



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

TERMO DE REFERÊNCIA

ANEXO I

CAPÍTULO I. DO OBJETO

1. O presente Termo de Referência tem por objeto determinar as condições que disciplinarão 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 atualização.
2. Aplicam-se à prestação dos serviços a serem contratados as condições indicadas neste Termo de Referência e na Minuta do Contrato, sendo estas complementadas, de forma subsidiária, pelas demais normas aplicadas ao objeto da contratação.
3. A contratação dos serviços objeto deste Termo de Referência será realizada mediante licitação, na modalidade de Pregão, em sua forma eletrônica, do tipo menor preço.

CAPÍTULO II. DO LOCAL DE INSTALAÇÃO, PREÇOS UNITÁRIOS E SOLICITAÇÃO DE ATIVAÇÃO DO SERVIÇO

1. A descrição resumida dos serviços, dos locais de instalação e preços máximos unitários e totais admitidos pelo TRE/MS constam indicados abaixo:

ITEM 01 - FORMADO PELOS SUBITEMS 1.1 A 1.6				
SUBITEM	BEM OU SERVIÇO	QTDE	VALOR MÁXIMO UNITÁRIO	VALOR MÁXIMO TOTAL
1.1	Software de gerenciamento de logs e eventos de segurança (SIEM), com licença SUBSCRIÇÃO, suporte e atualização para o primeiro ano de uso.	01	R\$ 396.414,20	R\$ 396.414,20
1.2	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	R\$ 99.435,00	R\$ 596.610,00
1.3	Suporte anual para software de gerenciamento de logs e eventos de segurança (SIEM), para módulo principal, descrito no subitem 1.1 , não incluindo o primeiro ano de uso.	02	R\$ 73.833,50	R\$ 147.667,00
1.4	Suporte anual para software de gerenciamento de logs e eventos de segurança (SIEM), para pacote adicional, descrito no subitem 1.2 , não incluindo o primeiro ano de uso.	15	R\$ 20.446,20	R\$ 306.693,00
1.5	Instalação e configuração da solução de SIEM, realizada de forma presencial.	01	R\$ 213.549,20	R\$ 213.549,20
1.6	Treinamento técnico para solução de SIEM, com no mínimo 16h, para até 8 pessoas.	01	R\$ 76.105,30	R\$ 76.105,30
VALOR TOTAL DO ITEM				R\$ 1.737.038,70
INTERVALO MÍNIMO ENTRE LANCES SOBRE O VALOR TOTAL				R\$ 200,00

2. O local de instalação e suporte deverá ocorrer no endereço **Av. Des. Leão Neto do Carmo, 23 – Parque dos Poderes, Campo Grande - MS**.
 - 2.1. Caso haja alteração no endereço indicado acima, o suporte deverá ser realizado no endereço indicado pelo fiscal da contratação, desde que no mesmo município, sem majoração do preço inicialmente contratado.
3. O período de vigência da contratação será de 36 (trinta e seis) meses, a partir do aceite definitivo da Nota Fiscal.

CAPÍTULO III – DA ANÁLISE DAS PROPOSTAS

1. A análise técnica das propostas, será realizada pelos integrantes da equipe responsável pelo planejamento da contratação (integrante da área demandante e/ou integrante técnico) e visa à verificação da conformidade dos produtos ofertados pelas licitantes com as especificações indicadas neste Termo de Referência, assim como os valores dos subitens.
2. De modo a permitir a análise técnica, a licitante deverá indicar em sua proposta o nome da solução, o tipo de licenciamento e as características do produto ofertado.
 - 2.1. A licitante poderá indicar, também, sítio(s) na internet, preferencialmente do fabricante, onde possam ser obtidas informações sobre o produto ofertado.
 - 2.2. A ausência e/ou insuficiência de informações sobre o produto ofertado poderá importar a desclassificação ou recusa da proposta.
3. O resultado da análise das propostas será informado às licitantes pelo Pregoeiro, através da ferramenta de conversação disponível no sistema COMPRASNET, em caso de desclassificação, será convocado o segundo colocado na licitação para apresentar proposta.

CAPÍTULO IV. DAS ESPECIFICAÇÕES DOS SERVIÇOS DISCRIMINADOS

1. CONSIDERAÇÕES GERAIS SOBRE A SOLUÇÃO:

Subitem 1.1 - 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 Termo de Referência.
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:
 1. Por volume de dados recebidos e tratados, partindo de **30 GBytes/dia** e sem limite de ativos geradores de eventos.
 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).
 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 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.

Subitem 1.2 - 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.

1. Pacotes de licenciamento de software para ampliação da capacidade da solução de software ofertada no **subitem 1.1**.
2. Cada pacote adicional previsto no **subitem 1.2** devem contemplar, no mínimo, de acordo com o tipo de licenciamento proposto para o **subitem 1.1**:
 1. Por volume de dados recebidos e tratados: **10 GBytes/dia** de logs.
 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).
 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 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;

Subitem 1.3 - 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 **subitem 1.1**, 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.

Subitem 1.4 - Suporte anual para software de gerenciamento de logs e eventos de segurança (SIEM), para pacote adicional (descrito no subitem 1.2), 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 **subitem 1.2**, 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 subitem 1.2, 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.

Subitem 1.5 - 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. A empresa terá o prazo de 15 dias úteis para instalação e configuração da ferramenta no ambiente da Contratante, contados a partir da comunicação da fiscalização.

Subitem 1.6 - Treinamento técnico para solução de SIEM, com no mínimo 16h:

1. Deverá ser ministrado por técnico certificado pelo fabricante da solução;
2. O certificação deverá ser apresentada antes da realização do treinamento;
3. 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 8 profissionais do TRE-MS.
4. Deverá contemplar a administração completa da ferramenta.
5. Poderá ser realizado *in company* (na sede da contratante) ou em centro de treinamento homologado pelo fabricante, em qualquer unidade da federação.
6. 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:

1. Todos os componentes da solução devem permitir sua instalação em ambiente virtual, servidores físicos de propósito genérico ou em *appliance* virtual especializado.
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.
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.
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.
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.
6. A solução deverá implementar compressão dos eventos em cada fase do ciclo de vida do evento: transmissão, armazenamento online e *offline* dos eventos.
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*).
8. Rotular eventos por zonas diferentes mesmo que estejam em redes com mesma faixa endereçamento IP.
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.
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.
11. Ofuscar os campos sensíveis dos eventos (como senhas, identidade funcional, números de cartões de crédito e outros similares).
12. Ser capaz de coletar, no mínimo, os logs dos sistemas e ativos listado abaixo:
 1. Firewalls: Checkpoint R80.x, VMWare NSX, PfSense;
 2. Switches: HPE e Aruba;
 3. Plataformas de Virtualização: VMware ESX, HyperV, Acropolis/KVM e Oracle VM;
 4. Sistemas Operacionais: Linux (Debian, RedHat, Ubuntu, CentOS, Oracle Linux), Windows Server (2008, 2012, 2016) e FreeBSD;
 5. Antivirus: TrendMicro, Clamav;
 6. Servidores de E-mail: Zimbra e Microsoft Exchange;
 7. Servidores de Aplicação e Web: Apache2, Squid, Nginx, HAProxy, Apache Tomcat, Jboss e MicroSoft IIS7 (ou superior);
 8. VPN: OpenVPN;
13. Para coleta de logs deve suportar, no mínimo, os seguintes métodos:
 1. Syslog (UDP, TCP e TLS);
 2. CIFS;
 3. FTP;
 4. MySQL;
 5. MS SQL;
 6. Oracle;
 7. API;
 8. JSON;
 9. CEF;
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.
15. A solução deve permitir coletar dados de *feeds* externos.
16. Suportar o modo de criptografia em todos os conectores.
17. Controlar a utilização da banda utilizada diretamente do conector sem a necessidade de usar recursos do sistema operacional.
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.
19. A solução deve ser capaz de normalizar e categorizar os eventos em um padrão único.

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.
 1. O envio dos dados em cache deve ocorrer imediatamente após a disponibilização do destino do evento.
21. A solução deve ser capaz de enviar o evento bruto (*raw*) para o armazenamento e consulta futura.
22. Deverá ter a capacidade de guardar eventos normalizados/tratados e brutos em forma comprimida.
23. A solução deve ser capaz de inserir nos eventos normalizados metadados sobre georreferência dos mesmos.
24. Tanto os eventos de segurança quanto os de conformidade devem ser normalizados para um único padrão de eventos utilizado pela solução.
25. A solução deve permitir múltiplos perfis de configuração.
26. A solução deverá enviar os eventos coletados para o correlacionador e permitir enviar para mais de um destino ao mesmo tempo.
27. Deverá implementar a coleta, processamento e correlação de informações de fluxo de rede *Netflow v9/SFlow*.
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.
29. Possuir a funcionalidade de atualização, gerenciamento e configuração centralizados de todos os conectores distribuídos da solução.
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.
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:
 1. O balanceamento de carga deverá implementar os métodos *Weighted Round Robin* ou *Round Robin*;
 2. Prover um IP virtual ou definir nos agentes todos os servidores que fazem função de correlacionador como destino das fontes geradoras de eventos.
 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.
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.
33. Ser capaz de armazenar logs por tempo determinado e personalizado, conforme necessidade do órgão.
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.
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.
 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.
36. Permitir o expurgo dos dados de forma automática de acordo com a personalização do prazo de retenção que precede o expurgo.
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.
38. Deverá permitir exportar eventos para formato pdf e csv.
 1. Deverá permitir que o usuário defina quais campos do evento serão exportados.
39. Deverá implementar funcionalidade de ajuda (*helper*) para facilitar a criação de queries.
40. Deverá implementar assistente gráfico para criação de queries.
41. Deverá implementar indexação baseada em campo e palavra-chave para acelerar buscas.
42. Deverá implementar alertas por *syslog*, *SNMP* e e-mail.
43. Deverá permitir visualização em tempo real de eventos que atendam ao critério de seleção definido pelo usuário.
44. Possuir relatórios pré-configurados (*templates*) separados em categorias.
45. Deverá suportar pelo menos 03 dos seguintes formatos de relatórios: html, pdf, csv, doc, xls, xml e zip.
46. Permitir o agendamento de geração de relatórios e o envio dos mesmos por e-mail.
47. Possuir ferramenta ou interface gráfica para desenho de modelos de relatórios ou *dashboards* personalizados.
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.
49. Deverá implementar tecnologia de pesquisa distribuída nos múltiplos elementos (componentes) da solução.
50. Apresentar relatórios de eventos, alertas e incidentes em nível técnico (analítico, *drill down*) e gerencial (sintético / *dashboards*).
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.
52. Possuir conformidade com as normas ISO 27001 e LGPD.
53. Deve utilizar algoritmos para verificação de integridade e autenticidade dos eventos armazenados para fins de auditoria devidamente reconhecidos como seguros.
54. Armazenar os eventos e os alertas, inclusive os normalizados, de forma indexada.
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.
56. Deverá permitir acrescentar campos de uma fonte em outra fonte.
57. Deverá ser fornecido com solução de gerenciamento central com as seguintes características mínimas:
 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. Deverá permitir a implementação de atualização e distribuição de novas políticas de segurança pelos elementos/componentes gerenciados;
 3. Deverá possuir regras de monitoração pré-configuradas, as quais podem ser editadas ou apagadas;
 4. Deverá interagir diretamente com a biblioteca de casos de uso do fabricante da solução para download e atualizações de conteúdo;
 5. Deverá possuir interface WEB acessível por HTTPS e CLI por SSH, com suporte ao padrão UTF-8;
 6. Deverá possuir tela de monitoração com as seguintes características:
 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. Listagem de todos os elementos/componentes que estão reportando problemas;
 3. Permitir a visualização do sumário de monitoração por tipo de produto;
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.
59. Deverá permitir o *backup* e a restauração da configuração da solução de gerenciamento, assim como a configuração de usuários e grupo de usuários.
60. Deverá ser possível visualizar o consumo de licenças da solução.
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.
62. Deverá permitir a visualização dos dispositivos gerenciados por localização, host e tipo.
63. Permitir adição, visualização, edição e exclusão da localização de dispositivos.

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.
65. Deverá permitir a apresentação de árvore hierárquica de dispositivos.
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.
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.
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.
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.
70. Deverá permitir o gerenciamento dos eventos arquivados.
71. Deverá permitir o gerenciamento de *peers* de centralizadores de logs.
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.
73. Deverá permitir a comparação de duas configurações e a checagem de configurações ativas com a configuração definida como base para aquele elemento/componente.
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.
75. Deverá permitir a configuração de usuários e grupos de usuários, seus dispositivos associados e os respectivos privilégios (administrador, relatórios, pesquisas, operação, gerenciamento).
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.
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.
78. O correlacionador deve ser capaz de receber eventos dos agentes, coletores e de outros correlacionadores.
79. O correlacionador deve efetuar a análise dos eventos em *near real-time* (tempo próximo ao real).
80. Deve permitir ao administrador a criação de novas regras e a edição das existentes.
81. O correlacionador deve identificar anomalias baseadas em eventos e análise de dados históricos conforme período a ser definido.
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.
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.
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.
85. O correlacionador deve ter a capacidade de fazer a correlação entre eventos oriundos de:
 1. Agentes (ou solução similar) ou coletores de outros correlacionadores;
 2. Diferentes ativos do mesmo tipo (por exemplo, Firewall A e Firewall B);
 3. Ativos de diferentes tipos (por exemplo, Firewall A e IPS B e Proxy C);
 4. Ativos e Banco de Dados (por exemplo, catraca e consultas (queries) a banco de dados);
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.
87. O correlacionador deve priorizar os eventos e alertas com base, pelo menos, nos seguintes critérios:
 1. Severidade do evento;
 2. Criticidade do ativo;
 3. Existência de vulnerabilidade no ativo;
88. Possuir a funcionalidade de geração de incidentes em módulos de tratamento interno.
89. Possuir a funcionalidade de definição de prioridade para os eventos, alertas e incidentes.
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.
91. O correlacionador deve armazenar os eventos, alertas e incidentes na base de dados da solução.
92. A solução deve possuir um mecanismo de correlação avançada para processar e comparar informações de logs de diferentes fontes e fluxos de rede.
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.
94. Fornecer a funcionalidade de geração de alertas (sonoros e/ou visuais) para incidentes de alta criticidade detectados na correlação de eventos.
95. A solução deve notificar e associar comportamentos anômalos baseados em múltiplos eventos que ocorrerem em um determinado período de tempo.
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.
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.
98. A solução deve possibilitar o envio de notificações ou alertas baseados no fator de importância e criticidade do ativo/dispositivo definidos pela contratada.
99. Permitir a instalação de certificado digital para prover o acesso seguro, e configurar o repositório de certificados confiáveis.
100. Manter seu próprio log de auditoria.
101. Ter a funcionalidade de visualização de eventos e alertas de segurança em tempo real;
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.
103. Permitir a inserção manual de anotações em alertas.
104. A solução deve ser capaz de notificar os administradores, ou usuários cadastrados, caso algum dispositivo monitorado pare de enviar eventos.
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).
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.

1. A solução, deverá ser instalada no prédio-sede do TRE/MS, sito na Rua Desembargador Leão Neto do Carmo, n.º 23, Parque dos Poderes, Campo Grande-MS, das 12:00h às 18h.
 1. A empresa deverá agendar previamente o dia, horário e local para a instalação da solução que, **no primeiro momento se tratará dos subitens 1.1, 1.3 e 1.5**, no horário das 12:00h às 18:00h, de segunda à sexta-feira, através do telefone (67) 2107- 7123 (Ulysses Almeida Neto ou Gustavo Pinho).
 2. **O treinamento previsto no subitem 1.6 também deverá ser agendado previamente, após a instalação dos subitens 1.1, 1.3 e 1.5.**
 3. **Os subitens 1.2 e 1.4 serão executados sob demanda, ou seja, apenas se verificado a insuficiência dos demais itens da solução.**
2. Nos termos do inciso III, art. 3º do Decreto nº 7.174/2010, para os produtos importados será exigido, no momento da entrega, a comprovação de origem dos mesmos e a quitação dos tributos de importação a eles referentes, sob pena de rescisão contratual e multa.
3. O PRAZO MÁXIMO DA INSTALAÇÃO E TREINAMENTO DA SOLUÇÃO (SUBITENS 1.1, 1.3, 1.5 e 1.6) será de, no máximo, 15 (quinze) dias, contados do dia útil subsequente à mensagem eletrônica responsável pelo encaminhamento da nota de empenho e/ou da Requisição de fornecimento.
 1. Caso a Nota de Empenho e/ou Requisição de fornecimento seja encaminhado através de serviço postal, fax ou outro meio disponível, a contagem do prazo se dará através da comprovação do efetivo recebimento do instrumento por parte do licitante.
 2. **Fica a licitante vencedora obrigada a enviar aviso de recebimento das mensagens eletrônicas que lhes são enviadas. Caso não o faça, considerar-se-á ciente do seu conteúdo, no 1º dia útil seguinte ao seu envio.**
4. Caso a empresa verifique a impossibilidade de cumprir com o prazo de entrega estabelecido, deverá encaminhar ao TRE/MS solicitação de prorrogação de prazo de entrega, da qual deverão constar: motivo do não cumprimento do prazo, devidamente comprovado, e o novo prazo previsto para entrega.
 1. A comprovação de que trata esta cláusula deverá ser promovida não apenas pela alegação da empresa contratada, mas por meio de documento que relate e justifique a ocorrência que ensejará o descumprimento de prazo, tais como: carta do fabricante/fornecedor, laudo técnico de terceiros, Boletim de Ocorrência de Sinistro, ou outro equivalente.
5. A solicitação de prorrogação de prazo será analisada pelo TRE/MS na forma da lei e de acordo com os princípios de razoabilidade e proporcionalidade, informando-se à empresa da decisão proferida.
6. Em caso de denegação da prorrogação do prazo de entrega, e caso não cumpra o prazo inicial, o fornecedor ficará sujeito às penalidades previstas para atraso na entrega.
7. O recebimento provisório e definitivo dos materiais será de responsabilidade da Equipe de Apoio à contratação, designada nos estudos preliminares desta contratação, conforme descrito a seguir:
 1. apresentação do documento fiscal, com identificação do fornecedor e do comprador (TRE/MS), descrição do equipamento entregue, quantidade, preços unitário e total; e
 2. compatibilidade do equipamento entregue com as especificações exigidas neste Termo de Referência e constantes da proposta da empresa fornecedora.
8. Atendidas as condições indicadas na cláusula 7 acima, será registrado o recebimento provisório mediante atestado no verso da Nota Fiscal, ou, em termo próprio.
 1. O atestado de recebimento registrado em canhoto de nota fiscal, ou documento similar, não configura o recebimento definitivo do material.
9. **O recebimento definitivo** deverá ser efetuado em até 10 (dez) dias úteis, contados da data do recebimento provisório, satisfeitas as condições abaixo:
 1. correspondência de nome da solução com os indicados na nota de empenho ou proposta da fornecedora;
 2. compatibilidade dos subitens com as especificações exigidas neste Termo de Referência e constantes da proposta da empresa fornecedora;
 3. realização de testes, quando previstos no Termo de Referência ou caso a unidade recebedora entenda necessário;
 4. conformidade do documento fiscal quanto à identificação do comprador (TRE/MS), descrição da solução, quantidade, preços unitário e total.
10. Verificada alguma falha no fornecimento, será feito o registro formal e informado à empresa fornecedora, para que proceda à sua correção no prazo de até 5 (cinco) dias úteis.
 1. Ao prazo previsto neste item, aplica-se o disposto nos itens 4 a 6 deste Capítulo.

CAPÍTULO IV - DA FISCALIZAÇÃO

1. A fiscalização, o acompanhamento e a orientação relativos a solução contratada ficarão a cargo da Equipe de Apoio à contratação, indicada nos estudos preliminares desta contratação, designada para esse fim.
2. O contato entre o Tribunal e a empresa contratada será mantido, prioritariamente, por intermédio da Fiscalização.
3. Caberão à fiscalização as seguintes funções:
 - a) acompanhar e fiscalizar o fornecimento e instalação do software;
 - b) verificar a conformidade do fornecimento e atestar o recebimento definitivo;
 - c) manter registro das ocorrências relacionadas ao fornecimento, para fins de acompanhamento do desempenho da contratada;
 - d) comunicar à contratada as falhas detectadas, através de Ordem de Serviço (O.S.) numerada e, de preferência, em 2 (duas) vias, uma das quais será visada pela(s) empresa(s), só assim produzindo seus efeitos;
 - e) comunicar à Administração o cometimento de falhas pela contratada, que impliquem comprometimento no fornecimento e/ou aplicação de penalidades previstas;
 - g) conferir e atestar a Nota Fiscal/Fatura emitida pela empresa contratada, encaminhando-a para pagamento;
 - i) outras atribuições pertinentes à contratação ou que lhe forem conferidas pela Administração.

CAPÍTULO VII. DA NOTA FISCAL/FATURA

1. A Nota Fiscal/Fatura deverá ser emitida, preferencialmente, em meio eletrônico e conter a indicação do material/serviço, conforme a discriminação da Nota de Empenho, quantidade, e os preços unitário e total.
2. Para fins de atendimento da IN/RBF 1.234, de 11/01/2012 (alterada pela IN/RBF nº 1.244/2012), a empresa deverá informar no documento fiscal os valores detalhados das contribuições federais a serem retidos na operação, exceto se a empresa for OPTANTE PELO SIMPLES.

CAPÍTULO VIII. DO PAGAMENTO

1. O pagamento será efetuado, mediante depósito em conta-corrente registrada em nome da pessoa jurídica vencedora do certame licitatório, no prazo de 7 (sete) dias úteis após o recebimento definitivo pela fiscalização e/ou do recebimento do documento fiscal.

1.1. O pagamento dos subitens 1.1, 1.3, 1.5 e 1.6 se dará após o recebimento definitivo de toda a solução, inclusive quanto ao treinamento (subitem 1.6);

1.2. O pagamento dos subitens 1.2 e 1.4 se dará sob demanda.

2. O procedimento de pagamento da Nota Fiscal só se efetivará após o Recebimento Definitivo e mediante a comprovação da existência de conta bancária válida e ativa em nome da empresa, além da regularidade fiscal (INSS/FGTS) e trabalhista.

3. Será retida na fonte, caso a empresa não seja OPTANTE PELO SIMPLES, sobre o valor da Nota Fiscal/Fatura, a alíquota dos seguintes impostos:

a) Imposto de Renda, Contribuição Social Sobre Lucro Líquido-CSLL, Cofins e Pis/Pasep, nos termos da Lei 9.430/96, salvo opção da empresa pelo SIMPLES – Sistema Integrado de Pagamento de Impostos e Contribuições das Microempresas e empresas de Pequeno Porte, hipótese em que o fornecedor deverá comprovar a Opção;

b) Imposto Sobre Serviços de Qualquer Natureza – ISSQN, se este for devido.

4. Em caso de atraso no pagamento por parte do Tribunal, os valores a serem pagos serão atualizados, desde a data final do período de adimplemento de cada parcela até a data do efetivo pagamento, mediante a aplicação da seguinte fórmula: $EM = I \times N \times VP$, onde: EM = Encargos Moratórios; N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento; VP = Valor da parcela em atraso; I = Índice de compensação financeira = 0,00016438, assim apurado: $i = \text{taxa percentual anual do valor de } 6\%, I = i / 365 \rightarrow I = (6/100) / 365$.

CAPÍTULO IX. DAS SANÇÕES ADMINISTRATIVAS

1. As sanções administrativas relativas ao objeto desta contratação serão disciplinadas no Termo de Contrato.

CAPÍTULO X. DOS DIREITOS E DEVERES DO TRE/MS

1. Sem prejuízo do que vier a ser disposto na minuta do Termo de Contrato, são direitos e deveres do TRE/MS:

1.1. Requisitar a prestação dos serviços objeto desta contratação, na forma prevista neste Termo de Referência e nas demais normas aplicáveis.

1.2. Exigir da contratada o fiel cumprimento das obrigações decorrentes desta contratação.

1.3. Verificar a manutenção pela contratada das condições de habilitação estabelecidas na licitação.

1.4. Aplicar penalidades à contratada, por descumprimento contratual.

1.5. Efetuar o pagamento à contratada, de acordo com as condições de preço e prazo estabelecidos neste Termo de Referência.

CAPÍTULO XI. DAS OBRIGAÇÕES DA(S) CONTRATADA(S)

1. Sem prejuízo do que vier a ser disposto na minuta do Termo de Contrato, são obrigações gerais a serem observadas por todas as empresas contratadas:

1.1. Prestar ao TRE/MS os serviços objeto desta contratação, conforme estabelecido neste Termo de Referência, no Edital de Licitação, na Minuta do Contrato e nos demais anexos, obedecendo à regulamentação aplicável.

1.2. Fornecer Serviço de Atendimento ao Cliente (SAC), 24 horas por dia, sete dias por semana, durante toda a vigência do CONTRATO, por meio de chamada telefônica, sem nenhum ônus ao TRE/MS, a fim de que seja possível registrar reclamações sobre o funcionamento do serviço contratado, obter suporte técnico e esclarecimentos.

1.3. Assumir inteira responsabilidade técnica e administrativa sobre o objeto contratado, não podendo transferir a outras empresas a responsabilidade por problemas de funcionamento do serviço. A FISCALIZAÇÃO não aceitará a transferência de qualquer responsabilidade das Contratadas para terceiros, exceto no caso de transferência de Contratos de Concessão ou de Permissão, ou de Termo de Autorização.

1.4. Responsabilizar-se pelas infrações à regulamentação aplicável ao objeto da contratação, que consistirão em infrações contratuais quando comprometerem os serviços prestados ao TRE/MS.

1.5. Manter, durante todo o prazo de execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na fase de habilitação da licitação.

1.6. Aceitar, nas mesmas condições contratuais, os acréscimos nos serviços, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato, **bem como as supressões que se fizerem necessárias, qualquer que seja o percentual a ser suprimido, implicando a simples participação no certame na anuência da empresa quanto a essas condições."**

1.7. Receber os valores que lhe forem devidos pelo pela prestação dos serviços, na forma disposta neste Termo de Referência.

1.8. Abster-se de praticar atos ilícitos, em especial os descritos no art. 5º da Lei Federal nº 12.846, de 2013, bem como observar os princípios da legalidade, moralidade, probidade, lealdade, confidencialidade, transparência, eficiência e respeito aos valores preconizados no Código de Conduta Ética do TRE/MS (Resolução 690/2020);

1.9. Dar plena ciência do disposto na Resolução 665/2019, a qual dispõe sobre o procedimento de apuração de responsabilidade e aplicação de penalidades a pessoa física ou jurídica decorrentes de descumprimento de regras licitatórias e/ou obrigações contratuais no âmbito do TRE/MS;

1.10. Dar conhecimento, aos funcionários de seus respectivos quadros que participarão da execução contratual, sobre o Código de Conduta Ética do TRE/MS para ciência e responsabilidade em sua observância.

1.10.1 O mesmo se aplica à subcontratada (se for o caso);

1.11. Proteger informações confidenciais e privilegiadas, conforme regulamento próprio.

CAPÍTULO XII. DEMAIS INFORMAÇÕES ACERCA DA CONTRATAÇÃO EXIGIDAS PELA RESOLUÇÃO N.º 182/2013 – CNJ (ART. 18, § 3º, INCISO II)

1. O presente Termo de Referência visa a melhoria da Segurança da Informação na Justiça Eleitoral de Mato Grosso do Sul.

A) MOTIVAÇÃO 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 armazenameto 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.

B e C) OBJETIVOS E BENEFÍCIOS A SEREM ALCANÇADOS:

- 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 ransomwares 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; e

- Garantir maior proteção aos dados hospedados no Datacenter do TRE-MS, sobretudo aos dados dos usuários.

D) ALINHAMENTO DA SOLUÇÃO:

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

E) Os estudos preliminares que nortearam a presente contratação encontram-se no Processo SEI 0007345-36.2020.6.12.8000.

F) RELAÇÃO ENTRE A DEMANDA PREVISTA E A SER CONTRATADA:

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.

G) SOLUÇÕES DISPONÍVEIS NO MERCADO:

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.

H) O objeto do certame enquadra-se como Locação de Softwares 33.90.40.06, de natureza comum no mercado.

I) 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.

J) A forma e o critério de seleção do fornecedor já se encontra indicada no Capítulo I (Pregão/menor preço); sendo que na fase de habilitação será exigida a comprovação da regularidade perante a Fazenda Nacional, a Seguridade Social, o Fundo de Garantia do Tempo de Serviço – FGTS e Justiça do Trabalho, além de Declaração de que a empresa não utiliza menores de 18 (dezoito) anos para trabalho noturno, perigoso ou insalubre; nem menores de 16 (dezesesseis) anos para qualquer trabalho, salvo na condição de aprendiz, a partir de 14 anos, em conformidade ao disposto no inciso XXXIII, do artigo 7º da Constituição Federal.

K) O TRE-MS já possui equipamentos adequados para a instalação das soluções ou já as utiliza e apenas irá atualizar ou melhorar as funcionalidades, não causando impacto ambiental.

L) A conformidade técnica e legal consta no capítulo III e IV deste termo de referência.

M) As obrigações contratuais, os papéis a serem desempenhados por cada envolvido na contratação e a dinâmica do fornecimento estão descritos nos Capítulos V, VI, VII, VIII, IX, X e XI.

DA TRANSFERÊNCIA DE CONHECIMENTO E DEPENDÊNCIA TÉCNICA: O TRE-MS possuirá independência tecnológica de operacionalização (haverá documentação de toda a solução e repasse de conhecimento).

Não há exigência especial de qualificação técnica ou formação profissional para os futuros envolvidos na execução do contrato objeto deste procedimento administrativo.

Nesta contratação serão adotados os modelos (templates) já utilizados por este Tribunal, no presente caso citamos a minuta do modelo de identificação complementar do licitante.



Lei 11.419/2006.



Documento assinado eletronicamente por **MARCELO SILVA DE NOVAES, Coordenador(a)**, em 27/10/2021, às 10:24, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **GUSTAVO LEITE PINHO, Técnico Judiciário**, em 28/10/2021, às 14:10, 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 **1106721** e o código CRC **B4E9F3B6**.