ANEXO I

TERMO DE REFERÊNCIA

1 - OBJETO

1.1 - Registro de preços para **renovação e ampliação da capacidade da solução de software para gerenciamento de *logs* e eventos de segurança (SIEM - *Security Information and Event Management*),** visando atender às necessidades do Tribunal Regional Eleitoral do Paraná, conforme especificações descritas no presente Termo de Referência. A contratação compreende:

1.1.1 - Atualização do modelo de licenciamento da solução de SIEM, IBM QRADAR, para o modelo cloud pak, licenciado inicialmente para 400 (quatrocentos) servidores, com Eventos por segundo (EPS) e Flows de rede ilimitados e previsibilidade de aumento de licenças conforme crescimento do parque de servidores, visando atender o crescimento exponencial de tráfego, EPS e Flows de rede, da infraestrutura do TRE-PR.

1.1.2 - Serviço de Instalação e configuração.

1.1.3 - Serviços técnicos do fabricante, denominado “IBM Cloud Pak For Security Expert on Demand” no total de 8 pacotes de 40 horas cada, para prestação de serviço com escopo aberto para utilização em Revisão de Arquitetura, Health Check, Treinamento, e Suporte a novas configurações, regras e casos de uso.

1.1.4 - Horas de serviços técnicos especializados para atender a demandas de administração, operação assistida, planejamento, tuning e reconfiguração da solução contratada.

2 - DA JUSTIFICATIVA PARA CONTRATAÇÃO

2.1 - Em atenção às diversas normativas e resoluções recentemente estabelecidas no Poder Judiciário, em especial na Justiça Eleitoral, faz-se necessário adequar o ambiente no qual os serviços prestados pela Secretaria de Tecnologia da Informação são hospedados e disponibilizados, de forma a garantir a aderência da Justiça Eleitoral do Paraná às referidas resoluções, ensejando um ambiente tecnológico robusto e capaz de prover serviços de qualidade e eficiência para a população.

2.2 - São destacados os seguintes normativos a serem atendidos:

2.3 - Resolução TSE nº 23644/2021 que dispõe sobre a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;

2.4 - Resolução CNJ nº 396/2021 que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

2.5 - Resolução CNJ nº 370/2021 que estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);

2.6 - Resolução nº 468/2022 que dispõe sobre diretrizes para as contratações de Soluções de Tecnologia da Informação e Comunicação pelos órgãos submetidos ao controle administrativo e financeiro do Conselho Nacional de Justiça/CNJ

2.7 - Além dos requisitos legais a serem cumpridos, observa-se diariamente o aumento significativo de ataques cibernéticos contra órgãos federais, em especial aos componentes do Judiciário, com o objetivo de interromper a prestação de serviços à população, o bom desenvolvimento das atividades do órgão e, ainda, tentam obter, sob coação, vantagens financeiras através do sequestro de dados cruciais das instituições. Sendo assim, torna-se imperioso tratar os riscos existentes e preparar medidas de proteção contra ações dessa natureza.

2.8 - A renovação e ampliação da capacidade da solução de SIEM será utilizado para o completo registro dos eventos dos sistemas de informação e ativos de rede, como acessos de usuários à internet, login em computadores, acesso aos sistemas, tentativas de login, falhas em sistemas, correlação de eventos a ameaças, monitoramento de ameaças de segurança em tempo real e elaboração de relatórios de conformidade, suprindo esta necessidade, incompatível com o volume de EPS (Eventos por segundo) que a ferramenta com a atual licenciamento pode suportar.

2.9 - A implementação da solução é premissa para melhorias de controles de segurança da informação e suporte na elaboração de relatórios gerenciais, auditoria nos sistemas informatizados e dispositivos de comunicação e na segurança da rede.

2.10 - Atendimento ao art. 7º da IN 02/2022 do TRE-PR que determina o armazenamento de

registros (log´s) por 12 meses.

2.11 - A solução também será utilizada para apoiar e fundamentar as atividades da ETIR (Equipe Técnica de Tratamento e Resposta a Incidentes de Redes) e da ASC (Assessoria de Segurança Cibernética).

3 - DAS ESPECIFICAÇÕES TÉCNICAS

3.1 - ITENS QUE COMPÕEM O LOTE**:** deverão ser fornecidos os seguintes softwares e seus respectivos licenciamentos de acordo com o ambiente computacional IBM QRadar já em uso no TRE-PR, além dos serviços e descritos neste Termo de Referência:

ITEM	P/N	Descrição	QTDE	TIPO	UNIDADE	Quantidade prevista para contratação imediata
01	D0AE2ZX	IBM Security QRadar XDR Package Software 100 Resource Unit Trade Up from Eligible Program Trade Up License + SW Subscription & Support 12 Months **Código SIASG 27022**	62	TRADE UP	Unidade	62
02	E0AE3ZX	IBM Security QRadar XDR Package Software 100 Resource Unit Annual SW Subscription & Support Renewal **Código SIASG 27022**	62	TRADE UP	Unidade	62
03	E0AE3ZX	IBM Security QRadar XDR Package Software 100 Resource Unit Annual SW Subscription & Support Renewal **Código SIASG 27022**	62	TRADE UP	Unidade	62
04	Serviço	Serviço de implementação, migração e customização para o Item 1, 2 e 3 (TradeUP) **Código SIASG 27022**	01	Serviço	Unidade	01
05	D0AE4ZX	IBM Security QRadar XDR Package Software 100 Resource Unit License + SW Subscription & Support 12 Months **Código SIASG 27022**	55	Ampliação	Unidade	35

06	E0AE3ZX	IBM Security QRadarXDR PackageSoftware 100 ResourceUnit Annual SW Subscription & SupportRenewal **Código SIASG 27022**	55	Ampliação	Unidade	35
07	E0AE3ZX	IBM Security QRadarXDR PackageSoftware 100 ResourceUnit Annual SW Subscription & SupportRenewal **Código SIASG 27022**	55	Ampliação	Unidade	35
08	-	Serviço de implementação e customização para os itens 5,6 e 7 **Código SIASG 27022**	03	Serviço	Unidade	01
09	D02CNZX	IBM Cloud Pak For Security Expert on Demand **Código SIASG 27022**	08	Serviço	Unidade	0
10	-	Consultoria da Contratada **Código SIASG 27022**	300	Serviço	Hora	0

3.1.1 – Da justificativa para o agrupamento de itens em lote único:

3.1.1.1 - Trata-se de solução integrada SIEM, prevendo renovação e ampliação da solução atualmente utilizada pelo TRE-PR, com agregação de serviços do modelo C4PS, como SOAR e XDR, que na sua essencialidade não pode ser individualizada, por uma questão de eficiência na gestão contratual e fiscalização, bem como na padronização quando da abertura e resolução de chamados técnicos. Desta forma, não há razão para desmembrar a solução, tendo em vista que ao se separar um PART NUMBER, corre-se o risco de um fornecedor transferir para outrem obrigação de sua responsabilidade e vice-versa, o que poderá trazer prejuízos na manutenção e suporte da ferramenta adquirida.

3.1.1.1.2 - Mantendo a solução em lote, com um único fornecedor, o risco à segurança da informação, por compartilhamento de acesso a terceiros para suporte e instalação a ambientes de ferramentas críticas como cofre de senhas, será reduzido.

3.1.2 **-** Este Tribunal se reserva ao direito de adquirir o quantitativo que julgar necessário, podendo ser parcial, integral ou não adquirir qualquer quantidade.

3.2 – Das especificações:

3.2.1 - **Itens 1, 2 e 3:** deverão ser fornecidos de acordo com a descrição de cada item ou possuir características técnicas superiores, obedecendo o respectivo quantitativo estabelecido nos itens;

3.2.2 - **Item 4:** serviço de Instalação, implantação, migração e customização para os Itens 1,2 e 3 (TradeUP), deverão ser fornecidos pela CONTRATADA.

3.2.3 - **Itens 5, 6 e 7:** referentes a ampliação da capacidade atual da solução, deverão ser fornecidos de acordo com a descrição de cada item ou possuir características técnicas superiores, obedecendo o respectivo quantitativo estabelecido nos itens;

3.2.4 **- Item 8:** serviço de implementação e customização para os itens 5, 6 e 7 deverão ser fornecidos pela CONTRATADA.

3.2.5 – **Item 9:** Part Number D02CNZX, referente ao serviço "IBM Cloud Pak For Security Expert on Demand" onde cada PN fornece 40 (quarenta) horas de serviços, com escopo aberto para construção de um *roadmap* de atividades junto com ao fabricante, podendo ser utilizado para atividades como Revisão de Arquitetura, Health Check, Treinamento, e Suporte a novas configurações, regras e casos de uso a serem executados de forma remota, e demais atividades, conforme solicitação do CONTRATANTE.

3.2.5.1 - A solução referente ao item 9 será solicitada em blocos de 4 (quatro) unidades, correspondendo a 160 (cento e sessenta) horas de serviço a ser executada em um prazo de 90 (noventa) dias.

3.2.5.2 - A CONTRATANTE deverá solicitar a consultoria com, pelo menos, 15 (quinze) dias de antecedência ao Fabricante, que deverá, em comum acordo com a CONTRATANTE, determinar o escopo da consultoria, avaliação de risco, prazo e agendamento para início das atividades solicitadas.

3.2.5.3 - Os serviços serão executados de forma remota, com o devido acompanhamento dos servidores do TRE-PR.

3.2.5.4 – Cada pacote de 160 (cento e sessenta) horas será consumido em até 90 (noventa) dias após a assinatura de contrato e serão consumidas em uma única contratação.

3.2.5.5 - O horário de execução das atividades deverá respeitar, a princípio, o expediente do TRE-PR, 13h às 19h.

3.2.6 - **Item 10** - A empresa contratada deverá prover até 300 (trezentas) horas de serviços especializados, para utilização em suporte a quaisquer demandas de administração, operação assistida, planejamento, *tuning* e reconfiguração da solução contratada, conforme solicitação prévia e acordo referente ao número de homens/hora a ser definido antecipadamente com o CONTRATANTE.

3.2.6.1 - Os serviços poderão ser executados de forma remota, com a devida anuência e acompanhamento dos servidores do TRE-PR.

3.2.6.2 - Horas para suporte de segundo nível na solução ofertada, abrangendo o apoio e execução dos procedimentos de administração, tais como atualização e ajustes, análise, revisões, tuning da solução, configurações das funções avançadas e novas funcionalidades quando aplicáveis.

3.2.6.3 - As horas de consultoria do CONTRATANTE serão contabilizadas em termos de homem/horas.

3.2.6.4 - As horas poderão ser utilizadas durante o período do contrato.

3.2.6.5 - As horas serão consumidas sob demanda, de acordo com a necessidade da CONTRATANTE, em pacotes de, no mínimo, 04 (quatro) horas.

3.2.6.7 - A CONTRATANTE deverá solicitar a consultoria com, pelo menos, 05 (cinco) dias de antecedência à CONTRATADA, que deverá, em comum acordo com a CONTRATANTE, determinar o escopo da consultoria, avaliação de risco, prazo e agendamento para início das atividades solicitadas.

3.2.6.8 - O horário de execução das atividades deverá respeitar, a princípio, o expediente do TRE-PR, 13h às 19h.

3.2.6.9 - Nas atividades executadas em horário comercial, ou seja, das 08h às 18h, cada HORA será contabilizada como 1 hora/homem.

3.3 - As demais licenças e quantitativos registrados serão adquiridos em caso de necessidade futura de ampliação e para atender demandas do TRE-PR.

4 - DOS REQUISITOS TÉCNICOS

4.1 Requisitos técnicos que a solução deve apresentar:

4.1.1 Permitir sua instalação em ambiente virtual (todos os componentes da solução devem permitir), dos servidores físicos de propósito genérico ou em *appliance* virtual especializado.

4.1.2 Permitir o controle de acesso dos usuários à solução por meio de autenticação em serviço de diretório como Microsoft *Active Directory* e LDAP.

4.1.3 Estar licenciada de forma a manter o processamento em tempo real ou realizar o buffer dos eventos, mesmo que o tráfego de eventos atinja rajadas de três vezes o volume licenciado nas horas de pico.

4.1.4 A comunicação entre os componentes da solução deve ser feita através de criptografia, garantindo a autenticidade, confidencialidade e integridade dos dados, utilizando o protocolo TCP/IP.

4.1.5 Juntamente com a licença de atualização dos componentes da solução pelo período do contrato de suporte, a contratada deverá prover acesso à biblioteca de casos de uso do fabricante, que contenha conteúdo para download que inclua pacotes especializados de *dashboards* e coletores desenvolvidos pelo fabricante.

4.1.6 Implementar os protocolos IPv4 e IPv6.

4.1.7 Implementar compressão dos eventos em cada fase do seu ciclo de vida: transmissão, armazenamento online e *offline* dos eventos.

4.1.8 O coletor da solução deverá ser capaz de coletar, aplicar *parsing*, normalizar e categorizar os eventos dos dispositivos monitorados em tempo próximo ao real (*near-real-time*).

4.1.9 Rotular eventos por zonas diferentes mesmo que estejam em redes com mesma faixa endereçamento IP.

4.1.10 Será considerada neste Termo de Referência, a seguinte definição para conector: software desenvolvido e suportado pelo fabricante da solução que tem como função básica fazer a interface com o dispositivo monitorado, recebendo ou buscando eventos relevantes que serão inseridos na solução, contendo obrigatoriamente documentação de todos coletores nativos com informações detalhadas de configurações de cada ativo suportado.

4.1.11 A coleta de eventos de dispositivos (ativos geradores de eventos) não suportados nativamente pode ser feita através de conectores customizados. Estes conectores customizados devem utilizar padrões de mercado como CSV, arquivo texto, XML, SYSLOG, ODBC, JDBC, entre outros.

4.1.12 Ajustar o horário dos eventos, com base em limites de diferença de hora entre os eventos originais e a hora correta obtida pelo sistema através de sincronização de NTP (*Network Time Protocol*) com os servidores locais.

4.1.13 Ofuscar os campos sensíveis dos eventos (como senhas, identidade funcional, números de cartões de crédito e outros similares).

4.1.14 Coletar, no mínimo, os logs dos sistemas e ativos listados abaixo:

a) Firewalls: Cisco ASA 5585x SSP10 com Firepower, Checkpoint 4600 e 5600, Fortinet 100F e 40F, VMWare NSX, PfSense;

b) Roteadores: Cisco Nexus, Cisco RV320, Huawei/H3C MSR;

c) Switches: Cisco, Huawei, Enterasys, Extreme e alcatel;

d) Plataformas de Virtualização: VMware ESX, Hyper-V, Acropolis/KVM e Oracle VM;

e) Sistemas Operacionais: Linux (Debian, RedHat, Ubuntu, CentOs, Oracle Linux), Windows Server (2008, 2012, 2016, 2019, 2022) e FreeBSD;

f) Antivírus: TrendMicro, Clamav;

g) Servidores de Aplicação e Web: Apache2, Squid, Nginx, HAProxy, Apache Tomcat, Jboss e Microsoft IIS 7 (ou superior);

h) VPN: OpenVPN, CiscoVPN; VPN Checkpoint, VPN Fortinet.

4.1.15 Para coleta de logs deve suportar, no mínimo, os seguintes métodos:

a) Syslog (UDP, TCP e TLS);

b) CIFS;

c) FTP;

d) MySQL;
e) Oracle;
f) API;
g) JSON;

4.1.16 Suportar a coleta de dados de no mínimo 400 (quatrocentos) servidores, físicos ou virtuais, além dos ativos de rede listados acima, como firewalls, roteadores e switchs, NAC´s, access points listados nesta especificação técnica além de demais equipamentos geradores de log´s.

4.1.17 Suportar o modo de criptografia em todos os conectores.

4.1.18 Controlar a utilização da banda utilizada diretamente do conector sem a necessidade de usar recursos do sistema operacional.

4.1.19 Marcar (através de *tag*, *label* ou similar) os eventos com base em unidade organizacional: departamento, setor, secretaria ou similar. Essa marcação pode ser feita por atributos da própria mensagem, da origem do log, ou do endereço de origem do evento.

4.1.20 Normalizar e categorizar os eventos em um padrão único.

4.1.21 Armazenar os dados localmente (*cache*) em caso de indisponibilidade da comunicação com os destinos dos eventos.

4.1.22 Enviar os em cache imediatamente após a disponibilização do destino do evento.

4.1.23 Enviar o evento bruto (*raw*) para o armazenamento e consulta futura.

4.1.24 Guardar eventos normalizados/tratados e brutos em forma comprimida.

4.1.25 Inserir nos eventos normalizados metadados sobre georreferência dos mesmos.

4.1.26 Tanto os eventos de segurança quanto os de conformidade devem ser normalizados para um único padrão de eventos utilizado pela solução.

4.1.27 Permitir múltiplos perfis de configuração.

4.1.28 Enviar os eventos coletados para o correlacionador e permitir enviar para mais de um destino ao mesmo tempo.

4.1.29 Implementar a coleta, processamento e correlação de informações de fluxo de rede *Netflow v9/ SFlow*.

4.1.30 Realizar no conector a agregação de eventos semelhantes que ocorram dentro de um limite de tempo e quantidade de eventos específicos, devendo permitir agregar os eventos cuja única diferença seja o horário de ocorrência.

4.1.31 Possuir funcionalidade de atualização, gerenciamento e configuração centralizada de todos os conectores distribuídos da solução.

4.1.32 Permitir a categorização manual de eventos (já normalizados) que não se encaixem em nenhuma categoria existente, cuja nova categoria poderá ser aplicada nos eventos futuros de mesma característica.

4.1.33 Buscar um conector com capacidade de processamento disponível, ao receber um evento, de forma a garantir que não haverá perda de eventos por sobrecarga de conectores.

4.1.34 Armazenar no mínimo os seguintes dados: eventos, alertas, e toda informação pertinente à solução, tais como configuração, usuários, trilhas de auditoria e informações de depuração.

4.1.35 Armazenar logs por tempo determinado e personalizado, conforme necessidade do órgão.

4.1.36 Definir políticas diferentes de retenção dos dados on-line por tecnologia, conectores, dispositivos e *compliance*, ou seja, poderão ser definidos tempos de retenção diferentes para cada tipo de dados mantidos no banco de dados da solução, disponíveis para consulta imediata.

4.1.37 De forma a permitir seu uso em auditorias e processos forenses, não deverá ser possível, sob nenhuma hipótese, a seleção, alteração e exclusão de eventos individuais.

4.1.38 Deve ser possível apenas o expurgo de eventos conforme a política de retenção, ou seja, todos os eventos mais antigos que extrapolam o tempo de retenção ou o tamanho do armazenamento definido para esse tipo de registros.

4.1.39 Permitir o expurgo dos dados de forma automática de acordo com a personalização do prazo de retenção que precede o expurgo.

4.1.40 Permitir a utilização de volumes de armazenamento locais e externos. Deverá permitir a segregação de tipos de eventos diferentes em grupos lógicos de armazenamento diferentes, com políticas de retenção diferentes, de forma a permitir a otimização de performance.

4.1.41 Permitir exportar eventos para formato pdf e csv.

4.1.42 Deverá permitir que o usuário defina quais campos do evento serão exportados.

4.1.43 Deverá implementar funcionalidade de ajuda (*helper*) para facilitar a criação de queries.

4.1.44 Deverá implementar assistente gráfico para criação de queries.

4.1.45 Deverá implementar indexação baseada em campo e palavras-chave para acelerar buscas.

4.1.46 Deverá implementar alertas por *syslog*, SNMP e e-mail.

4.1.47 Deverá permitir visualização em tempo real de eventos que atendam ao critério de seleção definido pelo usuário.

4.1.48 Possuir relatórios pré-configurados (*templates*) separados em categorias.

4.1.49 Deverá suportar pelo menos 03 dos seguintes formatos de relatórios: html, pdf, csv, doc, xls, e xml.

4.1.50 Permitir o agendamento de geração de relatórios e o envio dos mesmos por e-mail.

4.1.51 Possuir ferramenta ou interface gráfica para desenho de modelos de relatórios ou *dashboards* personalizados.

4.1.52 Apresentar painéis de controles gráficos (*dashboards*) que mostram o status do ambiente, dos logs de eventos, além de apresentar resultados de consultas tempestivas, quando se fizerem necessárias.

4.1.53 Deverá implementar tecnologia de pesquisa distribuída nos múltiplos elementos (componentes) da solução.

4.1.54 Apresentar relatórios de eventos, alertas e incidentes em nível técnico (analítico, *drill down*) e gerencial (sintético / *dashboards*).

4.1.55 Permitir pesquisa nos eventos, e a partir de um dado evento ou conjunto de eventos, mostrar de forma gráfica seus relacionamentos e permitir o *drill-down* (detalhamento) até o nível dos dados brutos (*raw*), para efetiva investigação de incidentes, identificação de causa raiz e análise forense.

4.1.56 Possuir conformidade com a norma ISO 27001.

4.1.57 Utilizar algoritmos para verificação de integridade e autenticidade dos eventos armazenados para fins de auditoria devidamente reconhecidos como seguros.

4.1.58 Armazenar os eventos e os alertas, inclusive os normalizados, de forma indexada.

4.1.59 Deverá permitir que os campos de logs de dispositivos diferentes estejam presentes no mesmo resultado, bem como deverá ser possível a seleção dos campos que estarão presentes no resultado.

4.1.60 Deverá permitir acrescentar campos de uma fonte em outra fonte.

4.1.61 Deverá ser fornecido com solução de gerenciamento central com as seguintes características mínimas:

a) Deverá implementar, de forma centralizada, a configuração de políticas e a monitoração de todos os conectores e da solução de centralização de eventos;

b) Deverá permitir a implementação de atualização e distribuição de novas políticas de segurança pelos elementos/componentes gerenciados;

c) Deverá possuir regras de monitoração pré-configuradas, as quais podem ser editadas ou apagadas;

d) Deverá interagir diretamente com a biblioteca de casos de uso do fabricante da solução para download e atualizações de conteúdo;

e) Deverá possuir interface WEB acessível por HTTPS e CLI por SSH, com suporte ao padrão UTF-8;

4.1.62 Deverá possuir tela de monitoração com as seguintes características:

a) Tabela com percentuais e gráfico de pizza do status dos elementos/componentes monitorados agregados por tipo, mostrando o número de elementos em cada estado, bem como o número total de nós;

b) Listagem de todos os elementos/componentes que estão reportando problemas;

c) Permitir a visualização do sumário de monitoração por tipo de produto;

4.1.63 Deverá possuir tela de gerenciamento de configuração para gerenciar e criar configurações, sincronizar a configuração entre componentes/elementos e automatizar a configuração inicial dos mesmos.

4.1.64 Deverá permitir o *backup e* a restauração da configuração da solução de gerenciamento, assim como a configuração de usuários e grupo de usuários.

4.1.65 Deverá ser possível visualizar o consumo de licenças da solução.

4.1.66 Deverá permitir a visualização das taxas em eventos por segundo (EPS), *flows* por minuto (FPM) ou volume de dados diário (conforme a métrica adotada pela solução) de entrada e de saída de cada conector.

4.1.67 Deverá permitir a visualização dos dispositivos gerenciados por localização, host e tipo.

4.1.68 Permitir adição, visualização, edição e exclusão da localização de dispositivos.

4.1.69 Permitir a adição de atributos de um dispositivo, a importação de dispositivos a partir de um arquivo CSV, visualização e remoção de dispositivos, visualização de todos os dispositivos de uma localidade e varredura (*scan*) de dispositivos para detecção de novos conectores.

4.1.70 Deverá permitir a apresentação de árvore hierárquica de dispositivos.

4.1.71 Deverá apresentar para cada dispositivo: nome ou endereço IP, versão do agente (se aplicável), status de problemas encontrados no dispositivo, modelo, tipo e versão.

4.1.72 Implementar as seguintes ações nos elementos/componentes de centralização de logs: *reboot*, *shutdown*, *upgrade* remoto, editar ou remover a configuração, configurar um ou múltiplos elementos/componentes.

4.1.73 Fornecer com os seguintes modelos para o desenvolvimento de conectores customizados: arquivo, banco de dados por ID, múltiplos bancos de dados, expressão regular para arquivo, expressão regular para pasta de arquivos, SNMP, banco de dados por tempo e arquivo xml.

4.1.74 Deverá permitir o gerenciamento dos eventos arquivados.

4.1.75 Deverá permitir o gerenciamento de *peers* de centralizadores de logs.

4.1.76 Deverá permitir que a configuração dos elementos/componentes seja criada diretamente na solução de gerenciamento, importada de um elemento ativo e enviada a múltiplos elementos gerenciados.

4.1.77 Deverá permitir a comparação de duas configurações e a checagem de configurações ativas com a configuração definida como base para aquele elemento/componente.

4.1.78 Deverá possuir o conceito de subscrição de configurações, em que elementos subscritos recebem em conjunto as configurações atualizadas ou novas diretamente da solução de gerenciamento.

4.1.79 Deverá permitir a configuração de usuários e grupos de usuários, seus dispositivos associados e os respectivos privilégios (administrador, relatórios, pesquisas, operação, gerenciamento).

4.1.80 Deverá implementar *dashboards* com funcionalidade de *drill down* para visualização do status dos dispositivos monitorados, incluindo informações de uso de CPU, fluxo de eventos, e estatísticas de utilização de disco, consumo do licenciamento.

4.1.81 Deverá implementar visão de topologia que apresenta graficamente a relação entre os dispositivos de origem dos eventos, os conectores e os destinos, com a visualização do status, tipo de dispositivo, número de dispositivos de cada tipo, dispositivos ativos e inativos, tráfego em EPS/volume de dados.

4.1.82 O correlacionador deve ser capaz de receber eventos dos agentes, coletores.

4.1.83 O correlacionador deve efetuar a análise dos eventos em *near real-time* (tempo próximo ao real).

4.1.84 Permitir ao administrador a criação de novas regras e a edição das existentes.

4.1.85 O correlacionador deve identificar anomalias baseadas em eventos e análise de dados históricos conforme período a ser definido.

4.1.86 O correlacionador 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.

4.1.87 O correlacionador deve permitir a correlação de eventos e alertas com dados existentes em listas (*watchlist*). Deve permitir também a criação de novas listas e a personalização das existentes.

4.1.88 O correlacionador deve permitir a execução das regras agendadas contra eventos passados para análise histórica de atividades suspeitas, que executam em frequência e horário específico.

4.1.89 O correlacionador deve ter a capacidade de fazer a correlação entre eventos oriundos de:

a) Diferentes ativos do mesmo tipo (por exemplo, Firewall A e Firewall B);
b) Ativos de diferentes tipos (por exemplo, Firewall A e IPS B e Proxy C);
c) Ativos e Banco de Dados (por exemplo, catraca e consultas (queries) a banco de dados);

4.1.90 O correlacionador deve ser capaz de inserir os alertas gerados no próprio fluxo de correlação ou no fluxo de eventos. Deve permitir a correlação de tais alertas/eventos, derivados de alertas, com novos eventos e/ou regras, no intuito de detectar padrões mais complexos de ameaças ou violações de conformidade.

4.1.91 O correlacionador deve priorizar os eventos e alertas com base, pelo menos, nos seguintes critérios:

a) Severidade do evento;
b) Criticidade do ativo;
c) Existência de vulnerabilidade no ativo;
d) Possuir funcionalidade de geração de incidentes em módulos de tratamento interno.
e) Possuir funcionalidade de definição de prioridade para os eventos, alertas e incidentes.

4.1.92 Como resultado da aplicação de regras, o correlacionador deve ser capaz de executar ações automáticas como: enviar e-mail, enviar mensagem para o usuário conectado ao console, executar comandos e abrir caso na ferramenta de incidentes interna.

4.1.93 O correlacionador deve armazenar os eventos, alertas e incidentes na base de dados da solução.

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

4.1.95 Incluir regras pré-programadas (*out-of-the-box*) tanto para normalização de logs quanto para correlação de eventos, bem como permitir que se escrevam / definam regras próprias / personalizadas.

4.1.96 Fornecer a funcionalidade de geração de alertas (sonoros e/ou visuais) para incidentes de alta criticidade detectados na correlação de eventos.

4.1.97 Notificar e associar comportamentos anômalos baseados em múltiplos eventos que ocorrerem em um determinado período de tempo.

4.1.98 A correlação de eventos deve possuir uma linha de base (*baseline*) comportamental da rede, definido por suas regras de correlações, fornecendo alertas sempre que ocorrer algum evento fora do comportamento normal.

4.1.99 Possuir a capacidade de prover contextualização de dados de alertas de fontes diversas (ativos de rede e/ou segurança, servidores, aplicações, etc.) em um único console, otimizando com isso a capacidade e prazos de análise no processo de resposta a incidentes de segurança.

4.1.100 Possibilitar o envio de notificações ou alertas baseados no fator de importância e criticidade do ativo/dispositivo definido pela contratada.

4.1.101 Permitir a instalação de certificado digital para prover o acesso seguro, e configurar o repositório de certificados confiáveis.

4.1.102 Manter seu próprio log de auditoria.

4.1.103 Ter a funcionalidade de visualização de eventos e alertas de segurança em tempo real;

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

4.1.105 Permitir a inserção manual de anotações em alertas.

4.1.106 Notificar os administradores, ou usuários cadastrados, caso algum dispositivo monitorado pare de enviar eventos.

4.1.107 Permitir a visualização de eventos e alertas de segurança em tempo próximo ao real, sem necessidade de refazer consultas no banco de dados e/ou *storage* para atualização das visualizações (atualização da visualização de eventos e alertas de segurança em contexto de memória).

4.1.108 Integrar-se com a ferramenta de incidentes externos, permitindo que o SIEM abra casos na ferramenta externa diretamente e automaticamente. Deve permitir o registro de ações tomadas e planejadas.

4.1.109 Incluir módulo de SOAR (Security Orchestration Automation and Response) integrado.

4.1.110 Permitir automação de resposta a incidentes através de software de SOAR incluso.

4.1.111 Possuir captura de EPS (Eventos por segundo) e Flow de rede ilimitados para pelo menos 400 servidores físicos ou virtuais, além de ativos de rede do TRE-PR.

5 - DA ENTREGA E RECEBIMENTO DO OBJETO

5.1 - Da entrega do objeto:

5.1.1 - As licenças deverão ser disponibilizadas no formato de "Certificado de prova de titularidade " em até **10 (dez) dias corridos**, contados a partir da assinatura do contrato pela contratada e/ou entregues de forma eletrônica através do e-mail da **Assessoria de Segurança Cibernética** **asc@tre-pr.jus.br** ou na sede do TRE-PR, Rua: João Parolin, 224, Bairro: Prado Velho, Cidade: Curitiba-PR, CEP: 80220-902.

5.1.2 - As licenças deverão constar no rol de licenças disponíveis na conta existente do Tribunal Regional Eleitoral do Paraná, a ser informada à contratada após a assinatura do contrato.

5.1.3 - Do local de realização dos serviços: serão realizados na sede do Tribunal Regional Eleitoral do Paraná, em Curitiba, na Rua João Parolin nº 224 – Prado Velho, **mediante prévio agendamento junto à Assessoria de Segurança Cibernética através do e-mail** **asc@tre-pr.jus.br** ou de forma remota caso autorizado pelo CONTRATANTE.

5.1.4 - Os serviços serão realizados em dias úteis: segunda a sexta-feira, no horário compreendido entre às 13h e 19 horas.

5.2 - DO RECEBIMENTO

5.2.1 - Do recebimento provisório: as licenças e serviços serão recebidos provisoriamente no prazo máximo de 2 (dois) dias úteis contados da data de entrega, pela Assessoria de Segurança Cibernética, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência.

5.2.2 - Do recebimento técnico: as licenças e serviços serão recebidos tecnicamente no prazo de até 2 dias úteis contados do recebimento provisório, por comissão técnica designada pela SECTI, para efeito de verificação de sua conformidade com as especificações constantes neste Termo de

Referência;

5.2.3 - As licenças e serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência devendo ser substituídos no prazo de 5 (cinco) dias úteis, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades;

5.2.4 - Do recebimento definitivo: as licenças e serviços serão recebidos definitivamente no prazo de 5 (cinco) dias úteis, contados do recebimento técnico, pelo setor demandante, após a verificação de sua conformidade com as especificações constantes neste Termo de Referência;

5.2.5 - Os bens contratados poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência devendo ser substituídos no prazo de 10 dias corridos, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

5.3 - Quadro resumo de prazos:

Item	Descrição	Prazo
5.3.1	Disponibilização de Licenças em Certificado de Prova de Titularidade	10 dias corridos contados a partir da assinatura do contrato.
5.3.2	Recebimento Provisório	2 dias úteis a partir da entrega
5.3.3	Recebimento Técnico	2 dias úteis após o recebimento provisório.
5.3.4	Recebimento Definitivo	5 dias úteis após o recebimento técnico.
5.3.5	Apresentar plano de instalação e configuração	5 dias úteis após o recebimento técnico.
5.3.6	Instalar e configurar sistemas	15 dias úteis após a entrega do plano de instalação e configuração.
5.3.7	Operação Assistida	5 dias úteis após a instalação e configuração.
5.3.8	Prazo Máximo para completude das atividades a partir da disponibilização das licenças.	44 dias úteis contados da disponibilidade das licenças.

6 - INSTALAÇÃO E CONFIGURAÇÃO

6.1 - Durante a etapa de instalação e configuração da solução, a CONTRATADA deverá:

6.1.1 - Apresentar plano de instalação e configuração, 5 (cinco) dias úteis após o recebimento técnico das licenças, contemplando todos os tipos de ativos em produção na rede da contratante.

6.1.2 - Instalar e configurar os sistemas operacionais, banco de dados e softwares da ferramenta necessários para o correto funcionamento da solução, de forma remota ou presencial na sede da contratante.

6.1.3 - Configurar, no mínimo, 10 fontes de dados, incluindo seus coletores, a serem escolhidos pela contratada.

6.1.4 - Atualizar os sistemas e demais softwares para a última versão disponível compatível com a solução ofertada.

6.1.5 - Criar 1 (um) relatório (com registro dos eventos mais significativos do período);

6.1.6 - Criar 1 (um) relatório de política de armazenamento;

6.1.7 - Configurar para que os eventos de segurança sejam armazenados por 180 dias on-line e 12 meses off-line (raw data);

6.1.8 - Repassar os conhecimentos básicos para incluir novas fontes de dados, configurar coletores, criar relatórios e modelos, criar filtros de pesquisa, fazer backups, criar dashboards, gerenciar usuários e utilizar os principais recursos da solução para:

a) Homologação e testes;
b) Entrega em produção;
c) Operação assistida (5 dias úteis);

6.1.9 - O processo de entrega das licenças e instalação completa e operação assistida deverá ocorrer em no máximo 50 (cinquenta) dias úteis contados da assinatura do contrato.

6.2 **- Item 4 -** Serviço de implementação, migração e customização para o Item 1(TradeUP)

corresponde a:

6.2.1 - Instalação e configuração da Evolução tecnológica da base QRADAR SIEM para o Cloud Pak for Security.

a) Preparação do ambiente para implementação da solução QRadar;
b) Etapa de Configuração do servidor deverá incluir:
c) Validação dos Pré-requisitos;
d) Instalação e Configuração do IBM Cloud Pak foundational services;
e) Instalação serviços básicos do ambiente;
f) Configuração das permissões Namespaces;
g) Configuração das Instâncias de Registro;
h) Configuração das Instâncias COperandRequest;
i) Configuração das Instâncias e Formulários YAML;
j) Validação das Instalações e Configurações;
k) Configuração dos acessos IAM da console;

6.2.2 - Upgrade QRADAR Base, incluindo:

a) Backup das regras e configurações, ativos fontes de logs e workflow.
b) Levantamento das Fontes de Logs e Regras:
c) Validação das conexões/sessões.
d) Mapeamento de todos endereços e IPs e dispositivos
e) Desmontagem das áreas de armazenamentos externos
f) Executar exportação dos Dados Customizados
g) Migrar os coletores de eventos do GlusterFS para o Distributed Replicated Block Device.
h) Realizar upgrade Incident Forensics, Network Insights, Packet Capture.
i) Start dos serviços e conexões
j) Validação dos acessos e capturas.

6.2.3 - Configuração da Plataforma XDR, incluindo os itens abaixo:

a) Levantamento das Fontes de Logs e Regras:
b) Configuração do GitOps;
c) Configuração do Lifecycle for CP4S;
d) Configuração dos serviços NDR, SOAR, XDR Connect;
e) Configuração dos Datasources;
f) Configuração do LDAP para CP4S users

g) Configuração do domain name para CP4S
h) Configuração do TLS certificates para CP4S
i) Configuração do SCALECNSA/StorageClass
j) Configuração para integração do CP4S com o IBMQRadar Base, Proxy LogSourceIn, SOAR
k) Definição das Regras e Referências.
l) Configuração de até 10 tipos de eventos (antivírus, endpoint, VPN);
m) Criação de 1 relatório (com registro dos eventos mais significativos do período);
n) Criação de 1 política de armazenamento:
o) Homologação e testes;

6.3 - **Item 8 -** Serviço de implementação e customização para o item 5, 6 e 7 (Ampliação):

6.3.1 - Expansão Base modelo Cloud Pak for Security (EPS/Flows/SOAR) deverá incluir:
a) Expansão para a quantidade de servidores contratada.
b) Configuração de até 10 tipos de fonte de logs;
c) Criação de regras correlacionamento para eventos exclusivos de TI (para os itens da expansão):
d) Configuração de até 10 tipos de eventos (antivírus, endpoint, VPN, etc);
e) Homologação e testes.

6.4 - DOS REQUISITOS DE INSTALAÇÃO

6.4.1 - A CONTRATANTE disponibilizará infraestrutura física para instalação e configuração da solução, devendo a instalação e configuração ser iniciada após a aprovação do desenho da arquitetura elaborado pela CONTRATADA.

6.4.2 - O início dos serviços profissionais de implementação da solução somente deverão ser realizados após comunicação direta e agendamento com a equipe técnica da CONTRATANTE, devendo iniciar em até 15 (quinze) dias corridos após a assinatura do contrato pela Contratada.

6.4.3 - A CONTRATADA designará um profissional responsável pelo gerenciamento do projeto de implementação da solução em conjunto com a CONTRATANTE, compreendendo as etapas de elaboração do desenho da arquitetura, instalação dos componentes e configuração do ambiente para início da operação.

6.4.4 - Deverá ser elaborado, pela Contratada, um cronograma do projeto em até 10 (dez) dias

corridos após a assinatura do contrato, em conjunto com a CONTRATANTE, com o escopo macro de todos os itens apresentados neste termo.

6.4.5 - Os serviços profissionais deverão ser executados por técnicos do fabricante da solução ou da contratada com experiência em atividades nas soluções descritas no documento, sendo da contratada a total responsabilidade pelo controle de frequência, disciplina e pelo cumprimento de todas as obrigações atinentes à prestação de serviço, contemplando o fornecimento de todo processo de planejamento e design, arquitetura e implementação da solução proposta, fornecendo a documentação do ambiente.

6.4.6 - Os profissionais técnicos do fabricante da solução ou CONTRATADA alocados para a execução do serviço, deverão atestar sua capacidade técnica por meio de certificado oficial do fabricante, na solução QRADAR. A documentação comprobatória da certificação dos profissionais envolvidos na prestação de serviços atividades descritas no quadro 3.1 deverão ser entregues aos gestores/fiscais do contrato em até 10 (dez) dias antes do início do projeto.

6.4.7 - Todos os componentes de licenças de softwares adicionais necessários ao pleno funcionamento da solução, de acordo com as especificações técnicas deste termo de referência, bem como, tudo que for necessário à instalação física e lógica dos softwares, migração e configuração dos ambientes, devem ser fornecidos pela CONTRATADA, sem custos adicionais ao CONTRATANTE.

6.4.8 - A CONTRATADA, em tempo de projeto, deverá auxiliar no levantamento de todos os requisitos do projeto no que tange a infraestrutura, unidades lógicas de armazenamento, configurações necessárias e quaisquer outros requisitos relacionados ao projeto em questão.

6.4.9 - Ao final da implementação, o ambiente deverá estar totalmente funcional na solução de segurança, balanceamento de carga e monitoramento de rede e segurança mediante aceite definitivo da CONTRATANTE.

7 - DAS OBRIGAÇÕES DA CONTRATADA

7.1 – Dos requisitos de garantia

7.1.1 - A garantia deverá ser na modalidade remota e ou presencial pelo **prazo mínimo de 36 (trinta e seis) meses**, bem como o mesmo prazo para os serviços de suporte, contados a partir do recebimento definitivo do produto, sem prejuízo de qualquer política de garantia adicional oferecida pelo fabricante.

7.1.2 - O serviço de suporte deverá ser prestado integralmente pelo fabricante do software.

7.1.3 - Todas e quaisquer atualizações disponibilizadas para os produtos contidos na Solução aqui pretendida estarão inclusas no serviço de garantia;

7.1.4 - A Contratada deverá manter, **durante os 36 (trinta e seis) meses de vigência da garantia**, e às suas expensas, central de atendimento para abertura de chamados técnicos em regime de 24 (vinte e quatro) horas, todos os dias da semana, nos 365 (trezentos e sessenta e cinco) dias do ano. A central deverá ser acionada por e-mail, canal para abertura de chamados técnicos por meio de serviço web da contratada ou por telefone 0800 no idioma Português;

7.1.5 - Na abertura do chamado técnico, deverá ser fornecido um número de registro único para cada chamado;

7.1.6 - A contratada deverá, durante a vigência do contrato, prestar todas as informações solicitadas pelos gestores, esclarecendo dúvidas, inclusive, dando todo o suporte necessário no que tange a levantamentos e estudos referentes ao objeto da contratação, **no prazo máximo de 05 (cinco) dias úteis.**

7.1.7 - A contratada deverá atender aos chamados para suporte em, no máximo, 8h em dias úteis ou não, sendo que a solução definitiva ou de contorno deverá ocorrer em, no máximo, 72h.

7.1.8 - Caso seja dada uma solução de contorno, a contratada deve garantir que a solução adotada atende às condições mínimas de funcionamento, e deverá, no prazo de 60 (sessenta) dias, aplicar solução definitiva.

7.2 – Dos Chamados Técnicos

7.2.1 - A CONTRATADA deverá disponibilizar sistema de solicitações via WEB que possibilite, no mínimo:

a) Abertura, acompanhamento, listagem e fechamento das solicitações a qualquer momento, 24 horas por dia, 7 dias por semana.
b) Armazenar e gerar os relatórios das atividades executadas associadas a solicitação de consultoria;
c) O Sistema WEB será o método preferencial para abertura de chamados, porém, não eximindo a sua obrigatoriedade, para os casos de indisponibilidade deste, a CONTRATADA também

deverá disponibilizar método alternativo para abertura de chamados, por meio de e-mail ou telefone.

d) Após a finalização de qualquer atendimento da consultoria, o profissional da contratada deverá elaborar relatório do atendimento, claro o suficiente para que os próprios técnicos do TRE-PR possam segui-lo em caso de necessidade;

7.3 – Da Sustentabilidade

7.3.1 - Trata-se de ferramenta já em utilização - aquisição de software, com preservação das configurações já realizadas. Assim, por se tratar de solução puramente baseada em software, não há critérios de sustentabilidade a serem adotados.

7.4 – Das demais obrigações

7.4.1 - Os produtos deverão obedecer às condições do Termo de Referência, aplicando-se as normas do Código de Defesa do Consumidor;

7.4.2 - Deverá ser fornecida documentação completa e atualizada (manuais, termos de garantia, etc.), no idioma Português;

7.4.3 - A contratada obrigar-se-á em manter-se em compatibilidade com a habilitação e com as obrigações assumidas na licitação até o adimplemento total da contratação.

7.4.4 - A CONTRATADA deve repassar ao CONTRATANTE todas as vantagens promocionais oferecidas pelo fabricante dos softwares, que impactam no objeto do contrato a ser firmado, bem como fornece acesso a documentação comprobatória dessas vantagens.

7.4.5 - Executar, fielmente, o objeto contratado, de acordo com as normas legais, em conformidade com a proposta apresentada e as orientações da CONTRATANTE, observando sempre os critérios de qualidade e boas práticas recomendadas pelo fabricante para implantação e configuração dos produtos objeto deste Termo de Referência e seus anexos.

7.4.6 - A CONTRATADA e seus colaboradores e/ou representantes deverão zelar pelo sigilo de quaisquer informações referentes a infraestrutura de hardware e software, sistemas, dados hospedados em algum dispositivo de armazenamento, usuários, topologia, configurações, políticas de segurança e ao modo de funcionamento e tratamento das informações da CONTRATANTE,

durante a vigência do contrato, bem como após o seu término, conforme Termo de Sigilo e Responsabilidade (Anexo III).

7.4.7 - A CONTRATADA deverá entregar todas as documentações produzidas nas Fases de implantação da solução em formato editável (.doc, .docx ou .odt).

7.4.8 - A CONTRATADA deverá elaborar os relatórios, apresentações e atas de reunião.

7.4.9 - É responsabilidade da CONTRATADA dimensionar adequadamente o quantitativo de recursos necessários para a perfeita execução dos serviços, devendo contar com profissionais que tenham plenas condições de cumprir as atividades, de maneira não cumulativa.

7.4.10 - A CONTRATADA quando expressamente solicitado pela CONTRATANTE deverá promover a substituição de técnicos cuja operação esteja em desacordo com a melhor técnica vigente, devendo a empresa alocar substituto com grau equivalente ou superior de qualificação técnica.

7.4.11 - A CONTRATADA deverá alocar profissionais para a execução das atividades de acordo com o projeto.

7.4.12 - Os profissionais deverão ter capacidade técnica atestada através de certificados oficiais do fabricante, nas soluções do objeto deste termo de referência, conforme cada fase do projeto.

7.4.13 - Todos os documentos comprobatórios das certificações exigidas dos profissionais deverão ser entregues aos gestores/fiscais do contrato em até 10 (dez) dias corridos da assinatura do contrato pela CONTRATADA.

7.4.14 - Aplicar as melhores práticas do fabricante das soluções descritas neste documento no que tange os procedimentos de instalação, configuração e operação das soluções.

8 - DA PROTEÇÃO DE DADOS

8.1 - As partes devem cumprir fielmente o disposto na Lei Geral de Proteção de Dados Pessoais (LGPD) – Lei 13.709/2018.

8.2 - A não observância das normas relativas à privacidade de dados pessoais, no contexto da Lei

Geral de Proteção de Dados Pessoais (LGPD) – Lei nº 13.709/2018 e dos demais normativos mencionados neste contrato, caracteriza falta grave e enseja MULTA DE 10% do valor total do contrato.

8.3 - É vedado o compartilhamento dos dados pessoais coletados ou repassados em razão da execução deste contrato com terceiros, bem como sua utilização para finalidade distinta daquela do objeto da contratação, sob pena de responsabilização administrativa, civil e criminal.

9 - DA GESTÃO E FISCALIZAÇÃO DA CONTRATAÇÃO

9.1 - A gestão e fiscalização da contratação serão realizadas por servidores formalmente designados para tal fim**.**

9.1.1 – Da gestão da contratação**:** Nos termos da Lei 8666/93, art. 67, parágrafos 1.º e 2.º, caberá aos Gestores:

a) Receber e atestar a nota fiscal referente à aquisição encaminhando a fatura pertinente ao setor responsável da Secretaria de Orçamento, Finanças e Contabilidade do TRE para pagamento;
b) Acompanhar o fornecimento de acordo com as condições contratadas, determinando o que for necessário para regularização das faltas ou defeitos observados, sob pena de responsabilização administrativa;
c) Comunicar à contratada via e-mail, carta ou ofício, defeitos, irregularidades ou problemas encontrados durante a execução do objeto, fixando prazos para solucioná-los e corrigi-los;
d) Se a inexecução persistir, o gestor deverá criar um PAD específico de abertura de processo administrativo e encaminhá-lo à Secretaria de Gestão Administrativa, devidamente instruído com todas as informações pertinentes constante em formulário específico, anexando-se cópia do e-mail do subitem acima, referente à intenção de abertura de Processo Administrativo.

9.2 - Caberá aos fiscais do contrato:

a) Acompanhar a execução do contrato encaminhando por escrito, ao gestor, todas as ocorrências relacionadas com a sua execução, inclusive pequenas falhas ou insatisfações.
b) No que tange a garantia técnica, comunicar à contratada via e-mail, carta ou ofício, a ocorrência de descumprimento contratual e a intenção de abertura de Processo Administrativo;
c) Criar um PAD específico de abertura de processo administrativo e encaminhá-lo ao Gestor da

Contratação, devidamente instruído com todas as informações pertinentes constante em formulário específico, anexando-se cópia do e-mail do subitem acima, referente à intenção de abertura de Processo Administrativo.

d) Nos termos do art. 67 da Lei nº 8.666/93, será designado representante para acompanhar e fiscalizar a entrega dos bens, anotando em registro próprio todas as ocorrências relacionadas com a execução e determinando o que for necessário à regularização de falhas ou defeitos observados.

10 - DAS DISPOSIÇÕES GERAIS

10.1 - Dúvidas poderão ser sanadas com a **Assessoria de Segurança Cibernética**, por meio do telefone (41) 3330-8767 ou pelo e-mail **asc@tre-pr.jus.br.**