1. Identificação do processo:

1.1. Consulta pública para prospecção de uma solução Tecnológica

2. Objeto:

2.1. A Companhia de Tecnologia da Informação do Estado de Minas Gerais, CNPJ nº 16.636.540/0001-04, doravante denominada **CONTRATANTE**, comunica que está prospectando, junto às empresas interessadas, doravante denominadas **PROPONENTES**, a aquisição de um Appliance de Segurança Cibernética - Network and Detection Response - NDR, incluindo garantia com assistência técnica, capacitação e serviços técnicos de instalação e configuração com operação assistida.

2.2. Importante ressaltar que esta especificação técnica faz parte do processo de prospecção que atendam às necessidades da CONTRATANTE e em função disto é uma especificação simplificada e sujeita a críticas e sugestões de melhoria pelo mercado.

2.3. Nesta consulta estamos prospectando soluções em dois cenários distintos, conforme definidos no item “Detalhamento do Objeto”. Não há restrição, nesta prospecção, para as PROPONENTES apresentarem mais de uma proposta.

2.4. Para esta prospecção, solicitamos às PROPONENTES, mesmo que não atendam todos requisitos, que preencham os formulários definidos nos anexos I-A e I-F e informem quais requisitos não serão atendidos pelas soluções propostas e quais alternativas.

2.5. Após o envio dos formulários estaremos à disposição para nos reunirmos com os PROPONENTES com o objetivo de avaliarmos, em conjunto, as soluções apresentadas, além das críticas e sugestões encaminhadas.

3. Detalhamento do Objeto:

3.1. A solução de Segurança Cibernética - Network and Detection Response - NDR doravante denominado APPLIANCE, será disponibilizada na modalidade, ON-PREMISES.

3.2. Appliance é uma solução composta por hardware e software, programada para executar uma única e bem definida função.

3.2.1. Os appliances diferem dos computadores de uso geral pelo fato de que seu software é normalmente personalizado para a função que executam, pré-carregado pelo fornecedor e não alterável pelo usuário.” – Fonte: SNIA (Storage Networking Industry Association).

3.2.2. No caso específico deste termo de referência, o APPLIANCE pode ser comercializado como um único produto ou composto por dois produtos distintos (hardware e software), com preços segmentados, conforme cenários definidos no item “Cenários de prospecção” deste anexo.

3.2.3. Demais termos técnicos utilizados neste termo de referência estão definidos no glossário, item 26 deste anexo.

3.3. Além da disponibilização do APPLIANCE, a proposta deverá contemplar os serviços de Garantia com Assistência Técnica, capacitação técnica e serviços técnicos de instalação, configuração e operação assistida.

3.4. A infraestrutura de data center que irá hospedar o APPLIANCE é de responsabilidade da CONTRATANTE.

3.5. Cenários de prospecção

3.5.1. A contratação será em lote único, por cenário.

3.5.2. CENARIO 1 – Hardware e Software segmentados

Item	Produtos e Serviços	Direcionador	Quantidade
1	Hardware de acordo com requisitos detalhados no anexo I-F	Unidade	1
2	Software de acordo com requisitos detalhados no anexo I-F	Licença	1
3	Serviços técnicos de Instalação e configuração com operação assistida	Prestação de serviço	1
4	Garantia com assistência técnica para o Hardware com suporte, manutenção e atualização de firmware e software embarcado por 36 meses.	Prestação de serviço	1
5	Garantia com assistência técnica para o Software com suporte, manutenção e atualização de versão por 36 meses.	Prestação de serviço	1
6	Capacitação Técnica para 6 alunos	Turma	2

tabela 1a – cenário 1

3.5.3. CENARIO 2 – Hardware e Software como um único produto

Item	Produtos e Serviços	Direcionador	Quantidade
7	Appliance composto por hardware e software de acordo com requisitos detalhados no anexo I-F	Unidade	1
8	Serviços técnicos com instalação e configuração com operação assistida	Prestação de serviço	1
9	Garantia com assistência técnica do Appliance com suporte, manutenção e atualização de firmware e software embarcado por 36 meses.	Prestação de serviço	1
10	Capacitação Técnica para 6 alunos	Turma	2

tabela 1b – cenário 2

4. Especificação Técnica do objeto:

4.1. Itens 1, 2 e 7 - Requisitos técnicos e funcionais do APPLIANCE

4.1.1. A especificação técnica do hardware e software que compõem o APPLIANCE, incluindo sondas de inspeção de rede e acessórios, para os dois cenários, está detalhada no Anexo I-F, deste termo de referência.

4.2. Itens 3 e 8 - Serviços técnicos de instalação, configuração e operação assistida

4.2.1. Estes serviços compreendem o conjunto de atividades necessárias para tornar o APPLIANCE operacional e integrado ao ambiente de tecnologia da CONTRATANTE e com desempenho validado, de acordo os requisitos técnicos definidos no Anexo I-F.

4.2.1.1. Será de responsabilidade da CONTRATANTE a disponibilização da infraestrutura (servidores, rede, armazenamento, sistema operacional) necessária para instalação da SOLUÇÃO, exceto o hardware e software necessário para instalação da solução de software do

APPLIANCE e das sondas de inspeção, cujo fornecimento é de responsabilidade da CONTRATADA.

4.2.2. O processo de instalação e configuração com operação assistida será executado em conjunto com a equipe técnica da CONTRATANTE, com presença on-site da equipe técnica da CONTRATADA, em horário comercial (8x5), no data center da CONTRATANTE.

4.2.2.1. A instalação e configuração poderá também ser realizada remotamente, desde que acertado em comum acordo entre CONTRATANTE e CONTRATADA e sem ônus adicional para a CONTRATANTE.

4.2.3. O planejamento destas atividades deverá ser alinhado entre a CONTRATANTE e a CONTRATADA, em até 15 (quinze) dias úteis, após a assinatura do contrato.

4.2.4. A CONTRATADA deverá apresentar um plano de instalação física, contendo os requisitos dos circuitos elétricos e lógicos para conexão do APPLIANCE.

4.2.5. Instalação e configuração

4.2.5.1. A CONTRATADA deverá:

4.2.5.1.1. Instalar e customizar o APPLIANCE e as sondas de inspeção no ambiente de infraestrutura disponibilizado pela CONTRATANTE.

4.2.5.1.2. Definir e criar os usuários administradores e operadores.

4.2.5.2. Preparar e executar teste de arquitetura para validar se o ambiente instalado atende aos requerimentos definidos e solicitados.

4.2.5.2.1. Instalar e customizar, para efeito de validação da solução, com testes de backup e recovery na plataforma de backup da CONTRATANTE.

4.2.5.2.2. Gerar documentação detalhada de todos os passos da instalação, configuração e ajustes, no ambiente de produção, a qual deverá ser entregue em meio digital antes da emissão do atestado de aceite técnico.

4.2.6. Operação Assistida:

4.2.6.1. Após a instalação e configuração da SOLUÇÃO, a CONTRATADA deverá acompanhar a CONTRATANTE no uso dela, durante 10 (dez) dias úteis, período em que a CONTRATANTE poderá operar no sistema com acompanhamento da CONTRATADA.

4.2.6.2. A operação assistida permitirá a equipe técnica da CONTRATANTE, acompanhar os especialistas da CONTRATADA na configuração e operação da SOLUÇÃO e suas funcionalidades.

4.2.6.3. A data de início será combinada em comum acordo entre a CONTRATANTE e a CONTRATADA.

4.2.6.4. A CONTRATADA deverá alocar um especialista para atuar presencialmente junto a equipe da CONTRATANTE, em dias úteis, das 8:00 horas às 18:00 horas.

4.2.6.5. O acompanhamento poderá ser feito remotamente, desde que acertado em comum acordo entre CONTRATANTE e CONTRATADA e sem ônus adicional para a CONTRATANTE.

4.2.6.6. Deve fazer parte desta transferência de conhecimento:

4.2.6.6.1. Customizar o APPLIANCE no data center da CONTRATANTE;

4.2.6.6.2. Validar as rotinas de backup e restore do ambiente customizado.

4.2.6.6.3. Executar ajustes de desempenho do ambiente (tuning).

4.2.6.6.4. Definir métricas e indicadores que serão utilizados para avaliação de desempenho de forma a garantir níveis de serviços;

4.2.6.6.5. Integrar a console de monitoração da CONTRATANTE, via SNMP, com sistema de alarmes da SOLUÇÃO.

4.2.7. Estes serviços técnicos de instalação, configuração e operação assistida somente serão finalizados com a emissão do laudo técnico,

pela PRODEMGE, atestando a execução dos serviços de acordo com os requisitos definidos neste termo de referência e seus anexos.

4.3. Itens 4, 5 e 9 - Garantia com assistência técnica

4.3.1. Durante o período de garantia a CONTRATADA deverá prestar assistência técnica com suporte técnico e manutenção.

4.3.2. A CONTRATADA deverá prestar suporte técnico de forma remota, por telefone, videoconferência, autoatendimento e e-mail.

4.3.2.1. Para os chamados de emergência (gravidade 1 e 2, conforme definido no item “Níveis de serviços” deste termo de referência), o serviço será prestado em regime 24 x 7, todos dias da semana, incluindo finais de semana e feriados.

4.3.2.2. Os demais chamados serão prestados em horário comercial, 8 x 5 (somente dias úteis).

4.3.2.3. Somente serão considerados os feriados oficiais Nacionais, do Estado de Minas Gerais e do Município de Belo Horizonte.

4.3.2.4. O suporte deverá ser prestado em Português.

4.3.3. A CONTRATADA deverá disponibilizar toda a documentação técnica necessária à adequada utilização da solução proposta, os manuais, os guias técnicos e suas atualizações, em Português e/ou Inglês.

4.3.4. Suporte Técnico

4.3.4.1. A CONTRATADA deverá apoiar a equipe técnica da PRODEMGE na configuração e uso da solução proposta no conhecimento da arquitetura e de suas funcionalidades, esclarecendo dúvidas a respeito de configurações, ajustes (tuning), monitoramento e segurança no uso da solução proposta.

4.3.5. Manutenção:

4.3.5.1. O serviço de manutenção consiste no conjunto de ações necessárias para restaurar as condições de

funcionamento dos equipamentos, garantindo alto desempenho e permitindo a sua utilização na capacidade máxima, com solução de eventuais problemas, danos ou defeitos existentes no equipamento, contemplando:

4.3.5.1.1. Correções de erro de código para corrigir desvios das especificações então aplicáveis que tenham sido relatados, sem ônus adicional para a CONTRATANTE.

4.3.5.1.2. Atualizações de código: com distribuição periódica de correções de código, aprimoramentos funcionais (inclusive modificações para cumprir exigências governamentais), podendo compreender atualizações de contingência, pacotes de serviços, novas versões e releases, sem ônus adicional para a CONTRATANTE.

4.3.5.1.3. Substituição de componentes de hardware, sondas de rede e acessórios defeituosos, sem ônus adicional para a CONTRATANTE.

4.3.5.2. Estes serviços podem ser executados de forma proativa, desde que devidamente comunicado, ou após a abertura de um chamado técnico pela CONTRATANTE.

4.3.5.3. Durante a execução dos serviços de suporte técnico ou de manutenção preventiva ou de atendimento a um incidente, caso seja identificada a necessidade de substituição de peças e, acessórios a CONTRATADA deverá substituí-los sem ônus adicional para a CONTRATANTE, conforme definido no item “Substituição de peças e componentes” deste anexo.

4.3.5.4. Para a execução dos serviços a CONTRATADA deverá:

4.3.5.4.1. Identificar falhas e defeitos e executar serviços especializados de manutenção nos equipamentos, para restabelecer as perfeitas condições de uso, permitindo sua utilização na capacidade máxima.

4.3.5.4.2. Realizar suporte remoto via internet, sempre que o equipamento apresentar problema operacional relacionado ao software, ou de forma presencial, caso o

problema não seja sanado, conforme definido nas cláusulas de níveis de serviços, detalhados deste anexo.

4.3.5.4.3. Identificar componentes de hardware, sondas de rede e acessórios que devem ser substituídos e de software que devem ser atualizados e agendar com a CONTRATANTE a manutenção e/ou substituição.

4.3.5.4.4. Durante a vigência do contrato caberá à CONTRATADA, manter em perfeito estado de uso, bem como reparar ou substituir sem ônus para a CONTRATANTE, quaisquer equipamentos e peças que acusem defeito de fabricação, instalação e programação conforme disposto neste termo de referência.

4.3.5.5. O prazo de subscrição de todo o conjunto de software embarcado nos equipamentos (BIOS, firmware, console) deve ser igual a vigência do contrato. Durante a vigência do contrato, a CONTRATANTE terá direito a atualização da versão dos softwares e patches de correção. Caberá à CONTRATADA a disponibilização destas novas versões. A atualização será realizada pela CONTRATANTE com suporte da CONTRATADA;

4.3.6. Substituição de Peças e Componentes:

4.3.6.1. A CONTRATADA deverá utilizar exclusivamente peças novas e compatíveis com as especificações do fabricante dos equipamentos, vedada à utilização de itens recondicionados ou remanufaturados.

4.3.6.2. Na impossibilidade de fornecimento do componente original e antes de realizar qualquer alteração da especificação técnica, a CONTRATADA deverá elaborar justificativa dirigida à CONTRATANTE, informando os motivos que levaram à necessidade da alteração da configuração original do equipamento e solicitando autorização para esta alteração no procedimento.

4.3.6.3. Antes de serem utilizadas, as peças novas deverão ser apresentadas à CONTRATANTE para que a mesma ateste se ela atende aos requisitos definidos neste instrumento.

4.3.6.3.1. As peças novas deverão manter a garantia, de acordo com a vigência do contrato.

4.3.6.3.2. Durante a vigência do contrato, a CONTRATADA obriga-se a reparar as falhas e substituir, às suas expensas, incluindo o serviço de técnico, a peça defeituosa, sem custos adicionais para a CONTRATANTE, desde que não sejam decorrentes de utilização indevida pela CONTRATANTE.

4.3.6.3.3. É de responsabilidade da CONTRATADA o ônus da prova da origem das falhas.

4.3.6.3.4. A substituição de peças e componentes deverá ocorrer em, no máximo, 8 (oitos) horas úteis após notificação formal pela CONTRATANTE, sem prejuízo para os prazos definidos no item “Níveis de serviços”, deste anexo.

4.3.6.3.5. Todos os itens de material rejeitados em inspeção devem ser substituídos, por conta da CONTRATADA, sem nenhum ônus para a CONTRATANTE.

4.3.6.3.6. A rejeição de qualquer material ou serviço, em virtude de falhas constatadas, não dispensa a CONTRATADA de cumprir as datas de entrega prometidas.

4.3.6.3.7. Se a rejeição tornar impraticável a entrega da solução contratada nas datas previstas, ou se tornar evidente que a CONTRATADA não será capaz de satisfazer as exigências estabelecidas nesta especificação, a CONTRATANTE se reserva o direito de rescindir todas as suas obrigações e de obter materiais e serviços de outro fornecedor. Em tais casos, a CONTRATADA será considerada infratora do contrato e estará sujeita às penalidades aplicáveis.

4.3.6.3.8. Caso os serviços de manutenção não possam ser executados nas dependências da CONTRATANTE, o procedimento de retirada das peças ou equipamentos para reparos, mesmo que o conserto seja realizado em outro local, será de inteira responsabilidade da CONTRATADA, inclusive o ônus integral do transporte

e seguro. A retirada do equipamento somente poderá ser efetuada após a autorização da CONTRATANTE e assinatura de um respectivo Termo de Responsabilidade.

4.3.6.4. A CONTRATADA deverá incluir no preço dos serviços ofertados todos os custos de mão de obra e peças necessários, incluindo encargos e despesas de transporte, translado e alimentação de sua equipe.

4.4. Itens 6 e 10 – Serviços de capacitação

4.4.1. Estes serviços têm como objetivo capacitar a equipe técnica da CONTRATANTE no uso do APPLIANCE, nos ajustes (tuning), segurança, administração e uso das funcionalidades.

4.4.2. As capacitações deverão ser ministradas de forma remota, ao vivo, em turma fechada para a CONTRATANTE, utilizando uma solução de videoconferência que permita a participação e interação dos participantes, sendo de responsabilidade da CONTRATADA o fornecimento de toda a infraestrutura (incluindo de videoconferência) necessária para o instrutor.

4.4.3. A CONTRATADA poderá realizar a capacitação de forma presencial, em comum acordo, desde que sem ônus adicional para a CONTRATANTE.

4.4.3.1. Seja remoto ou presencial, os custos com material, plataforma de capacitação, instrutor, hospedagem, alimentação, passagens e translado são de responsabilidade da CONTRATADA.

4.4.3.2. A CONTRATADA deverá disponibilizar um laboratório para realização do treinamento, com acesso via INTERNET. A capacitação não pode fazer uso do equipamento entregue.

4.4.4. A CONTRATADA deverá submeter à CONTRATANTE, em até 5 (cinco) dias úteis anteriores à data de realização de cada módulo da capacitação, os seguintes entregáveis:

4.4.4.1. Plano da capacitação, incluindo carga horária, conteúdo programático e 12 (doze) questões para avaliação dos

alunos. As questões devem ser objetivas, com quatro alternativas de respostas e apenas uma correta, no idioma português. Devem ser de nível intermediário e permear todo o conteúdo programático do curso.

4.4.4.2. Material didático, que deverá ser disponibilizado em idioma português ou inglês, que contenha todos os assuntos abordados, o qual deverá ser analisado e aprovado pela CONTRATANTE.

4.4.4.3. A CONTRATADA deverá disponibilizar as instruções do treinamento em mídia eletrônica, em formato HTML ou PDF, ilustrado com imagens para que a PRODEMGE possa fazer a divulgação interna.

4.4.4.4. Será facultado à CONTRATANTE proceder com a gravação das aulas em vídeo, registrando a imagem do instrutor e o conteúdo projetado aos alunos, de forma possibilitar a capacitação futura de seus profissionais que porventura venham a ser alocados às atividades objeto das capacitações.

4.4.5. A entrega dos materiais deve acontecer por meio digital para a Gerência de Desenvolvimento de Pessoas através do e-mail capacitar@prodemge.gov.br.

4.4.5.1. A CONTRATANTE irá proceder com a avaliação do material didático e das qualificações dos instrutores em até 5 (cinco) dias úteis.

4.4.5.2. Caso julgue ser necessário algum ajuste no material didático ou no conjunto de instrutores, a CONTRATANTE solicitará a adequação formalmente à CONTRATADA que, a partir de então, deverá promover os ajustes necessários em até 5 (cinco) dias úteis.

4.4.5.3. A todo o material de capacitação entregue, disponibilizado e utilizado pela CONTRATADA para a execução dos serviços de capacitação, incluindo material de apoio, como apresentações, apostilas, manuais, vídeos de demonstração, dentre outros correlatos, serão concedidos o direito de uso e de reprodução à CONTRATANTE, de forma irrestrita, para

sua aplicação e uso em capacitações internos para seus colaboradores.

4.4.5.4. Relação dos profissionais que irão ministrar a capacitação doravante denominados instrutores, acompanhado por documentação que comprove que são capacitados.

4.4.6. O treinamento não poderá ser meramente expositivo, devendo contemplar o uso prático da solução proposta e o desenvolvimento de estudos de caso. O conteúdo programático deverá abranger, no mínimo, os seguintes requisitos:

4.4.6.1. Introdução teórica das funcionalidades do APPLIANCE

4.4.6.2. Instalação do APPLIANCE no ambiente da CONTRATANTE.

4.4.6.3. Administração, segurança, configuração, ajustes (tuning) e monitoração do APPLIANCE.

4.4.6.4. Uso das funcionalidades do APPLIANCE.

4.4.6.5. Estudos de caso.

4.4.7. O programa de treinamento deverá prever a capacitação do corpo técnico, para 6 (seis) especialistas.

4.4.8. Serão aceitos cursos oficiais ou não oficiais do fabricante do software do APPLIANCE.

4.4.8.1. Para o curso não oficial, este deverá possuir a mesma carga horária e ementa do curso oficial.

4.4.8.1.1. Neste caso a PROPONENTE deverá proceder a gravação da capacitação e ceder as aulas em vídeo para a CONTRATANTE.

4.4.9. O planejamento da capacitação deverá ser alinhado entre a PRODEMGE e CONTRATADA, em até 15 (quinze) dias corridos, após a assinatura do contrato.

4.4.10. Avaliação e critério de aceite da capacitação.

4.4.10.1. Ao final do treinamento, os alunos devem estar aptos a utilizar os recursos da solução proposta.

4.4.10.2. A CONTRATADA deverá aplicar avaliação de conhecimento, baseado nas questões entregues para mensurar o aproveitamento dos alunos na capacitação em questão. Os resultados deverão ser entregues em formato de relatório à CONTRATANTE.

4.4.10.3. A CONTRATADA deverá emitir, ao final do treinamento, o certificado de conclusão para cada participante, no qual deverão constar a identificação do treinando, o período de realização, o conteúdo e a carga horária do treinamento;

4.4.10.4. Após a realização de cada uma das turmas de capacitação, e tendo sido a capacitação aprovada, a CONTRATANTE emitirá o “Laudo técnico de execução de serviços” (anexo I-E) atestando a execução da capacitação da turma.

4.4.10.5. Caso a qualidade do treinamento em alguma turma seja considerada insatisfatória pela maioria simples dos alunos, a PRODEMGE poderá exigir que o mesmo seja refeito, sem ônus para a PRODEMGE, no prazo máximo de até 10 (dez) dias úteis após a notificação;

5. Detalhes dos Itens do Objeto:

5.1. Marca e Modelo:

5.1.1. Não se aplica.

5.2. Justificativa de Marca e Modelo:

5.2.1. Não se aplica.

5.3. Forma de Entrega

5.3.1. A CONTRATADA deverá enviar, via e-mail gga@prodemge.gov.br ou correspondência, o acesso ao site do fabricante, e-mail e telefone de

contato para acesso aos serviços de suporte e para download do conjunto de software embarcado na solução proposta, atualizações de versões, *releases* e manuais.

5.3.2. A CONTRATADA deverá fornecer as licenças de software de forma eletrônica, evitando a confecção e transporte de mídias, a partir do acesso ao site do fabricante para download;

5.3.2.1. A entrega de cada software será caracterizada pela disponibilização das credenciais de acesso e das licenças, com seus respectivos quantitativos, no site do fabricante, em área de acesso exclusivo da CONTRATANTE, por meio de utilização de credenciais especificas;

5.3.2.2. Como alternativa o fornecedor poderá também liberar o acesso ao portal do fabricante através de uma conta da Prodemge, identificada pelo email gga@prodemge.gov.br.

5.3.3. Todos os produtos de hardware, sondas de inspeção e acessórios contratados devem estar acondicionados em embalagens apropriadas para o transporte, de acordo com as recomendações dos fabricantes;

5.3.4. A CONTRATADA deverá entregar toda a documentação técnica necessária à adequada instalação e utilização dos equipamentos.

5.3.5. As embalagens devem ser indelevelmente identificadas com as seguintes informações:

5.3.5.1. Nome do fabricante ou marca do produto;

5.3.5.2. Designação do tipo, modelo ou equivalente;

5.3.5.3. Número de série;

5.3.5.4. O nome da empresa licitante, o número do pregão e do item a que se referem;

5.3.5.5. Posição de transporte e instruções de manuseio;

5.3.5.6. Massa total do volume em quilogramas.

5.3.5.7. Instruções para o correto acondicionamento e manuseio.

5.3.6. Processo de recepção técnica dos equipamentos, software e serviços

5.3.6.1. A CONTRATANTE deverá efetuar a recepção técnica da entrega do hardware/software, sondas de inspeção, acessórios e execução de serviços e emitir laudo atestando a entrega correta ou não.

5.3.6.2. A CONTRATANTE terá até 5 (cinco) dias úteis para emitir o laudo.

5.3.6.3. Ocorrendo problemas na recepção, a CONTRATADA terá o prazo de 10 (dez) dias úteis, a partir da data da recepção para solução das pendências.

5.3.6.3.1. Todos os itens rejeitados em inspeção devem ser substituídos, por conta da CONTRATADA, sem nenhum ônus para a CONTRATANTE.

5.3.6.3.2. A rejeição de qualquer material ou serviço, em virtude de falhas constatadas, não dispensa a CONTRATADA de cumprir as datas de entrega prometidas.

5.3.6.4. Se a rejeição tornar impraticável a entrega dos equipamentos ou dos serviços contratados nas datas previstas, ou se tornar evidente que a CONTRATADA não será capaz de satisfazer as exigências estabelecidas nesta especificação, a CONTRATANTE se reserva o direito de rescindir todas as suas obrigações e de obter materiais e serviços de outro fornecedor.

5.3.6.4.1. Em tais casos, a CONTRATADA será considerada infratora do contrato e estará sujeito às penalidades aplicáveis.

5.3.6.5. O aceite ou aprovação do objeto desta licitação, não exclui a responsabilidade civil nem a ético-profissional da CONTRATADA por vícios de quantidade, qualidade ou disparidades com as especificações estabelecidas

neste Edital verificadas posteriormente, garantindo-se à Administração Pública as faculdades previstas no Art. 18 da Lei nº. 8.078/90 – Código de Defesa do Consumidor.

5.3.7. Critérios de aceitabilidade das entregas.

5.3.7.1. **ENTREGA 1** – APPLIANCE (correspondente aos itens 1 e 2 do cenário 1 e item 7 do cenário 2).

5.3.7.1.1. Para aceite do APPLIANCE haverá uma recepção técnica na etapa de instalação, configuração e testes (entrega 3).

5.3.7.2. Somente será considerado o aceite, mediante a apresentação do documento “Laudo técnico de fornecimento do APPLIANCE”, constante do Anexo I-C e de acordo com o processo de recepção técnica definido no item “Processo de recepção técnica dos equipamentos, software e serviços” deste anexo.

5.3.7.2.1. O aceite da entrega estará vinculado ao aceite do Laudo de execução dos serviços técnicos de instalação, configuração e operação assistida do APPLIANCE, conforme definido na entrega 2.

5.3.7.2.2. O prazo da entrega será avaliado pelo indicador de qualidade detalhado no item “Níveis de serviço” deste anexo.

5.3.7.2.3. O aceite não será fracionado.

5.3.7.3. **ENTREGA 2** - Serviços técnicos de instalação, configuração e operação assistida (item 3 do cenário 1 e item 8 do cenário 2)

5.3.7.3.1. Estes serviços somente serão considerados entregues após a realização de testes comprovando a execução dos serviços e o aceite da CONTRATANTE, mediante a apresentação do documento “Laudo Técnico de Execução de Serviços”, constante do Anexo I-E, atestando a realização da totalidade dos serviços previstos e atendimento aos critérios definidos no item

"Processo de recepção técnica dos equipamentos, software e serviços", deste anexo.

5.3.7.3.2. O prazo de finalização deste serviço será avaliado pelo indicador de qualidade detalhado no item "Níveis de serviços", deste anexo.

5.3.7.3.3. O aceite não será fracionado.

5.3.7.4. **ENTREGA 3** - Garantia com assistência técnica (itens 4 e 5 do cenário 1 e item 9 do cenário 2)

5.3.7.4.1. O serviço somente terá seu início após o aceite da instalação, configuração e testes do APPLIANCE (entrega 3). Os serviços de assistência técnica serão prestados mensalmente, durante 36 (trinta e seis) meses.

5.3.7.4.2. Nos chamados de gravidade 1, 2 e 3 a CONTRATADA deverá emitir, ao final do atendimento, o "Laudo Técnico de execução de serviços de assistência técnica", conforme detalhado no anexo I-B, deste termo de referência.

5.3.7.4.3. Mensalmente a CONTRATADA deverá enviar à CONTRATANTE o relatório de apuração de níveis de serviços, conforme detalhado no item "Níveis de serviços" e no anexo I-D, deste termo de referência.

5.3.7.4.4. Os serviços prestados serão avaliados mensalmente conforme indicadores de qualidade detalhados no item "Níveis de serviços".

5.3.7.5. **ENTREGA 4** - Serviços de capacitação (item 6 no cenário 1 e item 10 no cenário 2)

5.3.7.5.1. Somente serão considerados entregues após a aprovação do curso de acordo com os requisitos definidos no item "Avaliação e critério de aceite da capacitação", deste anexo, com a emissão do certificado de conclusão e com o aceite da CONTRATANTE.

5.3.7.5.2. O aceite dos serviços de capacitação será após a conclusão da turma treinada, mediante a apresentação do documento “Laudo Técnico de Execução de Serviços”, constante do Anexo I-E, atestando a realização da totalidade dos serviços previstos

5.4. Local de Entrega/Execução dos serviços

5.4.1. Todos os equipamentos deverão ser entregues nas dependências da Prodemge, localizada na Rua da Bahia, 2277 – CEP 30.160-019, Bairro Savassi - Belo Horizonte/MG.

5.4.2. As entregas deverão ser realizadas em horário comercial, de 2ª a 6ª feira, com agendamento prévio de 3 (três) dias úteis, com a Gerência de Gestão de Ativos, através do telefone (31) 3339-1257 e e-mail: gga@prodemge.gov.br

5.4.3. A entrega de cada software será caracterizada pela disponibilização das credenciais de acesso e das licenças, com seus respectivos quantitativos, no site do fabricante, em área de acesso exclusivo da CONTRATANTE, por meio de utilização de credenciais especificas;

5.4.4. Todos os serviços serão prestados de forma remota, via videoconferência ou presencialmente nas dependências da Prodemge, de acordo com requisitos definidos em cada serviço.

5.4.5. Os dados de contato deverão ser repassados conforme definido no item 5.3.1 deste anexo.

5.5. Prazo de Entrega/Execução

5.5.1. Em até 7 (sete) dias úteis após a assinatura do contrato deverá ser agendada reunião, entre a CONTRATANTE e a CONTRATADA, para definição do cronograma da prestação dos serviços, devendo o cronograma estar ajustado entre as partes em até 7 (sete) dias úteis após a reunião.

5.5.1.1. Caberá à CONTRATADA elaborar o planejamento para estas atividades.

5.5.1.2. Nessa reunião serão definidos os pré-requisitos necessários para a instalação, configuração,

capacitação e operação assistida do APPLIANCE e o cronograma dos trabalhos envolvendo as equipes da CONTRATANTE e da CONTRATADA.

5.5.2. Devem ser observados os seguintes prazos máximos definidos nos itens abaixo, para o fornecimento dos produtos e a execução dos serviços.

5.5.3. ENTREGA 1 – APPLIANCE (itens 1 e 2 do cenário 1 e item 7 do cenário 2)

5.5.3.1. Prazo de entrega do equipamento, sondas de inspeção, acessórios e software: máximo de **60 (sessenta) dias corridos** após assinatura do contrato.

5.5.3.2. Não será aceito a entrega parcial.

5.5.3.3. O processo de aceite desta entrega somente terá seu início após o aceite dos serviços de instalação, configuração e operação assistida (entrega 2).

5.5.4. ENTREGA 2 – Instalação, configuração e operação assistida (item 3 do cenário 1 e item 8 do cenário 2)

5.5.4.1. O prazo para execução destes serviços não poderá ultrapassar 30 (trinta) dias úteis após a entrega do APPLIANCE (Entrega 1)

5.5.4.2. O prazo para o aceite destes serviços será de 5 (cinco) dias úteis após o término do serviço, conforme processo definido no item “Processo de recepção técnica dos equipamentos, software e serviços”, deste anexo.

5.5.4.3. Ocorrendo problemas na execução dos serviços, a CONTRATADA deverá manter a operação assistida até a solução de todas pendências.

5.5.5. ENTREGA 3 – Garantia com assistência técnica (itens 4 e 5 do cenário 1 e item 9 do cenário 2)

5.5.5.1. Prazo para prestação de serviços: mensalmente, com a vigência de 36 (trinta e seis) meses a partir do aceite técnico da entrega 3 (instalação, configuração e testes).

5.5.6. ENTREGA 4 – Capacitação

5.5.6.1. As capacitações para os usuários deverão ser ministradas após a instalação, configuração e operação assistida (entrega 3).

5.5.6.2. Ocorrendo problemas na capacitação, a CONTRATADA deverá atender os critérios definidos no item “Avaliação e critério de aceite da capacitação”, deste anexo.

5.6. Validade dos produtos

5.6.1. O hardware, incluindo sondas de inspeção de rede e acessórios e software terão a validade da garantia de 36 (trinta e seis) meses após o aceite da recepção técnica (entrega 1).

5.7. Condições de pagamento

5.7.1. **ENTREGA 1** – APPLIANCE (itens 1 e 2 do cenário 1 e item 7 do cenário 2)

5.7.1.1. Não haverá pagamento pela entrega do APPLIANCE, até o aceite da instalação, configuração e operação assistida”. A CONTRATANTE pagará à CONTRATADA, conforme detalhado no item “Demais condições de pagamento”, em parcela única. O pagamento somente será efetuado, após o aceite dos laudos e relatórios abaixo relacionados:

5.7.1.1.1. Do documento "Laudo técnico de fornecimento de APPLIANCE" (anexo I-C).

5.7.1.1.2. Do documento “Laudo técnico de execução de serviços” (anexo I-E), referente ao aceite dos serviços e instalação, configuração e operação assistida (Entrega 3) realizados.

5.7.1.1.3. Do aceite do relatório de apuração de níveis de serviços (anexo I-D) referente ao indicador definido no item “Níveis de serviços”, com o desconto no pagamento, se for o caso.

5.7.1.2. A CONTRATANTE pagará à CONTRATADA, conforme detalhado no item “Demais condições de pagamento.

5.7.1.3. Não será admitido fracionamento na entrega.

5.7.2. **ENTREGA 2** - Serviços de instalação, configuração e operação assistida (item 3 do cenário 1 e item 8 do cenário 2).

5.7.2.1. A CONTRATANTE pagará à CONTRATADA, conforme detalhado no item “Demais condições de pagamento”, em parcela única após a emissão e ateste:

5.7.2.2. Do documento “Laudo técnico de execução de serviços” (anexo I-E), referente ao aceite dos serviços realizados.

5.7.2.3. Do aceite do relatório de apuração de níveis de serviços (anexo I-D) referente ao indicador definido no item “Níveis de Serviços, deste anexo, com o desconto no pagamento, se for o caso.

5.7.2.4. Não será admitido fracionamento na entrega.

5.7.3. **ENTREGA 3** - Pela garantia com assistência técnica (itens 4 e 5 do cenário 1 e item 9 do cenário 2).

5.7.3.1. A CONTRATANTE pagará à CONTRATADA em 36 (trinta e seis) parcelas mensais, iguais e sucessivas, conforme detalhado no item “Demais condições de pagamento” após a emissão e ateste do relatório de apuração de níveis de serviços (anexo I-D), referente aos indicadores definidos no item “Níveis de serviços”, com o desconto no pagamento, se for o caso.

5.7.3.2. Os serviços somente terão seu início com o aceite da instalação, configuração e operação assistida do APPLIANCE (Entrega 2).

5.7.4. **ENTREGA 4** - Serviços de capacitação (item 6 do cenário 1 e item 10 do cenário 2).

5.7.4.1. Serão faturados após conclusão da turma, conforme detalhado no item “Demais condições de pagamento”, após a emissão do aceite da capacitação, pela CONTRATANTE, através do ateste do documento “Laudo técnico de execução de serviços” (anexo I-E).

5.7.4.2. Não será admitido fracionamento na entrega da turma.

5.7.5. Demais condições de pagamento:

5.7.5.1. Nenhum serviço ou entrega será considerado executado e nenhum pagamento será efetivado sem que a Unidade Administrativa da PRODEMGE responsável pelo acompanhamento ateste que o mesmo foi correta e integralmente prestado.

5.7.5.2. Para as entregas 3, 4, 5, 6, 8, 9, 10:

5.7.5.2.1. Os documentos de cobrança deverão ser emitidos e entregues até o dia 25 (vinte e cinco) no mês da efetiva prestação do serviço e de seu aceite. O vencimento será programado em até 30 (trinta) dias após o seu recebimento no Correio Central da PRODEMGE, na Rua da Bahia, nº 2.277, Bairro Savassi, CEP 30.160-019, Belo Horizonte/MG.

5.7.5.3. Para as entregas 1, 2 e 7:

5.7.5.3.1. Os documentos de cobrança deverão ser emitidos e entregues até o dia 25 (vinte e cinco) do mês subsequente ao da efetiva entrega dos produtos e de seu aceite. O vencimento será programado em até 30 (trinta) dias após o seu recebimento no Correio Central da PRODEMGE, na Rua da Bahia, nº 2.277, Bairro Savassi, CEP 30.160-019, Belo Horizonte/MG.

5.7.5.4. O atraso na entrega do documento de cobrança implicará prorrogação do vencimento em tantos dias úteis quantos forem os dias de atraso.

5.7.5.5. Não será aceito, pela CONTRATANTE, a cobrança de eventuais diferenças vinculadas a questões trabalhistas, tais como férias, horas extras, sobreaviso etc., bem como os gastos provenientes de deslocamento, estadia e alimentação, caso sejam necessários.

5.8. Prazo de Garantia/Assistência Técnica

5.8.1. O prazo de garantia e assistência técnica será de 36 (trinta e seis) meses para o APPLIANCE e todos seus acessórios, software e sondas de inspeção de rede. Os serviços terão seu início após o aceite da instalação, configuração e operação assistida (entrega 2).

5.8.2. Optou-se pelo prazo de 36 (trinta e seis) meses de garantia, por se tratar de um equipamento de uso corporativo pela Prodemge, com segurança e disponibilidade, sendo essencial para o bom funcionamento e segurança do data center da companhia.

5.9. Amostras/Prova de Conceito

5.9.1. Não se aplica.

6. Justificativa de contratação

6.1. Não se aplica na prospecção.

7. Justificativa da modalidade

7.1. Não se aplica na prospecção.

8. Justificativa para agrupamento dos itens em um único lote

8.1. Não se aplica na prospecção

9. Justificativa de quantitativos

9.1. Não se aplica na prospecção

10. Visita técnica

Não se aplica.

11. Qualificação Técnica:

11.1. A PROPONENTE classificada em primeiro lugar, no processo licitatório, deverá apresentar, para qualificação técnica, atestado(s) de capacidade técnica, fornecido(s) por pessoa jurídica de direito público ou privado, que comprove(m) que a mesma já disponibilizou, satisfatoriamente, APPLIANCE(s) de Network Detection and Response (NDR).

11.1.1. Será considerado similar ao objeto a entrega de um Appliance, com um mínimo de capacidade para processamento conforme itens 4.8.43 e subitens. Atestando, inclusive, o bom desempenho e cumprimento a contento das obrigações contratuais..

11.1.2. Todos os atestados apresentados deverão conter, obrigatoriamente, a especificação dos serviços executados, o nome, o cargo, e a empresa do declarante.

11.2. Todos os atestados, documentos e certificações emitidos em idioma diferente do português ou inglês, deverão ser acompanhados de traduções, simples ou juramentadas.

12. Critérios de aceitabilidade da proposta

12.1. Não se aplica nesta prospecção.

13. Cronograma físico-financeiro

13.1. Não se aplica.

14. Níveis de Serviço

14.1. A CONTRATADA oferecerá, dentro do período de contrato, os serviços de ASSISTÊNCIA TÉCNICA por meio de telefone e e-mail, em idioma português do Brasil, durante o período do contrato.

14.2. O serviço compreende o diagnóstico e identificação de problemas, apoio técnico na utilização, correção de erros, defeitos (bugs) ou mau funcionamento sobre qualquer funcionalidade, recurso, componente ou módulo disponível de forma nativa na solução, ou decorrente de qualquer adaptação (customização) e ajuste (tuning) efetuada pela CONTRATADA.

14.3. O atendimento a um chamado de suporte técnico deverá ocorrer por qualquer uma das seguintes formas:

14.3.1. Atendimento presencial no local de instalação do software (on-site);

14.3.2. Acesso remoto;

14.3.3. Contato telefônico;

14.3.4. Videoconferência;

14.3.5. Envio de mensagem eletrônica (e-mail); ou

14.3.6. Acesso a site web com controle de acesso por senha.

14.4. O serviço de atendimento e gerenciamento de chamados da CONTRATADA deverá funcionar em regime 24 x 7, todos os dias, incluindo finais de semana e feriados.

14.4.1. Toda solução deverá ter suporte centralizado em uma única central de atendimento tanto para o hardware, sondas de rede, acessórios quanto para software.

14.4.2. O serviço deve garantir à CONTRATANTE o pleno acesso aos sites dos fabricantes dos produtos ofertados (hardware e software), incluindo a aberturas de chamados técnicos e consultas a quaisquer bases de dados disponíveis para usuários/clientes, e também efetuar downloads de quaisquer atualizações de software ou documentação.

14.4.3. Importante ressaltar que a CONTRATADA sempre será a responsável contratualmente pelos serviços.

14.5. A CONTRATADA realizará a prestação de serviços de atendimento por telefone, e-mail ou internet, para orientações em casos de dúvidas e/ou problemas em programas, assistindo remotamente a CONTRATANTE no uso e instalação de programas específicos e nos sistemas operacionais para produtos suportados e com versões correntes.

14.6. O atendimento telefônico sempre que aplicável e viável, deverá ser realizado no idioma português do Brasil, por meio de ligação local em Belo Horizonte/MG ou ligação interurbana gratuita (0800) e deverá ter um único número de contato para todos os produtos do APPLIANCE.

14.7. A CONTRATANTE poderá efetuar um número ilimitado de chamados técnicos para a CONTRATADA, por qualquer uma das formas disponíveis, durante a vigência do contrato.

14.8. Na abertura ou registro de um chamado técnico, por qualquer uma das formas disponíveis, a CONTRATANTE deverá informar: descrição da solicitação, nível de severidade e identificação completa do solicitante.

14.9. Cada chamado técnico será classificado em um dos 4 (quatro) graus de gravidade, de acordo com a tabela abaixo:

Gravidade	Descrição
1	**Solução inoperante** Significa situação da solução ofertada inoperante com impacto em um ambiente de produção para o qual não há uma Solução Alternativa imediatamente disponível, como: (i) queda do serviço de produção ou de outros sistemas de missão crítica devido à falta dos serviços ofertados pela solução contratada; (ii) uma parte substancial de dados de missão crítica apresentar risco de perda ou de ser corrompido; (iii) perda substancial de serviço; (iv) as operações comerciais serem seriamente interrompidas; Significa um problema em que a solução cause falha catastrófica que comprometa a integridade do ambiente em geral ou a integridade dos dados ou quando estiver em operação (ou seja, travamento do sistema, perda ou corrompimento de dados, ou perda de segurança do sistema), e que impacte significativamente as operações contínuas em um ambiente de produção.
2	**Problema Grave** Significa uma situação comercial de alto impacto que possivelmente coloque em risco um ambiente de produção. A solução ofertada pode operar, mas apresenta graves restrições

3	**Problema Leve** Significa uma situação comercial de baixo impacto, podendo a maioria das funções da solução ainda ser usada; entretanto, alguma intervenção pode ser necessária para a prestação dos serviços.
4	**Solicitação de Informações** Significa (i) problema ou questão secundários que não afete o funcionamento do software, (ii) um erro na documentação do produto que não tenha efeito significativo sobre as operações; (iii) uma sugestão para novos recursos ou aperfeiçoamento do produto (iv) consulta técnica sobre funcionalidades / operação da solução ofertada

Tabela 2 – Níveis de Gravidade

14.10. Cobertura

14.10.1. Modalidade 24x7x365 para severidades 1 e 2.

14.10.2. Modalidade 8x5 para as severidades 3 e 4.

14.11. A tabela a seguir apresenta os prazos máximos, contados a partir abertura do chamado, a serem atendidos pela CONTRATADA para cada grau de severidade:

Severidade	**Tempo de Atendimento**	
	Tempo para o primeiro contato a partir da abertura do chamado	Tempo de Solução, após a abertura do chamado
1	2 horas corridas	Até 6 horas corridas
2	2 horas corridas	Até 12 horas corridas
3	4 horas úteis	Até 16 horas úteis
4	4 horas úteis	Até 24 horas úteis

Tabela 3 – Tempo de atendimento

14.12. Indicadores de Qualidade

14.12.1. Prazo de Entrega do APPLIANCE (itens 1 e 2 do cenário 1 e item 7 do cenário 2)

ICPE – Índice de Cumprimento de Prazo de ENTREGA	
Atributo	**Valor**
Descrição	Mede a quantidade de dias de atraso na entrega, no data center da PRODEMGE, da solução proposta.
Objetivo	Reduzir o risco de atrasos na entrega da solução proposta
Meta	Prazo de entrega menor ou igual **a 60 (sessenta) dias corridos após a assinatura do contrato**
Periodicidade	Uma medição após a entrega do APPLIANCE
Unidade de Representação	Dias corridos de atraso
Forma de Cálculo	**ICPE = NDA**, **Onde:** NDA = Número de dias corridos de atraso na finalização da atividade.
Mecanismo de Medição e Gestão	**Ao final do 90º. dia corrido, após a assinatura do contrato, o** Fiscal deverá verificar se o foi realizada ou não. Se o serviço foi concluído, não haverá penalidade. Mas, se o serviço não foi concluído, o FISCAL deverá calcular o ICPE.
Proporcionalização do Pagamento	Meta não atingida implicará em desconto no valor do pagamento, pela PRODEMGE, do valor do APPLIANCE Considera-se a seguinte tabela para o cálculo do desconto referente a este indicador de qualidade: - Sem desconto, se ICPE ≤ 60 dias - Desconto de 1%, se 61 ≤ ICPE < 90 dias

	- Desconto de 3%, se 91 ≤ ICPE < 120 dias - Desconto de 5%, se 121 ≤ ICPE < 150 dias - Desconto de 7%, se ICPE > 149
Observação	Atrasos decorrentes de atividades de responsabilidade da PRODEMGE, e devidamente documentados, deverão ser desprezados no cálculo do número de dias corridos de atraso na finalização da atividade de instalação, configuração e testes

Tabela 4a – indicador de qualidade ICPE

14.12.2. Prazo de instalação, configuração e operação assistida

ICPP – Índice de Cumprimento de Prazo Previsto para Instalação, configuração e operação assistida	
Atributo	**Valor**
Descrição	Mede a quantidade de dias de atraso no processo de instalação, configuração e operação assistida do APPLIANCE
Objetivo	Reduzir o risco de atrasos na instalação, configuração e operação assistida do APPLIANCE
Meta	Prazo de instalação, configuração e testes da solução menor ou igual **a 30 (trinta) dias úteis após a entrega do appliance (entrega 1)**
Periodicidade	Uma medição **ao final do 30º dia útil,** após a entrega do APPLIANCE e, mensalmente, até o final do serviço.
Unidade de Representação	Dias corridos de atraso
Forma de Cálculo	**ICPP = NDA**, **Onde:** NDA = Número de dias corridos de atraso na finalização da atividade.
Mecanismo de Medição e Gestão	**Depois de 30 dias úteis**, após a entrega do Appliance o Fiscal deverá verificar se o serviço foi concluído ou não. Se o serviço foi concluído, não haverá penalidade. Mas, se o serviço não foi concluído, o FISCAL deverá calcular o ICPP.

Proporcionalização do Pagamento	Meta não atingida implicará em desconto no valor do pagamento, pela PRODEMGE, do serviço de instalação, configuração e testes. Considera-se a seguinte tabela para o cálculo do desconto referente a este indicador de qualidade: - Sem desconto, se ICPP ≤ 30 dias úteis - Desconto de 2%, se 31 ≤ ICPP < 41 dias - Desconto de 3%, se 41 ≤ ICPP < 51 dias - Desconto de 5%, se 51 ≤ ICPP < 65 dias - Desconto de 7%, se ICPP > 64 dias
Observação	Atrasos decorrentes de atividades de responsabilidade da PRODEMGE, e devidamente documentados, deverão ser desprezados no cálculo do número de dias corridos de atraso na finalização da atividade de instalação, configuração e testes

Tabela 4b – indicador de qualidade ICPP

14.12.3. Prazo de resposta aos Chamados Críticos

ICSPP – Índice de Chamados Solucionados no Prazo Previsto	
Atributo	Valor
Descrição	Percentual dos chamados técnicos solucionados, nível de gravidade 1, 2 e 3, pela CONTRATADA, no prazo máximo previsto, em relação a todos os chamados técnicos, de gravidade 1,2 e 3 efetuados durante o período de apuração.
Objetivo	Reduzir os atrasos na resolução de problemas, defeitos e no esclarecimento de dúvidas e questionamentos técnicos pela CONTRATADA.
Meta	Maior ou igual a 90%
Periodicidade	Mensal

Unidade de Representação	Valor percentual
Forma de Cálculo	ICSPP = (TCP / TC) x 100, Onde: TCP = Total de chamados de nível de severidade 1 e 2, solucionados dentro do prazo máximo definido neste Termo de Referência, durante o período de apuração. TC = Total de chamados com nível de severidade 1 e 2, solucionados durante o período de apuração. Se TC for menor ou igual a 3 (três) chamados, o ICSPP será igual a 100%, independentemente do valor de TCP.
Gestão do indicador (Coleta, Medição e Acompanhamento)	Conforme detalhado no item "**Gestão dos Níveis de Serviço"** deste anexo.
Proporcionalização do Pagamento	Meta não atingida implicará em desconto no valor do pagamento mensal, pela CONTRATANTE, dos valores mensais devidos. Considera-se a seguinte tabela para o cálculo do desconto referente a este indicador de qualidade: - Sem desconto, se 90% ≤ ICSSP ≤ 100% - Desconto de 2%, se 80% ≤ ICSSP < 90% - Desconto de 3%, se 70% ≤ ICSPP < 80% - Desconto de 5%, se ICSPP < 70% -

Tabela 4c – Indicador ICSPP

14.12.4. Disponibilidade mensal

DispH - Índice de disponibilidade mensal dos serviços ofertados	
Atributo	Valor
Descrição	Percentual de disponibilidade mensal dos serviços ofertados, pela CONTRATADA, durante o período de apuração.
Objetivo	Mensurar o nível de disponibilidade mensal dos serviços ofertados.

Meta	Maior ou igual a 99%
Periodicidade	Mensal
Unidade de Representação	Valor percentual
Forma de cálculo	DispH = ((Tdisp - Sdown) / Tdisp) * 100 Onde**:** DispH = Disponibilidade do APPLIANCE medida em %. Tdisp = Tempo acordado para funcionamento da solução em horas, referente ao mês de medição (considerando 24 X 7, inclusive finais de semana e feriados). Sdown = Somatório dos tempos de falha (*downtime*), em horas. O tempo acordado para funcionamento (Tdisp), em horas, será calculado multiplicando 24 horas pela quantidade de dias no mês de apuração. Cada tempo de falha (*downtime*) será calculado considerando a data e hora de registro do chamado e de seu contingenciamento ou finalização. O somatório dos tempos de falha (Sdown) será dado pela soma de todos os tempos de falha ocorridos no mês de medição, sejam eles concluídos ou em estando ainda em aberto. Importante ressaltar que no cálculo da variável “Sdown” não serão consideradas as indisponibilidades em função de manutenção planejada. Também não serão considerados no cálculo da varável “Sdown” as indisponibilidades decorrentes de atividades de responsabilidade da PRODEMGE ou decorrentes de problemas de infraestrutura no data center (rede, energia elétrica, refrigeração adequada) da PRODEMGE.

Gestão do Indicador (Coleta, Medição e Acompanhamento)	Conforme detalhado no item "**Gestão dos Níveis de Serviço"** deste anexo.
Proporcionalização do Pagamento	Meta não atingida implicará em desconto no valor do pagamento mensal, pela CONTRATANTE, dos valores mensais devidos. Considera-se a seguinte tabela para o cálculo do desconto referente a este indicador de qualidade: - Sem desconto, se 99% ≤ ICSSP ≤ 100% - Desconto de 3%, se 95% ≤ ICSSP < 99% - Desconto de 5%, se 90 ≤ ICSPP < 95% - Desconto de 7%, se ICSPP < 90%

Tabela 4d – Indicador DispH

14.13. Em caso de meta não atingida por 2 meses seguidos, sem uma justificativa plausível, a CONTRATANTE poderá abrir processo punitivo contra a CONTRATADA, conforme definido no item "Sanções cabíveis" deste anexo.

14.14. Em caso de adoção de solução de contingência, sem prejuízo da solução definitiva cabível, a CONTRATADA deve emitir laudos, na periodicidade exigida pela CONTRATANTE, informando sobre a evolução dos trabalhos para solucionar o problema de forma definitiva.

14.14.1. O chamado deverá continuar aberto, com status de contingenciado, até sua solução definitiva, que poderá vir com correções de código, nova release ou atualização de versão.

14.15. Paradas planejadas para manutenção do APPLIANCE não serão consideradas severidades.

14.15.1. Paradas planejadas são manutenções previamente agendadas, através de comunicação formal entre a CONTRATANTE e a CONTRATADA, para manutenções na solução. Estas paralisações devem ser solicitadas com um mínimo de 10 (dez) dias corridos de antecedência, ou de comum acordo entre as partes.

14.15.2. Somente serão consideradas como severidades se excederem os prazos pactuados para a manutenção e a responsabilidade por esta falha for comprovadamente da CONTRATADA.

14.16. Gestão dos Níveis de Serviço

14.16.1. Na abertura (registro) dos chamados, a CONTRATANTE irá comunicar à CONTRATADA que deverá retornar via mensagem eletrônica (e-mail) as seguintes informações:

14.16.1.1. Data e hora de abertura do chamado.

14.16.1.2. Código de identificação do chamado.

14.16.1.3. Descrição do chamado.

14.16.1.4. Nível de severidade do chamado.

14.16.1.5. Identificação (nome completo e matrícula) do solicitante da CONTRATANTE.

14.16.1.6. Identificação do atendente da CONTRATADA.

14.16.2. O contingenciamento do chamado será confirmado através do aceite pela CONTRATANTE na ordem de serviço (OS) correspondente, desde que incluso as seguintes informações:

14.16.2.1. Código alfanumérico de identificação do chamado.

14.16.2.2. Data e hora de conclusão do contingenciamento.

14.16.2.3. Descrição detalhada do serviço executado.

14.16.3. A conclusão definitiva de cada chamado será confirmada através do aceite pela CONTRATANTE do atendimento correspondente, conforme definido no anexo I-B (“Laudo técnico de execução de serviços de Assistência Técnica”).

14.16.4. Deve ser emitido pela CONTRATADA um relatório mensal consolidado de atendimento (Relatório de Apuração de Níveis de serviços - Anexo I-D), contemplando todos os chamados registrados no mês, contendo as seguintes informações: número de identificação do chamado, data e hora da abertura do chamado, data e hora de contingenciamento do chamado (se for o caso), data e hora de fechamento do chamado (se for o caso).

14.16.4.1. A CONTRATADA deverá elaborar e enviar à CONTRATANTE até o 5º (quinto) dia útil do mês, o relatório de apuração de níveis de serviço.

14.16.4.2. Neste relatório serão apresentados os resultados referentes aos indicadores de qualidade com período de apuração encerrando no mês que precede à data de sua emissão e, se for o caso, o valor do desconto no pagamento referente ao serviço gerenciado pelo indicador de qualidade.

14.16.4.3. Caso não ocorra nenhum chamado técnico no período de apuração, a emissão deste relatório será dispensada, considerando, neste caso, que todos os indicadores de qualidade alcançaram a meta prevista.

15. Da participação em consórcios

15.1. Por se tratar de serviços comuns no mercado, amplamente disseminados, não será aceito neste processo de aquisição a formação de consórcio, uma vez que existem diversos fornecedores no mercado capazes de prestar os serviços de forma independente.

16. Subcontratação:

16.1. Será permitida a subcontratação dos serviços, desde que seja com o fabricante do APPLIANCE, ou seu distribuidor autorizado no Brasil, no máximo, nas proporções abaixo:

16.1.1. Cenário 1

Item	Produtos e Serviços	% de subcontratação
6	Capacitação Técnica para 6 alunos	100%

Tabela 5a – Subcontratação de serviços – cenário 1

16.1.2. Cenário 2

Item	Produtos e Serviços	% de subcontratação
10	Capacitação Técnica para 6 alunos	100%

Tabela 5b – Subcontratação de serviços – cenário 2

16.2. A gestão dos serviços subcontratados ficará sob responsabilidade integral da CONTRATADA uma vez que a prestação dos serviços sem a gestão de um único fornecedor pode acarretar situações adversas como dificuldade no diagnóstico de problemas e/ou dificuldade operacional, trazendo prejuízos em possíveis implantações, manutenções e reparos no ambiente. Isto não impede

este fornecedor de subcontratar serviços de outras empresas, desde que sejam qualificadas e estejam sob sua administração e responsabilidade.

16.3. Em casos de problemas ou de descumprimento da execução do objeto contratual, a responsabilidade recairá inteiramente sobre a CONTRATADA, não sendo permitida a transferência de culpabilidade à subcontratada.

17. Vigência da contratação

17.1. O prazo de vigência de cada um dos contratos será de 41 (quarenta e um) meses, a contar da data de sua assinatura.

17.2. O prazo se justifica:

17.2.1. Pelo uso contínuo do APPLIANCE, do nível de configuração e otimização de acordo com as necessidades da PRODEMGE, da capacitação dos técnicos da PRODEMGE no uso de suas funcionalidades, não sendo razoável a contratação, configuração, migração de dados e capacitação de um APPLIANCE similar por um período menor, sem que os serviços prestados sejam severamente impactados.

17.2.2. A contratação dos serviços prevê o uso do APPLIANCE em um período de 36 (trinta e seis) meses e estima-se que as etapas de entrega do produto, instalação, capacitação e operação assistida terão uma duração estimada de 5 (cinco) meses. Portanto, de forma cautelar, prevê-se como vigência do contrato, o prazo de 41 (quarenta e um) meses.

18. Garantia financeira

18.1. Não se aplica.

19. Sustentabilidade ambiental

19.1. Não se aplica.

20. Unidade Fiscalizadora

20.1. Não se aplica nesta prospecção

21. Orçamento estimado:

21.1. Não se aplica na prospecção.

22. Obrigações da CONTRATADA:

22.1. Manter, durante a vigência do contrato, todas as condições que ensejaram sua contratação, atendendo os requisitos constantes neste Termo de Referência e seus anexos.

22.2. Manter o APPLIANCE disponível para uso pela CONTRATANTE, 24 horas por dia, todos os dias, inclusive finais de semana e feriados.

22.3. Reportar para CONTRATANTE, qualquer problema ou divergência que venha a impactar a execução dos serviços descritos neste contrato;

22.4. Disponibilizar um ponto focal para tratar dos assuntos técnicos com a CONTRATANTE.

22.5. Comprovar, na assinatura do contrato, que possui corpo técnico com, no mínimo, 2 (dois) profissionais devidamente qualificados, com certificação ou declaração do fabricante do equipamento atestando a proficiência desses profissionais em exercer as atividades de instalação, configuração e/ou uso da solução.

22.6. Na assinatura do contrato, informar o e-mail e telefone de contato para acesso aos serviços de suporte.

22.6.1. Os links para as reuniões de videoconferência deverão ser repassados para a CONTRATANTE, via e-mail, até 4 (quatro) horas antes de cada evento.

22.7. Interagir, por meio de seu ponto focal, com os gestores da CONTRATANTE sempre que solicitado.

22.8. Comunicar aos responsáveis pela fiscalização do contrato, por escrito, qualquer anormalidade identificada na prestação dos serviços, bem como atender prontamente o que lhe for solicitado.

22.9. Elaborar e entregar o planejamento e o cronograma das atividades a serem executadas, conforme definido nesse Termo de Referência e seus anexos.

22.10. Enviar a PRODEMGE ao final de cada serviço o relatório de conclusão;

22.11. Responsabilizar-se por todos os custos decorrentes do serviço de assistência técnica ofertada.

22.12. Garantir a confidencialidade, disponibilidade e integridade dos dados da CONTRATANTE gerenciados pela solução.

22.13. Ativar todas as funcionalidades solicitadas neste termo de referência, para uso imediato pela CONTRATANTE, após a instalação do APPLIANCE.

22.14. Possuir capacidade técnica operacional para prestar os serviços.

22.15. Realizar o atendimento por pessoal técnico especializado próprio ou de terceiros especializados e credenciados, especialmente contratados para esse fim, quando aplicável.

22.16. Substituir, de imediato, em até 15 dias úteis, a qualquer tempo e por determinação do responsável pelo acompanhamento e fiscalização operacional da execução do Contrato, os profissionais que não atenderem às exigências e aos requisitos e padrões de qualidade necessários ao adequado desempenho das funções e atividades relativas aos serviços contratados.

22.17. Responsabilizar-se pelo integral cumprimento do Contrato, bem como arcar com os eventuais prejuízos causados à CONTRATANTE ou a terceiros, provocados por ineficiência no fornecimento dos produtos, respondendo integralmente pelo ônus decorrente, o que não exclui nem diminui a responsabilidade pelos danos que se evidenciarem, independentemente do controle e fiscalização exercidos pela CONTRATANTE.

22.18. Fazer cumprir as normas de segurança e medicina do trabalho, responsabilizando-se por qualquer acidente que venha a ocorrer em decorrência da execução dos serviços contratados.

22.19. Arcar, durante a prestação dos serviços, com quaisquer cobranças adicionais decorrentes de eventuais diferenças vinculadas a questões trabalhistas, tais como férias, horas extras, sobreaviso, etc., bem como os gastos provenientes de deslocamento, estadia e alimentação, caso sejam necessários.

22.19.1. Responder pelas despesas relativas a encargos trabalhistas, seguro de acidentes, contribuições previdenciárias, impostos e quaisquer outras que forem devidas e referentes aos serviços executados por seus empregados, uma vez que os mesmos não têm nenhum vínculo empregatício com a CONTRATANTE;

22.20. Realizar reuniões entre as equipes técnicas da CONTRATANTE e da CONTRATADA, em datas agendadas de comum acordo, no mínimo 2 (duas) vezes em um período de 12 (doze) meses, para nivelamento e aperfeiçoamento de conhecimento.

22.20.1. O tema será definido pela CONTRATANTE, com antecedência mínima de 20 (vinte) dias úteis.

22.20.2. CONTRATADA deve alocar técnicos capacitados para participar das reuniões.

22.20.3. Estas atividades serão realizadas remotamente, via videoconferência, podendo, em comum acordo, serem realizadas de forma presencial, desde que sem ônus para a CONTRATANTE.

22.20.4. A duração de cada reunião será de, no mínimo, 2 (duas) horas.

22.21. Iniciar e concluir os serviços de atendimento e suporte técnico nos prazos estipulados conforme os níveis de serviços acordados.

22.22. Apresentar mensalmente os relatórios previstos no item “Níveis de serviço” deste anexo.

23. Obrigações da CONTRATANTE:

23.1. Garantir o acesso dos especialistas técnicos da CONTRATADA no local da execução dos serviços contratados;

23.2. Disponibilizar um ambiente seguro para os especialistas técnicos da CONTRATADA e/ou para seus prestadores de serviços, que estejam executando os serviços contratados;

23.3. Fornecer as informações necessárias para a configuração inicial da solução no prazo acordado entre as partes.

23.4. Disponibilizar um ponto focal para tratar dos assuntos técnicos com a CONTRATADA.

23.5. Fiscalizar regularmente os serviços prestados pela CONTRATADA, verificando as condições em que as tarefas estão sendo realizadas.

23.6. Comunicar tempestivamente à CONTRATADA qualquer anormalidade detectada na prestação do serviço.

23.7. Notificar à CONTRATADA para que corrija, de acordo com os níveis de serviços acordados, problemas de software que não permitam o seu funcionamento com regularidade plena.

23.8. Exigir da CONTRATADA o fiel cumprimento das obrigações;

23.9. Verificar a manutenção pela CONTRATADA das condições de habilitação estabelecidas;

23.10. Aplicar penalidades a CONTRATADA, por descumprimento das obrigações;

23.11. Prestar as informações e esclarecimentos necessários ao desenvolvimento das tarefas que se fizerem necessárias a perfeita execução do serviço.

23.12. Proporcionar todas as facilidades para que a CONTRATADA possa desempenhar seus serviços, dentro das especificações da presente especificação.

24. Sanções Cabíveis

24.1. Em caso de atraso injustificado na execução do contrato (mora) e/ou a sua inexecução total ou parcial pela CONTRATADA, serão aplicadas as normas dos artigos 187 a 206 do Regulamento Interno de Licitações e Contratos da Prodemge.

24.2. O atraso injustificado na execução do contrato sujeita a CONTRATADA à multa de mora, nos termos do art. 82 da Lei Federal nº 13.303/2016, limitada a 0,3% (três décimos por cento) por dia, até o trigésimo dia de atraso.

24.3. A inexecução total ou parcial, aqui incluído o descumprimento de qualquer cláusula do contrato, sujeita o contratado às seguintes sanções, nos termos do art. 83 da Lei Federal nº 13.303/2016:

24.3.1. Advertência;

24.3.2. Multa de 10% (dez por cento) sobre o valor do saldo remanescente do contrato para o caso de inexecução parcial;

24.3.3. Multa de 20% (vinte por cento) sobre o valor total do contrato para o caso de inexecução total;

24.3.4. Suspensão temporária de participação em licitação e impedimento de contratar com a Prodemge, por prazo não superior a 2 (dois) anos.

24.4. As sanções previstas, quando aplicadas, deverão levar em consideração a natureza e a gravidade dos fatos, a extensão e a relevância da obrigação descumprida, a culpabilidade da CONTRATADA, os fins a que a sanção se destina, os princípios da razoabilidade e da proporcionalidade.

24.5. Os procedimentos para a aplicação de sanções estão previstos nos arts. 187 a 206 do Regulamento Interno de Licitações e Contratos da Prodemge, o qual observa o devido processo legal, garantindo o contraditório e a ampla defesa.

25. Matriz de Risco

25.1. Não se aplica.

26. Glossário

26.1. Assistência técnica – Para este Termo de Referência, são as atividades de apoio técnico da CONTRATADA com vistas a solucionar problemas no uso da solução proposta, nas sugestões de melhorias, ajustes nas configurações, esclarecimentos de dúvidas e de manutenção preventiva e corretiva dos serviços ofertados.

26.2. Backup - Cópia de segurança de dados de um instancia computacional para um ambiente de armazenamento distinto com vistas à recuperação em caso de perda dos dados originais.

26.2.1. Backup Primário – Neste Termo de Referência, é uma cópia de segurança mais recente de uma base de dados.

26.2.2. Backup Secundário – Neste Termo de Referência, é uma cópia de segurança de uma base de dados, mas defasado em relação ao backup Primário.

26.3. CORREÇÃO DE ERRO - Qualquer alteração que se fizer no software, inclusive alterações feitas para manter a compatibilidade do sistema, melhoria de operação aprimorada e segurança, bem como SOLUÇÕES DE CONTINGÊNCIA que estabeleçam ou ajudem a restabelecer a funcionalidade substancial com as especificações na DOCUMENTAÇÃO referente a esse software.

26.3.1. Em geral, é uma solução provisória para um problema específico do cliente e, normalmente, é fornecida por meio de point patch específico ou hot fix. Uma “Correção” também incluirá quaisquer recomendações

ou avisos feitos a um cliente, inclusive recomendações para que um cliente migre para uma versão atual ou novo release, análise do problema no desenvolvimento de uma versão futura do software ou outras medidas para encerrar um atendimento aberto.

26.4. Data center - Instalação construída com o objetivo de alojar recursos de infraestrutura de TIC, como servidores, dispositivos de rede, storage e outros equipamentos. Um datacenter é uma infraestrutura que centraliza as operações e os equipamentos de tecnologia da informação.

26.4.1. Data Center Privado – Instalação alocada para uso exclusivo de uma organização e de suas unidades vinculadas. Sua propriedade e gerenciamento de seus recursos, segurança e operação podem ser realizados pela própria organização, bem como por terceiros ou ambos;

26.4.2. Data Center Público – Instalação onde diversas empresas compartilham os recursos de infraestrutura de TIC. É um modelo no qual os recursos de computação pertencem a uma empresa (CSP) e são operados por ela, que os compartilha entre vários locatários, com uma separação lógica por cliente.

26.5. Documentação – Compreende as especificações, a documentação do usuário, os manuais e os guias técnicos entregues com a solução proposta.

26.6. Hot-swap – Característica de dispositivos de um equipamento que podem ser removidos e instalados sem interrupção de funcionamento do equipamento e sem afetar o desempenho ou recursos do mesmo.

26.7. Incidente - Uma interrupção não planejada de um serviço de TI ou uma redução da qualidade de um serviço de TI ou uma falha de um componente de hardware ou software.

26.8. On-Premises – Neste Termo de Referência, corresponde a instalação e uso de recursos de infraestrutura de TIC dentro do data center da PRODEMGE.

26.9. Release – Compreende a liberação de um produto de software que pode conter uma pequena funcionalidade da próxima VERSÃO do software, código ou compatibilidade e incorpora todos os PACOTES DE SERVIÇOS e CORREÇÕES DE ERRO anteriores (se houver) desde a última VERSÃO.

26.9.1. Geralmente a liberação requer uma nova instalação, em vez de uma sobreposição para o software já instalado. Salvo disposição em

contrário, a liberação está ligada à versão anterior e é designada por um número à direita do ponto decimal, como 1.1, 1.2, 1.3, etc.

26.10. Recovery - Restauração de dados e informações de um backup retido em um dispositivo de armazenamento.

26.11. Sensor de inspeção de rede – Dispositivo capaz de analisar o trafego de dados na velocidade solicitada para a execução de determinadas funcionalidades do software controlador.

26.12. Solução de Contingência - significa uma solução provisória de um problema e poderá incluir modificações específicas ao software para tratar de problemas críticos (podendo ser denominada também como “hot fixes”).

26.12.1. Em alguns casos, o problema tratado por uma solução de contingência será definitivamente solucionado quando o usuário realizar o próximo UPGRADE (atualização). A Solução Alternativa em si poderá ser considerada final caso estabeleça uma forma diferente de uso do software pelo usuário, de modo a reduzir substancialmente o impacto de um erro ou defeito.

26.13. Suporte de autoatendimento – Suporte com acesso às ferramentas de autoajuda oferecidas no suporte online, tais como informações sobre compatibilidade de produto, correções publicadas anteriormente, soluções alternativas, documentos informativos e outras soluções de produto.

26.14. Upgrade (atualizações) - Incluem revisões de Documentação, CORREÇÕES DE ERRO, PACOTES DE SERVIÇO, VERSÕES e RELEASES da solução proposta para o qual é fornecido o SUPORTE TÉCNICO, e não incluem opções ou produtos que sejam licenciados separadamente.

26.14.1. Estas Atualizações poderão ser denominadas como “atualizações de produto” ou “atualizações de software”.

26.15. Versão – Compreende um RELEASE de um produto de software que contém grandes mudanças na funcionalidade do produto de software, código ou compatibilidade e incorpora as liberações anteriores (se tiverem ocorrido).

26.15.1. Normalmente, a versão requer uma nova instalação, em vez de uma sobreposição para o software já instalado. Salvo disposição em contrário, a Versão é designada pelo número à esquerda do ponto decimal, como 1.0, 2.0, 3.0, etc.

27. Demais condições

27.1. Não se aplica**.**

28. Fazem parte do anexo I deste Termo de Referência:

28.1. Anexo I-A: Formulário de precificação

28.2. Anexo I-B: Laudo técnico de execução de serviços de assistência técnica

28.3. Anexo I-C: Laudo técnico de fornecimento do Appliance

28.4. Anexo I-D: Relatório de apuração de níveis de serviços

28.5. Anexo I-E: Laudo técnico de execução de serviços

28.6. Anexo I-F: Especificação técnica

As proponentes deverão preencher os formulários abaixo, não existindo restrição para a quantidade de cenários propostos nesta consulta pública.

28.6.1. CENARIO 1 – Hardware e Software segmentados

Item	Produtos e Serviços	Direcionador	Quantidade	Valor unitário	Valor total
1	Hardware de acordo com requisitos detalhados no anexo I-F	Unidade	1		
2	Software de acordo com requisitos detalhados no anexo I-F	Licença	1		
3	Serviços técnicos de Instalação e configuração com operação assistida	Prestação de serviço	1		
4	Garantia com assistência técnica para o Hardware com suporte, manutenção e atualização de firmware e software embarcado por 36 meses.	Prestação de serviço	1		
5	Garantia com assistência técnica para o Software com suporte, manutenção e atualização de versão por 36 meses.	Prestação de serviço	1		
6	Capacitação Técnica para 6 alunos	Turma	2		

Anexo I-A – cenário 1

28.6.2. CENARIO 2 – Hardware e Software como um único produto

Item	Produtos e Serviços	Direcionador	Quantidade		
7	Appliance composto por hardware e software de acordo com requisitos detalhados no anexo I-F	Unidade	1		
8	Serviços técnicos com instalação e configuração com operação assistida	Prestação de serviço	1		
9	Garantia com assistência técnica do Appliance com suporte, manutenção e atualização de firmware e software embarcado por 36 meses.	Prestação de serviço	1		
10	Capacitação Técnica para 6 alunos	Turma	2		

Anexo I-A – cenário 2

A PROPONENTE deverá preencher os formulários acima, detalhando os valores unitários de cada item e valores totais propostos, considerando o quantitativo total de cada item.

- Os preços devem ser apresentados em Reais (R$), com todos os impostos, taxas e despesas inclusas.

ANEXO I-B – Laudo Técnico de Execução de Serviços de Assistência Técnica

Identificação do contrato:

Data do Chamado ou de início da manutenção programada: ___/___/___
Horário do Chamado (para chamados):
Horário de início de atendimento (para chamados):
Horário de início do serviço:
Data e horário de termino do serviço:

Problema detectado:

Descrição do serviço realizado:

Identificação de peças, componentes e/ou atualização de software:

Procedimentos realizados:

(Assinatura)

_____

Nome do responsável técnico pela manutenção

(Assinatura)

_____

Nome do Fiscal do contrato

ANEXO I-C – Laudo técnico de fornecimento do Appliance

Identificação do contrato:

Descrição:

Número de série do equipamento e identificação do conjunto de software:

Data e horário da entrega:

Atesto que a entrega ocorreu de acordo com os critérios estabelecidos no contrato supracitado.

_____

Nome do Fiscal do contrato

_____

Local e data

ANEXO I-D – Relatório de apuração de níveis de serviços

Identificação do contrato:

Código do indicador de qualidade:

Período de apuração: ___ /___ /___ a ___ /___ /___

Valor apurado: _____

Desconto no pagamento: SIM ou NÃO

( ) desconto de R$_____ (_____) na parcela devida no mês ou na garantia contratual, conforme estipulado no contrato supracitado.

Relação dos chamados no período (código do chamado, descrição sumária, data de hora do chamado, do início de atendimento e de conclusão)

ANEXO I-E – Laudo Técnico de Execução de Serviços

Identificação do contrato:

Serviço executado:

( ) Capacitação para uso e operação do APPLIANCE
( ) Serviço técnicos de instalação, configuração e operação assistida

Data de início do serviço:
Data de termino do serviço:

Descrição do serviço realizado:

:

(Assinatura)

_____
Nome do responsável técnico da CONTRATADA

(Assinatura)

_____
Nome do Fiscal do contrato

Número do Requisito	**Detalhamento técnico** do **requisito**	Sugestões
1	**O APPLIANCE ofertado é composto por hardware, software e sensores de inspeção de rede.**	
1.1	Todos equipamentos, acessórios e componentes ofertados devem ser novos, sem uso anterior, não remanufaturados ou recondicionados e estar na linha de produção atual do fabricante, devendo fazer parte do catálogo de produtos comercializados pelo fabricante de equipamentos, não ter sido descontinuado e nem ter previsão de "end of service life".	
1.2	A solução de APPLIANCE proposta deverá ser do mesmo fabricante ou possuir total compatibilidade comprovada em documentação oficial	
1.2.1	Exceto pelo sistema operacional do Appliance, todo software fornecido deve ser de um único fabricante	
1.3	A Proponente deverá referenciar explicitamente o nome(s) do(s) fabricante(s), códigos e part numbers de todas as partes (hardware, software, agentes, acessórios, componentes, etc) que compõem a solução proposta.	
2	**Sondas de inspeção de rede**	
2.1	Deverão ser fornecidos um conjunto mínimo de 2 (duas) sondas de inspeção de rede e sandboxing com capacidade de analisar, em conjunto, no mínimo, **20 Gbps**, para protocolos HTTP, HTTPS, DNS, FTP, SMTP, POP3, SMB, Telnet, RDP, Kerberos, SQL, ARP, incluindo protocolos mascarados ou tunelados em ICMP, IP, UDP e TCP;	
3	**Características do hardware do Appliance**	
3.1	Deverão ser fornecidos 2 appliances físicos, onde cada um deve analisar, no mínimo, **10 Gbps de tráfego** através de interfaces disponíveis no equipamento, de acordo com a relação abaixo:	
3.1.1	4 interfaces UTP RJ45 1 Gbps	
3.1.2	Mínimo de 3 (três) portas óticas de 10/25 Gbps, compatíveis com switch CISCO Nexus C93240YC-FX2. Os transceivers deverão ser fornecidos para cada velocidade (10 e 25), transceivers, conforme especificações abaixo:	
3.1.2.1	6 transceivers - Porta ótica de 10 Gbps – 10GBase-SR – IEEE 802.3ae – SFP-10G-SR	

Número do Requisito	**Detalhamento técnico** do **requisito**	Sugestões
3.1.2.2	6 transceivers - Porta ótica de 25 Gbps – 25GBase-SR – IEEE 802.3by - SFP-25G-SR	
3.1.3	O appliance também deve incluir 2 interfaces de gerenciamento 1Gb base-T RJ45 e gerenciamento externo como iDrac Enterprise ou similar;	
3.2	As portas solicitadas devem ser fornecidas em controladoras distintas (mínimo duas) ou em placa on-board e controladora, sendo permitido a configuração dual-port em cada placa.	
3.3	Devem ser fornecidos 2 (dois) cabos de fibra ótica para todas as interfaces óticas solicitadas - todos resistentes a tração;	
3.3.1	6 (seis) cabos de 10 (dez) a 15 (quinze) metros e 6 (seis) cabos de 25 (vinte e cinco) a 30 (trinta) metros.	
3.3.2	As fibras óticas serão multimodo, OM4, para conexão aos switches da Rede ETHERNET da CONTRATANTE. Os conectores devem seguir o padrão LC/LC, short-wave.	
3.4	Além dos cabos, devem ser fornecidos todos os componentes necessários para conexão e a plena utilização com todas as funcionalidades, conforme as normas técnicas de fabricação e especificações do fabricante, tanto do lado da solução ofertada como do lado das Switches.	
3.5	Cada Appliance deve ter capacidade mínima de 2 TB de armazenamento líquido, no mínimo em duas unidades SSD NvMe, hot swap, considerando o uso de RAID 5, 6 ou DP.	
3.6	Controladora de disco PCIe, taxa de transferência de 12 GB/s SAS, com memória cache mínima de 1 GB (um gigabyte), bateria ou memória flash	
3.7	Deve possuir dimensões e acompanhar todos os acessórios necessários para instalação, fixação e organização de cabos em rack padrão de 19 polegadas (EIA-310).	
3.8	Tensão de 127/220 VAC e frequência de 50/60 Hz.	
3.9	Temperatura (faixa mínima de operação): 12ºC a 35ºC.	

Número do Requisito	**Detalhamento técnico** do **requisito**	Sugestões
3.10	Deve possuir, no mínimo, duas fontes de alimentação internas e redundantes, tipo hot-swap. Cada fonte de alimentação deve ter sua tomada de alimentação independente. Em caso de queda de uma das fontes, as demais devem manter todo o equipamento em operação.	
3.11	Deve possuir, no mínimo, dois sistemas de ventilação internos redundantes, tipo hot-swap. Cada sistema de ventilação deve ter sua tomada de alimentação independente. Em caso de queda de um dos sistemas, os demais devem manter a temperatura adequada do equipamento em operação. Entende-se por sistema de ventilação um único ventilador ou um conjunto de ventiladores.	
3.12	Conectores de energia	
3.12.1	Para consumo elétrico de até 32 Amperes: plug de tomada (plug macho) com trava de 3P+T 30A com tensão de até 440V com saída axial. Prolongador (plug fêmea) 3P+T30A com tensão de até 440V.	
3.12.2	Para consumo elétrico acima de 32 Amperes e até 63 Amperes: plug de tomada (plug macho) com trava 3P+T63A com faixa de tensão entre 200 à 250V e (plug fêmea) acoplamento de 3P+T63A com faixa de tensão 200-250V.	
3.12.3	Os conectores do tipo “macho”, necessários para a alimentação elétrica dos equipamentos, devem ser fornecidos no novo padrão brasileiro, tripolar 3x0,75mm, 1,50m, NBR 14136, de 10A a 20A / 250V.	
3.13	Devem ser fornecidos 2 (dois) cabos de fibra ótica para todas as interfaces óticas solicitadas - todos resistentes a tração;	
3.14	Um dos cabos deverá ter 10 (dez) a 15 (quinze) metros e o outro de 25 (vinte e cinco) a 30 (trinta) metros.	
3.15	As fibras óticas serão multimodo, OM4, para conexão aos switches da Rede ETHERNET da CONTRATANTE. Os conectores devem seguir o padrão LC/LC, short-wave.	
3.16	Além dos cabos, devem ser fornecidos todos os componentes necessários para conexão e a plena utilização com todas as funcionalidades, conforme as normas técnicas de fabricação e especificações do fabricante, tanto do lado da solução ofertada como do lado das Switches.	

Número do Requisito	**Detalhamento técnico** do **requisito**	Sugestões
3.17	Não serão aceitos appliances de Unified Threat Management (UTM) e Next-Generation Firewall (NGFW) para monitoramento do tráfego, ainda que possua recurso e licenciamento específico para análise de ameaças em rede;	
3.18	Deve permitir fazer upgrade e downgrade do firmware	
4	**Funcionalidades da solução**	
4.1	Deve detectar ameaças avançadas no ambiente da CONTRATANTE, inspecionando o tráfego de rede;	
4.2	Deve aplicar técnicas de análise de tráfego avançadas e machine learning;	
4.3	Deve implementar características de NDR baseado em comportamento como complemento às soluções baseadas em assinatura;	
4.4	Deve permitir que o administrador escolha uma implementação em modo inline ou em modo de monitoramento através de tráfego espelhado;	
4.4.1	Caso seja implementada no modo inline, a solução deverá permitir criar um by-pass para casos de falhas de interface;	
4.5	Deve analisar tráfego de rede (pacotes e/ou flows) em tempo real, com capacidade para identificar, gerar alertas em casos de tráfego suspeito e prover orquestração para bloqueio de tais ameaças;	
4.6	Deve analisar arquivos em sandbox, permitindo identificar ataques avançados (APT), Zero Days, códigos de exploração (exploits) embutidos, vulnerabilidades conhecidas e arquivos maliciosos no tráfego de rede, de forma automática e quando aplicável;	
4.7	Ter a capacidade de analisar tráfego TLS;	
4.8	**Deverá fornecer solução integrada de proteção contra ameaças avançadas de acordo com funcionalidades e características técnicas especificadas neste documento, contendo, no mínimo os seguintes módulos:**	
4.8.1	Monitoramento, Identificação, Análise e Resposta de Incidentes de Segurança;	
4.8.2	Detecção de ataques direcionados;	

Número do Requisito	**Detalhamento técnico** do **requisito**	Sugestões
4.8.3	Analisador virtual de ameaças (sandbox);	
4.8.4	Correlação de regras para detecção de conteúdo malicioso;	
4.8.5	Análise de todos os estágios de uma sequência de ataques;	
4.8.6	Plataforma de integração com outras soluções de segurança;	
4.8.7	Orquestração de bloqueio de ameaças na rede.	
4.8.8	Serviço de Monitoração e Análise de Ameaças Digitais em rede;	
4.8.9	Serviço de Monitoração e gestão de riscos que permita a identificação de ameaças digitais conhecidas e não conhecidas por soluções de antivírus tradicionais, permitindo a composição de serviços de mitigação complementares para a segurança do ambiente;	
4.8.10	Serviço que entenda ameaça digital como a representação de um software malicioso	
4.8.11	Visibilidade e relatório de incidentes de conexões da rede interna com sites maliciosos ou servidores de central de comando (C&C) externos;	
4.8.12	Análise e correlação de atividades maliciosas tais como: Detecção específica de malwares conhecidos e arquivos contaminados através de assinaturas de antivírus tradicional no tráfego da rede; Detecção de worm de rede e de e-mail no tráfego de rede; Detecção de programas de exploração de vulnerabilidades (Exploits) na rede; Detecção de empacotamentos maliciosos no tráfego da rede;	
4.8.13	Validação de tráfego web malicioso através de consultas a sistemas de reputação na Internet;	
4.8.14	Visibilidade e relatório de estatísticas de ameaças, fontes de infecção na rede monitorada e máquinas comprometidas.	
4.8.15	Permitir a identificação da criticidade dos eventos de segurança	
4.8.16	Permitir realizar pesquisas customizadas dos incidentes de segurança através da console de gerenciamento;	

Número do Requisito	**Detalhamento técnico** do **requisito**	Sugestões
4.8.17	Possibilidade de criação de filtros para visualização de eventos específicos conforme contexto, localização e outras variáveis que permitam investigação profunda sobre causa raiz de incidentes de segurança;	
4.8.18	Permitir a customização de alertas em base ao tipo de incidente de segurança através da console de gerenciamento;	
4.8.19	Permitir a integração com sistemas de serviço de diretório;	
4.8.20	Capacidade de verificar em tempo real a reputação de endereços web (URL's) e servidores de correio SMTP;	
4.8.21	A análise de SMTP poderá ser realizada em uma solução separada do sensor de HTTP e demais protocolos;	
4.8.22	A solução deverá possuir mecanismo de conhecimento de senhas de palavras chaves, em seu vocabulário de conhecimento, para derivação de arquivos protegidos;	
4.8.23	Capacidade de criar e salvar investigações customizadas dos incidentes de segurança;	
4.8.24	Deve possuir a capacidade de detectar ameaças direcionadas, ataques do dia zero e documentos que viabilizem ataques;	
4.8.25	Deve detectar atividades maliciosas que trafegam na rede através de motor de análise de comportamento de tráfego até o nível 7 (camada de aplicação) em protocolo TCP/IP;	
4.8.26	Capacidade de detectar ameaças web tais como vulnerabilidades e download de conteúdo malicioso;	
4.8.27	Deve possuir capacidade de disponibilizar facilmente as amostras dos arquivos suspeitos detectados e do arquivo PCAP do contexto de captura;	
4.8.28	Capacidade de oferecer informações para análise forense de artefatos suspeitos de serem maliciosos;	
4.8.29	Gerenciamento centralizado de todas as etapas dos eventos de segurança identificados como possíveis ameaças;	

Número do Requisito	**Detalhamento técnico** do **requisito**	Sugestões
4.8.30	Capacidade de identificar artefatos maliciosos direcionados para dispositivos moveis rodando o sistema operacional Android e IOS, tais como telefones inteligentes e tablets;	
4.8.31	Deve analisar em tempo real o comportamento através de simulação de execução de arquivos provenientes do tráfego de rede incluindo arquivos executáveis (scripts), PDF´s, executáveis, PPTX, DOCX, XLSX, LNK, CHM, RTF, DLLs, JAR, ZIP ou RAR;	
4.8.32	A solução deve detectar ameaças do dia zero, vulnerabilidade, URL's maliciosas e spams dirigidos no protocolo SMTP;	
4.8.33	A solução de análise em sandbox deve ter a capacidade de analisar, de forma estática e dinâmica, ameaças com características de autoinicialização ou alteração de arquivos de sistema, rootkits/cloakings, arquivos mal-formados, engenharia social, dentre outros;	
4.8.34	A análise de sandbox deve identificar e analisar ameaças que tenham características de evitar a segurança e análise em sandbox, e auto-preservação;	
4.8.35	A solução deve possuir recurso de prevenção de ameaças avançadas, com capacidade de apresentar em seus logs, visibilidade de acordo com o framework ATT&CK MITRE Matrix, pontuando características de táticas e técnicas de acordo com a ameaça detectada/bloqueada pela solução;	
4.8.36	Deve possuir tecnologia de análise de arquivos binários através de simulação e avaliação de execução dos artefatos suspeitos para identificação de comportamento malicioso, com capacidade de operar vários ambientes simultâneos e integrados a solução para processamento de alto desempenho;	
4.8.37	Deve permitir o uso de base de conhecimento na Internet do próprio fabricante para correlacionamento de informações sobre ameaças conhecidas e prover recomendações de ações;	
4.8.38	Deve permitir o uso de portas espelhadas de switch (mirror port) para monitorar o tráfego e detectar potenciais riscos à Segurança;	

Número do Requisito	**Detalhamento técnico** do **requisito**	Sugestões
4.8.39	Deverá permitir o rastreio por malwares utilizando métodos de detecção baseados no tipo de arquivo (True File Type), múltiplas camadas de empacotamento (Multi-packed/Multi-layered files) e arquivos comprimidos (compactados);	
4.8.40	Deverá analisar arquivos maliciosos na rede utilizando vacinas e técnicas de heurística;	
4.8.41	Deve possuir foco em proteção contra APTs (Advanced Persistent Threats);	
4.8.42	Deve possuir tecnologia de proteção contra ameaças desconhecidas (ataques dirigidos e ameaças de dia zero), sendo que este módulo deve pertencer ao mesmo fabricante;	
4.8.43	Deverá possuir suporte para monitorar múltiplas interfaces de rede conectadas a diferentes VLANs, VRFs (MPLS) ou Switches para tráfego equivalente a um total 20GB/s;	
4.8.43.1	Deverá conter no mínimo 3 (três) interfaces de 10GB/s cada para coleta;	
4.8.44	Deverá possuir suporte para balanceamento de carga no sensor de inspeção de tráfego, possibilitando assim obter uma melhor performance;	
4.8.45	Deverá permitir a análise específica de eventos de segurança de computadores suspeitos de atividade maliciosa;	
4.8.46	Os módulos que compõem a solução devem atuar de forma integrada com soluções via Syslog, com logs de incidentes em ponto único;	
4.8.47	Deve possuir atualização automática de regras e assinaturas, sendo que estas devem ser disponibilizadas via web pelo fabricante da solução;	
4.8.48	Deve possuir mecanismo de consultas automáticas em bases de reputação externas de propriedade do fabricante da solução;	
4.8.49	Deve ser capaz de identificar movimentos laterais em uma rede corporativa;	
4.8.50	Deve possuir interface web para busca e investigação local de incidentes;	

Número do Requisito	Detalhamento técnico do requisito	Sugestões
4.8.51	Deve possuir capacidade de envio de artefatos para analisador virtual dedicado, externo, sendo que este deverá suportar no mínimo os sistemas operacionais distribuição CentOS 6 ou superior, Red Hat Enterprise Linux 5 ou superior Windows 7 ou superior, Oracle Linux 6 ou superior, Windows Server 2003 ou superior ;	
4.8.52	Deve suportar a criação de sandboxes que repliquem os sistemas operacionais e aplicações da CONTRATANTE, para avaliação do real impacto da ameaça no ambiente;	
4.8.53	O sensor deverá suportar a análise em sandbox de, pelo menos, 50 arquivos simultaneamente Caso um único appliance não tenha tal capacidade, é permitido o empilhamento ou agrupamento;	
4.8.54	Possibilitar a predefinição de políticas para determinar quais tipos de arquivos deverão ser enviados para análise;	
4.8.55	Deve possuir possibilidade de habilitação e desabilitação de regras de inspeção, individualmente, através de interface de gerenciamento web;	
4.8.56	Deve possuir regras que identifiquem comunicações dos seguintes tipos: C&C, Exploits, Executáveis Maliciosos, Comunicação com Sites Maliciosos, backdoors e Botnets;	
4.8.57	Deve possuir regras que identifiquem comunicações de estações de trabalho e servidores com serviços não autorizados, tais como: consultas DNS em servidor não autorizado, utilização de SMTP server não autorizado, Proxy Server não autorizado;	
4.8.58	Deve possuir regras que identifiquem comunicações p2p, instant messengers e streaming;	
4.8.59	Deve possuir capacidade de geração de relatórios dos seguintes tipos e contendo as seguintes características:	
4.8.60	Resumidos;	
4.8.61	Visão Geral dos Incidentes de Segurança	
4.8.62	Discriminação dos Tipos de Incidentes	
4.8.63	Top Ameaças Analisadas	
4.8.64	Top Hosts Infectados	

Número do Requisito	Detalhamento técnico do requisito	Sugestões
4.8.65	Recomendações de Segurança	
4.8.66	Executivos;	
4.8.67	Deve possuir detalhes técnicos dos incidentes detectados;	
4.8.68	Deve possuir estatística do tráfego analisado;	
4.8.69	Deve possuir indicadores de risco do ambiente;	
4.8.70	Recomendações de Segurança.	
4.9	Deve ser capaz de identificar, filtrar e exibir em interface gráfica, e dinamicamente atualizada, hosts com alto nível de risco, classificando os tipos de riscos/eventos detectados;	
4.10	Deve possuir interface que apresente em tempo real estatísticas de top ameaças detectadas, top arquivos analisados, top hosts afetados, top URL's maliciosas acessadas etc.;	
4.11	Quando detectada uma ameaça, a solução deve prover, podendo esta realizar consultas em site do fabricante, informações sobre ameaça, família da ameaça, estatísticas de segmentos de mercado afetados e recomendações de segurança para eliminar ameaça, correlacionando estas informações com sites ou outros vetores por onde esta ameaça é disseminada;	
4.12	As atualizações do produto (patterns e outros componentes) não devem causar downtime ou impacto na operação;	
4.13	Deve ser capaz de identificar ameaças que afetam dispositivos móveis (Ex: Detecção de comunicação de aplicativo malicioso na plataforma Android);	
4.14	Deve ser capaz de detectar tentativas de mascaramento ou evasão de detecção através do uso de portas comuns ou protocol tunneling;	
4.15	Deve ser capaz de detectar tentativas de scan de rede;	
4.16	Deve ser capaz de detectar propagação de malwares na rede;	
4.17	Deve ser capaz de detectar tentativas de brute-force;	
4.18	Deve ser capaz de detectar tentativas de fuga e roubo de informação;	

Número do Requisito	Detalhamento técnico do requisito	Sugestões
4.19	Deve ser capaz de detectar ameaças que se replicam na rede;	
4.20	Deve ser capaz de detectar Exploits na rede;	
4.21	O Monitoramento de protocolos de comunicação deve ser feito através dos appliances que compõe a solução;	
4.22	A console de gerenciamento deve possuir mapa mundial, onde são marcadas origens de ataques e eventos de segurança monitorados pela solução;	
4.23	Deve permitir busca por informações do destino e origem, incluindo estas: endereço IP, endereço MAC, porta e protocolo;	
4.24	Deve permitir consultas personalizáveis, usando comandos SQL ou atributos pré-definidos;	
4.25	Capacidade de salvar uma investigação antes de ser finalizada;	
4.26	Capacidade de restaurar uma investigação para continuá-la ou consultá-la;	
4.27	Capacidade de emitir relatórios baseados nas investigações;	
4.28	Deve permitir apresentação dos dados consultados em vários formatos, incluindo tabela e gráficos;	
4.29	Deve trabalhar com geo-localização para identificar a origem geográfica de um ataque;	
4.30	Deve ter a capacidade de sugerir termos de busca, de acordo com o conteúdo já buscado numa investigação, para agilizar a obtenção do resultado;	
4.31	Deve permitir exportar sob demanda os logs em texto puro (CSV ou PDF ou similar);	
4.32	Deve sugerir consultas a bases de reputação e whois quando encontrados hosts e nomes de domínio;	
4.33	Deve permitir investigação por tags (palavras-chave) pré-configuradas para facilitar a busca de eventos;	
4.34	Deve permitir recebimento de logs via syslog;	
4.35	Deve permitir encaminhamento de logs via syslog;	
4.36	Deve permitir receber logs de diferentes dispositivos;	
4.37	Deve possuir engine de correlação de eventos;	
4.38	Deve inserir tags personalizadas nos logs, de acordo com regras especificadas pelo usuário;	

Número do Requisito	**Detalhamento técnico** do **requisito**	Sugestões
4.39	Deve enviar alertas via e-mail;	
4.40	Deve permitir a configuração de alarmes personalizados, com base em investigações;	
4.41	Deve informar em sua console alarmes que dispararam, até que o usuário tome alguma ação;	
4.42	A solução deve ser escalável horizontalmente, permitindo que novas instâncias sejam habilitadas, aumentando suas capacidades de detecção e análise;	
4.43	A console de gerenciamento deverá ter dashboards para facilidade de monitoração. As janelas deverão ser customizadas pelo administrador em quantidade e período de monitoração;	
4.44	O administrador deve poder optar por janelas de monitoramento no dashboard a sua disposição e poderá livremente adicionar ou remover de acordo com sua necessidade de visualização;	
4.45	Deverá possuir mapa geográfico que permita a identificação visual sobre a origem de ameaças de modo a facilitar a visualização de eventos críticos para que ações imediatas sejam providenciadas;	
4.46	Deverá possuir a capacidade de atualizar as vacinas, engines, assinaturas e recursos de inspeção de conteúdo de forma agendada e automática;	
4.47	A console de gerenciamento deverá ser gerenciada por Microsoft Edge, Google Chrome ou Firefox;	
4.48	Solução deverá ter mecanismo de busca em sua console de gerenciamento de modo que seja facilitada a busca por detecções;	
4.49	Deve permitir a integração com plataforma de detecção e resposta do próprio fabricante, com objetivo de correlacionar as detecções do NDR com as demais tecnologias de segurança implantadas nas camadas de endpoint, servidores e email;	
4.50	A integração com a solução de detecção e resposta deve permitir que as ameaças sejam rastreadas desde a entrada na rede até tentativas de roubo de dados, exibindo etapas gráficas da ação do atacante;	
4.51	Deve exibir de forma e em tabela, as transações identificadas contendo detalhes do ataque, bem como os Indicadores de Comprometimento (IOCs);	

Número do Requisito	**Detalhamento técnico** do **requisito**	Sugestões
4.52	Deverá ser capaz de identificar ameaças evasivas em tempo real com o provimento de análise profunda e inteligência para identificar e prevenir ataques;	
4.53	Deverá ser capaz de correlacionar regras de detecção de conteúdo malicioso durante todas as fases de um ataque;	
4.54	O sensor de inspeção de rede deve ter a capacidade de integrar-se com a plataforma de investigação e resposta centralizada, a fim de enviar objetos suspeitos e metadados das detecções locais para correlação com as demais soluções de segurança do ambiente;	
4.55	A funcionalidade deve ser licenciada para analisar o throughput total do appliance;	
4.56	Deve permitir a adição e remoção dos diversos recursos de visualização de informações na tela principal de monitoramento da ferramenta, permitindo no mínimo a visualização das seguintes informações:	
4.56.1	Uso de CPU	
4.56.2	Uso de Disco;	
4.56.3	Uso de Memória;	
4.56.4	Tráfego malicioso analisado;	
4.56.5	Todo o tráfego analisado.	
4.57	A solução deverá permitir o envio de logs dos recursos para servidor de logs por meio do protocolo syslog e deverá conter no mínimo:	
4.57.1	Tipo de evento de detecções: Conteúdo malicioso, reputação de URL's, comportamentos maliciosos, comportamentos suspeitos, Exploits, correlações de eventos, Grayware;	
4.57.2	Tipo de eventos de sistemas: Eventos de sistema e eventos de atualizações.	
4.58	A solução deverá ter integração com ferramentas de SIEM;	

Número do Requisito	**Detalhamento técnico** do **requisito**	Sugestões
4.59	Deve possuir capacidade de entregar relatório contendo informações da sequência de execução do artefato malicioso, assim como, detalhes de alterações locais da máquina, conexões externas e envio da informação para fora da rede corporativa;	
4.60	A solução deve ter capacidade de agregação e correlação de logs de eventos de segurança possibilitando coleta de fontes de monitoração para proporcionar informação e identificação de ameaças digitais conhecidas e desconhecidas em trânsito através de logs de sensor;	
4.61	Solução deverá apresentar relatórios customizados de todas as suas funcionalidades e deverá conter no mínimo:	
4.61.1	Computadores infectados;	
4.61.2	Origem de infecções;	
4.61.3	Estatísticas de ameaças;	
4.61.4	Riscos potenciais de segurança;	
4.61.5	Riscos de perda de informações;	
4.61.6	Risco de sistema comprometido;	
4.61.7	Risco de disseminação de ameaças;	
4.61.8	Eventos suspeitos;	
4.61.9	Infecções de malware.	
4.62	A solução deverá apresentar função de pesquisa por logs contendo no mínimo:	
4.62.1	Critérios de pesquisa por dia, mês e ano.	
4.62.2	Possibilidade de pesquisa pelo nome do computador, domínio ou conta, endereço IP, endereço MAC e grupos;	
4.62.3	Possibilidade de pesquisa por ameaças, URL's maliciosas, análises virtuais, correlação de incidentes, nome de malware, protocolo e direção da detecção;	
4.62.4	Os relatórios e logs deverão ser exportados nos formatos PDF ou CSV ou similar.	

Número do Requisito	Detalhamento técnico do requisito	Sugestões
5	**Plataforma de Detecção e Resposta**	
5.1	Plataforma de investigação e correlação de incidentes hospedada em nuvem do próprio fabricante, com data lake próprio para detecção e investigação de atividades maliciosas ou suspeitas para os seguintes contextos:	
5.1.1	Estações de trabalho e servidores;	
5.1.2	Dispositivos móveis (iOS e Android);	
5.1.3	E-mails hospedados no Microsoft Office 365 e outros serviços SMTP;	
5.1.4	Sensores de rede.	
5.2	A solução deve permitir a integração dos eventos ocorridos em outros segmentos de rede e outros appliances com objetivo de correlacionar os ataques na rede;	
5.3	A plataforma deverá permitir a integração com sensores externos para coleta de dados e tomada de ação, incluindo: BigIP F5, Checkpoint, Office 365 , Active Directory, BlockBit, Proxy McAfee, Netscout, Hyper-V, VMWare, logs Apache Web Server, logs HAProxy, logs KeepAlived, ferramentas de Endpoint Security;	
5.4	Deve permitir a integração com outras ferramentas de segurança para compartilhamento de inteligência através de padrões abertos como STIX, TAXII, MISP ou API;	
5.5	Deve permitir a análise em linha de tempo gráfica, representando a sequência da comunicação dos ativos, bem como seu protocolo e direção;	
5.6	Deve identificar tentativas de ataques avançados na rede da CONTRATANTE e correlacionar com eventos das soluções de estação de trabalho, servidores e e-mail, a fim de rastrear o passo-a-passo do ataque na rede;	
5.7	Ao clicar em um dos objetos identificados pela solução de inspeção de rede, a plataforma deverá informar um resumo do ataque em questão, contendo o IP/hostname envolvido, quais protocolos, atividades maliciosas, severidade do incidente, fases do ataque;	

Número do Requisito	**Detalhamento técnico** do **requisito**	Sugestões
5.8	A solução deve ser capaz de associar diferentes modelos de ameaças e associá-los a um único incidente/evento;	
5.9	Deve ter capacidade de apresentar informações relacionadas ao framework MITRE ATT&CK para cada um dos eventos detectados no ambiente nos logs;	
5.10	A visualização das técnicas e táticas deve ser feita através de matriz clicável para detalhamento do item selecionado;	
5.11	A plataforma deve apresentar uma lista com todos os modelos de detecção pré-definidos que a solução possui;	
5.12	Cada modelo deve possuir uma descrição e um score para auxiliar na identificação do risco e priorização da investigação e resposta;	
5.13	Os modelos de detecção deverão possuir níveis de severidade (score) individuais para cada modelo em pelo menos os seguintes níveis:	
5.13.1	Crítico;	
5.13.2	Alto;	
5.13.3	Médio;	
5.13.4	Baixo.	
5.14	Deve permitir ativar ou desativar qualquer modelo de detecção caso necessário;	
5.15	Permitir criação de listas de exceção de objetos para redução de falso-positivo.	
5.16	Deve fazer uso de inteligência artificial e inteligência de ameaças do fabricante da solução para analisar e correlacionar as atividades dos sensores do ambiente;	
5.17	A solução deverá permitir configuração de Single Sign-On (SSO) com suporte a SAML 2.0;	
5.18	Deve ser possível realizar buscas através de strings parciais, exatas, valores nulos, wildcards e caracteres especiais;	

Número do Requisito	**Detalhamento técnico** do **requisito**	Sugestões
5.19	A solução deve prover diferentes níveis de administração e acesso a ferramenta para os usuários em pelo menos: Master Administrator, Administrator, Senior Analyst, Analyst e Auditor;	
5.20	Deve permitir configuração de duplo fator de autenticação para acesso dos usuários à console de gerenciamento;	
5.21	Deve registrar os logs de atividades realizados na console de gerência para fins de auditoria;	
5.22	Ter capacidade de enviar os eventos e detecções para aplicações de SIEM, incluindo Splunk, QRadar ou Azure Sentinel;	
5.23	Deve permitir configuração de notificações por e-mail (SMTP) para envio de alertas e notificações;	
5.24	Possuir painéis que apresentem visualização executiva dos principais incidentes e atividades no ambiente com base nos usuários, aplicações em nuvem acessadas, estações de trabalho e contas de email;	
5.25	A plataforma deve apresentar uma visão unificada do risco baseada nos sensores integrados (do fabricante e de terceiros);	
5.26	A visão de risco apresentada deverá ser exibida através de tendência de evolução;	
5.27	Ao detalhar o indicador de risco, a plataforma deverá exibir o grau de exposição dos dispositivos internos e publicados, os tipos de ataques que o ambiente tem recebido;	
5.28	A plataforma deverá exibir indicadores de risco do ambiente como o tempo médio para correção de vulnerabilidades e qual a relação do indicador com a média global;	
5.29	Possuir modelos pré-definidos pelo fabricante de atividades suspeitas e/ou maliciosas para identificação e categorização de ameaças no ambiente;	
5.30	Utilizar bases de inteligência de ameaças integrando relatórios de inteligência do fabricante e de terceiros para ajudar a identificar ameaças no ambiente e defender-se de maneira proativa;	
5.31	Apresentar os alertas consolidados e correlacionados de ameaças para melhor investigação e resposta;	

Número do Requisito	**Detalhamento técnico** do **requisito**	Sugestões
5.32	Permitir tomar diferentes ações de resposta no ambiente e monitorar cada ação tomada, com opção de desfazê-la;	
5.33	Fornecer a capacidade de realizar buscas avançadas para localizar dados ou objetos no ambiente para análise avançada de atividades ou detecções;	
5.34	Deve integrar relatórios de inteligência criados por especialistas em ameaças do fabricante e terceiros para ajudar na identificação de ameaças;	
5.35	Os relatórios de ameaças do fabricante deverão gerar alertas de detecção caso sejam identificadas atividades presentes nos relatórios dentro do ambiente;	
5.36	Deve ser possível identificar individualmente cada relatório de ameaça;	
5.37	Cada relatório deverá possuir informações como, região/país alvo, plataforma alvo ou campanha de ataques relacionadas a estes relatórios;	
5.38	Deve permitir adicionar bases de inteligência terceiras de forma manual, por API, importando arquivos com base CSV ou STIX através de assinatura de feeds de inteligência de ameaças terceiros;	
5.39	A partir dos relatórios de inteligência, a plataforma deve permitir a varredura automática nos logs para identificação de hosts comprometidos com a ameaça dentro da rede da CONTRATANTE;	
5.40	Deve permitir adicionar no mínimo os seguintes indicativos de comprometimento (IOCs) à base de inteligência:	
5.40.1	Hashes SHA-1;	
5.40.2	URLs;	
5.40.3	IPs;	
5.40.4	Domínios.	
5.41	A base de inteligência terceira deve ser integrada através dos protocolos TAXII 2.0 ou TAXII 2.1;	
5.42	Deve exibir, em forma de tabela, as transações identificadas contendo detalhes do ataque, bem como os Indicadores de Comprometimento (IOCs).	

Número do Requisito	**Detalhamento técnico** do **requisito**	Sugestões
5.43	Os sensores agregados deverão receber comandos enviados pelo NDR para realizar bloqueios de ameaças dentro das cargas de trabalho e estações de trabalho;	
5.44	O sensor deve possuir módulo de investigação, detecção e resposta integrados;	
5.45	Deve incluir agentes para 500 cargas de trabalho para execução das atividades de investigação profunda, correlação de logs e resposta automática;	
5.45.1	O agente para cargas de trabalho deverá ser compatível com os sistemas operacionais conforme item 4.8.51;	
5.45.2	Deve permitir que as detecções sejam correlacionadas com sensores de endpoint, rede e email do próprio fabricante através de plataforma de detecção e resposta;	
5.45.3	Deve possuir capacidade de encaminhar as atividades suspeitas identificadas nas cargas de trabalho para a plataforma de detecção e resposta;	
5.45.4	Deve permitir realizar buscas em todos os dados de atividades enviadas pelas cargas de trabalho que estejam conectados na plataforma, ainda que estas não sejam detectadas como maliciosas;	
5.45.5	Deve prover visualização em linha do tempo com informações dos eventos monitorados em cada carga de trabalho;	
5.45.6	Deve permitir a visualização entre usuários, servidores, processos/comandos, arquivos e demais componentes correlacionados em determinado ataque;	
5.45.7	Deve mostrar, pelo menos, o timestamp, objetos envolvidos (comandos, processos, usuários, servidores)	
5.45.8	Ao clicar em quaisquer dos objetos, a solução deve permitir realizar buscar específicas pelo objeto ou ainda executar ações como executar investigações mais aprofundadas;	
5.45.9	Em caso de incidente, o sensor deverá ter a capacidade de realizar bloqueios automáticos baseados no comando enviado pela plataforma de detecção e resposta ou pelo NDR, pelo menos para solução CheckPoint;	

Número do Requisito	**Detalhamento técnico** do **requisito**	Sugestões
5.46	A plataforma deverá permitir a investigação dentro de cada carga de trabalho para tomar ações de respostas através da console, incluindo:	
5.46.1	Isolar a carga de trabalho;	
5.46.2	Coletar arquivos suspeitos;	
5.46.3	Executar uma sessão de shell remoto;	
5.46.4	Bloquear hashes, URLs, IPs e domínio;	
5.46.5	Submeter o arquivo para análise em sandbox.	
5.47	Os agentes de carga de trabalho deverão ser capazes de executar rastreamento nas máquinas onde estão instalados e após isso deverão fornecer uma lista de todas as recomendações de segurança para os softwares que estejam instalados nas máquinas bem como do sistema operacional;	
5.47.1	Esses rastreamentos devem ocorrer de forma periódica a ser definida pelo administrador;	
5.48	Deverá permitir ainda a configuração de componentes de integração com o vCenter, a fim de permitir a sincronização das máquinas virtuais conectadas a ele;	
5.49	Brechas de segurança descobertas deverão ser protegidas de forma automática e transparente, interrompendo somente o tráfego de rede malicioso nas cargas de trabalho;	
5.50	Deve permitir que a inclusão de exceção de proteção para vulnerabilidades a um determinado perfil ou host;	
5.51	Precisa ter a capacidade de detectar e bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do SO e demais aplicações;	
5.52	Precisa ter a capacidade de varrer a carga de trabalho protegida detectando o tipo e versão do SO, detectando também as demais aplicações, recomendando e aplicando automaticamente regras IDS/IPS que blindem vulnerabilidades existentes no SO e aplicações. Esta varredura deverá poder ser executada sob demanda ou agendada;	

Número do Requisito	**Detalhamento técnico** do **requisito**	Sugestões
5.53	A solução deverá conter regras pré-definidas para detecções de ransomware para as principais famílias deste tipo de malware;	
5.54	Precisa ter a capacidade de detectar uma conexão maliciosa, com a possibilidade de bloquear esta conexão;	
5.55	Sistemas que compõem o item 4.8.51 somados a Solaris, AIX, Virtualizadores (VMWare e Hyper-v). Além de regras para aplicações padrão de mercado, incluindo: Microsoft IIS, Apache Web Server, Joomla, Wordpress, PHP, Java, Apache Tomcat, NodeJS, JBoss, Oracle Application Server, Microsoft Exchange, Oracle Database, SQL Server, MySQL, PostgreSQL, Adobe Acrobat, Microsoft Office, protocolo SMB e navegadores Web (Mozilla Firefox, Microsoft Internet Explorer, Microsoft Edge, Google Chrome e demais derivados Chromium).	
5.56	Precisa ter a capacidade de armazenamento do pacote capturado quando detectado um ataque;	
5.57	As vulnerabilidades deverão ser protegidas antes do lançamento do patch oficial do fabricante, permitindo proatividade na proteção;	
5.58	Deverá possibilitar a criação de regras de vulnerabilidades customizadas, para proteger aplicações desenvolvidas pela CONTRATANTE;	
5.59	Precisa possuir a capacidade de detectar e controlar conexões de aplicações específicas incluindo ferramentas de acesso remoto tipo Team Viewer, programas P2P e instant Messaging;	
5.60	Precisa ter a capacidade de detectar e bloquear ataques em aplicações Web tais como SQL Injection e Cross Site Scripting. Deverá ainda existir a possibilidade de captura do pacote relacionado ao ataque para fins de investigação do incidente;	
5.61	Deverá permitir customização avançada e criação de novas regras de proteção de aplicações web, protegendo contra vulnerabilidades específicas de sistemas web legados e/ou proprietários;	
5.62	Ser capaz de permitir ou negar que métodos utilizados por Webservers por regras de proteção de vulnerabilidades;	

Número do Requisito	**Detalhamento técnico** do **requisito**	Sugestões
5.63	Deverá ser capaz de inspecionar tráfego criptografado de entrada nas cargas de trabalho;	
5.64	Deverá inspecionar tráfego de aplicações Web em servidores buscando identificar: SQL injection, Crossite script, tamanho de URI fora de padrão, caracteres fora de padrão para requisição de URI, Double Decoding Exploit;	
5.65	As regras de blindagem contra vulnerabilidades deverão conter links com referências externas, isto quando aplicável, explicando a vulnerabilidade do fabricante ou CVE relacionado;	
5.66	Deverá possibilitar a criação de regras manuais para o bloqueio de tráfego customizado. Como por exemplo, bloquear acesso a um determinado website ou bloquear acesso de uma aplicação X;	
5.67	Deverá possibilitar a criação de regras manuais baseadas em padrão XML, forma de assinatura ou padrões que possuam começo e fim coincidentes;	
5.68	Deverá bloquear tráfego por aplicação independente da porta que a aplicação utilize, de modo que a aplicação não consiga comunicar na rede, como por exemplo, bloqueio de tráfego de uma determinada web browser ou aplicação de backup;	
5.69	Deve ser capaz de habilitar modo debug na coleta dos pacotes de forma a capturar o tráfego anterior e posterior ao que foi bloqueado para facilidade de análise;	
5.70	As regras de vulnerabilidade do sensor poderão atuar detectando ou bloqueando os eventos que as violem de modo que o administrador possa optar por qual ação tomar;	
5.71	As regras de vulnerabilidade deverão apresentar severidade baseada em CVEs;	
5.72	As regras de IPS poderão ter sua capacidade de LOG desabilitado;	
5.73	As regras devem ser atualizadas automaticamente pelo fabricante;	
5.74	Poderá atuar no modo em linha para proteção contra-ataques ou modo escuta para monitoração e alertas.	
5.75	A solução deverá receber comandos enviados pelo NDR para realizar bloqueios de ameaças dentro das estações de trabalho;	

Número do Requisito	**Detalhamento técnico** do **requisito**	Sugestões
5.77.13.1	Isolar a estação de trabalho;	
5.77.13.2	Coletar arquivos suspeitos;	
5.77.13.3	Executar uma sessão de shell remoto;	
5.77.13.4	Bloquear hashes, URLs, IPs e domínio;	
5.77.13.5	Submeter o arquivo para análise em sandbox.	
5.77.14	O agente deverá coletar informações acerca das aplicações em nuvem acessadas pelo usuário, exibindo, pelo menos, sua categoria, quantidade de acessos, quais os usuários, quais os dispositivos e o nível de risco da aplicação (baseado no compliance com normas e vazamentos ocorridos);	
5.77.15	Deverá coletar informações sobre vulnerabilidades nas estações de trabalho e exibir na plataforma centralizada pelo menos, CVE/ID, atividades de explorações no mundo, CVSS Score, sistemas afetados, dispositivos internos com a vulnerabilidades, regras de proteção disponíveis e quantidade de tentativas de exploração;	
5.77.16	Quando detectado um ataque, a solução deverá permitir que o administrador faça uma análise de causa raiz diretamente pela console para identificar todas as atividades realizadas pela ameaça;	
5.77.17	Deve permitir que o administrador realize a investigação dos processos e atividades maliciosas dentro das estações de trabalho em formato de cadeia ou linha do tempo de eventos.	
6	**Demais requisitos**	
6.1	A SOLUÇÃO não poderá ter nenhuma restrição atrelada ao uso de software e hardware vinculado à volumetria analisa	
6.1.1	O licenciamento necessário para uso de toda capacidade deve fazer parte da proposta.	
6.1.2	Não será aceito vincular o aumento de qualquer volumetria no custo do APPLIANCE contratado.	
6.2	Deve permitir a utilização de todas as funcionalidades, tecnologias e recursos especificados, de maneira perpétua, irrestrita e sem necessidade de licenciamentos, renovações ou ônus adicionais;	

Número do Requisito	**Detalhamento técnico** do **requisito**	Sugestões
6.3	A CONTRATANTE poderá utilizar todas funcionalidades e recursos de hardware e software entregues, ativas, com o APPLIANCE de acordo com suas necessidades, sem custo adicional.	