TRIBUNAL REGIONAL ELEITORAL DA BAHIA
Seção de Contratos

ATA DE REGISTRO DE PREÇOS N.º 13/2022

PROCESSO (SEI) N.º 0015838-60.2021.6.05.8000

A UNIÃO, por intermédio do TRIBUNAL REGIONAL ELEITORAL DA BAHIA, com sede na 1ª Avenida do Centro Administrativo da Bahia, n.º 150, Salvador - BA, inscrito no CNPJ/MF sob o n.º 05.967.350/0001-45, neste ato representado pelo seu Diretor-Geral, Raimundo de Campos Vieira, considerando o resultado do Pregão Eletrônico n.º 02/2022, cujo objeto se constitui no Registro de Preços para eventual aquisição de equipamentos e programas de datacenter, RESOLVE, com amparo nas Leis nº 8.666/93 e n.º 10.520/2002, nos Decretos n.ºs 10.024/2019 e 7.892/2013, e na Resolução Administrativa n.º 10/2007 do TRE da Bahia, registrar os preços da empresa **SEVEN SECURE TECNOLOGIA DA INFORMAÇÃO LTDA**, inscrita no CNPJ/MF n.º 30.896.451/0001-10, com sede no Setor SMAS, Trecho 03, Conjunto 03, Bloco C, Sala 15, Ed. The Union, Zona Industrial, Guará, Brasília – DF, CEP: 71.215-300, telefone n.º (61) 99871-0900, e-mail contato@7secure.com.br e douglas@7secure.com.br, representada neste ato pelo Sr. Douglas Souza Araújo, portador da Carteira de Identidade n.º F0742502 DPF/DF, inscrito no CPF/MF sob n.º 001.230.551-05, **indicados no Anexo I desta Ata**, observadas as condições do Edital que integra este instrumento de registro, independentemente de transcrição.

Será incluído nesta Ata, no Anexo II, o registro das **licitantes** que aceitaram cotar os bens ou serviços com preços iguais aos da **licitante vencedora** na sequência da classificação do certame, excluído o percentual referente à margem de preferência, quando o objeto não atender aos requisitos previstos no art. 3º da Lei n.º 8.666/93.

O prazo de validade improrrogável da Ata de Registro de Preços é de 12 (doze) meses, contado da data da sua assinatura, excluído o dia do começo e incluído o do vencimento.

A assinatura da presente Ata implicará na plena aceitação, pelo fornecedor, das condições estabelecidas no Edital da licitação e seus anexos.

A licitante vencedora somente será liberada, sem penalidade, do compromisso previsto nesta Ata, nas hipóteses previstas no art. 18, § 1º, art. 19, inciso I e art. 21, incisos I e II, do Decreto n.º 7.892/2013.

REAJUSTE: 1. Os preços pactuados serão reajustados, observado o interregno mínimo de um ano, a contar da data de apresentação da proposta, aplicando-se a variação do IPCA, calculado e divulgado pelo IBGE. **2.** Caso o índice estabelecido para reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado em substituição o que vier a ser determinado pela legislação em vigor, à época. **3.** Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial para reajustamento dos preços. **4.** Caso os preços contratados, após o cálculo referente ao reajuste citado no item anterior, venham a ser superiores aos praticados no mercado, as partes deverão rever os preços para adequá-los às condições existentes no início do contrato firmado.

Passam a fazer parte desta Ata, para todos os efeitos, a documentação e propostas apresentadas pela licitante.

Fica eleito o foro da Seção Judiciária da Justiça Federal de Salvador, capital do estado da Bahia, para dirimir qualquer dúvida oriunda da execução deste ajuste.

E, por estarem justas e contratadas, assinam as partes o presente instrumento, em 02 (duas) vias de igual teor e forma, para que produza seus jurídicos e legais efeitos.

RAIMUNDO DE CAMPOS VIEIRA:13353578587
Assinado de forma digital por RAIMUNDO DE CAMPOS VIEIRA:13353578587
Dados: 2022.03.24 12:39:09 -03'00'

SEVEN SECURE TECNOLOGIA DA INFORMACAO LTDA:30896451000110
Assinado de forma digital por SEVEN SECURE TECNOLOGIA DA INFORMACAO LTDA:30896451000110
Dados: 2022.03.24 12:06:30 -03'00'

Raimundo de Campos Vieira
Diretor-Geral do TRE-BA

Douglas Souza Araújo
CPF Nº 001.230.551-05
SEVEN SECURE TECNOLOGIA DA INFORMAÇÃO LTDA

ANEXO I – PREÇOS

Item	Descrição	Quantidade	Valor Unitário (R$)	Valor Total (R$)
6	Programa de Prospecção de Vulnerabilidades em Computadores. As especificações detalhadas constam no Anexo A do Termo de Referência.	01 unidade	268.470,50	268.470,50

ANEXO II – CADASTRO DE RESERVA

Não houve Cadastro de Reserva.

ANEXO III – TERMO DE REFERÊNCIA

1. OBJETO

1.1 Registro de Preços para Eventual Aquisição de Equipamentos e Programas de Datacenter, conforme especificações constantes do Anexo A deste termo.

2. JUSTIFICATIVA

2.1 Troca de equipamentos críticos em fim de vida útil ou defeituosos, bem como a ampliação do quantitativo existente por conta de novas necessidades, conforme detalhado nos estudos preliminares. Fazem parte dessa iniciativa: Servidores, Unidades de Armazenamento NAS, Unidades de Cópia de Segurança Automatizadas, Programa de Rede Definida por *Software*, Firewall de Aplicações com Balanceador de Carga, Programa de Prospecção de Vulnerabilidades, Certificados Digitais, Sistemas Operacionais e suporte técnico para E-mail Zimbra.

A modalidade de registro de preços é a que mais se adequa às aquisições, visto que todos os itens aqui estão sujeitos a um grau de indeterminação quanto ao quantitativo da eventual aquisição ou quanto ao momento da sua eventual aquisição, considerando-se que ou estão associados a demandas em quantidades variáveis, pois podem requerer ampliações imediatas motivadas por novas demandas de uso pela Administração do Tribunal, ou estão dependentes de conclusão de fases das complexas implantações, traduzindo-se na prática em condições de entregas parceladas ou quantitativo não definido previamente, em consonância ao previsto no art. 3º do Decreto 7892/2013, incisos II e IV:

> *II - quando for conveniente a aquisição de bens com previsão de entregas parceladas ou contratação de serviços remunerados por unidade de medida ou em regime de tarefa;*
>
> *IV – quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela Administração.*

Para todos os itens a modalidade de licitação indicada é o **pregão eletrônico**. Por questões técnicas como compatibilidade ou de estratégia de implantação visando assegurar uma transição primorosa, adequada a ambientes críticos de produção, houve indicação de marca e modelo para os itens 1, 4, 8, 9, 10, 12 e 13. De maneira sintética, o item 1 expande um quantitativo de equipamentos que só possuem compatibilidade com equipamentos iguais em federação; o item 4 precisa ser compatível com o VMWare VSphere e os

sistemas de virtualização dos servidores atuais, que serão expandidos no item 1; o item 8 é serviço de suporte para o produto já adquirido Zimbra; e os itens 9, 10, 12 e 13, conforme detalhado nos estudos preliminares, são licenças de um sistema operacional do qual diversos sistemas em produção no Tribunal são dependentes.

Para todos os itens constam as especificações gerais com a indicação dos modelos de referência. Exceto os itens 9 , 10, 12 e 13, nenhum outro item poderá ter aplicação especificamente do inciso III do artigo 48 da Lei Complementar nº 123/2006 e do inciso IV do artigo 2º do Decreto nº 8.538/2015 devido à necessidade de padronização desses equipamentos, por motivo da implementação da gerência remota centralizada.

O prazo contratual para os itens deverá ser de 60 meses após a assinatura, refletindo o tempo de vigência do suporte técnico. Para os itens 7, 8, 9, 10, 12 e 13, o termo de contrato pode ser substituído por Nota de Empenho. A modalidade de licitação sugerida para este registro de preços é o **pregão eletrônico**, com **preço por item**.

2.1.1. Relação Demanda Prevista e Quantidade a Ser Contratada.

ITEM	DESCRIÇÃO	QUANTIDADE
1	Nó de Hiperconvergência HPE Simplivity Extra-Large. As especificações detalhadas constam no Anexo A deste Termo de Referência.	05 unidades
2	Servidor de Rede. As especificações detalhadas constam no Anexo A deste Termo de Referência.	03 unidades
3	Unidade de Armazenamento NAS. As especificações detalhadas constam no Anexo A deste Termo de Referência.	03 unidades
4	VMWare Network Virtualization and Security Platform Advanced Edition (VMware NSX). As especificações detalhadas constam no Anexo A deste Termo de Referência.	20 unidades
5	Appliance Virtual de Balanceamento de Carga com Firewall de Aplicações. As especificações detalhadas constam no Anexo A deste Termo de Referência.	02 unidades
6	Programa de Prospecção de Vulnerabilidades em Computadores. As especificações detalhadas constam no Anexo A deste Termo de Referência.	01 unidade
7	Certificados Digitais A1 SSL. As especificações detalhadas constam no Anexo A deste Termo de Referência.	100 unidades
8	Assinatura de Suporte técnico e atualizações para 2000 unidades de Zimbra Network Edition Standard e 250 unidades de Zimbra Network Edition	01 unidade

ITEM	DESCRIÇÃO	QUANTIDADE
	Professional. As especificações detalhadas constam no Anexo A deste Termo de Referência.	
9	Licença de Windows Server Datacenter 2019. As especificações detalhadas constam no Anexo A deste Termo de Referência.	7 unidades
10	Windows Server Datacenter 2019 CAL. As especificações detalhadas constam no Anexo A deste Termo de Referência.	403 unidades
11	Unidade de cópia de segurança automatizada. As especificações detalhadas constam no Anexo A deste Termo de Referência.	02 unidades
12	Licença de Windows Server Datacenter 2019. As especificações detalhadas constam no Anexo A deste Termo de Referência.	93 unidades
13	Windows Server Datacenter 2019 CAL. As especificações detalhadas constam no Anexo A deste Termo de Referência.	1597 unidades

3. LOCAL E PRAZO DE ENTREGA

3.1 A Contratada deverá entregar o material na SEGEP localizada no Edifício-Sede do Tribunal Regional Eleitoral da Bahia (TRE-BA), sito na 1ª Avenida do Centro Administrativo da Bahia, nº 150, Salvador – Bahia, ou, ainda, no Centro de Apoio Técnico – CAT, localizado no Loteamento Porto Seco Pirajá, Quadra A, Lote 16/17, Rua A, Via Marginal da BR 324, Salvador-Ba, conforme opção da Administração a ser informada quando do agendamento da entrega.

3.2 Horários de entrega: 13h às 18h, de segunda à quinta-feira, e 08h às 12h, às sextas-feiras.

3.3 A Contratada deverá, obrigatoriamente, consultar a SEGEP, através dos telefones (71 - 3373-7077 ou 71 - 3373-7357), ou através do e-mail segep@tre-ba.jus.br, para fazer o agendamento da entrega.

3.4 O prazo para a entrega do material solicitado será de 30 dias, contados do recebimento, pela Contratada, do "Pedido de Fornecimento". O Pedido de Fornecimento será emitido pela Fiscalização do Contrato, no prazo máximo de 5 dias, contados da data do recebimento da via contratual/nota de empenho pela Contratada.

3.5 Correrão por conta da Contratada quaisquer providências relativas à descarga do material, incluindo-se aí a necessária mão de obra.

3.6 Em caso de paralisação das atividades dos setores responsáveis pelo recebimento dos bens durante o Recesso Forense (entre 20 de dezembro e 6 de janeiro do ano subsequente), haverá a suspensão dos prazos de entrega em favor da Contratada. Neste caso, a empresa será previamente notificada pela Fiscalização do Contrato.

3.7 Os *softwares* deverão ser entregues suas chaves eletrônicas por e-mail seinfra@tre-ba.jus.br, no prazo máximo de 05 dias úteis, a partir do recebimento do "Pedido de Fornecimento".

4. RECEBIMENTO

4.1 O recebimento ocorrerá em duas etapas:

a) **Recebimento provisório**: o material será recebido provisoriamente no momento da entrega, para efeito de posterior verificação de sua conformidade com as especificações constantes do Edital e da proposta, ficando, nesta ocasião, suspensa a fluência do prazo de entrega inicialmente fixado.

b) **Recebimento definitivo**: no prazo de 05 dias após o recebimento provisório, a Fiscalização do Contrato avaliará as características do material que, estando em conformidade com as especificações exigidas, será recebido definitivamente.

4.2 A Contratada garantirá a qualidade do material fornecido, obrigando-se a substituir aquele que apresentar vícios ou incorreções resultantes da fabricação ou de sua correta utilização que o tornem impróprio ou inadequado para o consumo a que se destina ou lhe diminuam o valor.

4.3 Em caso de irregularidades apuradas no momento da entrega, o material poderá ser recusado de pronto, mediante termo correspondente, ficando dispensado o recebimento provisório, e fazendo-se disso imediata comunicação escrita ao fornecedor.

4.4 Se após o recebimento provisório, constatar-se que o fornecimento foi efetuado em desacordo com o pactuado ou foi entregue quantitativo inferior ao solicitado, a Fiscalização do Contrato notificará por escrito a Contratada para substituir, às suas expensas, o material recusado ou complementar o material faltante, no prazo que lhe restar daquele indicado para entrega.

4.5 Se a Contratada não substituir ou complementar o material entregue em desconformidade com as condições exigidas no edital, o fiscal do contrato glosará a nota fiscal, no valor do material não entregue ou recusado, e a encaminhará para pagamento, acompanhada de relatório circunstanciado, informando, ainda, o valor a ser retido cautelarmente, para fazer face a eventual aplicação de multa.

4.6 Caso a Contratada não retire, no prazo de 90 dias, a contar do recebimento da notificação, o material recusado, ficará caracterizado o seu abandono, nos termos do disposto no artigo 1.275, Inciso III, do Código Civil, podendo a Contratante incorporá-lo ao seu patrimônio, encaminhá-lo a outros órgãos da Administração Pública ou, ainda, doá-lo nos termos do disposto no Decreto nº 9.373/2018.

4.7 A Contratada fará constar da nota fiscal os valores unitários e respectivos valores totais em conformidade com o constante da correspondente nota de empenho/contrato, atentando-se para as inexatidões que poderão decorrer de eventuais arredondamentos.

4.8 Consoante o disposto no artigo 32 da Lei n° 12.305/2010, as embalagens dos materiais devem ser fabricadas com materiais que propiciem a reutilização ou a reciclagem, devendo-se assegurar que sejam restritas em volume e peso às dimensões requeridas à proteção do conteúdo e à comercialização do

produto, projetadas de forma a serem reutilizadas de maneira tecnicamente viável e compatível com as exigências aplicáveis ao produto que contêm, ou recicladas, se a reutilização não for possível.

5. GARANTIA DE ADEQUAÇÃO DO PRODUTO

5.1 A Contratada, no ato de entrega dos bens, deverá apresentar o Termo de Garantia.

5.2 A Contratada deverá oferecer garantia, pelo prazo mínimo de 60 meses (ou pelo prazo constante na descrição de cada item), contado a partir do recebimento definitivo.

5.3 Na vigência da garantia, a Contratada obrigar-se-á a reparar, sem ônus para a Contratante (garantia on site), o objeto contratado que apresentar vícios ou incorreções resultantes da fabricação ou de sua correta utilização que o tornem impróprio ou inadequado para o consumo a que se destina ou lhe diminuam o valor no prazo máximo de 30 dias úteis, a contar do primeiro dia útil seguinte ao do recebimento, pela Contratada, da comunicação de inconformidade.

5.4 O término do atendimento ocorrerá no dia de conclusão do reparo e da disponibilidade do objeto em perfeito estado de uso nas dependências da Contratante.

5.5 O pedido de substituição ou de reparo do objeto contratado, durante o período de garantia, poderá ser formalizado por telefone, e-mail, fax ou outro meio hábil de comunicação.

5.6 Não sendo o vício sanado no prazo do subitem 5.3, a Contratada será notificada para que substitua o produto por outro novo da mesma espécie, marca e modelo, em perfeitas condições de uso, em no máximo 30 dias, a contar do primeiro dia útil seguinte ao do recebimento da notificação, sob pena de serem-lhe aplicadas as sanções previstas no edital e no contrato.

5.7 A garantia, em todos os casos, engloba a proteção contra vícios, defeitos ou incorreções advindas da fabricação, montagem e desgaste excessivo.

6. OBRIGAÇÕES DA CONTRATADA

6.1 São obrigações da Contratada, além daquelas explícita ou implicitamente contidas no presente termo de referência e na legislação vigente:

a) entregar os bens no prazo, nas especificações e na quantidade constantes neste termo de referência, assim como com as características descritas na proposta;

b) atender às solicitações da Contratante nos prazos estabelecidos neste instrumento;

c) não fornecer quantidade ou modelo diversos do solicitado;

d) substituir os produtos danificados em razão de transporte, descarga ou outra situação que não possa ser imputada à Administração;

e) responder pelos encargos previdenciários, trabalhistas, fiscais e comerciais resultantes da execução do contrato;

f) responder por quaisquer danos pessoais ou materiais causados por seus empregados à Administração e/ou a terceiros na execução deste Contrato;

g) manter, durante a execução do ajuste, todas as condições de habilitação exigidas para a contratação;

h) reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções;

i) não subcontratar, ceder ou transferir, no todo ou em parte, o objeto do contrato, salvo se autorizado neste termo de referência;

j) prestar garantia de adequação dos produtos (qualidade, segurança, durabilidade e desempenho), em conformidade com as condições estabelecidas neste termo de referência.

7. OBRIGAÇÕES DA CONTRATANTE

7.1 A Contratante obriga-se a:

a) acompanhar e fiscalizar a execução do ajuste, anotando em registro próprio as ocorrências acaso verificadas, determinando o que for necessário à regularização das faltas ou defeitos observados;

b) prestar esclarecimentos que venham a ser solicitados pela Contratada;

c) efetuar os pagamentos nas condições e nos prazos constantes neste termo de referência e no edital;

d) zelar para que, durante a vigência do Contrato, a Contratada cumpra as obrigações assumidas, bem como sejam mantidas as condições de habilitação e qualificação exigidas no processo licitatório;

e) determinar a reparação, a correção, a remoção ou a substituição do objeto do contrato em que se verificarem vícios, defeitos ou incorreções.

8. INADIMPLEMENTO E PENALIDADES

8.1 A Administração poderá aplicar à licitante vencedora, pelo descumprimento total ou parcial das obrigações assumidas, as sanções previstas na Lei e no Contrato, sendo a multa calculada dentro dos seguintes parâmetros:

a) atrasar injustificadamente a entrega do objeto contratado – **0,5%, sobre o valor do material entregue em atraso, por dia de atraso, até o máximo de 20 dias;**

b) inexecução parcial – **20% sobre o valor do material não entregue;**

c) inexecução total – **20% sobre o valor total contratado;**

d) atrasar, até no máximo **15 dias**, o atendimento para a reparação do vício ou incorreções ou a substituição do produto que apresentou, dentro do prazo de garantia, vícios ou incorreções decorrentes da fabricação ou do seu uso correto que o tornem impróprio ou inadequado para o consumo a que se destina ou lhe diminuam o valor – **1% do valor de aquisição do bem, por dia de atraso;**

e) não realizar a reparação do vício ou incorreções ou a substituição do produto que apresentou, dentro do prazo de garantia, vícios ou incorreções decorrentes da fabricação ou do seu uso correto que o tornem impróprio ou inadequado para o consumo a que se destina ou lhe diminuam o valor – **20% do valor de aquisição do material não substituído.**

8.2 Ultrapassado o prazo estabelecido no **subitem 8.1, alínea "a",** a Administração poderá não receber os itens pendentes de entrega.

8.3 A aplicação da penalidade estabelecida no **subitem 8.1, alínea "e"** não afasta a obrigação da devolução do valor pago pela aquisição do bem.

9. MEDIDAS ACAUTELADORAS

9.1 Ocorrendo inadimplemento contratual, a Administração poderá, com base no artigo 45 da Lei nº 9.784/1999 e *artigo 26, § 1º, da Portaria nº 305/2019*, do TRE/BA, reter de forma cautelar, dos pagamentos devidos à Contratada, valor relativo a eventual multa a ser-lhe aplicada.

9.2 Finalizado o processo administrativo de apuração das faltas contratuais cometidas pela Contratada, tendo a Contratante decidido pela penalização, o valor retido cautelarmente será convertido em multa. Não havendo decisão condenatória, o valor será restituído, monetariamente corrigido pelo mesmo índice de reajuste dos pagamentos devidos à Contratada.

10. PAGAMENTO

10.1 Observada a ordem cronológica estabelecida no art. 5º da Lei 8.666/93, o pagamento será efetuado sem qualquer acréscimo financeiro, mediante depósito através de ordem bancária, nos seguintes prazos e condições:

10.1.1 Para valor igual ou inferior a R$ 17.600,00: até o 5º dia útil subsequente à apresentação da nota fiscal;

10.1.2 Para valor superior a R$ 17.600,00: até o 10º dia útil subsequente à apresentação da nota fiscal.

10.2 Condiciona-se o pagamento a:

I – Apresentação da nota fiscal discriminativa da execução do objeto contratado;

II – Declaração da Fiscalização do Contrato de que o fornecimento se deu conforme pactuado.

10.3 A Contratada indicará na nota fiscal o nome do Banco e os números da agência e da conta corrente para efetivação do pagamento.

10.4 A Contratante, observados os princípios do contraditório e da ampla defesa, poderá deduzir, do montante a pagar à Contratada, os valores correspondentes a multas, ressarcimentos ou indenizações por esta devidos.

11. MEIOS DE COMUNICAÇÃO

11.1 As notificações emitidas pela Administração que implicarem abertura de prazo para cumprimento de obrigações, assim como as intimações dos despachos ou decisões que imponham deveres, restrições de direito ou sanções à Contratada, deverão ser feitas pessoalmente, mediante ciência nos autos, ou por meio eletrônico, com confirmação inequívoca do recebimento.

11.1.1 Frustradas as tentativas de comunicação pelos meios acima citados, esta deverá ser realizada por correspondência com aviso de recebimento ou por qualquer outro meio idôneo que assegure a certeza da ciência do interessado, ou ainda, em caso de aplicação de sanção, por edital, no Diário Oficial da União – DOU, quando ignorado, incerto ou inacessível o lugar em que o fornecedor se encontrar.

11.1.2 A comunicação dos atos processuais será dispensada quando o representante da Contratada revelar conhecimento de seu conteúdo, manifestado expressamente por qualquer meio.

12. DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) – LEI 13709/18

12.1 O TRE-BA e a Contratada se comprometem a proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, relativos ao tratamento de dados pessoais, inclusive nos meios digitais, atuando da seguinte forma:

12.2 Mediante prévia e fundamentada aprovação do TRE-BA, responsabilizando-se a Contratada por obter o consentimento dos titulares (salvo nos casos em quer opere outra hipótese legal de tratamento). Os dados assim coletados só poderão ser utilizados na execução dos serviços especificados neste contrato, e em hipótese alguma poderão ser compartilhados ou utilizados para outros fins;

12.3 Encerrada a vigência do contrato ou não havendo mais necessidade de utilização dos dados pessoais, sejam eles sensíveis ou não, a Contratada providenciará seu descarte de forma segura.

12.4 A Contratada dará conhecimento formal aos seus empregados das obrigações e condições acordadas neste item, inclusive no tocante à Política de Privacidade do TRE-BA, cujos princípios deverão ser aplicados à coleta e tratamento dos dados pessoais de que trata a presente cláusula.

12.5 O eventual acesso, pela Contratada, às bases de dados que contenham ou possam conter dados pessoais ou segredos de negócio implicará para a mesma e para seus prepostos – devida e formalmente instruídos nesse sentido – o mais absoluto dever de sigilo, no curso do presente contrato e pelo prazo de até 10 anos contados de seu termo final.

12.6 Representante da Contratada manterá contato formal com representante do TRE-BA, no prazo de 24 (vinte e quatro) horas da ocorrência de qualquer incidente que implique violação ou risco de violação de dados pessoais, para que este possa adotar as providências devidas, na hipótese de questionamento das

autoridades competentes.

12.7 A critério do TRE-BA, a Contratada poderá ser provocada a preencher um relatório de impacto, conforme a sensibilidade e o risco inerente dos serviços objeto deste contrato, no tocante a dados pessoais.

ANEXO A

Especificações

DO TERMO DE REFERÊNCIA

Os códigos e descrições do CATMAT, constantes do SIASG, citados pelo COMPRASNET podem eventualmente divergir da descrição dos itens licitados quanto a especificações e outras características. Havendo divergência quanto ao código/descrição CATMAT, valem as especificações detalhadas neste Termo de Referência.

ESPECIFICAÇÕES DO ITEM 6 (CATSER 27472)

ITEM 6 – PROGRAMA DE PROSPECÇÃO DE VULNERABILIDADES	
1.	PROGRAMA DE PROSPECÇÃO DE VULNERABILIDADES
1.1	A solução deve possuir licenciadas todas as funcionalidades para realizar varreduras (scans) de vulnerabilidades, avaliação de configuração e conformidade (baseline e compliance), indícios e padrões de códigos maliciosos conhecidos (malware);
1.2	A solução deve possuir recurso de varredura ativa, onde o scanner comunica-se com os alvos (ativos) através da rede;
1.3	A solução de gestão de vulnerabilidades deve suportar varreduras de dispositivos de IoT;
1.4	Deve ser capaz de identificar no mínimo 50.000 CVEs (Common Vulnerabilities and Exposures);
1.5	A solução deve ter a capacidade de adicionar etiquetas (tags) aos ativos de maneira automática, manual e possibilitar ouso de regras com parâmetros específicos para aplicação das mesmas;
1.6	Deve atribuir a todas as vulnerabilidades uma severidade baseada no CVSSv3 score;
1.7	A solução deve calcular a criticidade com base nos dados agregados e consolidados do ativo, dados de segurança, sistema e conformidade, bem como hierarquias e prioridades;
1.8	A solução deve fornecer criptografia de ponta a ponta dos dados de vulnerabilidades;
1.9	A solução deve possuir a capacidade de armazenar informações dos ativos descobertos no ambiente;
1.10	Deve possuir um sistema de busca de informações de um determinado ativo com no mínimo as eguintes características:
1.10.1	Por sistema operacional;
1.10.2	Por um determinado software instalado;

ITEM 6 – PROGRAMA DE PROSPECÇÃO DE VULNERABILIDADES
1.10.3 Por Ativos impactados por uma determinada vulnerabilidade.4.1.11. A solução deve possuir suporte para a adição de detecções personalizadas usando o OVAL (Open Vulnerability Assessment Language);
1.11 Deve permitir aceitar o risco de uma determinada vulnerabilidade encontrada no ambiente;
1.12 Possibilitar alterar a criticidade de determinada vulnerabilidade de forma manual;
1.13 A solução deve possuir um sistema de pontuação e priorização das vulnerabilidades;
1.14 A solução deve ser capaz de aplicar algoritmos de aprendizagem de máquina (machine learning) para analisar as características relacionadas a vulnerabilidades;
1.15 O sistema de pontuação e priorização de vulnerabilidades deve avaliar no mínimo as seguintes características:
1.15.1 CVSSv3 Impact Score;
1.16 Idade da Vulnerabilidade;
1.17 Se existe ameaça ou exploit que explore a vulnerabilidade;
1.18 Número de produtos afetados pela vulnerabilidade;
1.19 Deve ser capaz de fazer a correlação em tempo real de ameaças ativas contra vulnerabilidades encontradas, incluindofeeds de inteligência de ameaças ao vivo;
1.20 Deve possuir uma API para automação de processos e integração com aplicações terceiras permitindo, no mínimo, aextração de dados para carga no SIEM.
1.21 Deve possuir uma API para automação de processos e integração com aplicações ITSM do órgão para asvulnerabilidades encontradas, permitindo o agrupamento no chamado por ações corretivas;
1.22 A solução deve permitir a instalação de agentes em estações de trabalho e servidores, para varredura diretamente nosistema operacional;
1.23 A solução deve ser capaz de produzir relatórios nos seguintes formatos: PDF, CSV e HTML;
1.24 A solução deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados;
1.25 A solução deve ser licenciada para o uso ilimitado de sensores passivos de rede para realizar o monitoramento emtempo real;
1.26 A solução deve possuir sensores, no mínimo, com as seguintes funcionalidades:
1.26.1 Execução de verificação completa do sistema (rede), adequada para qualquer host;
1.26.2 verificação sem recomendações da rede, para que se possa personalizar totalmente as

ITEM 6 – PROGRAMA DE PROSPECÇÃO DE VULNERABILIDADES
configurações da verificação;
1.26.3 Autenticação de hosts e enumeração de atualizações ausentes;
1.26.4 Execução de varredura simples para descobrir hosts ativos e portas abertas;
1.26.5 Utilização de um scanner para verificar aplicativos da web;
1.26.6 Avaliação de dispositivos móveis;
1.26.7 Auditoria de configuração de serviços em nuvem de terceiros;
1.26.8 Auditoria de configuração dos gerenciadores de dispositivos móveis;
1.26.9 Auditoria de configuração dos dispositivos de rede;
1.26.10 Auditoria de configurações do sistema em relação a uma linha de base conhecida;
1.26.11 Detecção de desvio de segurança Intel AMT;
1.26.12 Verificação de malware nos sistemas Windows e Unix;
1.27 Deve ser possível determinar em tempo real quais portas de serviços (UDP/TCP) estão abertas em determinado ativo;
1.28 A solução deve ser capaz de realizar em tempo real a descoberta de novos ativos para no mínimo:
1.28.1.1 Bancos de dados;
1.28.1.2 Hypervisors (no mímino VMWare ESX/ESXi);
1.28.1.3 Dispositivos móveis;
1.28.1.4 Dispositivos de rede;
1.28.1.5 Endpoints;
1.28.1.6 Aplicações;
1.29 A solução deve ser capaz de em tempo real detectar logins e downloads de arquivos em um compartilhamento de rede;
1.30 Permitir identificar vulnerabilidades associadas a servidores SQL no tráfego de rede;
1.31 A solução deve possuir interface para integração com as principais soluções de SIEM de mercado, tais como IBMQRadar, Microfocus ArcSight e Splunk.
1.32 A solução deve possibilitar a realização de cópias de segurança, funcionamento em alta disponibilidade e criptografia detodos os dados armazenados, além de incluir todo o software e licenciamento necessários para o funcionamento completo deacordo com as funcionalidades

ITEM 6 – PROGRAMA DE PROSPECÇÃO DE VULNERABILIDADES
previstas neste Termo de Referência.
1.33 A atualização das ameaças deve ocorrer diariamente e sem interrupção dos serviços.
1.34 Configuração de segurança e acesso à gerência da solução:
1.34.1 Todos os dados armazenados nos servidores da solução devem ser criptografados e possuir logs de acesso;
1.34.2 Os dados em trânsito devem usar ao menos o algoritmo TLS 1.2 de chave 2048 bits;
1.34.3 Os dados em trânsito devem ser criptografados ao menos com o algoritmo AES-128 bits;
1.34.4 Os algoritmos de hash devem usar ao menos o algoritmo SHA-256;
1.34.5 Será aceito como comprovação critérios de criptografia publicação em site do fabricante ou declaração do próprio fabricante;e) Os dados armazenados devem ser criptografados ao menos com o algoritmo AES-256 bits;
1.34.6 Somente servidores da Contratante ou pessoa por ela autorizada poderão ter acesso aos dados da solução;
1.34.7 A solução deve permitir a criação de, no mínimo, 20 contas para gerência e acesso aos relatórios, sem custo adicional;
1.34.8 A empresa contratada não deverá ter acesso a rede interna da contratante e todo tráfego de dados deverá ser de saída e iniciado pelos scanners (on-premise).
1.35 Todas as licenças de uso de software devem ser registradas, na data da entrega, em nome da Contratante no site do fabricante.
1.36 Dos Relatórios:
1.37 Deve ser capaz de executar relatórios periódicos de acordo com a frequência estabelecida pelo administrador, bem como a geração de relatórios sob demanda;
1.38 A solução deve possibilitar a criação de relatórios baseados na seleção de ativos, permitindo inclusive a seleção de todos os ativos existentes;
1.39 Deve suportar a criação de relatórios criptografados (protegidos por senha configurável);
1.40 A solução deve suportar o envio automático de relatórios para destinatários específicos;
1.41 Deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual;
1.42 Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos;
1.43 A solução deve fornecer relatórios do tipo “scorecard” para as partes interessadas da empresa;

ITEM 6 – PROGRAMA DE PROSPECÇÃO DE VULNERABILIDADES	
1.44	A solução deve fornecer relatórios de correções aplicadas, classificados pelos seguintes critérios: grupo de ativos, usuários e vulnerabilidades;
1.45	A solução deve permitir mecanismo de varredura baseado em inferência com técnicas de varredura não intrusivas;
1.46	A solução deve possuir ou permitir a criação de relatórios com as seguintes informações:
1.47	Hosts verificados sem credenciais;
1.48	Top 100 Vulnerabilidades mais críticas;
1.49	Top 10 Hosts infectados por Malwares;
1.50	Hosts exploráveis por Malwares;
1.51	Total de vulnerabilidades que podem ser exploradas pelo Metasploit;
1.52	Vulnerabilidades críticas e exploráveis;
1.53	Máquinas com vulnerabilidades que podem ser exploradas;
1.54	A solução deve possuir dashboards customizáveis onde o administrador pode criar, editar ou remover painéis de acordo com a necessidade;
1.55	A solução deve ser capaz de inventariar todos os ativos da rede local e publicados na Internet, sem limites de endereços IPs.
1.56	O fornecedor assinará, no ato da entrega das licenças e do serviço, Termo de Confidencialidade, em que se comprometerá a não acessar, não divulgar e proteger todos os dados de infraestrutura e de vulnerabilidades do contratante aque tiver acesso, que abrangerá todos os seus colaboradores e terceiros, sob as penas da lei.
1.57	A plataforma de software deve ser capaz de realizar varreduras (scans) de vulnerabilidades, de acordo com a quantidade de endereços IP licenciados;
1.58	A plataforma de software deve ser licenciada para um número ilimitado de scanners (prevendo redundância);
1.59	Deve permitir a configuração de vários painéis e widgets;
1.60	Deve ser capaz de medir e reportar ameaças;
1.61	Deve ser capaz de visualizar ameaças críticas ao ambiente monitorado;
1.62	A plataforma de software deve realizar varreduras em uma variedade de sistemas operacionais, suportando pelo menoshosts baseados em Windows, Linux e Mac OS, bem como appliances virtuais;

ITEM 6 – PROGRAMA DE PROSPECÇÃO DE VULNERABILIDADES	
1.63	A plataforma de software deve suportar vários mecanismos de varredura distribuídos em diferentes localidades e regiõese gerenciar todos por uma console central;
1.64	A plataforma de software deve fornecer agentes instaláveis em sistemas operacionais, pelo menos Windows, Linux e MacOS, para o monitoramento contínuo de configurações e vulnerabilidades;
1.65	A plataforma de software deve permitir o monitoramento através de agentes instalados, até o limite de licenças adquiridas, para varredura diretamente no sistema operacional.
1.66	A plataforma de software deve permitir o monitoramento sem a necessidade de agentes instalados, até o limite de licenças adquiridas, para varredura diretamente no sistema operacional.
1.67	A plataforma de software deve incluir a capacidade de programar períodos de tempo e data onde varreduras nãopodem ser executadas, como por exemplo em determinados dias do mês ou determinados horários do dia;
1.68	No caso em que uma atividade de varredura seja interrompida por invadir o período não permitido, o mesmo deve sercapaz de ser reiniciado de onde parou;
1.69	A plataforma de software deve ser configurável para permitir a otimização das parametrizações de varredura;
1.70	A plataforma de software deve permitir a entrada e o armazenamento seguro de credenciais do usuário, incluindocontas locais, de domínio (LDAP e Active Directory) e root para sistemas Linux;
1.71	A plataforma de software deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrãoaté acesso de sistema ou administrativo;
1.72	A plataforma de software deve ser capaz de realizar pesquisas de dados confidenciais
1.73	A solução deve ser licenciada para uso perpétuo. As funcionalidades da solução devem permanecer ativas após o períodode garantia mesmo que desatualizadas e com todas as atualizações e assinaturas que forem disponibilizadas até data final doperíodo que foram aplicadas ou instaladas na solução;
1.74	A aquisição dos itens poderá ser composta em relação ao tempo e a quantidade de ativos e aplicações Web:
1.75	A solução deve estar licenciadas e inclusas todas as funcionalidades para realizar varreduras (scans) de vulnerabilidades,avaliação de configuração e conformidade (baseline e compliance), indícios e padrões de códigos maliciosos conhecidos(malware);
1.76	A solução deve possuir recurso de varredura ativa, onde o scanner comunica-se com os alvos (ativos) através da rede;
1.77	A solução de gestão de vulnerabilidades deve suportar varreduras de dispositivos de IoT;

ITEM 6 – PROGRAMA DE PROSPECÇÃO DE VULNERABILIDADES	
1.78	Deve ser capaz de identificar no mínimo 50.000 CVEs (Common Vulnerabilities and Exposures);
1.79	A solução deve ter a capacidade de adicionar etiquetas (tags) aos ativos de maneira automática, manual e possibilitar ouso de regras com parâmetros específicos para aplicação das mesmas;
1.80	Deve atribuir a todas as vulnerabilidades uma severidade baseada no CVSSv3 score;
1.81	A solução deve calcular a criticidade com base nos dados agregados e consolidados do ativo, dados de segurança,sistema e conformidade, bem como hierarquias e prioridades;
1.82	A solução deve fornecer criptografia de ponta a ponta dos dados de vulnerabilidades;
1.83	A solução deve possuir a capacidade de armazenar informações dos ativos descobertos no ambiente;
1.84	Deve possuir um sistema de busca de informações de um determinado ativo com no mínimo as seguintes características:
1.85	Por sistema operacional;
1.86	Por um determinado software instalado;
1.87	Por Ativos impactados por uma determinada vulnerabilidade.4.1.11. A solução deve possuir suporte para a adição de detecções personalizadas usando oOVAL Open Vulnerability Assessment Language);
1.88	Deve permitir aceitar o risco de uma determinada vulnerabilidade encontrada no ambiente;
1.89	Possibilitar alterar a criticidade de determinada vulnerabilidade de forma manual;
1.90	A solução deve possuir um sistema de pontuação e priorização das vulnerabilidades;
1.91	A solução deve ser capaz de aplicar algoritmos de aprendizagem de máquina (machine learning) para analisar as características relacionadas a vulnerabilidades;
1.92	O sistema de pontuação e priorização de vulnerabilidades deve avaliar no mínimo as seguintes características:
1.93	CVSSv3 Impact Score;
1.94	Idade da Vulnerabilidade;
1.95	Se existe ameaça ou exploit que explore a vulnerabilidade;
1.96	Número de produtos afetados pela vulnerabilidade;
1.97	Deve ser capaz de fazer a correlação em tempo real de ameaças ativas contra vulnerabilidades encontradas, incluindofeeds de inteligência de ameaças ao vivo;
1.98	4Deve possuir uma API para automação de processos e integração com aplicações terceiras

ITEM 6 – PROGRAMA DE PROSPECÇÃO DE VULNERABILIDADES
permitindo, no mínimo, aextração de dados para carga no SIEM.
1.99 Deve possuir uma API para automação de processos e integração com aplicações ITSM do órgão para as vulnerabilidades encontradas, permitindo o agrupamento no chamado por ações corretivas;
1.100 A solução deve permitir a instalação de agentes em estações de trabalho e servidores, para varredura diretamente nosistema operacional;
1.101 A solução deve ser capaz de produzir relatórios nos seguintes formatos: PDF, CSV e HTML;
1.102 A solução deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados;
1.103 A solução deve ser licenciada para o uso ilimitado de sensores passivos de rede para realizar o monitoramento em tempo real;
1.104 A solução deve possuir sensores, no mínimo, com as seguintes funcionalidades:
1.104.1Execução de verificação completa do sistema (rede), adequada para qualquer host;
1.104.2verificação sem recomendações da rede, para que se possa personalizar totalmente as configurações da verificação;
1.104.3Autenticação de hosts e enumeração de atualizações ausentes;
1.104.4Execução de varredura simples para descobrir hosts ativos e portas abertas;
1.104.5Utilização de um scanner para verificar aplicativos da web;
1.104.6Avaliação de dispositivos móveisg. Auditoria de configuração de serviços em nuvem de terceiros;
1.104.7Auditoria de configuração dos gerenciadores de dispositivos móveis;
1.104.8Auditoria de configuração dos dispositivos de rede;
1.104.9Auditoria de configurações do sistema em relação a uma linha de base conhecida;
1.104.10 Detecção de desvio de segurança Intel AMT;
1.104.11 Verificação de malware nos sistemas Windows e Unix;
1.105 Deve ser possível determinar em tempo real quais portas de serviços (UDP/TCP) estão abertas em determinado ativo;
1.106 A solução deve ser capaz de realizar em tempo real a descoberta de novos ativos para no mínimo:
1.106.1Bancos de dados;
1.106.2Hypervisors (no mímino VMWare ESX/ESXi);
1.106.3Dispositivos móveis;

ITEM 6 – PROGRAMA DE PROSPECÇÃO DE VULNERABILIDADES
1.106.4 Dispositivos de rede;
1.106.5 Endpoints;
1.106.6 Aplicações;
1.107 A solução deve ser capaz de em tempo real detectar logins e downloads de arquivos em um compartilhamento de rede;
1.108 Permitir identificar vulnerabilidades associadas a servidores SQL no tráfego de rede;
1.109 A solução deve possuir interface para integração com as principais soluções de SIEM de mercado, tais como IBMQRadar, Microfocus ArcSight e Splunk.
1.110 A solução deve possibilitar a realização de cópias de segurança, funcionamento em alta disponibilidade e criptografia de todos os dados armazenados, além de incluir todo o software e licenciamento necessários para o funcionamento completo de acordo com as funcionalidades previstas neste Termo de Referência.
1.111 A atualização das ameaças deve ocorrer diariamente e sem interrupção dos serviços.
1.112 Configuração de segurança e acesso à gerência da solução:
1.112.1 Todos os dados armazenados nos servidores da solução devem ser criptografados e possuir logs de acesso;
1.112.2 Os dados em trânsito devem usar ao menos o algoritmo TLS 1.2 de chave 2048 bits;
1.112.3 Os dados em trânsito devem ser criptografados ao menos com o algoritmo AES-128 bits;
1.112.4 Os algoritmos de hash devem usar ao menos o algoritmo SHA-256;
1.112.5 Será aceito como comprovação critérios de criptografia publicação em site do fabricante ou declaração do próprio fabricante;
1.112.6 Os dados armazenados devem ser criptografados ao menos com o algoritmo AES-256 bits;
1.112.7 Somente servidores da Contratante ou pessoa por ela autorizada poderão ter acesso aos dados da solução;
1.112.8 A solução deve permitir a criação de, no mínimo, 20 contas para gerência e acesso aos relatórios, sem custo adicional;
1.112.9 A empresa contratada não deverá ter acesso a rede interna da contratante e todo tráfego de dados deverá ser de saída e iniciado pelos scanners (on-premise).
1.113 Todas as licenças de uso de software devem ser registradas, na data da entrega, em nome da Contratante no site do fabricante.

ITEM 6 – PROGRAMA DE PROSPECÇÃO DE VULNERABILIDADES	
1.114	Dos Relatórios:
1.115	Deve ser capaz de executar relatórios periódicos de acordo com a frequência estabelecida pelo administrador, bem como a geração de relatórios sob demanda;
1.116	A solução deve possibilitar a criação de relatórios baseados na seleção de ativos, permitindo inclusive a seleção de todos os ativos existentes;
1.117	Deve suportar a criação de relatórios criptografados (protegidos por senha configurável);
1.118	A solução deve suportar o envio automático de relatórios para destinatários específicos;
1.119	Deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual;
1.120	Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos;
1.121	A solução deve fornecer relatórios do tipo “scorecard” para as partes interessadas da empresa;
1.122	A solução deve fornecer relatórios de correções aplicadas, classificados pelos seguintes critérios: grupo de ativos, usuários e vulnerabilidades;
1.123	A solução deve permitir mecanismo de varredura baseado em inferência com técnicas de varredura não intrusivas;
1.124	A solução deve possuir ou permitir a criação de relatórios com as seguintes informações:
1.125	Hosts verificados sem credenciais;
1.126	Top 100 Vulnerabilidades mais críticas;
1.127	Top 10 Hosts infectados por Malwares;
1.128	Hosts exploráveis por Malwares;
1.129	Total de vulnerabilidades que podem ser exploradas pelo Metasploit;
1.130	Vulnerabilidades críticas e exploráveis;
1.131	Máquinas com vulnerabilidades que podem ser exploradas;
1.132	A solução deve possuir dashboards customizáveis onde o administrador pode criar, editar ou remover painéis de acordo com a necessidade;
1.133	A solução deve ser capaz de inventariar todos os ativos da rede local e publicados na Internet, sem limites de endereços IPs.
1.134	O fornecedor assinará, no ato da entrega das licenças e do serviço, Termo de Confidencialidade, em que se comprometerá a não acessar, não divulgar e proteger todos os dados de infraestrutura e de vulnerabilidades do contratante a que tiver acesso, que abrangerá todos os seus colaboradores e

ITEM 6 – PROGRAMA DE PROSPECÇÃO DE VULNERABILIDADES	
	terceiros, sob as penas da lei.
1.135	A plataforma de software deve ser capaz de realizar varreduras (scans) de vulnerabilidades, de acordo com a quantidade de endereços IP licenciados;
1.136	A plataforma de software deve ser licenciada para um número ilimitado de scanners (prevendo redundância);
1.137	Deve permitir a configuração de vários painéis e widgets;
1.138	Deve ser capaz de medir e reportar ameaças;
1.139	Deve ser capaz de visualizar ameaças críticas ao ambiente monitorado;
1.140	A plataforma de software deve realizar varreduras em uma variedade de sistemas operacionais, suportando pelo menos hosts baseados em Windows, Linux e Mac OS, bem como appliances virtuais;
1.141	A plataforma de software deve suportar vários mecanismos de varredura distribuídos em diferentes localidades e regiões e gerenciar todos por uma console central;
1.142	A plataforma de software deve fornecer agentes instaláveis em sistemas operacionais, pelo menos Windows, Linux e MacOS, para o monitoramento contínuo de configurações e vulnerabilidades;
1.143	A plataforma de software deve permitir o monitoramento através de agentes instalados, até o limite de licenças adquiridas, para varredura diretamente no sistema operacional.
1.144	A plataforma de software deve permitir o monitoramento sem a necessidade de agentes instalados, até o limite de licenças adquiridas, para varredura diretamente no sistema operacional.
1.145	A plataforma de software deve incluir a capacidade de programar períodos de tempo e data em que varreduras não podem ser executadas, como por exemplo em determinados dias do mês ou determinados horários do dia;
1.146	No caso em que uma atividade de varredura seja interrompida por invadir o período não permitido, deve ser capaz de ser reiniciado de onde parou;
1.147	A plataforma de software deve ser configurável para permitir a otimização das parametrizações de varredura;
1.148	A plataforma de software deve permitir a entrada e o armazenamento seguro de credenciais do usuário, incluindo contas locais, de domínio (LDAP e Active Directory) e root para sistemas Linux;
1.149	A plataforma de software deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrãoaté acesso de sistema ou administrativo;
1.150	A plataforma de software deve ser capaz de realizar pesquisas de dados confidenciais

ITEM 6 – PROGRAMA DE PROSPECÇÃO DE VULNERABILIDADES
1.151 A solução deve ser licenciada para uso perpétuo. As funcionalidades da solução devem permanecer ativas após o período de garantia mesmo que desatualizadas e com todas as atualizações e assinaturas que forem disponibilizadas até data final do período que foram aplicadas ou instaladas na solução;