TRIBUNAL REGIONAL ELEITORAL DE MATO GROSSO DO SUL
R. Desembargador Leão Neto do Carmo, 23 - Bairro Parque dos Poderes - CEP 79037-100 - Campo Grande - MS

# ESTUDO PRELIMINAR

1 ESTUDOS PRELIMINARES

1.1 SOLUÇÃO DE TI A CONTRATAR

O presente estudo preliminar visa a contratação de uma solução de software para gerenciamento de eventos e logs de segurança da informação (SIEM - Security Information and Event Management) com suporte e garantia de 36 meses.

1.2 EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

A equipe responsável pelo planejamento da contratação é composta pelos seguintes membros:

| Nome | Lotação | Tipo | Email |
|---|---|---|---|
| Gustavo Pinho | SSOP/COINF/STI | Técnico | gustavo.pinho@tre-ms.jus.br |
| Érika Murackami Duarte da Rosa | SAF/CRM/SLC | Administrativo | erika.rosa@tre-ms.jus.br |

1.3 NECESSIDADE DA CONTRATAÇÃO

O ambiente computacional do TRE-MS gera diversas informações de registro de atividades (logs). Atualmente essas informações não são tratadas de forma centralizada e o armazenametno também não são por longos períodos, o que inviabiliza a transformação dessa massa de dados em inteligência operacional. Realizar essa transformação é absolutamente necessário para monitorar, pesquisar, analisar, visualizar e agir sobre os grandes fluxos de dados gerados por sites, aplicativos, servidores, redes, dispositivos móveis e outros que alimentam o negócio do Órgão.

Dessa forma, buscamos implementar uma solução de software capaz de transformar esses dados de registro de atividades em inteligência operacional em tempo real para que o TRE-MS possa preventivamente verificar possíveis grandes fluxos de dados oriundos de equipamentos com a função de derrubar a infraestrutura do Tribunal ou mesmo visando a invasão/coleta de informações do Tribunal.

2 ANÁLISE DA VIABILIDADE DA CONTRATAÇÃO (ART.14)

2.1 DEFINIÇÃO E ESPECIFICAÇÃO DOS REQUISITOS DA DEMANDA (ART. 14, I)

| ITEM | BEM OU SERVIÇO | QTDE |
|---|---|---|
| **01** | Software de gerenciamento de logs e eventos de segurança (SIEM), com licença SUBSCRIÇÃO, suporte e atualização para o primeiro ano de uso | **01** |
| **02** | Pacote adicional para software de gerenciamento de logs e eventos de segurança (SIEM), com licença SUBSCRIÇÃO, suporte e atualização para o primeiro ano de uso | **06** |
| **03** | Suporte anual para software de gerenciamento de logs e eventos de segurança (SIEM), para módulo principal, descrito no **item 01**, não incluindo o primeiro ano de uso. | **02** |
| **04** | Suporte anual para software de gerenciamento de logs e eventos de segurança (SIEM), para pacote adicional, descrito no **item 02**, não incluindo o primeiro ano de uso | **15** |
| **05** | Instalação e configuração da solução de SIEM, realizada de forma presencial. | **01** |
| **06** | Treinamento técnico para solução de SIEM, com no mínimo 16h, para até 8 pessoas. | **01** |

**Considerações gerais sobre a solução:**

**Item 01 - Software de gerenciamento de logs e eventos de segurança (SIEM), com licença SUBSCRIÇÃO, suporte e atualização para o primeiro ano de uso.**

**1.** Solução completa de SIEM (*Security Information and Event Management*), que deve implementar todos os requisitos previstos neste estudo preliminar.

**2.** A proposta deverá contemplar todas as licenças de software, sistemas operacionais, bancos de dados, subscrições ou qualquer outro tipo de licenciamento necessário para seu completo funcionamento, de acordo com as características e prazos estipulados. A infraestrutura de virtualização será fornecida pela contratante.

**3.** A solução ofertada poderá ser composta por um ou mais softwares, desde que sejam do mesmo fabricante, totalmente interoperáveis entre si, gerenciados através de uma interface única e em número de licenças suficientes para atender aos volumes de dados e/ou quantidades de eventos solicitados.

**4.** Devido aos modelos de licenciamento dos mais importantes fabricantes serem diferentes, a solução poderá ser ofertada por ao menos uma das formas de licenciamento citadas a seguir, ou combinação delas, devidamente descrito na proposta comercial, desde que atenda os volumes de dados e eventos esperados:

**4.1.** Por volume de dados recebidos e tratados, partindo de **30 GBytes/dia** e sem limite de ativos geradores de eventos.

**4.2.** Por quantidade de eventos recebidos e tratados por segundo em tempo real, partindo de **1100 EPS** (Eventos por Segundo) medidos pela quantidade instantânea (rajada) e **15000 FPM** (Flows por minuto).

**4.3.** Por quantidade de eventos recebidos e tratados por segundo, partindo de **600 EPS** (Eventos por segundo) medidos pela média diária.

**5.** As licenças de software deverão ser registradas junto ao fabricante da solução em nome da contratante.

**6.** O primeiro ano de suporte deverá estar incluso no valor deste item.

**7.** O tipo de licenciamento é **licença de usu (subscrição)** para instalação *on-premises*, com possibilidade de atualização enquanto durar o contrato de suporte.

**8.** Deverá ser ofertada a última versão estável de todos os softwares.

**9.** Poderão ser considerados servidores para armazenamento de logs e tratamento de eventos em separado.

**Item 02 - Pacote adicional para software de gerenciamento de logs e eventos de segurança (SIEM), com licença perpétua, suporte e atualização para o primeiro ano de uso.**

**1.** Pacotes de licenciamento de software para ampliação da capacidade da solução de software ofertada no **item 01**.

**2.** Cada pacote adicional previsto no **item 02** devem contemplar, no mínimo, de acordo com o tipo de licenciamento proposto para o **item 01**:

**2.1.** Por volume de dados recebidos e tratados: **10 GBytes/dia** de logs.

**2.2.** Por quantidade de eventos recebidos e tratados por segundo: **400 EPS** (Eventos por segundo) medidos pelo **máximo instantâneo** (rajada) ou **5000 FPM** (*Flows* por minuto).

**2.3.** Por quantidade de eventos recebidos e tratados por segundo: **250 EPS** (Eventos por segundo) medidos pela média diária.

**3.** O primeiro ano de suporte deverá estar incluso no valor deste item;

**4.** O tipo de licenciamento é **licença de uso (subscrição)** para instalação *on-premises*, com possibilidade de atualização enquanto durar o contrato de suporte.

**5.** Deverá ser ofertado a última versão estável de todos os softwares;

**Item 03 - Suporte anual para software de gerenciamento de logs e eventos de segurança (SIEM), para módulo principal (descrito no item 01), não incluindo o primeiro ano de uso.**

**1.** Subscrição de suporte, oferecida pelo fabricante, suficientes para suportar todos os softwares que compuserem a solução ofertada;

**2.** Deverá contemplar todos os softwares oferecidos no **item 01**, em módulos anuais;

**3.** Poderão ser adquiridos pacotes para até **2 anos** de suporte, subsequentes e ininterruptos, não incluído o primeiro ano de uso;

**4.** Os serviços de suporte, com exceção das atividades realizadas até a homologação do produto, poderão ser feitos por telefone, e-mail, Webex ou outro meio tecnológico acordado entre as partes, sempre no idioma português.

**5.** Deverá permitir a atualização do produto, seja para novas versões, seja para instalação de patches de atualizações e segurança;

**6.** 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.

**Item 04 - Suporte anual para software de gerenciamento de logs e eventos de segurança (SIEM), para pacote adicional (descrito no item 02), não incluindo o primeiro ano de uso:**

**1.** Subscrição de suporte, oferecida pelo fabricante, suficientes para suportar todos os softwares que compuserem a solução ofertada;

**2.** Deverá contemplar todos os pacotes adicionais de softwares oferecidos no **item 02**, em módulos anuais;

**3.** Poderão ser adquiridos pacotes para até **2 anos** de suporte, subsequentes e ininterruptos, não incluído o primeiro ano;

**4.** Cada pacote de suporte será relativo a 01 pacote adicional de software (por exemplo, se forem adquiridos 03 pacotes adicionais de software no item 02, para um período de suporte de 02 anos serão considerados 06 pacotes de suporte);

**5.** Os serviços de suporte, com exceção das atividades realizadas até a homologação do produto, poderão ser feitos por telefone, e-mail, Webex ou outro meio tecnológico acordado entre as partes, sempre no idioma português.

**6.** Deverá permitir a atualização do produto, seja para novas versões, seja para instalação de patches de atualizações e segurança;

**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.

**Item 05 - Instalação e configuração da solução de SIEM, realizada de forma presencial:**

**1.** Instalar e configurar os sistemas operacionais, bancos de dados e softwares da solução, de forma presencial, na sede da contratante.

**2.** Configurar, no mínimo 30 fontes de dados, incluindo seus coletores, a serem escolhidos pela contratada, dentro de sua base de ativos.

**3.** 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,

**4.** Apresentar plano de instalação e configuração, que deverá contemplar todos os tipos de ativos em produção na rede da contratante.

**Item 06 - Treinamento técnico para solução de SIEM, com no mínimo 16h:**

**1.** Deverá ser ministrado por técnico certificado pelo fabricante da solução;

**2.** Deverá ter, no mínimo, 16h ou o equivalente ao curso oficial de administração da solução, prevalecendo o que tiver maior número de horas, para turma de até 10 profissionais do TRE-MS.

**3.** Deverá contemplar a administração completa da ferramenta.

**4.** Poderá ser realizado *in company* (na sede da contratante) ou em centro de treinamento homologado pelo fabricante, em qualquer unidade da federação.

**5.** A contratada poderá optar pela entrega de voucher para a participação em curso oficial. Neste caso, os vouchers terão a validade mínima de 365 dias corridos.

2. ESPECIFICAÇÃO TÉCNICA DA SOLUÇÃO:

**2.1.** Todos os componentes da solução devem permitir sua instalação em ambiente virtual, servidores físicos de propósito genérico ou em *appliance* virtual especializado.

**2.2.** Deverá permitir o controle de acesso dos usuários à solução por meio de autenticação em serviço de diretório como Microsoft *Active Directory* ou LDAP.

**2.3.** A solução deverá 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.

**2.4.** 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.

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

**2.6.** A solução deverá implementar compressão dos eventos em cada fase do ciclo de vida do evento: transmissão, armazenamento online e *offline* dos eventos.

**2.7.** 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*).

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

**2.9.** Será considerada nesse Edital 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.

**2.10.** 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.

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

**2.12.** Ser capaz de coletar, no mínimo, os logs dos sistemas e ativos listado abaixo:

**2.12.1.** Firewalls: Checkpoint R80.x, VMWare NSX, PfSense;

**2.12.2.** Switches: HPE e Aruba;

**2.12.3.** Plataformas de Virtualização: VMware ESX, HyperV, Acropolis/KVM e Oracle VM;

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

**2.12.5.** Antivirus: TrendMicro, Clamav;

**2.12.6.** Servidores de E-mail: Zimbra e Microsoft Exchange;

**2.12.7.** Servidores de Aplicação e Web: Apache2, Squid, Nginx, HAProxy, Apache Tomcat, Jboss e MicroSoft IIS7 (ou superior);

**2.12.8.** VPN: OpenVPN;

**2.13.** Para coleta de logs deve suportar, no mínimo, os seguintes métodos:

**2.13.1.** Syslog (UDP, TCP e TLS);

**2.13.2.** CIFS;

**2.13.3.** FTP;

**2.13.4.** MySQL;

**2.13.5.** MS SQL;

**2.13.6.** Oracle;

**2.13.7.** API;

**2.13.8.** JSON;

**2.13.9.** CEF;

**2.14.** Suportar a coleta de dados de no mínimo 250 (duzentos e cinquenta) tipo de ativos geradores de eventos distintos, com documentação completa individual por tecnologia.

**2.15.** A solução deve permitir coletar dados de *feeds* externos.

**2.16.** Suportar o modo de criptografia em todos os conectores.

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

**2.18.** A solução deve ser capaz de 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.

**2.19.** A solução deve ser capaz de normalizar e categorizar os eventos em um padrão único.

**2.20.** O coletor da solução deverá ser capaz de armazenar os dados localmente (*cache*) em caso de indisponibilidade da comunicação com os destinos dos eventos.

**2.20.1.** O envio dos dados em cache deve ocorrer imediatamente após a disponibilização do destino do evento.

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

**2.22.** Deverá ter a capacidade de guardar eventos normalizados/tratados e brutos em forma comprimida.

**2.23.** A solução deve ser capaz de inserir nos eventos normalizados metadados sobre georreferência dos mesmos.

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

**2.25.** A solução deve permitir múltiplos perfis de configuração.

**2.26.** A solução deverá enviar os eventos coletados para o correlacionador e permitir enviar para mais de um destino ao mesmo tempo.

**2.27.** Deverá implementar a coleta, processamento e correlação de informações de fluxo de rede *Netflow v9/ SFlow*.

**2.28.** A solução deverá 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.

**2.29.** Possuir a funcionalidade de atualização, gerenciamento e configuração centralizados de todos os conectores distribuídos da solução.

**2.30.** 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.

**2.31.** No caso de a solução ofertada utilizar arquitetura distribuída, de forma a evitar a perda de eventos por sobrecarga ou indisponibilidade de correlacionadores, deverá fornecer função, interna ou externa, de balanceamento de cargas de serviço:

**2.31.1.** O balanceamento de carga deverá implementar os métodos *Weighted Round Robin* ou *Round Robin*;

**2.31.2.** Prover um IP virtual ou definir nos agentes todos os servidores que fazem função de correlacionador como destino das fontes geradoras de eventos.

**2.31.3.** Ao receber um evento, a solução deverá buscar um conector com capacidade de processamento disponível, de forma a garantir que não haverá perda de eventos por sobrecarga de conectores.

**2.32.** Deverá 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.

**2.33.** Ser capaz de armazenar logs por tempo determinado e personalizado, conforme necessidade do órgão.

**2.34.** Ter a capacidade de 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.

**2.35.** 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.

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

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

**2.37.** Deverá 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.

**2.38.** Deverá permitir exportar eventos para formato pdf e csv.

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

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

**2.40.** Deverá implementar assistente gráfico para criação de queries.

**2.41.** Deverá implementar indexação baseada em campo e palavra-chave para acelerar buscas.

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

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

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

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

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

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

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

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

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

**2.51.** 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.

**2.52.** Possuir conformidade com as normas ISO 27001 e LGPD.

**2.53.** Deve utilizar algoritmos para verificação de integridade e autenticidade dos eventos armazenados para fins de auditoria devidamente reconhecidos como seguros.

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

**2.55.** 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.

**2.56.** Deverá permitir acrescentar campos de uma fonte em outra fonte.

**2.57.** Deverá ser fornecido com solução de gerenciamento central com as seguintes características mínimas:

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

**2.57.2.** Deverá permitir a implementação de atualização e distribuição de novas políticas de segurança pelos elementos/componentes gerenciados;

**2.57.3.** Deverá possuir regras de monitoração pré-configuradas, as quais podem ser editadas ou apagadas;

**2.57.4.** Deverá interagir diretamente com a biblioteca de casos de uso do fabricante da solução para download e atualizações de conteúdo;

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

**2.57.6.** Deverá possuir tela de monitoração com as seguintes características:

**2.57.6.1.** 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;

**2.57.6.2.** Listagem de todos os elementos/componentes que estão reportando problemas;

**2.57.6.3.** Permitir a visualização do sumário de monitoração por tipo de produto;

**2.58.** 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.

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

**2.60.** Deverá ser possível visualizar o consumo de licenças da solução.

**2.61.** 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.

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

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

**2.64.** 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.

**2.65.** Deverá permitir a apresentação de árvore hierárquica de dispositivos.

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

**2.67.** Deverá 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.

**2.68.** Deverá implementar o gerenciamento de conectores: adição, edição de conectores, atualização de parâmetros, gerenciar os destinos e *failover* de logs de múltiplos conectores, gerenciamento de configurações em lote, envio de comandos, visualização interativa de diagnóstico, edição de conectores customizados, compartilhamento de conectores, download e upload de conectores.

**2.69.** Deverá ser fornecido 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.

**2.70.** Deverá permitir o gerenciamento dos eventos arquivados.

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

**2.72.** 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.

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

**2.74.** 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.

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

**2.76.** 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.

**2.77.** Deverá implementar visão de topologia que apresente 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.

**2.78.** O correlacionador deve ser capaz de receber eventos dos agentes, coletores e de outros correlacionadores.

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

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

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

**2.82.** 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.

**2.83.** 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.

**2.84.** 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.

**2.85.** O correlacionador deve ter a capacidade de fazer a correlação entre eventos oriundos de:

**2.85.1.** Agentes (ou solução similar) ou coletores de outros correlacionadores;

**2.85.2.** Diferentes ativos do mesmo tipo (por exemplo, Firewall A e Firewall B);

**2.85.3.** Ativos de diferentes tipos (por exemplo, Firewall A e IPS B e Proxy C);

**2.85.4.** Ativos e Banco de Dados (por exemplo, catraca e consultas (queries) a banco de dados);

**2.86.** 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.

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

**2.87.1.** Severidade do evento;

**2.87.2.** Criticidade do ativo;

**2.87.3.** Existência de vulnerabilidade no ativo;

**2.88.** Possuir a funcionalidade de geração de incidentes em módulos de tratamento interno.

**2.89.** Possuir a funcionalidade de definição de prioridade para os eventos, alertas e incidentes.

**2.90.** 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.

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

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

**2.93.** A solução deve 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.

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

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

**2.96.** 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.

**2.97.** A solução deve 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.

**2.98.** A solução deve possibilitar o envio de notificações ou alertas baseados no fator de importância e criticidade do ativo/dispositivo definidos pela contratada.

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

**2.100.** Manter seu próprio log de auditoria.

**2.101.** Ter a funcionalidade de visualização de eventos e alertas de segurança em tempo real;

**2.102.** 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.

**2.103.** Permitir a inserção manual de anotações em alertas.

**2.104.** A solução deve ser capaz de notificar os administradores, ou usuários cadastrados, caso algum dispositivo monitorado pare de enviar eventos.

**2.105.** Deve 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).

**2.106.** Deverá se integrar 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.

2.1.1 Soluções Disponíveis no Mercado de TIC (Art. 14, I, a)

As ferramentas disponíveis no mercado trabalham por:

- volume de dados recebidos e tratados, sem limite de ativos geradores de eventos e é medido pela total de Gbytes/dia

- quantidade de eventos recebidos e tratados por segundo em tempo real EPS (Eventos por Segundo) medidos pela quantidade instantânea (rajada) e FPM (Flows por minuto).

- quantidade de eventos recebidos e tratados por segundo **EPS** (Eventos por segundo) medidos pela média diária.

2.1.2 Contratações Públicas Similares (art. 14, I, b)

TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO SUL - ARP Nº 31/2019 - R$ 1.696.000,00

TELETEX (Orçamento) - R$ 2.712.878,79

ALLTECH (Orçamento) - R$ 1.761.477,10

2.2 IDENTIFICAÇÃO DAS DIFERENTES SOLUÇÕES DE TIC (ART. 14, II)

2.2.1 Disponibilidade de STIC similar em outro órgão (Art. 14, II, a)

Foi procurado na Internet algum software desenvolvido por outro órgão e que atendesse às especificações solicitadas, porém nenhum foi encontrado.

2.2.2 STIC existente no Portal de Software Público Brasileiro (Art. 14, II, b)

Foi procurado no portal https://softwarepublico.gov.br/ algum software relativo às Soluções informadas, porém nenhum foi encontrado.

2.2.3 A capacidade e as alternativas do mercado de TIC (Art. 14, II, c)

Não se aplica, uma vez que não existe nenhum órgão público, de qualquer esfera, que forneça os softwares objetos deste estudo.

2.2.4 Observância ao Modelo Nacional de Interoperabilidade (Art. 14, II, d)

Não se aplica, uma vez que se trata de item relacionado a desenvolvimento de software e a solução aqui pretendida trata-se de solução de software.

2.2.5 Aderência às regulamentações da ICP-Brasil (Art. 14, II, e)

Não se aplica, uma vez que se trata de item relacionado a desenvolvimento de software e a solução aqui pretendida trata-se de soluções de software.

2.2.6 Observância ao Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário (Moreq-Jus) (Art. 14, II, f)

Não se aplica, uma vez que se trata de item relacionado a desenvolvimento de software e a solução aqui pretendida trata-se de solução de segurança.

2.2.7 Orçamento estimado (Art. 14, II, g)

| ITEM | BEM OU SERVIÇO | QTDE | TRE-RS | TELETEX | COMPWIRE | MÉDI VAL |
|---|---|---|---|---|---|---|
| **01** | Software de gerenciamento de logs e eventos de segurança (SIEM), com licença perpétua, suporte e atualização para o primeiro ano de uso. | **01** | R$ 299.000,00 | R$ 566.200,01 | R$ 152.622,14 | R$ 339.2 |
| **02** | Pacote adicional para software de gerenciamento de logs e eventos de segurança (SIEM), com licença perpétua, suporte e atualização para o primeiro ano de uso. | **06** | R$ 375.000,00 | R$ 1.145.337,69 | R$ 317.244,30 | R$ 612.5 |
| **03** | Suporte anual para software de gerenciamento de logs e eventos de segurança (SIEM), para módulo principal, descrito no **item 01**, não incluindo o primeiro ano de uso. | **02** | R$ 130.000,00 | R$ 225.845,05 | R$ 305.244,28 | R$ 220.3 |
| **04** | Suporte anual para software de gerenciamento de logs e eventos de segurança (SIEM), para pacote adicional, descrito no **item 02**, não incluindo o primeiro ano de uso. | **15** | R$ 270.000,00 | R$ 457.658,87 | R$ 793.110,75 | R$ 506.9 |
| **05** | Instalação e configuração da solução de SIEM, realizada de forma presencial. | **01** | R$ 188.000,00 | R$ 200.000,00 | R$ 57.379,00 | R$ 148.4 |
| **06** | Treinamento técnico para solução de SIEM, com no mínimo 16h, para até 10 pessoas. | **01** | R$ 67.000,00 | R$ 117.837,17 | R$ 135.876,63 | R$ 106.9 |
| TOTAIS | | | R$ 1.329.000,00 | R$ 2.712.878,79 | R$ 1.761.477,10 | R$ 1.934. |

A ARP do TRE-RS (0950598) data de 22/11/2019. Não encontramos nenhuma contratação similar no Painel de Preços. Como em 2020 tivemos uma alta significativa do dólar, houve a necessidade de fazer uma cotação no mercado para atualização dos valores, conforme Proposta Comercial da TELETEX IT Solutions (1091385) e COMPWIRE Informática SA (1091388).

2.3 ANÁLISE E COMPARAÇÃO ENTRE OS CUSTOS TOTAIS DAS STICs (ART. 14, III)

As ferramentas de análise de log (SIEM) de referência, disponíveis no mercado, atendem as necessidades do TRE-MS. A média dos valores de orçamento e contratação do TRE-RS ficou em R$1.934.451,95 (hum milhão, novecentos e trinta e quatro mil, quatrocentos e cinquenta e um Reais e noventa e cinco centavos). Num primeiro momento, o TRE-MS irá utilizar apenas os itens 1, 3, 5 e 6. Os itens 2 e 4 serão utilizados sob demanda. Então, nesse primeiro momento, o valor para os itens 1, 3, 5 e 6 ficam em R$815.001,42 (oitocentos e quinze mil, um real e quarenta e dois centavos).

2.4 DA ESCOLHA E JUSTIFICATIVA DA STIC ESCOLHIDA (ART. 14, IV)

Todos os itens descritos fazem parte de uma mesma Solução, alguns são acessórios,  mas são interdependentes. No caso dos itens 2 e 4 que serão solicitados conforme demanda, devem ser do mesmo fornecedor dos itens 1 e 3, sob pena de se contratar soluções diferentes. Ou seja, os itens 1 e 2 são equivalentes e os itens 3 e 4 também são equivalentes. O item 3 está ligado diretamente ao item 1 e o item 4 diretamente ao item 2, mas o item 2 é dependente do item 1 (tem que ser a mesma ferramenta).

Foi realizado um levantamento buscando estimar o volume de eventos que serão monitorados, porém, estas estimativas podem ter uma considerável margem de variação.

Sendo assim, caso a aquisição do item 1 não seja suficientemente capaz de suportar todos os ativos, poderá ser necessário a utilização dos itens 02 e 04.

A complementação dos itens 02 e 04 será ativada com o uso da ferramenta já em produção, sendo esta uma alternativa para uma possível expansão da solução.

Como não fechamos o escopo por uma solução específica, qualquer das soluções contratadas atenderão à necessidade do TRE-MS. As ferramentas open source, não foram considerados no estudo por não atenderem as necessidades, bem como terem fragilidade de segurança e não permitir a escalabilidade.

2.4.1 DESCRIÇÃO DA SOLUÇÃO (ART. 14 IV, A)

A solução deve possuir a seguinte característica:

Fornecimento de software, instalação, suporte, documentação e treinamento na solução de software para gerenciamento de eventos e logs de segurança da informação (SIEM - Security Information and Event Management).

2.4.2 ALINHAMENTO DA SOLUÇÃO (ART. 14, IV, B)

A Solução escolhida atende às necessidades do Órgão quando contribui para atender às necessidades de TI, uma vez que melhora o KR 7.1: “Númro de vulnerabilidades críticas e altas", constante do PDTIC do TRE-MS 2021-2026.

2.4.3 BENEFÍCIOS ESPERADOS (ART. 14, IV, C)

- Atender requisito da resolução CNJ nº 396/2021 (Artigo 11, inciso IV - utilizar tecnologia que possibilite a análise consolidada dos registros de auditorias coletados em diversas fontes de ativos de informação e de ações de usuários, permitindo automatizar ações de segurança e oferecer inteligência à análise de eventos de segurança);
- Garantir a proteção dos dados pessoais dos usuários através de: proteção contra ataques cibernéticos, tais como malwares e ramsonwares em servidores; inspeção de logs e monitoramento de integridade de arquivos e de bibliotecas utilizadas no desenvolvimento de aplicações do TRE-MS, conforme LGPD;
- Adquirir e implantar ferramenta de Análise de Logs até março/2022, conforme previsto na Estratégia Nacional de Cibersegurança da Justiça Eleitoral aprovada em 2021;
- Garantir maior proteção aos dados hospedados no Datacenter do TRE-MS, sobretudo aos dados dos usuários.

2.4.4 RELAÇÃO ENTRE A DEMANDA PREVISTA E A SER CONTRATADA (ART. 14, IV, D)

A demanda prevista é a aquisição de uma Ferramenta de Análise de Logs para 36 meses. A demanda a ser contratada é igual à quantidade prevista, e tem o intuito de ser a solução definitiva ao problema apresentado neste estudo e implantá-la em tempo hábil.

2.5 ADEQUAÇÃO DO AMBIENTE (ART. 14, V, A, B, C, D, E, F)

Não será necessária nenhuma adequação do ambiente.

3 SUSTENTAÇÃO DO CONTRATO (ART. 15)

**Critério de sustentabilidade**:

Esta equipe de planejamento realizou estudos de viabilidade para inserção de critérios socioambientais para a presente licitação. Não foram verificadas possibilidades porque se trata de fornecimento de software, não gerando impacto nos recursos naturais.

3.1 RECURSOS MATERIAIS E HUMANOS (ART. 15, I)

Todos os Recursos Materiais necessários para a implantação deverão ser fornecidos pela empresa contratada, conforme os requisitos listados no item 2.4.1.

Em relação aos Recursos Humanos, serão necessários:

- 02 (dois) servidores do quadro para atuarem como fiscais do contrato.

3.2 DESCONTINUIDADE DO FORNECIMENTO (ART. 15, II)

A descontinuidade do fornecimento de atualização causará a desatualização da solução, perdendo o papel de proteção previsto. Será necessária a aquisição/implantação de outra solução de software com as mesmas funcionalidades ou superior.

3.3 TRANSIÇÃO CONTRATUAL (ART. 15, III, A, B, C, D, E)

Em caso de necessidade de transição contratual, será necessária a aquisição/implantação de novo software com funcionalidade igual ou superior.

3.4 ESTRATÉGIA DE INDEPENDÊNCIA TECNOLÓGICA (ART. 15, IV, A, B)

O TRE-MS possuirá independência tecnológica de operacionalização (haverá documentação de toda a solução e repasse de conhecimento).

4 ESTRATÉGIA PARA A CONTRATAÇÃO (ART. 16)

4.1 NATUREZA DO OBJETO (ART. 16, I)

Trata-se da aquisição de solução de software, o objeto pode ser fornecido por diversas revendas e possui características comuns e usuais no mercado de TIC, cujos padrões de desempenho e de qualidade estão objetivamente definidos.

4.2 PARCELAMENTO DO OBJETO (ART. 16, II)

Para esta aquisição não haverá parcelamento do objeto, pois o sucesso da implantação da Solução (uso integral de toda a potencialidade de aumento da segurança da Solução), depende de cada componente da Solução a ser adquirida, sejam eles componentes principais ou secundários. Portanto, faz-se necessário o agrupamento para garantir o uso por completo do que venha a ser adquirido, evitando assim, que componentes da Solução venham a ser adquiridos e não utilizados.

4.3 ADJUDICAÇÃO DO OBJETO (ART. 16, III)

O objeto será licitado em item único, com subitens, portanto, a adjudicação será realizada somente para uma empresa fornecedora.

Dado às características do objeto, a presente licitação poderia se dar por Registro de preços (inciso IV do art. 3º do decreto 7.892), devido à impossibilidade de mensurar previamente o quantitativo total .

Apesar disso, esta equipe entende ser economicamente mais vantajoso a contratação em sua totalidade, com previsão de que os itens 02 e 04 possam ser dispensados caso o item 01 seja suficiente para a demanda.

O entendimento de equipe de planjemanto se dá face às caracterísiticas do objeto (software), a probabilidade de utilização dos itens mencionados, e o momento econômico atual de instabilidade cambial, o que poderia causar um desinteresse dos eventuais participantes.

4.4 MODALIDADE E TIPO DE LICITAÇÃO (ART. 16, IV)

De início, esta Seção informa que a contratação se dará na modalidade de Pregão, nos termos da Lei 10.520/2002, uma vez que os materiais licitados podem ser enquadrados como bens comuns, nos termos do inciso II do art. 3º do Decreto nº 10.024/2019.

> *Art. 3º Para fins do disposto neste Decreto, considera-se:*
>
> ---
>
> *II - bens e serviços comuns - bens cujos padrões de desempenho e qualidade possam ser objetivamente definidos pelo edital, por meio de especificações reconhecidas e usuais do mercado;*

Considerando a disposição contida no §1º do art. 1º do Decreto nº 10.024/2019, a licitação se dará na modalidade eletrônica:

> *Art. 1º Este Decreto regulamenta a licitação, na modalidade de pregão, na forma eletrônica, para a aquisição de bens e a contratação de serviços comuns, incluídos os serviços comuns de engenharia, e dispõe sobre o uso da dispensa eletrônica, no âmbito da administração pública federal.*
>
> *§ 1º A utilização da modalidade de pregão, na forma eletrônica, pelos órgãos da administração pública federal direta, pelas autarquias, pelas fundações e pelos fundos especiais é obrigatória.*

No que tange à escolha do **tipo** de licitação, por se tratar de serviços comuns, não resta outra opção a não ser o do tipo MENOR PREÇO.

Em atendimento ao disposto no cap. V da Lei Complementar 123/2006 alterada pela Lei Complementar 147/2014, observado o art. 8º do Decreto 7.174/2010 deverá ser observado as preferências na contratação (art. 3º da Lei 8.248/1991), explicitado no art. 5º a 8º do retromencionado diploma legal.

4.5 CLASSIFICAÇÃO E INDICAÇÃO ORÇAMENTÁRIA (ART. 16,V)

As despesas decorrentes do objeto desta licitação, serão custeadas com recursos aprovados na Lei Orçamentária da União nº 14.144 de 23 de abril de 2021, que estima a receita e fixa a despesa da União para o exercício financeiro 2021 (LOA), Unidade 14112 – TRE-MS, Ação: 20GP– Julgamento de Causas e Gestão Administrativa, Programa de Trabalho: 02.122.0570.20GP.0054, Elementos de Despesa: 4490.40 - Aquisição de Softwares.

Este item poderá sofrer alteração pela COPEG, unidade responsável pela Informação quanto à reserva e enquadramento orçamentários para cobrir a despesa, e de sua compatibilização com a Lei Orçamentária Anual, Plano Plurianual e a Lei de Diretrizes Orçamentárias.

4.7 VIGÊNCIA DA PRESTAÇÃO DE SERVIÇO (ART. 16, VI)

O período de vigência desta contratação será de até 36 (trinta e seis) meses, período de prestação de suporte on-site, contados da assinatura do contrato.

4.7 EQUIPE DE APOIO À CONTRATAÇÃO (ART. 16, VII)

Sugestão da equipe de apoio e fiscais do contrato:

- Gustavo Pinho
- Ulysses Almeida

4.8 EQUIPE DE GESTÃO DA CONTRATAÇÃO (ART. 16, VIII)

As atribuições cabíveis à fiscalização administrativa podem ser desempenhadas pela fiscalização técnica, auxiliada, no que couber, pela Seção de Gestão de Contratos Administrativos.

## 5 ANÁLISE DE RISCOS

| RISCO 1 - Licitação deserta | | | |
|---|---|---|---|
| Probabilidade | ID | Dano | Impacto |
| Média | 1 | Não realizar a contração | Médio |
| ID | Ação de Mitigação e Contingência | | Responsável |
| 1 - Mitigação | Solicitar a realização de nova licitação ou Dispensa nos mesmos moldes do edital. | | Marcelo Novaes |

## 6 DECLARAÇÃO DA VIABILIDADE DA CONTRATAÇÃO

A equipe de planejamento, diante dos dados expostos, entende que a contratação é viável e necessária e aumentará, a partir de sua implantação, a segurança das informações armazenadas e disponibilizadas pelo TRE-MS.

Documento assinado eletronicamente por **ÉRIKA MURACKAMI DUARTE DA ROSA**, **Técnico Judiciário**, em 01/10/2021, às 15:33, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **GUSTAVO LEITE PINHO**, **Técnico Judiciário**, em 01/10/2021, às 16:37, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.tre-ms.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0915917** e o código CRC **77AA6F01**.