.

1.12.18. Permitir a criação de modelos de relatórios e alteração dos existentes através de interface gráfica.

1.12.19. Permitir o agendamento de geração de relatórios periódicos e enviar automaticamente os relatórios gerados para os destinatários deles.

1.12.20. Permitir a criação de listas de observação (watchlist) e alteração das existentes.

1.12.21. Deve permitir a inserção e remoção dos dados de forma manual e automática através de regras.

1.12.22. Possuir a funcionalidade de gerenciamento e configuração centralizados de todas as partes distribuídas da solução.

1.12.23. Possuir a funcionalidade de atualização centralizada dos principais componentes da solução.

1.12.24. Permitir a inserção manual de anotações em alertas e incidentes.

1.12.25. Permitir a categorização manual de eventos (já normalizados) inéditos não categorizados por padrão. Esta categorização deverá ser aplicada nos eventos futuros de mesma característica.

1.12.26. Deve permitir a visualização de eventos, alertas e incidentes de segurança em tempo próximo ao real, sem necessidade de refazer consultas no banco de dados para atualização das visualizações.

1.13. Requisitos de orquestração e automatização

1.13.1. Possuir plataforma de orquestração para implementação futura. Não será necessário o fornecimento de licenciamento nesta aquisição.

1.13.1.1. Serviço para orquestração;

1.13.1.2. Serviço Web para acesso a interface de gerência;

1.13.1.3. Ambiente virtual para execução de playbooks (Python);

1.13.1.4. Ambiente isolado para interpretações python do OS;

1.13.1.5. Serviço de banco de dados para gestão e armazenamento de dados o orquestrador;

1.13.1.10. Suporte a Node.js, Python ou demais interpretadores de código para interpretação de scripts customizados;

1.13.1.11. Serviço de agendamento de comandos.

1.13.2. Deve possuir uma interface gráfica que contemple ao menos os itens abaixo para melhor organização, gerencia e ação durante possíveis investigações ou automatizações de atividades internas.

1.13.2.1. Dashboard;

1.13.2.2. Guia de chamados;

1.13.2.3. Playbooks;

1.13.2.4. Scripts;

1.13.3. Deve possuir plugins predefinidos e compatíveis com as diferentes tecnologias que a entidade possui no nível de segurança cibernética.

1.13.4. Deve fornecer uma biblioteca de plug-ins que permita integrar fluxos de trabalho e automação com vários tipos de tecnologias, para no mínimo:

1.13.4.1. TIPs - plataformas de inteligência;

1.13.4.2. Ferramentas de análise de malware;

1.13.4.3. EDR - Detecção e resposta do terminal;

1.13.4.4. SIEM;

1.13.4.5. Armazenamento - baseado em nuvem;

1.13.4.6. Sistemas de chamados;

1.13.4.7. Soluções de endpoint;

1.13.4.8. Firewalls;

1.13.4.9. Switches;

1.13.4.10. Ferramentas de sandbox;

1.13.4.11. Servidores de email;

1.13.4.12. Ferramentas de chat;

1.13.5. A solução deve ter um ambiente gráfico que permita a criação dos fluxos para interação com as diferentes tecnologias.

1.13.6. A solução deve permitir a automação das atividades de resposta a incidentes com base nas necessidades e processos da entidade.

1.13.7. A solução deve poder registrar as métricas de desempenho e tempo economizado nas tarefas usando a orquestração.

1.13.8. Deve permitir etapas para escalação e aprovação em fluxos de trabalho.

1.13.9. Deve suportar a definição de tarefas ou ações assíncronas.

1.13.10. A solução deve suportar SMTP para envio de e-mails.

1.13.11. Deve permitir nível de acesso a console e componentes de forma granular.

1.13.12. No nível de gerenciamento de caso/ticket a solução deve ser capaz de alterar dinamicamente a prioridade dos casos, alterar a atribuição e o status de acordo com o fluxo definido.

1.13.13. Deve permitir a criação de novos plugins em Python, além de fornecer a habilidade de customização de playbooks através de linguagens de programação.

1.13.14. Deve fornecer um serviço HTTP server para receber informações através de um método POST e então converter o conteúdo recebido para JSON a fim de obter melhores integrações e expandir as capacidades com integrações web.

1.13.15. Deve suportar operações básicas no processamento de fluxo, como:

1.13.16. Realizar operações matemáticas básicas (+, -, *, /,%, **), suportando retornar o resultado com decimais ou números exatos (arredondados);

1.13.17. Programar a ocorrência de eventos no futuro semelhante para Windows ou Unix;

1.13.18. Conectar-se a um servidor IMAP ou POP3;

1.13.19. Executar localmente os seguintes comandos: Ping, Telnet para uma porta, traceroute, whois e\ou aguardar alguns segundos;

1.13.20. Exibir hora local;

1.13.21. Operar arquivos locais através das seguintes operações: criar arquivos, adicionar a um arquivo (anexar), excluir arquivos, mover arquivos, ler arquivos, listar diretórios etc.;

1.13.22. Realizar uma captura de tela de uma página do site, de modo manual ou via script. Deve permitir armazenar a imagem em um arquivo;

1.13.23. Enviar dados através de uma porta TCP;

1.13.24. Oferecer suporte ao SFTP de modo nativo ou por meio de script, através das seguintes operações: Listar diretório, ver se existe um arquivo, ver se existe um diretório, buscar um arquivo, buscar um diretório e seu conteúdo recursivamente, fazer upload de um arquivo;

1.13.26. Enviar uma mensagem via SMTP;

1.13.27. Executar comandos remotamente via SSH e coletar a saída de execução assim como seus erros de execução;

1.13.28. Criar um elemento STIX a partir de um indicador de consolidação do índice de comprometimento (Hash, IP, URL, HostName, Domínio);

1.13.29. Gerar uma solicitação HTTP para uma API Web generic;

1.13.30. Oferecer suporte ao uso de cabeçalhos HTTP personalizados;

1.13.31. Adicionar tags para fácil identificação de ativos envolvidos em um playbook;

1.13.32. Possuir a capacidade de executar sequências condicionais que mudem a direção ou fluxo de um playbook em execução.

1.13.32.1. Deve suportar a interpretação de dados como:

1.13.32.2. Extrair o domínio de uma URL;

1.13.32.3. Extrair o domínio de um email;

1.13.32.4. Extrair um ou mais URLs de um texto;

1.13.32.5. Codifique um texto em base64;

1.13.32.6. Decodifique base64 em texto;

1.13.32.7. Decodifique um texto JSON usando uma expressão jsonpath;

1.13.32.8. Extrair um subtexto do XML usando um filtro xpath;

1.13.32.9. Codifique uma string usando urlEncode;

1.13.32.10. Decodifique um URL usando urlDecode;

1.13.32.11. Resolver do IP para o domínio;

1.13.32.12. Resolver do domínio para o IP;

1.13.32.13. Converter de texto em campo Hash MD5;

1.13.32.14. Filtrar de uma lista de textos aqueles que contêm um determinado subtexto;

1.13.32.15. Aplicar uma substituição em expressão regular;

1.13.32.16. Verificar se um texto corresponde a uma determinada expressão regular;

1.13.32.17. Contar os itens em uma lista.

1.13.33. Deve suportar pelo menos os seguintes dispositivos:

1.13.33.1. AlienVault OTX

1.13.33.2. Amazon EC2

1.13.33.3. Amazon IAM

1.13.33.4. Amazon S3

1.13.33.5 Amazon WAF

1.13.33.6. Cisco Umbrella

1.13.33.7. Citrix

1.13.33.8. Elasticsearch

1.13.33.9. GitHub

1.13.33.10. Have I Been Pwned?

1.13.33.11. Infoblox

1.13.33.12. Microsoft SharePoint

1.13.33.13. Microsoft SMB

1.13.33.14. Microsoft Windows

1.13.33.15. MISP

1.13.33.16. Pastebin

1.13.33.17. PhishTank

1.13.33.18. Shodan

1.13.33.19. VirusTotal

1.13.34. Deve possuir um guia de API documentado com diversas possibilidades de consumo, não limitando-se a:

1.13.34.1. Listar requisições dos usuários;

1.13.34.2. Criar novas requisições;

1.13.34.3. Atualizar informações sobre requisições e chamados;

1.13.34.4. Enviar solicitação de troca de senha para usuário;

1.13.34.5. Deletar requisição;

1.13.34.6. Gerenciar e executar playbooks.

1.14. Análise de malware - Componente adicional

1.14.1. Sandbox para análise automatizada de malware a ser utilizado 1 (uma) licença por vez por profissional atuando em investigação de incidente. Deverão ser fornecidas 2 (duas) licenças;

1.14.2. Ferramenta e licença referência: contas individuais de HUNTER do ANY.RUN, com as seguintes funcionalidades:

1.14.3. Análise Interativa de Malware:

1.14.4. Acesso interativo

1.14.5. Controle total sobre a atividade do malware

1.14.6. Interage com a simulação de sandbox conforme necessário.

1.14.7. Análise de URLs em Diferentes Navegadores:

1.14.8. Verifica URLs com múltiplos navegadores.

1.14.9. Ferramentas otimizadas para pesquisa de ataques de phishing.

1.14.10. Mapeamento MITRE ATT&CK:

1.14.11. Compreensão estrutural dos ataques.

1.14.12. Identifica ações que o malware executa passo a passo.

1.14.13. Gráficos de Processos Interativos:

1.14.14. Visualização interativa do padrão de ataque.

1.14.15. Análise de Diversos Tipos de Arquivos:

1.14.16. Reanálise de dados em seu sistema ou exportação para análise externa.

1.14.17. Relatórios de Malware:

1.14.18. Formatação dos resultados da análise de malware para compartilhamento ou impressão.

1.14.19. Análise de Eventos de Rede:

1.14.20. Investiga requisições e respostas HTTP(s)

1.14.21. Exporta PCAP e chaves SSL para uso em ferramentas externas de análise de malware.

1.14.22. Resumo de Indicadores de Compromisso (IoCs):

1.14.23. Informações sobre artefatos de rede e sistema operacional encontrados durante a análise.

1.14.24. Feeds de Inteligência de Ameaças em Tempo Real:

1.14.25. Mantém os sistemas de segurança atualizados com os últimos IPs maliciosos, URLs e domínios.

2. Item 2 do Grupo 1 - Infraestrutura de processamento, conectividade e armazenamento de dados necessária e suficiente às operações da solução de gerenciamento e correlação de eventos de segurança da informação – SIEM (a ser instalado nas dependências do Contratante).

2.1. Todos os equipamentos que compuserem o Item 2 do Grupo 1 da solução devem ser dimensionados para operar com carga de qualquer componente com no máximo 70% cada. Será calculada a média no intervalo de 5 minutos, em uma janela de 24 horas para aferir o indicador. Caso seja identificado, durante a execução do contrato, um equipamento com operação de hardware acima deste limite, este deverá ser substituído ou atualizado, sem ônus adicional para o CONTRATANTE, num prazo máximo de até 60 (sessenta) dias úteis, a partir da notificação à contratada, sob pena de multa.

2.2. Deverá haver a atualização/upgrade dos componentes de hardware quando ultrapassarem 80% (oitenta) porcento de uso dos recursos, caso o hardware não seja capaz de processar os 30.000 (trinta mil) EPS até esse limiar de uso de recursos do hardware, sob pena de multa.

2.3. Deve possuir infraestrutura de banco de dados própria especializada em solução SIEM.

2.4. Deve armazenar os dados: eventos, alertas, incidentes, bases de conhecimento, workflow nativo e toda informação pertinente à solução, tais como configuração, usuários, trilhas de auditoria e informações de depuração.

2.5. Deve possuir a capacidade de definir política de retenção dos dados on-line, ou seja, dados mantidos no banco de dados da solução, disponíveis para consulta imediata.

2.6. Possuir capacidade para armazenar os eventos em formato original (“raw”), por no mínimo 180 (cento e oitenta) dias.

2.7. Ser capaz de armazenar logs por tempo determinado e personalizado, conforme necessidade da Tribunal Superior Eleitoral.

2.8. Deve possuir nível de compressão compatível com o mercado para armazenamento de dados.

2.9. Expandir as áreas de armazenamento de eventos do banco de dados sem necessidade de interrupção do serviço.

2.10. Distribuir a base de dados em diferentes volumes, inclusive quando usado armazenamento externo.

2.11. Expandir as áreas de armazenamento do banco de dados para novos volumes, inclusive quando usado armazenamento externo, sem necessidade de reconstruir a base de dados.

2.12. Permitir o expurgo dos dados de forma automática com a personalização do período de tempo do expurgo.

2.13. Implementar políticas de controle de acesso aos dados e auditoria.

2.14. Para cada hardware, a CONTRATADA deverá fornecer deverá fornecer cabos compatíveis com switch de rede CISCO N9K-C93180YC-FX, atualmente em uso no datacenter do TSE. O equipamento fornecido pela contratada deverá possuir, obrigatoriamente:

2.14.1. Pelo menos 2 interfaces para Ethernet 10/25 GbE (dez/vinte e cinco) gigabits Ethernet padrão SFP+;

2.14.2. Deverá vir acompanhada de todos conectores, cabos (de energia, de rede ethernet), parafusos e demais acessórios necessários à sua instalação, funcionamento e conexão às redes da CONTRATANTE.

2.14.3. Os equipamentos serão conectados na rede lógica do TSE, devendo ser compatíveis com os switches modelo Nexus9000 N9K-C93180YC-FX. Devem ser fornecidos CABO DE CONEXÃO DAC/AOC (DIRECT ATTACH COPPER/ACTIVE OPTICAL CABLE) para a velocidade da interface.

2.15. O TSE fornecerá sala cofre e ambiente com ar-condicionado adequado a operação da solução. Caberá ao fornecedor, por meio de vistoria, identificar quais ativos e passivos de rede deverão ser entregues ao TSE para operação adequada da solução, dentre eles – não exaustivamente: patch cord, cabo de tomada, conexão de rede, switch/gbic, fibra ótica, equipamento PDU, demais acessórios, bem como infraestrutura de conexão. Para a instalação o fornecedor poderá utilizar, no máximo, 20U do rack a ser fornecido pelo TSE para instalação dos equipamentos.

2.16. Hardware especializado no tratamento de evidências forenses a ser utilizado na análise e tratamento de incidentes de segurança, contendo, no mínimo, a seguinte especificação:

2.16.1. Dispositivo especializado projetado para a recuperação forense de evidências digitais e análise de dados. Ele é configurado com recursos de alto desempenho e tecnologia de ponta para atender às demandas rigorosas de forense digital e eDiscovery. Equipamento referência: Equipamento FRED 1R.

2.16.2. Características Gerais:

2.16.2.1. Chassi de RAID: Single chassi de RAID com capacidade para cinco discos.

2.16.2.2. Placa-Mãe: Placa-mãe com chipset Intel® Z790.

2.16.2.3. Sistema Operacional: Windows 11 Pro 64 bits (T0045).

2.16.2.4. Processador: Processador Intel® Core™ i9-14900K de 24 núcleos, 8 núcleos P/16 E, até 5,8 GHz, 36 MB de cache inteligente Intel® (T1068).

2.16.2.5. Memória RAM: 128 GB de memória PC5-38500 DDR5 4800 MHz (4X32GB) (T2022).

2.16.2.6. Placa de Vídeo: Nvidia RTX 4090, 24 GB, GDDR6X de 384 bits, 16384 núcleos CUDA, ou superior.

2.16.2.7. Armazenamento Primário: SSD M.2 NVMe PCIe de 500 GB - Série PRO (T3043B) como unidade de sistema operacional.

2.16.2.8. Armazenamento Adicional: três SSDs M.2 NVMe PCIe de 8 TB - Série Rocket 4 Plus (T3239) e um SSD SATA de 8 TB - Série QVO (T3230B) para armazenamento de dados.

2.16.3. Conectividade:

2.16.3.1. porta Ethernet Realtek de 2,5 Gigabits (RJ45).

2.16.3.2. WiFi 6 (802.11 a/b/g/n/ac/ax) / Bluetooth® v5.2 para conectividade sem fio.

2.16.4. Combo de Teclado e Mouse de 103 teclas - Sem fio.

2.16.5. Caixa de ferramentas forense contendo adaptadores de disco e cabos de energia / sinal (SAS, SATA, IDE, microSATA, SATA LIF, MacBook Air, Blade SSD).

2.16.6. Adaptadores de unidade SSD PCIe (PCIe SSD m.2 NVMe, SSD MacBook Pro de 2013 ou mais recente e SSD PCIe de classe servidor).

2.16.7. Conjunto de chaves de fenda de segurança com bits variados para abrir invólucros.

2.16.8. A empresa deverá encaminhar proposta de preços especificando marca, modelo e descrição técnica do produto ofertado.

2.16.9. Será aceita a oferta de produtos com marcas diferentes da marca de referência desde que atendam a todas as especificações exigidas neste Termo de Referência.

3. Item 3 do Grupo 1 – Subscrição, com licenciamento somente para o TSE, para simulação de ataque e verificação de brechas de segurança do ambiente de rede corporativa, incluindo serviço de diretório e firewall de aplicações. Tipo de ferramenta referência: Ferramentas BAS (breach and attack simulation).

3.1. Para fins de licenciamento deve ser considerado apenas o domínio tse.jus.br - incluindo seus subdomínios - com corpo funcional com 897 (oitocentos e noventa e sete) funcionários.

3.2 Deve proporcionar simulação, avaliação e gestão estendida da postura de segurança da organização, permitindo medir a efetividade através de testes e avaliações do nível de proteção do perímetro e de ambientes internos para que haja uma compreensão completa quanto a efetividade dos controles de segurança.

3.3. Deve permitir que os profissionais de segurança possam identificar, diagnosticar, gerenciar, controlar e validar sua postura de segurança cibernética de ponta a ponta.

3.4. Deve permitir recriar cenários reais de ataques à infraestrutura de segurança da organização sem gerar impactos ao ambiente.

3.5. Deve fornecer a possibilidade de executar os ataques baseados em táticas, técnicas e procedimentos que os atacantes e grupos de criminosos cibernéticos utilizam, sendo eles utilizados em pelo menos os seguintes cenários:

3.6. Reconhecimento – Validação de domínios e subdomínios a fim de identificar fraquezas e vulnerabilidades expostas na internet referente a organização. Nesta fase, a solução deverá utilizar de fontes de inteligência aberta (OSINT) para descoberta de credencias e outras informações as quais possam beneficiar um atacante.

3.7. Base Inicial – Ataques relacionados a fase de acesso inicial, execução, persistência e escalação de privilégio.

3.8. Execução & C2C – Técnicas de evasão de defesa, acesso de credenciais e descoberta do ambiente.

3.9. Propagação na rede – Movimentação lateral, coleção e comunicação externa C2C, permitindo que o atacante mova para seus objetivos finais.

3.10. Ações com objetivos – Comunicação externa para exfiltração de dados e geração de impacto.

3.11. Deve permitir simulações automáticas, orientadas a avaliar os ajustes e configurações de distintos controles de segurança.

3.12. Deve permitir a simulação de táticas, técnicas e procedimentos maliciosos de forma individual, assim como permitir a simulação de forma secundária respeitando o ciclo de vida de um ataque.

3.13. Deve identificar quais testes foram executados com êxito e quais falharam durante o processo de prevenção. Para os resultados, deve haver a possibilidade de criação de evidência da detecção e/ou bloqueio através de uma integração com um SIEM, e/ou no próprio dispositivo que detectou e/ou bloqueou a simulação.

3.14. As simulações serão executadas a partir de componentes da solução ou equipamento reservado exclusivamente para ela.

3.15. Deve ser implementada em modelo de nuvem SaaS, podendo ela permitir a implementação em regiões de nuvem disponíveis para o território brasileiro quando necessário.

3.16. Deve possuir suporte e licenciamento para realização de avaliações em diferentes vetores de ataque tais como, endpoint, rede, web e cloud.

3.17. Deve possuir um módulo capaz de fornecer através de sua rede de inteligência ameaças emergentes e relevantes para a plataforma, fornecendo informações detalhadas sobre tais ameaças e quais medidas de remediação recomendadas.

3.18. Deve permitir integração com soluções de gestão de vulnerabilidades, fornecendo apoio para priorização de riscos encontrados na organização, através do consumo dos relatórios fornecidos pela ferramenta de gestão de vulnerabilidades, deve ser possível apresentar de forma clara quais CVEs estão disponíveis na plataforma de ataques para simulação.

3.19. Deve permitir integração com diferentes serviços de SSO, tais como: ADFS, Azure AD, OKTA, JumpCloud entre outros.

3.20. Deve permitir a integração com diferentes plataformas de segurança via API.

3.21. Todos os componentes devem poder ser gerenciados por uma console central, permitindo a configuração, monitoração e atualização dos agentes de forma automática.

3.22. Toda a comunicação entre os componentes deve ser feita através de protocolos seguros como HTTPS com TLS 1.2 ou superior.

3.23. Deve suportar a comunicação dos componentes instalados por meio de um proxy web.

3.24. O processo de instalação dos agentes deve ser feito de forma manual, automatizada ou em lote.

3.25. Deve fornecer em cada um de seus vetores o nível de risco encontrado após cada simulação, devendo a plataforma comparar o resultado atual com o anterior para fornecer uma visão de avanço ou regresso dos testes, estes dados poderão ser utilizados para definição de baseline do ambiente.

3.26. Deve suportar regras SIGMA e fornecer para alguns cenários a opção de convertê-las em buscas (queries) as quais poderão ser utilizadas para buscas em plataformas de SIEM ou até mesmo criação de regras de correlação.

3.27. Deve ser capaz de poder trocar informações com outras tecnologias de segurança do ambiente para fornecer, melhor visibilidade na detecção, gestão de vulnerabilidades, automação de playbooks e validação de processos internos. Permitindo no mínimo as seguintes integrações:

3.27.1. Azure Sentinel;

3.27.2. Carbon Black;

3.27.3. CrowdStrike Falcon;

3.27.4. IBM Qradar;

3.27.5. LogRhythm;

3.27.6. Microsoft Defender;

3.27.7. Palo Alto Cortex;

3.27.8. Qualys VM;

3.27.9. RSA Netwitness;

3.27.10. SentinelOne;

3.27.11. Splunk;

3.27.12. Tenable IO;

3.28. Todos os produtos de segurança que não possuírem integração direta, devem poder ser integrados por meio da solução de correlacionamento de eventos (SIEM) a ser fornecida pela CONTRATADA, permitindo a integração com produtos não homologados.

3.29. Deve permitir a visualização do status de conexão e versão de software dos agentes, permitindo através da console realizar operações como reinicialização, deleção ou mesmo desinstalação do componente.

3.30. Deve permitir avaliar as capacidades de defesa da organização contra táticas, técnicas e procedimentos utilizados por grupos criminosos conhecidos.

3.31. Deve possuir uma biblioteca de ataques associada a criminosos cibernéticos e deve atualizá-la de forma automática quando novas ameaças emergentes surgirem.

3.32. Deve permitir a criação de perfis de adversários.

3.33. O portfólio de ataques deve ser baseado em frameworks e padrões de segurança cibernética, tais como MITRE ATTACK, OWASP, CVSS, Microsoft DRAPE e NIST.

3.34. As simulações de ataque devem corresponder, sempre que possível, a uma técnica descrita pelo MITRE e apresentar detalhes sobre os respectivos TTPs.

3.35. As simulações de ataque também devem possuir mapeamentos com NIST 800-53 facilitando assim a adequação de padrões e frameworks.

3.36. Deve incluir diversas simulações de ataque predefinidas, que incluem minimamente os seguintes tipos de ataques:

3.37. Para validação do vetor de endpoint a plataforma deve oferecer simulações de ataque para:

3.37.1. Ransomware: Validação da efetividade de recursos para detecção de anomalias (comportamento) durante a execução segura de ransomwares, devendo estes buscar arquivos sensíveis no host e utilizar chaves geradas de forma segura e controlada para criptografia de arquivos.

3.37.2. Worm: Validação da efetividade de recursos para detecção de anomalias (comportamento) durante a execução segura de worms, devendo estes realizar a descoberta de hosts vulneráveis e simular a proliferação para eles através de técnicas utilizando protocolos tais como SMB.

3.37.3. Trojan: Validação da efetividade de recursos para detecção de anomalias (comportamento) durante a execução segura de trojans, estes deverão coletar informações gerais do host como nome de usuário, e-mail e outras. Podendo também estabelecer comunicação utilizando diferentes métodos de reverse shell.

3.37.4. Antivírus: Validação da efetividade de inspeção e proteção de ameaças contra arquivos maliciosos, os malwares escritos em disco devem ser atualizados diariamente através de diversos feeds de segurança.

3.37.5. MITRE ATT&CK: Validação da efetividade dos recursos de anti-malware através da execução de comandos customizados que devem simular o comportamento de adversários mapeados no framework ATT&CK.

3.38. Para validação do vetor de web gateway a plataforma deve oferecer simulações de ataque para:

3.38.1. Ransomware: Validação da efetividade dos recursos de filtragem dinâmica de URL e proteção contra ransomware, acessando IPs e URLs reais associados ao Ransomware, como servidores Botnet, C&C, sites de distribuição e pagamento.

3.38.2. C&C: Validação da efetividade dos recursos de filtragem dinâmica de URL e proteção contra malwares, acessando IPs e URLs reais associados a atividades de C&C como Botnet.

3.38.3. Política: Validação da efetividade da proteção de filtro de categorias do gateway da web. A validação é feita através do acesso a diferentes sites divididos por categorias, como pornografia, jogos de azar etc.

3.38.4. Arquivos: Validação da efetividade dos recursos de inspeção de tráfego de entrada e eficácia da proteção contra arquivos maliciosos. A validação é realizada através da tentativa de baixar por HTTPS uma variedade de malwares simulados que imitam o comportamento de worms, trojans e ransomware.

3.38.5. Exploits: Validação da efetividade dos recursos de inspeção de tráfego de entrada e eficácia da proteção contra arquivos maliciosos. A validação é realizada através da tentativa de baixar por HTTPS uma variedade de malwares que simulam o comportamento de worms, trojans e ransomware.

3.39. Para validação do vetor de e-mail gateway a plataforma deve oferecer simulações de ataque para:

3.39.1. Ransomware: Validação da efetividade dos recursos de proteção de e-mail através de técnicas de execução de códigos utilizadas por ransomwares, toda execução deve ser realizada de forma segura sem gerar impactos ao ambiente.

3.39.2. Worm: Validação da efetividade dos recursos de proteção de e-mail através de técnicas de execução de códigos utilizadas por worms, toda execução deve ser realizada de forma segura sem gerar impactos ao ambiente.

3.39.3. Malware: Validação da efetividade dos recursos de proteção de e-mail através de técnicas de execução de códigos utilizadas por diferentes códigos maliciosos (malwares), estas validações devem poder simular cenários interativos envolvendo técnicas de exploração de controles como UAC, roubo de credenciais e C&C. Toda execução deve ser realizada de forma segura sem gerar impactos ao ambiente.

3.39.4. Payload: Validação da efetividade dos recursos de proteção de e-mail através de técnicas de execução de códigos em payloads, toda execução deve ser realizada de forma segura sem gerar impactos ao ambiente.

3.39.5. Exploits: Validação da efetividade dos recursos de proteção de e-mail através da execução de diversos arquivos que exploram diferentes vulnerabilidades em programas, toda execução deve ser realizada de forma segura sem gerar impactos ao ambiente.

3.39.6. Dummy: Validação da efetividade dos recursos de proteção de e-mail através da execução de diferentes técnicas de execução de códigos, isto deve incluir uso de recursos conhecidos como payloads do metasploit como exemplo MessageBox. Toda execução deve ser realizada de forma segura sem gerar impactos ao ambiente.

3.39.7. True File Type Detection: Validação da efetividade dos recursos de proteção de e-mail através do envio de arquivos com diferentes extensões não pertencentes ao seu formato de arquivo original, este teste deve apoiar na identificação de possíveis brechas que podem ser utilizadas para comprometer o ambiente através da falsificação de formatos originais de arquivos.

3.40. Para validação do vetor de web application firewall (WAF) a plataforma deve oferecer simulações de ataque para minimamente:

3.40.1. SQL injection

3.40.2. Cross-site scripting (XSS)

3.40.3. File inclusion for remote code execution

3.40.4. Command injection

3.41. Para validação de vazamento de dados (DLP) a plataforma deve oferecer simulações de

ataque que permitam validação dos seguintes métodos:

3.41.1. HTTP & HTTPS: Exfiltração de dados por HTTP/S, injetando dados confidenciais em cabeçalhos de solicitação HTTP/S enviados para um servidor remoto.

3.41.2. Browser HTTP & HTTPS:Exfiltração de dados através de navegadores como IE, Edge e/ou Chrome.

3.41.3. DNS: Exfiltração de dados pela porta 53.

3.41.4. Tunelamento DNS: Exfiltração de dados sobre o protocolo DNS (túnel através de servidores DNS públicos). Injetando dados confidenciais em uma solicitação de DNS enviada a servidores DNS públicos.

3.41.5. Tunelamento ICMP: Exfiltração de dados sobre cabeçalhos ICMP. Injetando dados confidenciais em um pacote de eco (ECHO) enviado para um servidor remoto.

3.41.6. Telnet: Exfiltração de dados pela porta de rede Telnet 23.

3.41.7. SFTP: Exfiltração de dados sobre o protocolo SFTP.

3.41.8. Outras Portas: Exfiltração através do upload de dados confidenciais para servidores de hospedagem de arquivos externos por meio de portas de rede abertas.

3.41.9. Email: Usando email corporativo no Outlook para transmitir dados confidenciais.

3.41.10. Serviços de nuvem: Exfiltração de dados confidenciais para ou por meio de serviços e aplicativos em nuvem.

3.41.11. Dispositivos Removíveis: Exfiltração de dados confidenciais através da cópia para dispositivos de mídia removíveis, como USB.

3.42. Para validação de movimentação lateral a plataforma deve oferecer simulações de ataque que permitam validação dos seguintes métodos:

3.42.1. Pass-the-Password;

3.42.2. Pass-the-Ticket;

3.42.3. Pass-the-Hash;

3.42.4. Brute Force;

3.42.5. LLMNR/NBT-NS Poisoning and Relay;

3.42.6. Kerberoast;

3.42.7. Password Spraying;

3.42.8. Steal LAPS passwords.

3.43. Deve fornecer a possibilidade de criar modelos customizados nos vetores de ataque sem causar impactos ao ambiente.

3.44. Para o cenário de movimentação lateral, o agente deve poder atuar exatamente como um atacante no ambiente, não devendo este depender da implementação de outros agentes para validação dos diferentes métodos. Deve possuir capacidade de realizar um “pivoting” na rede e fornecer um mapa de toda trilha percorrida e alvos alcançados, podendo os alvos serem considerados ou não joias da coroa (Crown Jewels).

3.45. Deve fornecer um caminho para validação completa da cadeia de ataque (Full Kill-chain), permitindo assim que seja avaliadas fases tais como pré-exploração, exploração e pós-exploração.

3.46. Deve permitir a criação de campanhas de phishing customizadas para avaliação da conscientização dos colaboradores em cenários reais, as campanhas devem minimamente permitir que sejam criados conteúdos através da plataforma em português.

3.47. Cada um dos testes ou ações hospedadas na base de conhecimento, deve ter uma descrição e o código da técnica ou das táticas de acordo com a nomenclatura do MITRE.

3.48. Deve ter a capacidade de repetir periodicamente os testes que o usuário deseja e comparar os resultados de cada execução com um resultado esperado, permitindo definir se o ataque foi detectado, bloqueado e que tipo de registro foi detectado no SIEM ou nas tecnologias de segurança testadas.

3.49. Os componentes de ataque devem poder ser instalados, minimamente, nos seguintes ambientes:

3.49.1. Windows 11 build 22000+, 10 build 1067

3. 49.2. Windows Server 2012 ou superior

3.49.3. Linux Alpine 3.12, Ubuntu 16.04, Debian 10, CentOS 7, RHEL 7, Fedora 33, openSUSE 15 e SUSE Enterprise 12 SP2 ou versões superiores

3.49.4. MacOS 10.15 ou superior

3.50. Deve realizar as simulações de ataque através de um agente único ao qual deverá ser capaz de executar ataques em diferentes vetores de forma individual ou simultânea.

3.51. Deve permitir através de um framework aberto a customização de diferentes cenários e cadeias de execução que sejam compatíveis minimamente com as seguintes plataformas:

Python/Bash/sh/cmd/Powershell;

3.52. Deve possuir uma console em nuvem a qual deverá ser utilizada para orquestração e envio dos ataques.

3.53. O painel principal (dashboard) deve apresentar de forma clara os vetores licenciados assim também como informações sobre controles de segurança, ameaças emergentes, integrações e outros detalhes importantes que possam ser utilizados para melhor compreensão dos testes realizados.

3.54. Deve permitir a criação de painéis dinâmicos aos quais permitam a customização e manipulação de dados a serem apresentados no novo painel (dashboard).

3.55. Deve possuir um dashboard que exiba todas as informações de vulnerabilidades baseadas em ataques, incluindo proteção geral de controles de segurança, principais vulnerabilidades encontradas em ativos de rede, principais ativos vulneráveis, principais CVEs e muito mais.

3.56. Deve possuir em seu painel principal a opção de rastreabilidade em tempo de execução dos testes.

3.57. Deve fornecer uma visão global dos itens que foram identificados.

3.58. Deve fornecer uma visão detalhada após integração com plataformas de gestão.

3.59. Deve possuir uma interface em seu agente para facilitar o gerenciamento de ataques em andamento, visualização de logs e configurações pertinentes aos recursos envolvidos no ataque, proxy, e-mail etc.

3.60. Após conclusão dos ataques envolvendo de forma individual ou conjunta os vetores de ataque deverá ser fornecido um score de risco, este score deve prover uma clara visão sobre a maturidade atual e histórica do ambiente.

3.61. Deve permitir a geração de relatórios técnicos ou gerenciais aos quais devem conter minimamente:

3.61.1. Informações sobre o score de risco atual;

3.61.2. Descrição e recomendação para correção dos problemas encontrados;

3.62. Deve permitir em sua guia de relatórios a extração de dados completos contendo informações gerais de todos os ataques realizados em um determinado vetor, assim também como oferecer opções para download de relatórios em formato PDF, CSV ou TXT.

3.63. Deve permitir a geração e download de relatórios através de sua interface assim como permitir o envio deles através de e-mail.

3.64. Deve permitir a geração de relatórios e visão detalhada por ambientes.

3.65. A solução deverá prover uma visão clara do desempenho individual de cada vetor de ataque assim como também possuir um gráfico de comparação para benchmark.

4. Item 4 do Grupo 1 - Serviço de operação assistida em regime de consultoria especializada para suporte, operação e parametrização da solução de gerenciamento e correlação de eventos de segurança da informação – SIEM. Requisitos gerais do atendimento do serviço de consultoria especializada:

4.1. A CONTRATADA deve adotar um modelo de Operação de Segurança prestado em regime 8 x 5 (oito horas por dia, 5 dias por semana).

4.2. Os prazos de atendimento deverão ser gerenciados conforme métricas postas neste TR.

4.3. A CONTRATADA deve garantir que os profissionais alocados para execução da atividade de suporte especializado tenham plena disposição para integração técnica com o time do SOC, por meio de reuniões – no mínimo, duas vezes por semana, relatórios e transferência de conhecimento no dia a dia.

4.4. O profissional em teletrabalho ou trabalho remoto que atenderá o TSE poderá realizar a customização, suporte e parametrização do SIEM remotamente, garantindo a qualidade na operação da ferramenta, conforme detalhado neste Termo de Referência.

4.5. Poderá ser convertida, a critério da CONTRATANTE, a modalidade de trabalho do profissional alocado em teletrabalho para o trabalho presencial (nas dependências do TSE).

4.5.1. A CONTRATADA deverá prover serviços mensais, dedicados ao suporte e parametrização da ferramenta, por profissionais capacitados, sem dedicação exclusiva para o TSE.

4.5.2. Para a prestação suporte técnico especializado por parte da CONTRATADA, a CONTRATANTE poderá exigir a alocação de mais de um profissional da CONTRATADA. Estas horas deverão ser executadas no seguinte formato:

4.5.2.1. A CONTRATANTE, deve alocar, no mínimo, 1 (um) profissional em teletrabalho ou trabalho remoto. Caso a CONTRATADA queira, mediante informação ao CONTRATANTE, poderá requerer atuar presencialmente no ambiente do TSE.

4.5.3. Os profissionais que proverão os serviços de suporte e consultoria especializada

mensalmente, devem passar por sindicância da vida pregressa, conforme especificado neste documento. A exigência visa mitigar riscos de vazamento de dados acerca de eventos e incidentes de segurança no contexto do TSE e Tribunais Eleitorais que vierem a serem utilizadores da solução.

4.5.4. O profissional que proverão os serviços de suporte mensais deverão possuir em conjunto as certificações de nível “professional ou engineer e de arquiteto” na solução de SIEM que for a ganhadora do certame já no início da prestação do serviço.

4.5.5. Os profissionais alocados pela CONTRATADA deverão apresentar os documentos comprobatórios exigidos neste TR bem como as documentações referentes a participação nos treinamentos que totalizem, já no início do contrato, 40 (quarenta) horas de capacitação nas áreas de tratamento de incidentes, defesa cibernética ou segurança ofensiva, dentre elas:

4.5.5.1. Tratamento de Incidentes de Segurança (RNP);

4.5.5.2. GOHACKING (GoHacking Security Operation Center Foundations);

4.5.5.3. SEC4US (Digital Forensics);

4.5.5.4. Foundations of Incident Management (CERT.BR);

4.5.5.5. Overview of Creating and Managing CSIRTs (CERT.BR);

4.5.5.6. Advanced Topics in Incident Handling (CERT.BR);

4.5.5.7. Outros treinamentos, exclusivamente, nas áreas de tratamento de incidentes de incidentes, defesa cibernética ou segurança ofensiva avaliados pela fiscalização do contrato.

4.5.5.8. Poderá ser aceita em substituição aos treinamentos supra, a apresentação de título de pós graduação estritamente nos temas de defesa cibernética ou segurança ofensiva;

4.5.6. A partir do segundo ano de contrato, os profissionais alocados pela contratada deverão apresentar, anualmente, certificados que comprovem a participação em no mínimo 80 (oitenta) horas de treinamentos de atualização estritamente nos temas de tratamento de incidentes, defesa cibernética ou segurança ofensiva.

4.6. O ambiente físico da CONTRATADA deve estar obrigatoriamente no Brasil.

4.7. A CONTRATADA será responsável pela aplicação de controles de segurança adequados (criptografia) para garantir a confidencialidade de qualquer dado ou informação da TRIBUNAL SUPERIOR ELEITORAL que receber em seu ambiente ou em terceiro contratado.

4.8. A infraestrutura tecnológica necessária à prestação dos serviços, compreendendo computadores, software básico e de apoio, bem como as conexões física e lógica à rede da TSE, será provida e gerida pela CONTRATADA e deve estar operacional prazos presentes no cronograma deste TR. Esse prazo poderá ser prorrogado a critério da TSE ou desde que acordado entre as partes.

4.9. A conexão lógica com o TSE será realizada por meio da Internet, utilizando de acesso remoto baseado em tecnologia ZTNA, em solução provida pela CONTRATADA para uso de seu(s) Técnico(s).

4.10. A CONTRATADA deverá prover infraestrutura compatível para a execução de seus profissionais em teletrabalho.

4.11. Os serviços a serem realizados envolvem a implementação de casos de uso, a exemplo dos relacionados abaixo:

4.11.1. Registro de ponto e sessão do sistema operacional divergente

4.11.1.1. Descrição:

4.11.1.2. Registro de ponto de usuário que não está autenticado na rede ou não está acessando remotamente.

4.11.1.3. Ações:

4.11.1.4. Abertura de incidente dentro do fluxo do SIEM;

4.11.1.5. Informação no dashboard;

4.11.1.6. Envio de e-mail para o gestor imediato

4.11.2. Histórico de registro de ponto

4.11.2.1. Descrição:

4.11.2.2. Identificar o registo do ponto de todos os empregados, relacionando-os com os acessos à rede corporativa, incluindo localização geográfica.

4.11.2.3. Ações:

4.11.2.4. Gerar relatório com as informações do registro de ponto e de acesso à rede de cada empregado.

4.11.3. Autenticação de usuário (local ou remoto) simultâneo em vários dispositivos

4.11.3.1. Descrição:

4.11.3.2. Autenticação de usuário em 2 ou mais dispositivos simultaneamente

4.11.3.3. Ações:

4.11.3.4. Abertura de incidente dentro do fluxo do SIEM para a área de segurança tecnológica;

4.11.3.5. Envio de e-mail para o responsável pela conta;

4.11.3.6. Informação no dashboard.

4.11.4. Utilização indevida de contas

4.11.4.1. Descrição:

4.11.4.2. Usuário desligado ou ausente por licença/férias, utilizando sua conta.

4.11.4.3. Ações:

4.11.4.4. Abertura de incidente dentro do fluxo do SIEM;

4.11.4.5. Informação no dashboard;

4.11.4.6. Envio de e-mail para o gestor imediato;

4.11.4.7. Bloquear usuário temporariamente.

4.11.5. Contas Windows ativas e sem utilização

4.11.5.1. Descrição:

4.11.5.2. Usuário utilizando qualquer sistema e sem registros de logon no AD;

4.11.5.3. Contas sem registro de login acima de 60 dias.

4.11.5.4. Ações:

4.11.5.5. Abertura de incidente dentro do fluxo do SIEM;

4.11.5.6. Informação no dashboard;

4.11.5.7. Envio de e-mail para o gestor imediato;

4.11.5.8. Bloquear usuário temporariamente.

4.11.6. Ataque de força bruta em contas de usuário e contas de serviço

4.11.6.1. Descrição:

4.11.6.2. Tentativas sequenciais com senha errada e em determinado período de tempo.

4.11.6.3. Ações:

4.11.6.4. Abertura de incidente dentro do fluxo do SIEM para a área de segurança tecnológica;

4.11.6.5. Envio de e-mail para o responsável pela conta;

4.11.6.6. Informação no dashboard.

4.11.6.7. Bloqueio temporário da conta.

4.11.7. Tentativas de acesso a sistemas e/ou recursos do RACF sem privilégio para tal:

4.11.7.1. Descrição:

4.11.7.2. Tentativas sequenciais de acesso a um mesmo recurso ou sistema sem sucesso.

4.11.7.3. Ações:

4.11.7.4. Abertura de incidente dentro do fluxo do SIEM para a área de segurança tecnológica;

4.11.7.5. Envio de e-mail para o responsável pela conta;

4.11.7.6. Informação no dashboard.

4.11.8. Acesso simultâneo em equipamentos distintos

4.11.8.1. Descrição:

4.11.8.2. Acesso a um ou mais recursos a partir de localizações diferentes

4.11.8.3. Ações:

4.11.8.4. Abertura de incidente dentro do fluxo do SIEM para a área de segurança tecnológica;

4.11.8.5. Envio de e-mail para o responsável pela conta e gestor imediato;

4.11.8.6. Informação no dashboard, incluindo geolocalização.

4.11.9. Acesso a partir de geolocalização distante, em curto espaço de tempo

4.11.9.1. Descrição:

4.11.9.2. Utilização de uma mesma conta em localizações distantes em um curto período de tempo

4.11.9.3. Ações:

4.11.9.4. Abertura de incidente dentro do fluxo do SIEM;

4.11.9.5. Envio de e-mail para o responsável pela conta;

4.11.9.6. Informação no dashboard.

4.11.10. Uso indevido de conta de serviço

4.11.10.1. Descrição:

4.11.10.2. Conta de serviço utilizada para autenticação em estações de trabalho.

4.11.10.3. Ações:

4.11.10.4. Abertura de incidente dentro do fluxo do SIEM;

4.11.10.5. Informação no dashboard;

4.11.10.6. Envio de e-mail para a unidade responsável pela conta de serviço.

4.11.11. Uso indevido de usuário root

4.11.11.1. Descrição:

4.11.11.2. Acesso remoto utilizando usuário root (ssh, telnet, rsh, rlogin...)

4.11.11.3. Ações:

4.11.11.4. Abertura de incidente dentro do fluxo do SIEM;

4.11.11.5. Envio de e-mail com as ações realizados pelo usuário.

4.11.12. Inclusão de usuários em grupos sensíveis

4.11.12.1. Descrição:

4.11.12.2. Usuário incluído no grupo sensível;

4.11.12.3. Usuário incluído sem solicitação formal.

4.11.12.4. Ações:

4.11.12.5. Abertura de incidente dentro do fluxo do SIEM.

4.11.13. Atividade de usuário com privilégios administrativos, originados de localização externa

4.11.13.1. Descrição:

4.11.13.2. Atividade realizada por usuário administrativo a partir de um endereço externo ao ambiente corporativo.

4.11.13.3. Ações:

4.11.13.4. Abertura de incidente dentro do fluxo do SIEM;

4.11.13.5. Informação no dashboard;

4.11.13.6. Envio de e-mail para as áreas pertinentes.

4.11.14. Identificação de usuário e/ou dispositivos que acessaram determinado sistema

4.11.14.1. Descrição:

4.11.14.2. Correlacionar logs SMF com logon no AD/LDAP para identificar qual usuário e/ou dispositivo que acessou determinado sistema

4.11.14.3. Ações:

4.11.14.4. Gerar novo log que será retroalimentado no fluxo de correlacionamento do SIEM;

4.11.14.5. Criar console para consulta, pesquisa e emissão de relatórios;

4.11.14.6. Gerar relatório com no mínimo as seguintes informações: (IP, endereço lógico, usuário, terminal, tipo do evento, data, hora e sistema acessado).

4.11.14. Histórico de acesso à rede corporativa

4.11.14.1. Descrição:

4.11.14.2. Identificar eventos de logon, logoff de todos os usuários

4.11.14.3. Ações:

4.11.14.4. Criar console para consulta, pesquisa e emissão de relatórios;

4.11.14.5. Gerar relatório com no mínimo as seguintes informações: (IP, endereço lógico, usuário, tipos de acesso (remoto/local), tipo do evento, data e hora).

4.11.16. Alteração no grupo local de administradores

4.11.16.1. Descrição:

4.11.16.2. Usuário incluído no grupo local de administradores

4.11.16.3. Ações:

4.11.16.4. Exclusão do usuário do grupo de administrador local;

4.11.16.5. Abertura de incidente dentro do fluxo do SIEM.

4.11.17. Falhas na execução de operações em bancos de dados

4.11.17.1. Descrição:

4.11.17.2. Tentativas de update para usuário sem permissão no banco de dados

4.11.17.3. Ações:

4.11.17.4. Abertura de incidente dentro do fluxo do SIEM;

4.11.17.5. Envio de relatório com ações realizados pelo usuário;

4.11.17.6. Informação no dashboard.

4.11.18. Ataque de força bruta em bancos de dados

4.11.18.1. Descrição:

4.11.18.2. Tentativas sequenciais de acesso ao banco de dados com senha errada

4.11.18.3. Ações:

4.11.18.4. Abertura de incidente dentro do fluxo do SIEM;

4.11.18.5. Informação no dashboard.

4.11.19. Conexão indevida com o banco de dados

4.11.19.1. Descrição:

4.11.19.2. Conexão direta ao banco de dados sem utilizar aplicação;

4.11.19.3. Conexão ao banco de dados com IP de origem diferente do balanceador de cargas;

4.11.19.4. Alteração no padrão de acesso do usuário ao banco de dados.

4.11.19.5. Ações:

4.11.19.6. Abertura de incidente dentro do fluxo do SIEM;

4.11.19.7. Informação no dashboard.

4.11.20. Alto volume de negações de acesso

4.11.20.1. Descrição:

4.11.20.2. Alto volume de negação de acesso para um mesmo destino;

4.11.20.3. Alto volume de negação de acesso a partir de uma mesma origem

4.11.20.4. Ações:

4.11.20.5. Informação no dashboard com timeline de acessos;

4.11.20.6. Informação no dashboard com o comportamento de fluxo de rede;

4.11.20.7. Abertura de incidente dentro do fluxo do SIEM para as áreas de sustentação;

4.11.20.8. Elaboração de template de configuração para bloqueio temporário.

4.11.21. Identificação de ataques DoS/DDoS no ambiente

4.11.21.1. Descrição:

4.11.21.2. Identificação de anomalia no fluxo de conexão e/ou tráfego de rede do ambiente.

4.11.21.3. Ações:

4.11.21.4. Informação no dashboard com timeline de acessos;

4.11.21.5. Informação no dashboard com o comportamento de fluxo de rede;

4.11.21.6. Abertura de incidente dentro do fluxo do SIEM;

4.11.21.7. Elaboração de template de configuração para bloqueio temporário.

4.11.22. Sessões simultâneas

4.11.22.1. Descrição:

4.11.22.2. Usuário com mais de uma sessão na VPN//VDI

4.11.22.3. Ações:

4.11.22.4. Abertura de incidente dentro do fluxo do SIEM;

4.11.22.5. Informação no dashboard;

4.11.22.6. Bloquear usuário temporariamente.

4.11.23. Usuário acessando sistema indevido via acesso remoto

4.11.23.1. Descrição:

4.11.23.2. Usuário conectado via acesso remoto tentando acessar um sistema sem as devidas credenciais.

4.11.23.3. Ações:

4.11.23.4. Abertura de incidente dentro do fluxo do SIEM;

4.11.23.5. Informação no dashboard.

4.11.24. Endereços internos acessando IP/URL inseridas em blacklists

4.11.24.1. Descrição:

4.11.24.2. Endereço IP interno acessando/tentando acessar IP/URL em blacklist

4.11.24.3. Ações:

4.11.24.4. Abertura de incidente dentro do fluxo do SIEM para as áreas de segurança tecnológica;

4.11.24.5. Elaboração de template de configuração para bloqueio temporário.

4.11.24.6. Mudança de regras de Firewall fora da janela de manutenção

4.11.25. Mudança de regras de Firewall fora da janela de manutenção

4.11.25.1. Descrição:

4.11.25.2. Modificação/configuração de política de firewall não alinhado com o período de janela de manutenção

4.11.25.3. Ações:

4.11.25.4. Abertura de incidente dentro do fluxo do SIEM para as áreas de segurança tecnológica;

4.11.25.5. Abertura de ticket no ITSM.

4.11.26. Mudança de regras no IPS fora da janela de manutenção

4.11.26.1. Descrição:

4.11.26.2. Modificação/configuração de políticas de IPS, sem autorização

4.11.26.3. Ações:

4.11.26.4. Abertura de incidente dentro do fluxo do SIEM para as áreas de segurança tecnológica;

4.11.26.5. Abertura de ticket no ITSM.

4.11.27. Evento de alto impacto no IPS

4.11.27.1. Descrição:

4.11.27.2. Detecção de eventos classificados como de alto impacto no IPS.

4.11.27.3. Ações:

4.11.27.4. Abertura de incidente dentro do fluxo do SIEM;

4.11.27.5. Informação no dashboard;

4.11.27.6. Abertura de ticket no ITSM;

4.11.27.7. Elaboração de template de configuração para bloqueio temporário.

4.11.28. Detecção de varredura de portas

4.11.28.1. Descrição:

4.11.28.2. Tentativas de conexão em múltiplas portas de um ou mais destinos

4.11.28.3. Ações:

4.11.28.4. Abertura de incidente dentro do fluxo do SIEM;

4.11.28.5. Informação no dashboard;

4.11.28.6. Elaboração de template de configuração para bloqueio temporário.

4.11.29. Detecção de eventos de segurança provenientes de alertas de múltiplas fontes

4.11.29.1. Descrição:

4.11.29.2. Correlacionar alertas de IPS/Firewall/Antivírus/DLP/NAC e verificar se são provenientes de uma mesma causa raiz

4.11.29.3. Ações:

4.11.29.4. Abertura de incidente dentro do fluxo do SIEM;

4.11.29.5. Informação no dashboard.

4.11.30. Ameaças não tratadas

4.11.30.1. Descrição:

4.11.30.2. Detecção de vírus e/ou malwares que foram identificados, porém não foram movidos para quarentena ou removidos

4.11.30.3. Ações:

4.11.30.4. Abertura de incidente dentro do fluxo do SIEM;

4.11.30.5. Informação no dashboard.

4.11.31. Equipamentos não autorizados acessando a rede corporativa

4.11.31.1. Descrição:

4.11.31.2. Correlacionar informações de tabela ARP de roteadores com endereços MAC reconhecidos como legítimos

4.11.31.3. Ações:

4.11.31.4. Abertura de incidente dentro do fluxo do SIEM;

4.11.31.5. Informação no dashboard;

4.11.31.6. Envio de e-mail para as áreas pertinentes.

4.11.32. Relatório estatístico de rede

4.11.32.1. Descrição:

4.11.32.2. Identificar os seguintes itens:

4.11.32.3. Portas altas mais e menos utilizadas;

4.11.32.4. Protocolos mais e menos utilizados;

4.11.32.5. Consumo de banda de rede por usuário e/ou dispositivo;

4.11.32.6. Endereços externos suspeitos.

4.11.32.7. Ações:

4.11.32.8. Informação no dashboard com os maiores consumidores de banda;

4.11.32.9. Geração de relatório com data e hora e os itens analisados.

4.11.33. Endereços internos tentando acessar a internet sem a utilização de proxy

4.11.33.1. Descrição:

4.11.33.2. Identificar usuários e/ou dispositivos que estejam acessando endereços externos (internet) sem a utilização de proxy.

4.11.33.3. Ações:

4.11.33.4. Abertura de incidente dentro do fluxo do SIEM para as áreas de segurança tecnológica;

4.11.33.5. Elaboração de template de configuração para bloqueio temporário.

4.11.34. Endereços internos acessando a internet com proxy não autorizado

4.11.34.1. Descrição:

4.11.34.2. Identificar usuários e/ou dispositivos que estejam acessando endereços externos (internet) com a utilização de proxy não autorizado.

4.11.34.3. Ações:

4.11.34.4. Abertura de incidente dentro do fluxo do SIEM para as áreas de segurança tecnológica;

4.11.34.5. Elaboração de template de configuração para bloqueio temporário.

4.11.35. Monitoração de comportamento de hosts suspeitos

4.11.35.1. Descrição:

4.11.35.2. Comunicação de múltiplos dispositivos internos com destino a endereços IP/URL desconhecidos e/ou suspeitos;

4.11.35.3. Hosts com hits em assinaturas de IPS ou Antivírus.

4.11.35.4. Ações:

4.11.35.5. Abertura de incidente dentro do fluxo do SIEM para a área de segurança tecnológica;

4.11.35.6. Envio de e-mail para o responsável;

4.11.35.7. Informação no dashboard.

4.11.36. Gestão de reincidência de ameaças

4.11.36.1. Descrição:

4.11.36.2. Identificação de usuários, dispositivos e sistemas envolvidos em situações problemáticas por mais de uma vez.

4.11.36.3. Ações:

4.11.36.4. Abertura de incidente dentro do fluxo do SIEM para a área responsável.

4.11.36.5. Informação no dashboard.

4.11.37. Colaborador trabalhando fora do horário habitual

4.11.37.1. Descrição:

4.11.37.2. Monitoração dos usuários de acordo com o horário de trabalho para possível identificação de hora extra indevida ou atividades não permitidas.

4.11.37.3. Ações:

4.11.37.4. Abertura de incidente dentro do fluxo do SIEM;

4.11.37.5. Informação no dashboard;

4.11.37.6. Envio de e-mail para as áreas pertinentes.

4.11.38. Utilização de dispositivos e/ou contas fora de sua geolocalização habitual

4.11.38.1. Descrição:

4.11.38.2. Dispositivos e/ou contas sendo utilizadas em localidade distinta do perfil habitual, sem registro de destacamento/mudança nas bases de RH.

4.11.38.3. Ações:

4.11.38.4. Abertura de incidente dentro do fluxo do SIEM;

4.11.38.5. Informação no dashboard;

4.11.38.6. Envio de e-mail as áreas pertinentes.

4.11.39. Padrão anormal de utilização da internet

4.11.39.1. Descrição:

4.11.39.2. Usuário efetuando download/upload fora do perfil habitual.

4.11.39.3. Ações:

4.11.39.4. Abertura de incidente dentro do fluxo do SIEM;

4.11.39.5. Informação no dashboard;

4.11.39.6. Envio de e-mail para o gestor imediato.

4.11.40. Padrão anormal de utilização de acesso remoto

4.11.40.1. Descrição:

4.11.40.2. Dispositivo e/ou usuário acessando o ambiente computacional remotamente em horários e/ou com duração divergente do perfil habitual.

4.11.40.3. Ações:

4.11.40.4. Abertura de incidente dentro do fluxo do SIEM;

4.11.40.5. Informação no dashboard;

4.11.40.6. Envio de e-mail para o gestor imediato.

4.11.41. Padrão anormal de utilização de conta de administrador e/ou de serviço

4.11.41.1. Descrição:

4.11.41.2. Conta de administrador e/ou de serviço sendo utilizada fora do perfil habitual.

4.11.41.3. Ações:

4.11.41.4. Abertura de incidente dentro do fluxo do SIEM;

4.11.41.5. Informação no dashboard;

4.11.41.6. Envio de e-mail para as áreas pertinentes.

4.11.42. Registro de ponto em dispositivo e/ou localidade divergente do padrão habitual.

4.11.42.1. Descrição:

4.11.42.2. Registro de ponto eletrônico a partir de dispositivo ou geolocalização fora do perfil habitual, sem registro no sistema de RH.

4.11.42.3. Ações:

4.11.42.4. Abertura de incidente dentro do fluxo do SIEM;

4.11.42.5. Informação no dashboard;

4.11.42.6. Envio de e-mail para as áreas pertinentes.

4.11.43. Desvio de comportamento no acesso a aplicações

4.11.43.1. Descrição:

4.11.43.2. Registro de acessos às aplicações fora do perfil habitual, inclusive de geolocalização

4.11.43.3. Ações:

4.11.43.4. Abertura de incidente dentro do fluxo do SIEM;

4.11.43.5. Informação no dashboard;

4.11.43.6. Envio de e-mail para as áreas pertinentes.

4.11.44. Monitorar interações entre usuários através do correio eletrônico

4.11.44.1. Descrição:

4.11.44.2. Correlacionar logs do correio eletrônico com listas de observação de usuários monitorados.

4.11.44.3. Ações:

4.11.44.4. Abertura de incidente dentro do fluxo do SIEM;

4.11.44.5. Gerar alerta quando houver interação entre usuários monitorados;

4.11.44.6. Envio de e-mail para as áreas pertinentes.

4.11.45. Monitorar interações entre usuários através do mensageiro

4.11.45.1. Descrição:

4.11.45.2. Correlacionar logs do mensageiro com listas de observação de usuários monitorados.

4.11.45.3. Ações:

4.11.45.4. Abertura de incidente dentro do fluxo do SIEM;

4.11.45.5. Gerar alerta quando houver interação entre usuários monitorados;

4.11.45.6. Envio de e-mail para as áreas pertinentes.

4.11.46. Correlacionar trilhas de auditoria

4.11.46.1. Descrição:

4.11.46.2. Correlacionar trilhas de auditoria de sistemas com os dados de bases de autenticação e origem de acesso.

4.11.46.3. Ações:

4.11.46.4. Criar console para consulta, pesquisa com aplicação de filtros e geração de relatórios.

4.11.47. Identificação de acessos à internet

4.11.47.1. Descrição:

4.11.47.2. Informar as URL acessadas por equipamentos e/ou usuários

4.11.47.3. Ações:

4.11.47.4. Criar console para consulta, pesquisa com aplicação de filtros e geração de relatórios.

4.11.48. Monitorar DHCP

4.11.48.1. Descrição:

4.11.48.2. Monitorar equipamentos conectados nos servidores DHCP, correlacionando as bases dos diversos servidores e blacklists construídas.

4.11.48.3. Ações:

4.11.48.4. Criar painel de monitoração no dashboard;

4.11.48.5. Gerar alertas no dashboard;

4.11.48.6. Enviar e-mail para as áreas pertinentes;

4.11.48.7. Cria template para bloqueio.

4.11.49. Monitorar acesso de equipamentos estranhos à rede corporativa

4.11.49.1. Descrição:

4.11.49.2. Correlacionar tabela ARP, servidores DHCP, registros do NAC, blacklists e whitelists, identificando equipamentos estranhos à rede.

4.11.49.3. Ações:

4.11.49.4. Gerar alertas no dashboard;

4.11.49.5. Enviar e-mail para a áreas pertinentes;

4.11.49.6. Criar template para bloqueio temporário do dispositivo.

4.12. Por meio dos serviços mensais deverá ainda ser prestado serviço de transferência de conhecimento

4.12.1. Consiste na passagem de conhecimento técnico para os servidores do TSE, das funcionalidades do ambiente de software objeto deste edital, de sua instalação, configuração, otimização e operação.

4.12.2. As atividades de transferência de conhecimento deverão ser realizadas para 5 (cinco) pessoas indicadas pelo TSE divididas em até 2 (duas) turmas, sob demanda do TSE.

4.12.3. A CONTRATADA, em até 15 (quinze) dias úteis após a solicitação formal do TSE, deverá realizar a transferência de conhecimento para a equipe de suporte do TSE visando prover os conhecimentos necessários para o acompanhamento da implantação da solução e para prestação dos serviços de configuração, operação e gerenciamento de todos os componentes da solução.

4.12.4. A transferência de conhecimento deverá abranger, no mínimo, os seguintes tópicos:

4.12.4.1. Tecnologias utilizadas, conceitos e arquitetura;

4.12.4.2. Instalação, configuração e operação dos equipamentos e softwares;

4.12.4.3. Administração e gerenciamento da solução;

4.12.4.4. Tópicos específicos do projeto técnico, a critério do TSE;

4.12.4.5. Implementação de regras de correlacionamento;

4.12.4.6. Outros tópicos relevantes para a implementação e operação no TSE.

4.12.5. A CONTRATADA deverá encaminhar conteúdo programático para validação pelo TSE em até 5 (cinco) dias úteis após a solicitação para realização da transferência de conhecimento.

4.12.6. As atividades de transferência de conhecimentos deverão ser realizadas de modo online/remotamente, a critério do TSE, por meio de ferramenta de videoconferência.

4.12.7. A transferência de conhecimento deverá ser baseada nos conteúdos programáticos oficiais do FABRICANTE da solução e realizada por instrutor devidamente certificado pelo FABRICANTE.

4.12.8. A transferência de conhecimento deverá ser ministrada, a critério do TSE, em turmas fechadas ou abertas.

4.12.9. O TSE poderá, a seu critério, alterar o cronograma citado nos subitens anteriores de forma a adequá-lo à disponibilidade dos técnicos que trabalham diretamente com a solução.

4.12.10. A transferência de conhecimento deverá ser realizada no idioma português (Brasil).

4.12.11. Para a realização das atividades, a CONTRATADA deverá providenciar todos os recursos necessários, tais como a infraestrutura e o material de apoio, exceto eventuais despesas com transporte, alimentação e hospedagem dos participantes do TSE.

4.12.12. Os custos referentes a deslocamento do profissional da CONTRATADA, se necessário, serão de responsabilidade da CONTRATADA, incluindo passagens, hospedagem e alimentação.

4.12.13. A carga horária mínima para a transferência de conhecimentos deverá ser de, no mínimo, 40 horas.

4.12.14. O hands on deverá ser prático.

4.12.15. A documentação será de propriedade do TSE, podendo ser utilizada para futuras reproduções sem objetivos comerciais.

5. Item 5 do grupo 1 - 240 (DUZENTAS E QUARENTA) HORAS, durante a vigência do contrato, de suporte técnico especializado realizado exclusivamente pelo fabricante.

5.1. Desenvolvimento e Implementação de Regras Customizadas: Criar regras específicas para capturar eventos e incidentes específicos que são únicos para o ambiente da Contratante.

5.2. Elaboração, apresentação e entrega do projeto executivo englobando, no mínimo:

5.2.1. Integração com Sistemas Externos: Integrar o SIEM com outros sistemas e tecnologias dentro do TSE, como sistemas de gestão de identidade, ferramentas de gestão de vulnerabilidades, ou outras plataformas de segurança que não sejam integradas nativamente ou por meio de parametrizações.

5.2.2. Desenvolver dashboards e relatórios customizados para atender às necessidades específicas de monitoramento e reporting do TSE.

5.2.3. Tunning de Desempenho: Ajustar a configuração do SIEM para melhorar o desempenho e a eficiência, o que pode incluir a configuração de índices, ajustes de banco de dados e otimização de consultas, dentre outras ações necessárias.

5.2.4. Implementar novas funcionalidades ou ajustes em capacidades de acordo com a necessidade do Contratante.

5.2.5. Otimizar a Inteligência de Segurança: Permita-nos fornecer uma revisão técnica e operacional abrangente do ambiente de SIEM. Fazer recomendações, sugerir melhorias e ajudar com o ajuste.

5.2.6. Suporte avançado na atualização da ferramenta para novas versões.

5.2.7. Fornecer cobertura especializada para necessidades variadas de projetos, incluindo conformidade específica do cliente, revisões de implantação, conselhos de arquitetura e assistência de otimização.

5.2.8. As horas técnicas deste tópico poderão ser utilizadas nas demandas de implantação ou outras atividades que a CONTRATANTE entender como necessária.

5.3 O TSE convocará a CONTRATADA para, em reunião conjunta, fazer o planejamento de trabalho e ações a serem executadas com o objetivo de detalhar as atuações das respectivas equipes técnicas.

5.4. A CONTRATADA terá 3 (três) dias úteis a partir do acionamento do TSE para gerar uma proposta de atendimento do serviço planejado, de acordo com as necessidades definidas.

5.5. A CONTRATADA terá 2 (dois) dias úteis a partir da aprovação pelo TSE e emissão de Ordem de Serviço para iniciar o atendimento do serviço planejado.

5.6. A CONTRATADA deverá disponibilizar profissional certificado na solução, com notório conhecimento e experiência profissional para a execução da consultoria especializada para o TSE.

5.7. Quando houver a entrega de serviços em desacordo com o especificado, que ensejarem retrabalho ou que apresentarem falhas, o fornecedor não será remunerado pela correção.

6. Item 6 - Subscrição de fornecimento de lista de reputação de endereços ip que cubram a proteção de serviços maliciosos de VPN, Proxy, bem como a visibilidade de tráfego malicioso no ambiente da Contratante (internet e rede local). Lista de referência: (SPUR.US e MAXMIND)

6.1. A lista deve ser capaz de registrar e armazenar endereços IP de forma única.

6.2. A lista de IPs deve ser atualizada diariamente para garantir que está sempre atualizado.

6.3. A lista de IPs deve ser fornecida em formato JSON, permitindo o download dela.

6.4. A lista deve possuir a contagem de usuários associados a um determinado IP.

6.5. Para cada IP, o sistema deve permitir a associação a uma organização/ISP específica.

6.6. Deve cobrir endereços IPv4 e IPv6.

6.7. O sistema deve mapear mais de 400 diferentes provedores de VPN e Proxy.

6.8. Identificação e Categorização de IPs:

6.9. Deve ser capaz de identificar a localização geográfica de um endereço IP.

6.10. A lista deve possuir o código do país para um determinado IP.

6.11. A lista deve ser capaz de categorizar IPs anônimos com base em seu uso, como VPN, proxy e nó de saída TOR.

6.12. Deve ser capaz de identificar, no mínimo, 4 milhões de IPs que são usados por serviços de proxy, VPNs, hosting providers e outros que podem ser usados para ocultar a verdadeira localização de um usuário.

6.13. Para comprovação de atendimento dos itens, o TSE poderá solicitar um exemplo da lista no momento da licitação.

7. SERVIÇO DE IMPLANTAÇÃO (Aplicável aos itens 1, 2 e 3 do Grupo 1 e Item 6)

7.1. Elaboração, apresentação e entrega do projeto executivo englobando, no mínimo:

7.1.1. Levantamento da infraestrutura tecnológica a ser monitorada no TSE;

7.1.2. Levantamento e classificação dos eventos de segurança críticos à monitoração do ambiente (a infraestrutura a ser monitorada);

7.1.3. Especificação dos itens necessários à implantação;

7.1.4.. Identificação dos aspectos da política de segurança e normas internas da TSE que possam impactar na geração e coleta de eventos;

7.1.5. Requisitos para implantação, levando em consideração o ambiente tecnológico da TSE;

7.1.6. Especificação técnica de toda a solução, funcionalidade e arquitetura a ser utilizada no TSE;

7.1.7. Especificação do dimensionamento dos elementos da solução (coletores,

correlacionadores, base de dados, storage, rede, etc);

7.1.8. Posicionamento dos elementos da solução na rede;

7.1.9. Segurança da solução e manutenção de capacidade de processamento em caso de falhas;

7.1.10. Projeto final contendo a forma de implantação a ser utilizada, agregando todos os elementos técnicos e executivos.

7.2. O projeto executivo a que se refere o item 7.1 deverá ser entregue em até 10 (dez) dias úteis, contados da ordem de fornecimento do(s) respectivo(s) item(ns).

7.3. O TSE terá 3 (três) dias úteis para aprovar ou solicitar ajustes no projeto executivo.

7.4. A Contratada terá 3 (três) dias úteis para ajustar o projeto às solicitações do TSE.

8. SINDICÂNCIA DA VIDA PREGRESSA (Aplicável ao Item 4 do Grupo 1)

8.1. Deverá ser apresentado, pela CONTRATADA, como requisito para alocar força de trabalho a este contrato a apresentação personalíssima por cada indivíduo. Apenas será necessário apresentar Sindicância da Vida Pregressa para o(s) técnico(s) que realizarem atendimento à operação assistida correspondente ao Item 4 do Grupo 1.

8.2. Certidão Judicial de Distribuição ("nada consta" ou "certidão negativa"), da esfera criminal, da Justiça Comum, Federal e Estadual.

8.3. Apresentar declaração quanto ao exercício de outro(s) cargo(s), emprego(s) ou função(ões) pública(s) e sobre recebimento de proventos decorrente de aposentadoria e pensão de qualquer ente da federação;

8.4. Não será aceita a indicação de colaborador por parte da CONTRATADA que, dentre outros:

8.4.1. Tenha sido condenado à pena privativa de liberdade transitada em julgado ou qualquer outra condenação incompatível com a função pública;

8.4.1. Tenha registro de antecedentes criminais, finalizado por meio de Termo de ajuste de conduta ou figura jurídica análoga;

8.4.3. Tenha registro de antecedentes criminais, transitado em julgado;

8.4.4. Tenha em seu histórico ilícitos administrativos, mesmo sem tipificação penal;

8.4.5. Tenha praticado atos que prejudiquem a imagem e confiança na Justiça Eleitoral;

8.4.6. Tenha efetuado declarações falsas ou omissões relevantes sobre qualificações ou antecedentes.

8.8. Apresentar outros documentos que se fizerem necessários, à época da alocação;

8.9. A sindicância da vida pregressa poderá pesquisar ou exigir a apresentação de documentos adicionais:

8.9.1. Histórico criminal, assegurando que não haja condenações por crimes graves ou incompatíveis com a função pretendida.

8.9.2. Histórico financeiro, buscando indícios de corrupção, fraude ou conduta financeira irresponsável

8.9.3. Histórico de emprego anterior, incluindo a realização de entrevistas com ex-empregadores e colegas para avaliar a conduta do profissional.

8.9.4. Mídias sociais e o comportamento online identificando posturas ou opiniões que possam ser consideradas incompatíveis com os valores e ética da instituição.

8.9.5. Entrevistas com referências pessoais, como amigos e familiares, para avaliar o caráter e a integridade.

8.9.6. Validação das qualificações educacionais e certificações apresentadas, assegurando sua autenticidade e relevância para o cargo.

8.9.7. Atestado de saúde mental e física do candidato através de exames médicos adequados, garantindo a aptidão para as responsabilidades do cargo.

8.9.8. Conformidade com todos os aspectos legais e regulatórios aplicáveis, como obrigações fiscais e militares, garantindo que o candidato esteja em dia com seus deveres civis.

8.10. Os candidatos a colaboradores para execução desde contrato deverão apresentar ciência prévia e formal acerca do processo de sindicância da vida pregressa passível de ser executado juntamente com a indicação nominal dos profissionais indicados.

8.11. A alocação de força de trabalho nas atividades do contrato deverá ser autorizada pela equipe de Gestora do contrato.

ANEXO I-VII - MODELO DE ORDEM DE SERVIÇO

ORDEM DE SERVIÇO (OS)			
N° da Ordem de Serviço	**Data de Emissão da OS**	**N° do Contrato**	**Data de Assinatura do Contrato**
Área Requisitante		**Requisitante Responsável**	
IDENTIFICAÇÃO DA EMPRESA CONTRATADA			
Nome da Empresa			
CNPJ		**Inscrição Estadual**	
Endereço			
Cidade	**Estado**	**CEP**	
Telefone	**E-mail institucional**		
Preposto			
OBJETO DO CONTRATO:			
ESPECIFICAÇÃO DOS SERVIÇOS A SEREM EXECUTADOS			

Item	**Descrição**	**Horas consumidas**	**Valor total (R$)**
01			
02			
03			
04			
		Valor total da OS:	

DETALHAMENTO DOS SERVIÇOS A SEREM EXECUTADOS E DAS ENTREGAS	
PERÍODO DE EXECUÇÃO DOS SERVIÇOS	
Data de Início da Execução: ___/___/_____	**Data de Término da Execução: ___/___/_____**
APROVAÇÃO DO GESTOR DO CONTRATO	
Solicitação:	

Solicitamos a realização do serviço acima caracterizado, nos termos constantes desta Ordem de Serviços, que tem por base as obrigações e responsabilidades da contratada constantes do contrato firmado, supra indicado.

<Nome do Fiscal Requisitante>

Matrícula

Fiscal Requisitante

Autorização

Autorizo a realização do serviço acima caracterizado, nos termos constantes desta Ordem de Serviços, que tem por base as obrigações e responsabilidades da contratada constantes do contrato firmado, supra indicado.

<Nome do Gestor do Contrato >

Matrícula

Gestor do Contrato

CIENTE DA CONTRATADA

Declaramos nossa ciência e concordância com as condições registradas nesta Ordem de Serviços para execução dos serviços solicitados.

<Nome do Representante Legal da Contratada>

CPF:

Preposto da Contratada

Obs: o modelo poderá ser ajustado visando melhor adequar-se à necessidade de serviço

ANEXO I-VIII - TERMO DE CONFIDENCIALIDADE PARA VISTORIA TÉCNICA

1. Eu <nome, nacionalidade, estado civil, cargo> inscrito(a) no CPF sob o nº XXX.XXX.XXX-XX, assumo o compromisso de manter a confidencialidade sobre todas as informações obtidas em função da participação em certame licitatório junto a CONTRATANTE. Por este termo de confidencialidade e sigilo comprometo-me:

2. A não utilizar as informações confidenciais a que tiver acesso, para gerar benefício próprio exclusivo e / ou unilateral, presente ou futuro, ou para o uso de terceiros.

3. A não efetuar nenhuma gravação ou cópia da documentação confidencial a que tiver acesso.

4. A não se apropriar para si ou para outrem de material confidencial e / ou sigiloso da tecnologia que venha a ser disponível.

5. A não repassar o conhecimento das informações confidenciais, responsabilizando-se por todas as pessoas que vierem a ter acesso às informações, por seu intermédio, e obrigando-se, assim, a ressarcir a ocorrência de qualquer dano e / ou prejuízo oriundo de uma eventual quebra de sigilo das informações fornecidas.

6. Neste Termo, as seguintes expressões serão assim definidas:

7. Informação Confidencial significará toda informação revelada através da apresentação da tecnologia, a respeito de, ou, associada com a Avaliação, sob a forma escrita, verbal ou por quaisquer outros meios.

8. Informação Confidencial inclui, mas não se limita, à informação relativa às operações, processos, planos ou intenções, informações sobre produção, instalações, equipamentos, sistemas, dados, habilidades especializadas, projetos, métodos e metodologia, fluxogramas, especializações, componentes, fórmulas, produtos e questões relativas ao desempenho das atividades laborais.

9. Avaliação significará todas e quaisquer discussões, conversações ou negociações entre, ou com as partes, de alguma forma relacionada ou associada com a apresentação da tecnologia, projetos ou produtos.

10. A vigência da obrigação de confidencialidade e sigilo, assumida pela minha pessoa por meio deste termo, terá a validade enquanto a informação não for tornada de conhecimento público por qualquer outra pessoa, ou mediante autorização escrita, concedida à minha pessoa pelas partes interessadas neste termo.

11. Pelo não cumprimento do presente Termo de Confidencialidade e Sigilo, fica o abaixo assinado ciente de todas as sanções judiciais que poderão advir.

Brasília, _____ de _____ de .

_____
Representante da licitante

ANEXO I-IX - MODELO DE TERMO DE CIÊNCIA

TERMO DE CIÊNCIA, VINCULADO AO CONTRATO TSE Nº

_____/_____, QUE ENTRE SI CELEBRAM O TRIBUNAL SUPERIOR ELEITORAL E EMPRESA _____.

Eu, _____, portador do documento de identidade nº _____, expedido pela _____, CPF nº _____, pelo presente Termo, assumo perante a empresa _____.
o compromisso de manutenção de sigilo sobre as informações a que tenha acesso ou conhecimento no âmbito do Tribunal em razão das atividades profissionais a serem realizadas em decorrência de meu contrato de trabalho com a empresa _____.

Comprometo-me a não as divulgar ou comentá-las interna ou externamente e cumprir as condutas adequadas contra destruição, modificação, divulgação indevida e acesso indevido, seja acidental ou intencionalmente.

Estou ciente de que esse Termo se refere a todas as informações do Tribunal – dados, processos, informações, documentos e materiais – seja qual for o meio através do qual seja apresentada ou compartilhada: escrita em papel ou nos sistemas eletrônicos, falada em conversas formais e informais, disseminada nos meios de comunicação internos como reuniões, televisão, etc., e da possibilidade de responsabilização nas esferas civil, penal e administrativa por eventuais prejuízos que tenha dado causa, decorrentes da prestação dos serviços objeto do contrato.

Este compromisso terá vigência a partir de sua assinatura, permanecendo em vigor até ____ (meses/anos) após o término do contrato, mantendo-se, da mesma forma, a obrigação de confidencialidade após o encerramento da vigência do contrato, inclusive em caso de rescisão contratual.

Declaro que o Tribunal tem minha permissão prévia para acesso e monitoramento do ambiente de trabalho.

Local e data:

Empresa:

Nome:

CPF: - RG:

Assinatura: _____

ANEXO I-X - MODELO DE TERMO DE CONFIDENCIALIDADE

TERMO DE CONFIDENCIALIDADE, VINCULADO AO CONTRATO TSE Nº _____/_____, QUE ENTRE SI CELEBRAM O TRIBUNAL SUPERIOR ELEITORAL E A EMPRESA _____.

O CONTRATANTE, TRIBUNAL SUPERIOR ELEITORAL, sediado no Setor de Administração Federal Sul - SAFS, Quadra 7, Lotes 1 e 2, Brasília/DF, CNPJ nº 00.509.018/0001-13, representado pelo (a) _____, Senhor(a) _____, portador(a) da Carteira de Identidade nº _____, CPF nº _____ e, de outro lado, a empresa CONTRATADA, _____, inscrita no CNPJ/MF sob o número _____, sediada em _____, neste ato, representada por _____, portador(a) da Carteira de Identidade nº _____, CPF nº _____, têm justo e acordado celebrar o presente TERMO DE CONFIDENCIALIDADE, VINCULADO AO CONTRATO TSE Nº _____/_____, por meio do qual a CONTRATADA compromete-se a observar as disposições das cláusulas seguintes:

CLÁUSULA PRIMEIRA
DO OBJETO

O presente Termo de Confidencialidade tem por objeto a necessária e adequada proteção às informações confidenciais a que a contratada tiver acesso na execução das atividades do Contrato nº _____/202__ contempladas especificamente no respectivo contrato.
Subcláusula primeira – A CONTRATADA reconhece que, em razão da prestação de serviços ao TSE, tem acesso às informações pertencentes ao TSE, descritas na Cláusula Segunda, que devem ser tratadas como controladas.

CLÁUSULA SEGUNDA
DAS INFORMAÇÕES CONFIDENCIAIS

As informações controladas abrangem toda informação, por qualquer modo apresentada ou observada, tangível ou intangível, podendo incluir, mas não se limitando a: técnicas, projetos, especificações, desenhos, cópias, diagramas, fórmulas, modelos, amostras, fluxogramas, croquis, fotografias, plantas, programas de computador, discos, disquetes, pen drives, fitas, contratos, planos de negócios, processos, projetos, conceitos de produto, especificações, amostras de ideia, clientes, nomes de revendedores e/ou distribuidores, preços e custos, definições e informações mercadológicas, invenções e ideias, outras informações técnicas, financeiras ou comerciais, entre outras a que, diretamente ou através de seus empregados, prepostos ou prestadores de serviço, venha à CONTRATADA ter acesso durante ou em razão da execução do contrato celebrado, incluindo-se, ainda, o presente Termo de Confidencialidade.
Subcláusula primeira – Subcláusula primeira – Em caso de dúvida acerca da natureza confidencial de determinada informação, a CONTRATADA deverá entrar em contato com TSE e aguardar o retorno, mantendo sigilo quanto à informação até manifestação expressa do TSE sobre a confidencialidade e permissão de acesso. Em hipótese alguma, a ausência de manifestação expressa do TSE poderá ser interpretada como liberação de qualquer dos compromissos ora assumidos.

CLÁUSULA TERCEIRA
DAS OBRIGAÇÕES

A CONTRATADA compromete-se a não utilizar, bem como a não permitir que seus diretores, consultores, prestadores de serviços, empregados e/ou prepostos utilizem, de forma diversa da prevista no contrato de prestação de serviços ao TSE, as informações controladas reveladas.
Subcláusula primeira – A CONTRATADA deverá cuidar para que as informações reveladas fiquem limitadas ao conhecimento dos diretores, consultores, prestadores de serviços, empregados e/ou prepostos que estejam diretamente envolvidos nas discussões, análises, reuniões e demais atividades relativas à prestação de serviços ao TSE, devendo cientificá-los da existência deste termo e da natureza confidencial das informações controladas reveladas.
Subcláusula segunda – A CONTRATADA deverá possuir ou firmar acordos por escrito com seus diretores, consultores, prestadores de serviços, empregados e/ou prepostos cujos termos sejam suficientes a garantir o cumprimento de todas as disposições do presente Termo de Confidencialidade.
Subcláusula terceira – A CONTRATADA obriga-se a informar imediatamente ao TSE qualquer violação das regras de sigilo estabelecidas neste Termo de Confidencialidade que tenha tomado conhecimento ou ocorrido por sua ação ou omissão, independentemente da existência de dolo.

CLÁUSULA QUARTA
DO DESCUMPRIMENTO

A quebra do sigilo das informações controladas reveladas, devidamente comprovada, sem autorização expressa do TSE, sujeitará a CONTRATADA, por ação ou omissão, ao pagamento de multa de acordo com os percentuais descritos a seguir, observada a natureza e gravidade da violação que deu causa à aplicação da multa, bem como as responsabilidades administrativa, civil e penal respectivas, as quais serão apuradas em regular processo judicial ou administrativo, possibilitando inclusive a rescisão do Contrato nº _____/202__, firmado entre o TSE e a CONTRATADA sem qualquer ônus para o TSE.

- 0,5% a 1% sobre o valor do contrato - para situações de baixa criticidade;
- 2,5% a 5% sobre o valor do contrato - para situações de criticidade média;
- 8% a 10% sobre o valor do contrato - para situações de criticidade alta.

CLÁUSULA QUINTA
DO RETORNO DAS INFORMAÇÕES

A CONTRATADA devolverá imediatamente ao TSE, ao término do Contrato, todo e qualquer material de propriedade deste, inclusive registro de documentos de qualquer natureza que tenham sido criados, usados ou mantidos sob seu controle ou posse, bem como de seus empregados, prepostos ou prestadores de serviço, assumindo o compromisso de não utilizar qualquer informação considerada confidencial, conforme este Termo de Confidencialidade, a que teve acesso em decorrência do vínculo contratual com o TSE.

CLÁUSULA SEXTA

DA VIGÊNCIA

O presente termo, de natureza irrevogável e irretratável, terá vigência a partir de sua assinatura, permanecendo em vigor até ____ (meses/anos) após o término do contrato, mantendo-se, da mesma forma, a obrigação de confidencialidade após o encerramento da vigência do contrato, bem como no caso de rescisão contratual.

CLÁUSULA SÉTIMA
DAS DISPOSIÇÕES FINAIS

Os casos omissos neste Termo de Confidencialidade, assim como as dúvidas surgidas em decorrência da sua execução, serão resolvidos pelo TSE.

Por estar de acordo, a CONTRATADA, por meio de seu representante, firma o presente Termo de Confidencialidade, assinando-o eletronicamente.

JULIANA MILAGRES DE LOYOLA FLEURY
SECRETÁRIA DE ADMINISTRAÇÃO

Documento assinado eletronicamente em **12/04/2025, às 16:45**, horário oficial de Brasília, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

Tribunal Superior Eleitoral

A autenticidade do documento pode ser conferida em https://sei.tse.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=3203594&crc=C5350D0F, informando, caso não preenchido, o código verificador **3203594** e o código CRC **C5350D0F**.