

MEMORIAL DESCRITIVO – MD

1. OBJETO:

- 1.1. Contratação de empresa especializada para fornecimento de licenças e serviços TrendAI (Trend Micro) destinados à modernização das ferramentas de Segurança da BAHIA – BAHIA GÁS e dos processos de Tecnologia da Informação (TI), assegurando a padronização e compatibilidade com a infraestrutura da COMPANHIA DE GÁS DA BAHIA – BAHIA GÁS. Inclui-se, ainda, apoio técnico especializados para implantação sob coordenação do time da BAHIA GÁS, bem como a garantia e o suporte técnico do fabricante pelo período de 30 (trinta) meses.

2. ESPECIFICAÇÃO DO OBJETO

- 2.1. Os entregáveis (softwares e serviços) previstos no escopo do certame são os seguintes:

2.1.1. Crédito de Licença Trend AI Endpoint Security Essentials

- 2.1.1.1. Código Microsiga: **S74031008500028**.
- 2.1.1.2. Part number: **VONA0000**
- 2.1.1.3. Quantidade: 81250 (oitenta e um mil, duzentos e cinquenta) unidades.
- 2.1.1.4. Deverão ser fornecidos créditos de licença Trend AI Endpoint Security Essentials, em versão mais atual, com vigência de 30 (trinta) meses, juntamente com acesso às atualizações, evolução tecnológica e suporte técnico da solução.
- 2.1.1.5. O licenciamento do pacote Essentials para Endpoint, descrito no item 2.1.1, deverá ser composto dos seguintes softwares:
 - 2.1.1.5.1. Standard Endpoint Protection.
 - 2.1.1.5.2. XDR for endpoint.

2.1.2. Crédito de Licença Trend AI Endpoint Security Pro

- 2.1.2.1. Código Microsiga: **S74031008500031**.
- 2.1.2.2. Part number: **VONA0000**
- 2.1.2.3. Quantidade: 120000 (cento e vinte mil) unidades.

2.1.2.4. Deverão ser fornecidos créditos de licença Trend AI Endpoint Security Pro, em versão mais atual, com vigência de 30 (trinta) meses, juntamente com acesso às atualizações, evolução tecnológica e suporte técnico da solução.

2.1.2.5. O licenciamento do pacote Essentials para Endpoint, descrito no item 2.1.2, deverá ser composto dos seguintes softwares:

2.1.2.5.1. Server & Workload Protection.

2.1.2.5.2. XDR for endpoints.

2.1.2.5.3. Log inspection.

2.1.2.5.4. Intrusion Prevention.

2.1.3. Licença Trend AI Virtual Deep Discovery Inspector - vDDI

2.1.3.1. Código Microsiga: **S74031008500027**.

2.1.3.2. Part number: **DRRA0021**

2.1.3.3. Quantidade: 01 (uma) unidade.

2.1.3.4. Deverá ser fornecida licença para Virtual Deep Discovery Inspector (vDDI), em versão mais atual, com vigência de 30 (trinta) meses, juntamente com acesso às atualizações, evolução tecnológica e suporte técnico da solução.

2.1.4. Crédito de Licença Trend AI Mobile Security

2.1.4.1. Código Microsiga: **S74031008500030**.

2.1.4.2. Part number: **VONA0000**

2.1.4.3. Quantidade: 2550 (dois mil, quinhentos e cinquenta) unidades.

2.1.4.4. Deverão ser fornecidos créditos de licença Trend AI Mobile Security, em versão mais atual, com vigência de 30 (trinta) meses, juntamente com acesso às atualizações, evolução tecnológica e suporte técnico da solução.

2.1.5. Crédito de Licença Trend AI Cyber Risk Exposure Management Essentials

2.1.5.1. Código Microsiga: **S74031008500032**.

2.1.5.2. Part number: **VONA0000**

2.1.5.3. Quantidade: 87500 (oitenta e sete mil e quinhentas) unidades.

2.1.5.4. Deverão ser fornecidos créditos de licença Trend AI Cyber Risk Exposure Management Essentials, em versão mais atual, com vigência de 30 (trinta) meses, juntamente com acesso às atualizações, evolução tecnológica e suporte técnico da solução.

2.1.6. Crédito de Licença Trend AI Sandbox Analysis – Manual Submission (Submissões diárias)

2.1.6.1. Código Microsiga: **S74031008500033**.

2.1.6.2. Part number: **VONA0000**

2.1.6.3. Quantidade: 9125 (nove mil, cento e vinte e cinco) unidades.

2.1.6.4. Deverão ser fornecidos créditos de licença Trend AI Sandbox Analysis – Manual Submission, em versão mais atual, com vigência de 30 (trinta) meses, juntamente com acesso às atualizações, evolução tecnológica e suporte técnico da solução.

2.1.7. Crédito de Licença Trend AI Sandbox Analysis – Automatic submissions with Vision One for Networks (500 Mbs)

2.1.7.1. Código Microsiga: **S74031008500025**.

2.1.7.2. Part number: **VONA0000**

2.1.7.3. Quantidade: 10000 (dez mil) unidades.

2.1.7.4. Deverão ser fornecidos créditos de licença Trend AI Sandbox Analysis – Automatic submissions with Vision One for Networks (500 Mbs), em versão mais atual, com vigência de 30 (trinta) meses, juntamente com acesso às atualizações, evolução tecnológica e suporte técnico da solução.

2.1.8. Crédito de Licença Trend AI Sandbox Analysis – Automatic submissions with Vision One Endpoint Security

2.1.8.1. Código Microsiga: **S74031008500029**.

2.1.8.2. Part number: **VONA0000**

2.1.8.3. Quantidade: 8750 (oito mil, setecentos e cinquenta) unidades.

2.1.8.4. Deverão ser fornecidos créditos de licença Trend AI Sandbox Analysis – Automatic submissions with Vision One Endpoint Security, em versão mais atual, com vigência de 30 (trinta) meses, juntamente com acesso às atualizações, evolução tecnológica e suporte técnico da solução.

2.1.9. Crédito de Licença Trend AI Agentic SIEM (Gigabytes diários)

2.1.9.1. Código Microsiga: **S74031008500026**.

2.1.9.2. Part number: **VONA0000**

2.1.9.3. Quantidade: 82125 (oitenta e dois mil, cento e vinte e cinco) unidades.

2.1.9.4. Deverão ser fornecidos créditos de licença Trend AI Agentic SIEM, em versão mais atual, com vigência de 30 (trinta) meses, juntamente com acesso às atualizações, evolução tecnológica e suporte técnico da solução.

2.1.10. Crédito de Licença Trend AI Zero Trust Private Access & AI Service Access

2.1.10.1. Código Microsiga: **S74031008500024**.

2.1.10.2. Part number: **VONA0000**

2.1.10.3. Quantidade: 106250 (cento e seis mil, duzentos e cinquenta) unidades.

2.1.10.4. Deverão ser fornecidos créditos de licença Trend AI Cloud App Security (CAS) para Mailboxes O365, em versão mais atual, com vigência de 24 (vinte e quatro) meses, juntamente com acesso às atualizações, evolução tecnológica e suporte técnico da solução.

2.1.11. Crédito de Licença Trend AI Zero Email and Collaboration Security Pro

2.1.11.1. Código Microsiga: **S74031008500023**.

2.1.11.2. Part number: **VONA0000**

2.1.11.3. Quantidade: 211313 (duzentos e onze mil, trezentos e treze) unidades.

2.1.11.4. Deverão ser fornecidos créditos de licença Trend AI Email and Collaboration Security Pro, em versão mais atual, com vigência de 30 (trinta) meses, juntamente com acesso às atualizações, evolução tecnológica e suporte técnico da solução.

2.1.12. Implantação de Infraestrutura de Segurança Trend AI

2.1.12.1. Código Microsiga: **S74031008500022**.

2.1.12.2. Quantidade: 01 (uma) unidade.

2.1.12.3. Este serviço consiste na implantação e configuração dos softwares em pleno funcionamento, em conformidade com o disposto neste Memorial Descritivo e em perfeitas condições de operação, de forma integrada ao ambiente de TI da BAHIAAGÁS, devendo contemplar, no mínimo, o seguinte:

2.1.12.3.1. Fase de Abertura:

- 2.1.12.3.1.1. Validar e Homologar escopo do projeto.
- 2.1.12.3.1.2. Validar objetivos e premissas do projeto.
- 2.1.12.3.1.3. Validar riscos e restrições do projeto.
- 2.1.12.3.1.4. Identificar e validar os requisitos do projeto.
- 2.1.12.3.1.5. Prazo: 01 (um) dia.

2.1.12.3.2. Fase de Planejamento:

- 2.1.12.3.2.1. Elaborar plano de projeto.
- 2.1.12.3.2.2. Definir as pessoas envolvidas por parte do CONTRATANTE no projeto.
- 2.1.12.3.2.3. Reunir as equipes da CONTRATADA e CONTRATANTE.
- 2.1.12.3.2.4. Apresentação do cronograma do projeto com os prazos e responsabilidades.
- 2.1.12.3.2.5. Verificar os pré-requisitos do projeto.
- 2.1.12.3.2.6. Apresentar plano do projeto para a homologação por parte do CONTRATANTE.
- 2.1.12.3.2.7. Prazo: 07 (sete) dias.

2.1.12.3.3. Fase de Execução para Mobile Security:

- 2.1.12.3.3.1. Atualização do Mobile Security para a versão mais atualizada para 20 (vinte) dispositivos móveis.
- 2.1.12.3.3.2. Orientar a equipe da CONTRATANTE para realizar o restante das instalações.
- 2.1.12.3.3.3. Prazo: 04 (quatro) dias.

2.1.12.3.4. Fase de Execução para Endpoint Security PRO:

- 2.1.12.3.4.1. Realização de migração da solução On-premise para solução atual de proteção para servidores.
- 2.1.12.3.4.2. Definição de política de proteção.
- 2.1.12.3.4.3. Treinamento Hands On.

2.1.12.3.4.4. Prazo: 10 (dez) dias.

2.1.12.3.5. Fase de Execução para Virtual Deep Discovery Inspector:

2.1.12.3.5.1. Realização de implantação do Virtual Deep Discovery Inspector na versão mais atual.

2.1.12.3.5.2. Treinamento Hands On.

2.1.12.3.5.3. Prazo: 04 (quatro) dias.

2.1.12.3.6. Fase de Execução do Agentic SIEM:

2.1.12.3.6.1. Integração com ambiente de operação do cliente, incluindo sistemas de segurança Trend AI e de terceiros.

2.1.12.3.6.2. Orientar a equipe da CONTRATANTE para utilização do sistema.

2.1.12.3.6.3. Treinamento Hands On.

2.1.12.3.6.4. Prazo: 05 (cinco) dias.

2.1.12.3.7. Fase de Execução do Zero Trust Private Access & AI Services Access:

2.1.12.3.7.1. Implantação e configuração do Zero Trust Private Access & AI Service Access.

2.1.12.3.7.2. Orientar a equipe da CONTRATANTE para utilização do sistema.

2.1.12.3.7.3. Definição de política de proteção.

2.1.12.3.7.4. Treinamento Hands On.

2.1.12.3.7.5. Prazo: 04 (Quatro) dias.

2.1.12.3.8. Fase de Encerramento:

2.1.12.3.8.1. Reunir as equipes CONTRATADA e CONTRATANTE para alinhamento de atividades pendentes, caso tenha.

2.1.12.3.8.2. Analisar e encerrar essas atividades.

2.1.12.3.8.3. Homologar o projeto.

2.1.12.3.8.4. Documentar as oportunidades de melhoria do processo.

2.1.12.3.8.5. Prazo: 03 (três) dias.

2.1.13. Gerenciamento Proativo e Preditivo de Ameaças Digitais

2.1.13.1. Código Microsiga: **S11S202K0010201**.

2.1.13.2. Quantidade: 30 (trinta) meses.

2.1.13.3. A CONTRATADA deverá prover todo o suporte das soluções de segurança Trend AI (Trend Micro), especificadas nos itens 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.1.6, 2.1.7, 2.1.8, 2.1.9, 2.1.10 e 2.1.11 e implantada conforme item 2.1.12.

2.1.13.4. O Gerenciamento Proativo e Preditivo de Ameaças Digitais deverá prever medidas para garantir a proteção dos dados, antecipando ameaças à privacidade, segurança e integridade, prevenindo acesso não autorizado às informações.

2.1.13.5. Suporte prioritariamente remoto.

2.1.13.5.1. Caso haja necessidade de acesso local às dependências da BAHIAGÁS, este acesso deverá ser previamente solicitado e será autorizado pela BAHIAGÁS de acordo com as suas necessidades.

2.1.13.6. A CONTRATA deverá prestar suporte técnico reativo na modalidade 24x7 (vinte e quatro horas, sete dias na semana) e em língua portuguesa, com a finalidade de sanar dúvidas, sua configuração ou quaisquer outros assuntos relacionados às soluções de segurança Trend AI atendendo aos seguintes requisitos:

2.1.13.6.1.1. Dispor de serviço de esclarecimento de dúvidas relativas à utilização das soluções e de abertura de chamado técnico por e-mail e telefone, por todo o período de vigência do licenciamento.

2.1.13.6.1.2. Realizar o atendimento observando a classificação dos problemas reportados de acordo com seu grau de gravidade, da seguinte forma:

2.1.13.6.1.2.1. Gravidade 1 – problemas que acarretem na inoperabilidade dos ativos ou sistemas protegidos pelas soluções de segurança implantadas.

2.1.13.6.1.2.2. Gravidade 2 – problemas ou dúvidas que prejudiquem a operação dos ativos ou sistema, mas que não interrompam a operação da CONTRATANTE.

2.1.13.6.1.2.3. Gravidade 3 – problemas ou dúvidas que criam algumas restrições à operação dos ativos e sistemas protegidos pelas soluções de segurança implantadas.

2.1.13.6.1.2.4. Gravidade 4 – Problemas ou dúvidas que não afetam a operação dos ativos e sistemas protegidos pelas soluções de segurança implantadas.

- 2.1.13.6.1.3. Considera-se SLA o período entre o horário que o chamado foi aberto até o horário em que acontece o primeiro contato do suporte da CONTRATANTE para resolução do problema.
- 2.1.13.6.1.3.1. Iniciar no prazo máximo de 04 (quatro) horas, o atendimento aos chamados de suporte técnico para soluções de problemas, com gravidades 1 e 2, contado a partir da abertura do chamado.
- 2.1.13.6.1.3.2. Iniciar no prazo máximo de 12 (doze) horas, o atendimento aos chamados de suporte técnico para soluções de problemas, com gravidades 3 e 4, contado a partir da abertura do chamado.
- 2.1.13.6.1.3.3. Os prazos para atendimento de chamados técnicos serão interrompidos somente se ficar caracterizado que se trata de falha de laboratório (bug), sendo necessário o encaminhamento da falha ao laboratório do fabricante e acompanhamento de sua solução.
- 2.1.13.7. Deverá ser prestado gerenciamento proativo e reativo, envolvendo as seguintes atividades:
- 2.1.13.7.1. Reunião de *Onboarding* no início do contrato. Essa reunião deverá acontecer no início do contrato afim de definir cronograma, requisitos e expectativas para o restante do contrato.
- 2.1.13.7.2. Reunião de acompanhamento mensal com a periodicidade mensal, com seu início após a realização da reunião de *Onboarding*, ou seja, 29 (vinte e nove) vezes ao longo de 30 (trinta) meses. Essas reuniões deverão sumarizar as ações realizadas a cada mês e apontar melhorias e recomendações com relação aos serviços executados.
- 2.1.13.7.3. Análise de alertas com a periodicidade mensal, ou seja, 30 (trinta) vezes ao longo de 30 (trinta) meses. Esta atividade terá como finalidade a análise de eventos de segurança e mitigá-los para evitar que ocorram eventos de grande magnitude e que gerem impactos na continuidade das operações da CONTRATADA.
- 2.1.13.7.4. Investigação de ameaças sob demanda, na modalidade 24x7x4 (vinte e quatro horas, sete dias na semana, primeiro atendimento em 04 horas) conforme seja necessário ao longo de 30 (trinta) meses. Esta atividade terá como finalidade investigar possíveis eventos de segurança de grande magnitude mitigá-los para evitar que gerem impactos na continuidade das operações da CONTRATADA.
- 2.1.13.7.5. Avaliação de *playbooks* em periodicidade trimestral, ou seja, 10 (dez) vezes ao longo de 30 (trinta) meses. Esta atividade terá como finalidade a elaboração de *playbooks* para automatizar respostas a ameaças comuns, identificadas no ambiente monitorado de acordo as melhores práticas do fabricante.
- 2.1.13.7.6. Health Check em periodicidade mensal, ou seja, 30 (trinta) vezes ao longo de 30 (trinta) meses. Este relatório deverá conter informações sobre a saúde das implantações e propostas de melhoria baseadas no que não estiver em conformidade com as melhores práticas do fabricante.

- 2.1.13.7.7. Análise do inventário de dispositivos monitorados em periodicidade mensal, ou seja, 30 (trinta) vezes ao longo de 30 (trinta) meses. Esta atividade terá como finalidade analisar a fundo os ativos inventariados e ajustar de forma granular a criticidade desses ativos.
- 2.1.13.7.8. Revisão de políticas em periodicidade trimestral, ou seja, 10 (dez) vezes ao longo de 30 (trinta) meses. Esta atividade terá como finalidade analisar se as políticas de segurança vigentes estão em conformidade com as melhores práticas do fabricante.
- 2.1.13.7.9. Atualizações dos produtos *onpremises* em periodicidade trimestral, ou seja, 10 (dez) vezes ao longo de 30 (trinta) meses. Esta atividade visa manter as implantações *onpremise* atualizadas evitando a existência de vulnerabilidades para estes serviços.
- 2.1.13.7.10. Mitigação de riscos cibernéticos em periodicidade mensal, ou seja, 30 (trinta) vezes ao longo de 30 (trinta) meses. Esta atividade tem como finalidade mitigar eventos de segurança que são detectados pelos sensores implantados.
- 2.1.13.7.11. Reunião de *followup* em periodicidade mensal, ou seja, 30 (trinta) vezes ao longo de 30 (trinta) meses. Esta atividade tem como finalidade alinhar as ações de mitigação entre as equipes da CONTRATANTE e a equipe da CONTRATADA.
- 2.1.13.7.12. Reunião de gestão de risco cibernético em periodicidade mensal, ou seja, 30 (trinta) vezes ao longo de 30 (trinta) meses. Esta reunião deverá apontar os principais resultados das atividades realizadas durante o mês, e avaliação do risco cibernético da organização.
- 2.1.13.7.13. Reunião de indicadores e métricas para alta gestão em periodicidade trimestral, ou seja, 10 (dez) vezes ao longo de 30 (trinta) meses. Esta reunião terá como foco principal apresentar de forma executiva os resultados obtidos através das atividades citadas anteriormente, para diretoria da CONTRATADA.
- 2.1.13.7.14. Análise de vulnerabilidades em periodicidade semanal, ou seja, 120 (cento e vinte) vezes ao longo de 30 (trinta) meses. Este relatório terá como foco principal apresentar de forma técnica os resultados obtidos através das análises das vulnerabilidades encontradas no ambiente da CONTRATADA.
- 2.1.13.7.15. Reunião de indicadores e métricas para alta gestão em periodicidade trimestral, ou seja, 10 (dez) vezes ao longo de 30 (trinta) meses. Esta reunião terá como foco principal apresentar de forma executiva os resultados obtidos através das atividades citadas anteriormente, para diretoria da CONTRATADA.
- 2.1.13.7.16. Realização de visitas preventivas (remotas ou presenciais) para efetuar as melhorias levantadas nos relatórios dos diagnósticos citados nos itens 2.1.13.7.6, 2.1.13.7.8, 2.1.13.7.9, 2.1.13.7.10, 2.1.13.7.12 e 2.1.13.7.14.

- 2.1.13.8. Deverão ser executadas em formato 24x7 (vinte e quatro horas x sete dias na semana) as atividades descritas nos itens 2.1.13.6 e 2.1.13.7.4 segundo suas especificidades.
- 2.1.13.9. As atividades contempladas nos itens 2.1.13.7.1, 2.1.13.7.2, 2.1.13.7.3, 2.1.13.7.4, 2.1.13.7.5, 2.1.13.7.6, 2.1.13.7.7, 2.1.13.7.8, 2.1.13.7.9, 2.1.13.7.10, 2.1.13.7.11, 2.1.13.7.12, 2.1.13.7.13, 2.1.13.7.14 e 2.1.13.7.15, deverão ser executadas na modalidade 8x5 (oito horas x cinco dias na semana) respeitando o horário de funcionamento da CONTRATANTE.
- 2.1.13.10. O suporte deverá ser realizado por profissional certificado, conforme especificado no item 9.5.

3. NECESSIDADE DA TÉCNICA EXIGIDA:

- 3.1. Não se aplica.

4. PRAZO EXECUÇÃO DO OBJETO:

- 4.1. O prazo de execução do deverá ser igual ao prazo de vigência do Contrato e deverá ser contado a partir da assinatura do contrato.

5. LOCAL(IS) DE ENTREGA OU EXECUÇÃO DO OBJETO E HORÁRIOS ADMITIDOS:

- 5.1. A entrega das licenças de softwares, descritos nos itens 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.1.6, 2.1.7, 2.1.8, 2.1.9, 2.1.10 e 2.1.11 deste Memorial Descritivo, deverão ser realizadas deverão ser realizadas através de envio para o e-mail CONTRATOS_GETIN@bahia gas.com.br.
- 5.2. A prestação do serviço de Gerenciamento Proativo e Preditivo de Ameaças Digitais, descrito no item 2.1.13 deste Memorial Descritivo, deverá ser realizada, prioritariamente, através de acesso remoto, devendo este ser previamente solicitado à CONTRATANTE e concedido mediante sua autorização.
- 5.2.1. Caso haja necessidade de acesso local às dependências da CONTRATANTE, este acesso deverá ser previamente solicitado e será autorizado pela CONTRATANTE de acordo com as suas necessidades.
- 5.3. Em comum acordo entre as partes, os serviços poderão ser realizados também em horários alternativos, dependendo da necessidade da CONTRATANTE.

6. OBRIGAÇÕES DA CONTRATADA RELACIONADAS À EXECUÇÃO DO OBJETO:

- 6.1. Os preços constantes na PLANILHA DE PREÇOS UNITÁRIOS devem incluir as despesas de transporte para entrega no local indicado bem como todos os impostos, inclusive o ICMS e ISS, que estarão a cargo da CONTRATADA.
- 6.2. A CONTRATADA deve fornecer os equipamentos descritos na PLANILHA DE PREÇOS UNITÁRIOS, em sua totalidade, no prazo máximo de 30 (trinta) dias.
- 6.3. Garantir que as Informações Confidenciais serão utilizadas apenas para os propósitos deste contrato, e que serão divulgadas apenas para seus diretores, sócios, administradores, empregados, prestadores de serviço, prepostos ou quaisquer representantes, respeitando o princípio do privilégio mínimo.
- 6.4. Atender a todas as exigências e prazos definidos neste Memorial Descritivo e em seus anexos.
- 6.5. Cumprir as normas e regulamentos internos da CONTRATANTE.
- 6.6. Cumprir com os prazos de entrega estabelecidos neste Memorial Descritivo.
- 6.7. Nomear previamente ao início da realização do serviço ponto único de contato para assuntos técnicos e comerciais para representar cada parte e para tomar decisões pertinentes à condução da atualização e configuração conforme acordado.
- 6.8. Responder pelos danos causados diretamente à CONTRATANTE ou a terceiros, decorrentes de sua culpa ou dolo na execução do contrato, não excluindo ou reduzindo essa responsabilidade à fiscalização ou ao acompanhamento pela CONTRATANTE.
- 6.9. Manter, durante a execução do contrato, em compatibilidade com as obrigações por ele assumidas, todas as condições de habilitação e qualificação exigidas na licitação.
- 6.10. Planejar, desenvolver, implantar, executar e manter os serviços objeto do contrato de acordo com os níveis mínimos estabelecidos nas especificações técnicas.
- 6.11. Refazer os serviços considerados inadequados pelo gestor ou fiscais do contrato, no prazo por eles estabelecido e sem ônus para a CONTRATANTE.
- 6.12. Reportar à CONTRATANTE, imediatamente, qualquer anormalidade, erro ou irregularidades que possam comprometer a execução dos serviços e o bom andamento das atividades da CONTRATANTE.
- 6.13. Solicitar à Fiscalização do Contrato os esclarecimentos de dúvidas, detalhes, nomenclaturas ou definições que, porventura, não constem neste instrumento ou nas Especificações Técnicas do Serviço.
- 6.14. Responsabilizar-se pelo pagamento de eventuais multas aplicadas por quaisquer autoridades federais, estaduais e/ou municipais, em consequência de fatos a si imputáveis, relacionados aos serviços contratados.

- 6.15. Tratar como confidenciais e zelar pelo sigilo de todos os dados, informações ou documentos que tomar conhecimento em decorrência da prestação dos serviços objeto desta contratação, bem como deverá submeter-se às normas e políticas de segurança da CONTRATANTE, devendo orientar seus empregados e/ou prepostos nesse sentido, sob pena de responsabilidade civil, penal e administrativa.
- 6.16. Assumir responsabilidade sobre todos os possíveis danos físicos e/ou materiais causados ao Órgão ou a terceiros, advindos de imperícia, negligência, imprudência ou desrespeito às normas de segurança.
- 6.17. Compromete-se a respeitar todas as obrigações relacionadas com sigilo, confidencialidade e segurança das informações pertencentes à CONTRATANTE, mediante ações ou omissões, intencionais ou acidentais, que impliquem na divulgação, perda, destruição, inserção, cópia, acesso ou alterações indevidas, independentemente do meio no qual estejam armazenadas, em que trafeguem ou do ambiente em que estejam sendo processadas.

7. OBRIGAÇÕES DA CONTRATANTE RELACIONADAS À EXECUÇÃO OBJETO:

- 7.1. Disponibilizar para a CONTRATADA os recursos necessários em tempo compatível com os estipulados para atendimento por parte da CONTRATADA dos níveis mínimos de serviço estabelecidos.
- 7.2. Prestar as informações e esclarecimentos pertinentes ao objeto que venham a ser solicitados pela CONTRATADA.
- 7.3. Permitir o acesso dos funcionários da CONTRATADA, devidamente credenciados e uniformizados, às dependências da CONTRATANTE, aos dados e demais informações necessárias ao desempenho das atividades previstas neste Memorial Descritivo, ressalvados os casos de matéria sigilosa.
- 7.4. Efetuar o pagamento à CONTRATADA, mediante entrega das Notas Fiscais/Faturas, após atesto das mesmas pelo respectivo Gestor do Contrato.
- 7.5. Avaliar a qualidade e acompanhar a execução de serviços, identificando eventuais não conformidades.
- 7.6. Proporcionar todas as facilidades indispensáveis à boa execução dos serviços, inclusive permitir o livre acesso dos empregados da CONTRATADA às dependências da CONTRATANTE.
- 7.7. Elaborar e encaminhar à CONTRATADA Termo de Confidencialidade, quando necessário.
- 7.8. Encaminhar demandas de correção à CONTRATADA.
- 7.9. Acompanhar o prazo de apresentação das notas fiscais ou faturas, bem como recebê-las, atestá-las e encaminhá-las para pagamento.

8. GESTÃO E FISCALIZAÇÃO PELA CONTRATANTE:

- 8.1. O acompanhamento e a fiscalização da execução do contrato serão exercidos por meio do Gestor e Fiscal e substitutos, designados pela CONTRATANTE, aos quais compete acompanhar, fiscalizar, conferir e avaliar a execução, bem como dirimir e desembaraçar quaisquer dúvidas e pendências que surgirem, determinando o que for necessário à regularização das faltas, falhas, problemas ou defeitos observados, e os quais de tudo darão ciência à CONTRATADA.
- 8.2. Não obstante ser a CONTRATADA a única e exclusiva responsável pela execução dos serviços, a CONTRATANTE reserva-se o direito de, sem que de qualquer forma restrinja a plenitude dessa responsabilidade, exercer a mais ampla e completa fiscalização.
- 8.3. O gestor e o fiscal do contrato deverão conferir os relatórios dos serviços executados pela CONTRATADA, por ocasião da entrega das Notas Fiscais ou Faturas, e atestar a prestação dos serviços, quando executados satisfatoriamente, para fins de pagamento.
- 8.4. Ao gestor do contrato fica assegurado o direito de exigir o cumprimento de todos os itens constantes do Memorial Descritivo, da proposta da CONTRATADA e das cláusulas do futuro contrato, além de solicitar a substituição de qualquer empregado da CONTRATADA que: comprometa a perfeita execução dos serviços; crie obstáculos à fiscalização; não corresponda às técnicas ou às exigências disciplinares da CONTRATANTE; e cujo comportamento ou capacidade técnica sejam inadequados à execução dos serviços, que venha causar embaraço a fiscalização em razão de procedimentos incompatíveis com o exercício de sua função.
- 8.5. São de exclusiva responsabilidade da CONTRATADA, sem qualquer espécie de solidariedade por parte do CONTRATANTE, as obrigações de natureza fiscal, previdenciária, trabalhista e civil, em relação ao pessoal que a CONTRATADA utilizar para prestação dos serviços durante a execução do contrato.
- 8.6. A gestão, acompanhamento e fiscalização serão exercidos no interesse exclusivo da CONTRATANTE e não excluem em hipótese alguma as responsabilidades da CONTRATADA, inclusive perante terceiros.

9. GARANTIA TÉCNICA DO OBJETO:

- 9.1. A garantia abrange todas as atividades desenvolvidas pela CONTRATADA durante a vigência do contrato, além de garantir sigilo absoluto das informações que tratará e manterá sob sua guarda.
- 9.2. A empresa LICITANTE deverá apresentar, no mínimo, 01 (um) Atestado de Capacidade Técnica, expedido por pessoa jurídica de direito público ou privado, comprovando que a mesma tenha fornecido equipamentos e serviços, semelhantes

e compatíveis com o objeto deste Memorial Descritivo.

- 9.3. A empresa CONTRATADA deverá apresentar carta emitida pelo fabricante, que comprove formalmente a existência de vínculo de parceria comercial vigente entre as partes, atestando sua condição de parceira autorizada para fins de fornecimento, implementação e/ou suporte das soluções objeto deste certame.
- 9.4. A empresa CONTRATADA deve possuir Plataforma de Gestão de Segurança de Perímetro, através de software próprio, que utilize os dados das soluções de proteção contra ameaças digitais da Trend AI e faça diagnósticos especializados, com intuito de apontar melhorias e recomendações com relação as melhores práticas do fabricante. A comprovação deve ser feita através de registro de software.
- 9.5. Para a execução das atividades previstas no objeto são necessários profissionais com perfil e experiência específicos, devidamente comprovados até o início da execução dos serviços, conforme listado a seguir:
 - 9.5.1. 02 (Dois) profissionais com certificação Trend Micro Apex One as a service Certified Professional. A comprovação deve ser feita através de certificado do fabricante.
 - 9.5.2. 01 (Um) profissional com certificação Trend Micro Deep Security 20. A comprovação deve ser feita através de certificado do fabricante.
 - 9.5.3. 02 (Dois) profissionais com certificação Trend Vision One - Security Operations Professional. A comprovação deve ser feita através de certificado do fabricante.
 - 9.5.4. 01 (Um) profissional com certificação em Sistema de Gestão em segurança da Informação ISO/IEC 27001 (Auditor Líder), comprovado através de certificado emitido.
 - 9.5.5. 01 (Um) profissional com certificação CompTIA Security +. A comprovação deve ser feita através de certificado do fabricante.
 - 9.5.6. 01 (Um) profissional com certificação CompTIA Network +. A comprovação deve ser feita através de certificado do fabricante.
 - 9.5.7. 01 (um) profissionais com certificação CompTIA Cysa +, comprovado através de certificado emitido.
- 9.6. Deverá ser fornecida declaração de que a LICITANTE possuirá em seu quadro funcional, no momento da contratação, os profissionais citados no item 9.5.
- 9.7. As certificações profissionais serão auditadas na assinatura do contrato.

10. TIPOS INFRACIONAIS PARA SANCIONAMENTO:

- 10.1. Havendo atraso no cumprimento das obrigações assumidas, sem justificativas fundamentadas por escrito e aceitas pelo CONTRATANTE, a CONTRATADA estará sujeita as sanções previstas no Anexo V – Manual de Apuração de Responsabilidades e Aplicação de Sansão do Regulamento de Licitações e

Contratos da CONTRATANTE, disponível em seu site.

- 10.2. O atraso ou descumprimento de qualquer obrigação contratual, sem justificativa por escrito aceita pelo CONTRATANTE, implicará nas sanções previstas no Anexo V – Manual de Apuração de Responsabilidades e Aplicação de Sansão do Regulamento de Licitações e Contratos da CONTRATANTE.
- 10.3. Caso haja a desistência da CONTRATADA na execução da prestação dos serviços, implicará nas sanções previstas no Anexo V – Manual de Apuração de Responsabilidades e Aplicação de Sansão do Regulamento de Licitações e Contratos da CONTRATANTE.
- 10.4. Ocorrendo quaisquer das situações previstas, a CONTRATADA será notificada para fins de apresentação de justificativas, as quais deverão ser apresentadas no prazo estabelecido no respectivo documento.
- 10.5. As notificações e respostas poderão se dar via carta ou e-mail, conforme conveniência das partes.
- 10.6. A ausência de apresentação de justificativas ou não aceitação das mesmas pelo CONTRATANTE, importará na ratificação dos termos da notificação e aplicação das sanções previstas no Anexo V – Manual de Apuração de Responsabilidades e Aplicação de Sansão do Regulamento de Licitações e Contratos da CONTRATANTE.
- 10.7. As multas e outras penalidades aplicáveis só poderão ser relevadas nos casos de força maior ou caso fortuito, devidamente comprovado, mediante decisão fundamentada.
- 10.8. Na aplicação das penalidades previstas no contrato e no instrumento convocatório, será considerada pelo CONTRATANTE motivadamente, a gravidade da falta, seus efeitos, bem como os antecedentes da CONTRATADA, podendo deixar de aplicá-las, se admitidas as justificativas apresentadas de forma antecipada pela mesma.
- 10.9. As multas serão descontadas do pagamento devido pela CONTRATANTE ou cobradas diretamente da CONTRATADA, amigável ou judicialmente, podendo ainda ser aplicadas cumulativamente com as demais sanções previstas no Anexo V – Manual de Apuração de Responsabilidades e Aplicação de Sansão do Regulamento de Licitações e Contratos da CONTRATANTE.
- 10.10. A CONTRATADA estará sujeita às penalidades administrativas, civis e penais pelo descumprimento da obrigação assumida.

11. EXIGÊNCIA DE AMOSTRA NA EXECUÇÃO DO CONTRATO:

- 11.1. Não se aplica.

12. INCLUSÕES NO PREÇO:

- 12.1. Os preços constantes na PLANILHA DE PREÇOS UNITÁRIOS devem incluir as despesas de transporte para entrega nos locais indicados bem como todos os impostos, inclusive o ICMS e ISS, que estarão a cargo da CONTRATADA e demais informações definidas no contrato.

13. DOCUMENTAÇÃO TÉCNICA:

- 13.1. Não se aplica.