GOVERNO DO ESTADO DA BAHIA
Procuradoria Geral do Estado
COORDENAÇÃO DE CONTRATOS - PGE/DG/DA/CC

CONTRATO QUE ENTRE SI CELEBRAM O ESTADO DA BAHIA, POR INTERMÉDIO DA PROCURADORIA GERAL DO ESTADO DA BAHIA E A EMPRESA CENTRO DE PESQUISAS EM INFORMÁTICA LTDA, PARA OS FINS QUE NELE SE DECLARAM.

Contrato nº. PGE 034/2022

O ESTADO DA BAHIA, neste ato representado pelo **DR. PAULO MORENO CARVALHO**, titular da **PROCURADORIA GERAL DO ESTADO**, CNPJ nº 04.139.403/0001-77, situada na 3ª avenida, n° 370, Centro Administrativo da Bahia, CEP 41.745-005, Salvador/BA, autorizado pelo Decreto de delegação de competência publicado no D.O.E. de 08/01/2015, denominado **CONTRATANTE**, e a Empresa **CENTRO DE PESQUISAS EM INFORMÁTICA LTDA**, CNPJ n° 40.584.096/0001-05, Inscrição Municipal nº 94.249/001-25, situada na Rua Edístio Pondé, Empresarial Tancredo Neves, nº 353, Salas 807 e 808, Stiep, CEP: 41.770-395, Salvador, Bahia, neste ato representada pelo **SR**. **JOÃO GUALBERTO RIZZO ARAÚJO,** portador da Cédula de Identidade nº 03.688.884-2, emitida por SSP/BA, inscrito no CPF/MF sob o n° 506.901.245-20, adjudicatária do **Pregão Eletrônico nº 007/2022**, processo administrativo nº 006.0409.2022.0008208-20, doravante denominada **CONTRATADA,** celebram o presente contrato, que se regerá pela Lei estadual nº 9.433/05, pelas normas gerais da Lei nº 8.666/93, e respectivas alterações, bem como pela legislação específica, mediante as cláusulas e condições a seguir ajustadas:

CLÁUSULA PRIMEIRA – OBJETO

Constitui objeto do presente contrato a contratação de empresa especializada para fornecimento de **licença de uso de Software de Gestão de Vulnerabilidades**, objetivando ampliar a segurança da rede e dos ativos da Procuradoria Geral do Estado da Bahia – PGE/BA, com garantia de 24 (vinte e quatro) meses, serviço de instalação, treinamento (Hands on), configuração e suporte on-site, de acordo com as especificações do Termo de Referência do instrumento convocatório e da proposta apresentada pela CONTRATADA, que integram este instrumento na qualidade de Anexos I e II, respectivamente:

§1º A CONTRATADA fica obrigada a aceitar, nas mesmas condições contratuais, acréscimos ou supressões que se fizerem no objeto, de até 25% do valor inicial atualizado do contrato, na forma dos §1º e 2º do art. 143 da Lei estadual nº 9.433/05.

§2º As supressões poderão ser superiores a 25%, desde que haja resultado de acordo entre os contratantes.

§3º É vedada a subcontratação parcial do objeto, a associação da CONTRATADA com outrem, a cessão ou transferência, total ou parcial do contrato, não se responsabilizando o CONTRATANTE por nenhum compromisso assumido por aquela com terceiros.

[SERVIÇOS CONTÍNUOS]

CLÁUSULA SEGUNDA – PRAZO

O prazo de vigência do contrato, a contar da data (**x**) da sua assinatura, será de 24 (vinte e quatro) meses.

§1º A prorrogação do prazo de vigência está condicionada à ocorrência de, ao menos, uma das hipóteses do art. 141 da Lei estadual nº 9.433/05.

§2º A prorrogação deverá ser previamente justificada e autorizada pela autoridade competente para celebrar o ajuste e será realizada por meio de termo aditivo, antes do termo final do contrato.

CLÁUSULA TERCEIRA – GARANTIA

(**x**) Não exigível

CLÁUSULA QUARTA – REGIME DE EXECUÇÃO

(**x**) **Serviço** com empreitada por preço ( ) Global (x) Unitário

CLÁUSULA QUINTA – PREÇO

O CONTRATANTE pagará à CONTRATADA pelos serviços efetivamente prestados os valores abaixo especificados:

LOTE ÚNICO

Item	Código SIMPAS	Descrição	Unidade de Fornecimento (UF)	Quantitativo	Preço unitário	Preço global
1	02.81.06.00000493-6	**LICENÇA DE USO DE SOFTWARE** de Gestão de Vulnerabilidades, Contratação de solução unificada de gestão de vulnerabilidade e conformidade de configurações para Ativos e Aplicações Web, em modelo de subscrição, incluindo instalação, implantação, suporte técnico e treinamento, pelo período de 24 meses	UN	2000	R$ 597,49	R$ 1.194.980,00
VALOR ESTIMADO GLOBAL						**R$ 1.194.980,00**

§1º Estima-se para o contrato o valor global de **R$ 1.194.980,00 (um milhão cento e noventa e quatro mil novecentos e oitenta reais).**

§2º Nos preços contratados estão incluídos todos os custos com material de consumo, salários, encargos sociais, previdenciários e trabalhistas de todo o pessoal da CONTRATADA, como também fardamento, transporte de qualquer natureza, materiais empregados, inclusive ferramentas, utensílios e equipamentos utilizados, depreciação, aluguéis, administração, tributos, impostos, taxas, emolumentos e quaisquer outros custos que, direta ou indiretamente, se relacionem com o fiel cumprimento pela CONTRATADA das obrigações.

CLÁUSULA SEXTA – DOTAÇÃO ORÇAMENTÁRIA

As despesas para o pagamento deste contrato correrão por conta dos recursos da Dotação Orçamentária a seguir especificada:

Unidade FIPLAN	Função	Subfunção	Programa	P/A/OE
06601	03	126	315	5121
Região/planejamento	Natureza da despesa	Destinação do recurso	Tipo de recurso orçamentário	
7800	339040	300/154	Normal	

CLÁUSULA SÉTIMA – OBRIGAÇÕES DA CONTRATADA

A CONTRATADA, além das determinações contidas no instrumento convocatório, bem como daquelas decorrentes de lei, obriga-se a:

I. designar de sua estrutura administrativa um preposto permanentemente responsável pela perfeita execução do contrato, inclusive para atendimento de emergência, servindo de interlocutor e canal de comunicação entre as partes;

II. executar o objeto deste contrato de acordo com as especificações técnicas constantes do instrumento convocatório e do presente contrato, nos locais, dias, turnos e horários determinados;

III. manter, sob sua exclusiva responsabilidade, toda a supervisão, direção e recursos humanos para execução completa e eficiente do objeto deste contrato;

IV. zelar pela boa e completa execução dos serviços contratados e facilitar, por todos os meios ao seu alcance, a ampla ação fiscalizadora dos prepostos designados pelo CONTRATANTE, atendendo prontamente às observações e exigências que lhe forem solicitadas;

V. comunicar ao CONTRATANTE qualquer anormalidade que interfira no bom andamento dos serviços;

VI. atender com presteza as reclamações sobre a qualidade dos serviços executados, providenciando sua imediata correção, sem ônus para o CONTRATANTE;

VII. respeitar e fazer com que seus empregados respeitem as normas de segurança do trabalho, disciplina e demais regulamentos vigentes no CONTRATANTE, bem como atentar para as regras de cortesia no local onde serão executados os serviços;

VIII. reparar, repor ou restituir, nas mesmas condições e especificações, dentro do prazo que for determinado, os equipamentos e utensílios eventualmente recebidos para uso nos serviços objeto deste contrato, deixando as instalações na mais perfeita condição de funcionamento;

IX. arcar com todo e qualquer dano ou prejuízo de qualquer natureza causado ao CONTRATANTE e terceiros, por sua culpa, ou em conseqüência de erros, imperícia própria ou de auxiliares que estejam sob sua responsabilidade, bem como ressarcir o equivalente a todos os danos decorrentes de paralisação ou interrupção dos serviços contratados, exceto quando isto ocorrer por exigência do CONTRATANTE ou ainda por caso fortuito ou força maior, circunstâncias que deverão ser comunicadas no prazo de 48 (quarenta e oito) horas após a sua ocorrência;

X. manter durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação, inclusive de apresentar, ao setor de liberação de faturas e como condição de pagamento, os documentos necessários;

XI. providenciar e manter atualizadas todas as licenças e alvarás junto às repartições competentes, necessários à execução dos serviços;

XII. efetuar pontualmente o pagamento de todas as taxas e impostos que incidam ou venham a incidir sobre as suas atividades e/ou sobre a execução do objeto do presente contrato

XIII. adimplir os fornecimentos exigidos pelo instrumento convocatório e pelos quais se obriga, visando à perfeita execução deste contrato;

XIV. emitir notas fiscais/faturas de acordo com a legislação;

XV. observar a legislação federal, estadual e municipal relativa ao objeto do contrato;

XVI. executar os serviços sem solução de continuidade durante todo o prazo da vigência do contrato;

XVII. prover as instalações, aparelhamento e pessoal técnico exigidos na licitação;

XVIII. alocar durante todo o período de execução do objeto a equipe técnica mínima exigida no instrumento convocatório, admitindo-se a sua substituição por profissionais de experiência equivalente ou superior, desde que aprovada pelo CONTRATANTE

XIX. providenciar o cadastramento de seu representante legal ou procurador no site www.comprasnet.ba.gov.br, para a prática de atos através do Sistema Eletrônico de Informações – SEI

Parágrafo único. Além das determinações acima descritas, a CONTRATADA que estiver sujeita à determinação do art. 429 do Decreto-Lei nº 5.452, de 1º de maio de 1943 (Consolidação das Leis do Trabalho - CLT), regulamentado pelo Decreto nº 5.598, de 1º de dezembro de 2005, deverá, no que concerne à aprendizagem

a) recrutar, preferencialmente, para a contratação de aprendizes prevista no art. 429 da CLT, os estudantes indicados nos incisos I e II do art. 9º da Lei estadual nº 13.459, de 10 dezembro de 2015, regulamentada pelo Decreto estadual nº 16.761, de 07 de junho de 2016, no percentual mínimo de 20% (vinte por cento) do quadro de aprendizes da CONTRATADA.

b) apresentar ao fiscal ou responsável pela gestão e acompanhamento do contrato, no prazo de até 05 (cinco) dias úteis contado do início efetivo da execução do serviço, a lista completa dos aprendizes, indicando aqueles selecionados no banco de dados de que trata o Decreto estadual nº 16.761/16, devendo justificar, perante o CONTRATANTE, a eventual impossibilidade de seu cumprimento.

CLÁUSULA OITAVA – OBRIGAÇÕES DO CONTRATANTE

O **CONTRATANTE,** além das obrigações contidas neste contrato por determinação legal, obriga-se a:

I. fornecer à CONTRATADA os elementos indispensáveis ao cumprimento do contrato no prazo máximo de 10 (dez) dias da assinatura;

II. realizar o pagamento pela execução do objeto contratual;

III. proceder à publicação resumida do instrumento de contrato e de seus aditamentos, na imprensa oficial, no prazo legal.

CLÁUSULA NONA – FISCALIZAÇÃO DO CONTRATO

Competirá ao CONTRATANTE proceder ao acompanhamento da execução do contrato, na forma do art. 154 da Lei estadual nº 9.433/05, ficando esclarecido que a ação ou omissão, total ou parcial da fiscalização não eximirá a CONTRATADA da total responsabilidade pela execução do contrato.

§1º O adimplemento da obrigação contratual por parte da CONTRATADA ocorrerá com a efetiva prestação do serviço, a realização da obra, a entrega do bem ou de parcela destes, bem como qualquer outro evento contratual cuja ocorrência esteja vinculada à emissão de documento de cobrança, nos termos do art. 8º, inc. XXXIV, da Lei estadual nº 9.433/05.

§2º Cumprida a obrigação pela CONTRATADA, caberá ao CONTRATANTE proceder ao recebimento do objeto, a fim de aferir os serviços ou fornecimentos efetuados, para efeito de emissão da habilitação de pagamento, conforme o art. 154, inc. V, e art. 155, inc. V, da Lei estadual nº 9.433/05

§3º Compete especificamente à fiscalização, sem prejuízo de outras obrigações legais ou contratuais:

I. exigir da CONTRATADA o cumprimento integral das obrigações pactuadas;

II. rejeitar todo e qualquer material de má qualidade ou não especificado;

III. relatar ao Gestor do Contrato ocorrências ou circunstâncias que possam acarretar dificuldades no desenvolvimento dos serviços em relação a terceiros;

IV. dar à autoridade superior imediata ciência de fatos que possam levar à aplicação de penalidades contra a CONTRATADA, ou mesmo à rescisão do contrato.

§4º Fica indicada como área responsável pela Gestão do Contrato: **Coordenação de Gestão Estratégica - CGE**

§5º Fica indicado como gestor deste Contrato o Servidor: **Eduardo Jorge Rodrigues Brandão, matrícula: 06.577.805-8.**

§6º Fica indicado como fiscal deste Contrato o Servidor: **Mauricio de Cerqueira Pereira, matrícula: 06.579.186-0.**

CLÁUSULA DÉCIMA – RECEBIMENTO DO OBJETO

O recebimento do objeto, consistente na aferição da efetiva prestação do serviço, realização da obra, entrega do bem ou de parcela destes, se dará segundo o disposto no art. 161 da Lei estadual nº 9.433/05, observando-se os seguintes prazos, se outros não houverem sido fixados no Termo de Referência:

I. se a verificação da conformidade do objeto com a especificação, bem assim do cumprimento das obrigações acessórias puder ser realizada de imediato, será procedido de logo o recebimento definitivo;

II. quando, em razão da natureza, do volume, da extensão, da quantidade ou da complexidade do objeto, não for possível proceder-se a verificação imediata de conformidade, será feito o recebimento provisório, devendo ser procedido ao recebimento definitivo no prazo de 15 (quinze) dias.

§1º Nos casos de aquisição de equipamentos de grande vulto, o recebimento definitivo far-se-á mediante termo circunstanciado e, nos demais, mediante recibo.

§2º Na hipótese de não ser lavrado o termo circunstanciado ou de não ser procedida a verificação dentro dos prazos fixados, reputar-se-ão como realizados, desde que comunicados ao CONTRATANTE nos 15 (quinze) dias anteriores à exaustão dos mesmos.

§3º O recebimento definitivo de compras ou serviços, cujo valor do objeto seja superior ao limite estabelecido para a modalidade de convite, deverá ser confiado a uma comissão de, no mínimo, 03 (três) membros.

§4º Esgotado o prazo de vencimento do recebimento provisório sem qualquer manifestação do CONTRATANTE, não dispondo o TERMO DE REFERÊNCIA de forma diversa, considerar-se-á definitivamente aceito pela Administração o objeto contratual, para todos os efeitos.

§5º Poderá ser dispensado o recebimento provisório nos seguintes casos:

I. gêneros perecíveis e alimentação preparada;

II. serviços profissionais;

III. serviços de valor até o limite previsto para compras e serviços, que não sejam de engenharia, na modalidade de convite, desde que não se componham de aparelhos, equipamentos e instalações sujeitos à verificação de funcionamento e produtividade.

§6º Salvo disposições em contrário constantes do TERMO DE REFERÊNCIA, os ensaios, testes e demais provas exigidas por normas técnicas oficiais para a boa execução do objeto do contrato correm por conta do contratado

§7º O CONTRATANTE rejeitará, no todo ou em parte, obra, serviço ou fornecimento em desacordo com as condições pactuadas, podendo, entretanto, se lhe convier, decidir pelo recebimento, neste caso com as deduções cabíveis.

§8º O recebimento provisório ou definitivo não exclui a responsabilidade civil pela solidez e segurança da obra ou do serviço, nem a ético-profissional pela perfeita execução do contrato, dentro dos limites estabelecidos pela lei ou pelo contrato

§9º Com a conclusão da etapa do recebimento definitivo, a CONTRATADA estará habilitada a apresentar as nota(s) fiscal(is)/fatura(s) para pagamento.

CLÁUSULA DÉCIMA-PRIMEIRA - PAGAMENTO

Os pagamentos devidos à CONTRATADA serão efetuados através de ordem bancária ou crédito em conta ~~corrente~~ aberta em instituição financeira contratada pelo Estado da Bahia, no prazo não superior a 08 (oito) dias úteis, contados da data da apresentação da fatura, após concluído o recebimento definitivo, em consonância com o disposto no art. 6º, §5º; art. 8º, XXXIV; art. 79, XI, "a"; art. 154, V e art. 155, V da Lei estadual nº 9.433/05.

§1º A(s) nota(s) fisca(l)is/fatura(s) somente deverá(ao) ser apresentada(s) para pagamento após a conclusão da etapa do recebimento definitivo, indicativo da satisfação pela CONTRATADA de todas as obrigações pertinentes ao objeto contratado.

§2º Ainda que a nota fiscal/fatura seja apresentada antes do prazo definido para recebimento definitivo, o prazo para pagamento somente fluirá após o efetivo atesto do recebimento definitivo.

§3º O CONTRATANTE descontará da fatura mensal o valor correspondente às faltas ou atrasos no cumprimento da obrigação, com base no valor do preço vigente.

§4º A(s) nota(s) fisca(l)is/fatura(s) deverá(ao) atender as exigências legais pertinentes aos tributos e encargos relacionados com a obrigação, sujeitando-se às retenções tributárias previstas em lei, e, as situações específicas, à adoção da forma eletrônica

§5º O processo de pagamento, para efeito do art. 126, inciso XVI, da Lei estadual nº 9.433/05, deverá ser instruído com a prova da manutenção das condições de habilitação e qualificação exigidas no certame, o que poderá ser aferido mediante consulta ao Registro Cadastral ou a sites oficiais, considerando-se como marco final desta demonstração a data de conclusão da etapa do recebimento definitivo.

§6º Em havendo alguma pendência impeditiva do pagamento, a exemplo de erro na apresentação da nota fiscal/fatura ou dos documentos pertinentes à contratação, ou, ainda, de circunstância que impeça a liquidação da despesa, como obrigações financeiras pendentes, decorrentes de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a CONTRATADA providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para o CONTRATANTE.

§7º Em caso de mora nos pagamentos devidos pelo CONTRATANTE, será observado o que se segue:

I. a atualização monetária será calculada considerando a data do vencimento da obrigação e do seu efetivo pagamento, de acordo com a variação do INPC do IBGE *pro rata tempore;*

II. nas compras para entrega imediata, assim entendidas aquelas com prazo de entrega até 15 (quinze) dias contados da data da celebração do ajuste, será dispensada a atualização financeira correspondente ao período compreendido entre as datas do adimplemento e a prevista para o pagamento, desde que não superior a quinze dias, em conformidade com o inc. II do art. 82 da Lei nº 9.433/05.

§8º Optando a CONTRATADA por receber os créditos em instituição financeira diversa da indicada no **caput**, deverá arcar com os custos de transferências bancárias, os quais serão deduzidos dos pagamentos devidos..

CLÁUSULA DÉCIMA-SEGUNDA – MANUTENÇÃO DAS CONDIÇÕES DA PROPOSTA

Os preços contratados são fixos e irreajustáveis durante o prazo de 12 meses da data de apresentação da proposta.

§1º Após o prazo de 12 meses a que se refere o *caput*, a concessão de reajustamento será feita mediante a aplicação do INPC/IBGE, nos termos do inc. XXV do art. 8º da Lei estadual nº 9.433/05, observada a seguinte fórmula:

§2º A revisão de preços, nos termos do inc. XXVI do art. 8º da Lei estadual nº 9.433/05, dependerá de requerimento da CONTRATADA quando visar recompor o preço que se tornou *insuficiente*, devendo ser instruído com a documentação que comprove o desequilíbrio econômico-financeiro do contrato.

§3º O requerimento de revisão de preços deverá ser formulado pela CONTRATADA no prazo máximo de um ano a partir do fato que a ensejou, sob pena de decadência, em consonância com o art. 211 da Lei nº 10.406/02.

§4º A revisão de preços pode ser instaurada pelo CONTRATANTE quando possível a redução do preço ajustado para compatibilizá-lo ao valor de mercado ou quando houver diminuição, devidamente comprovada, dos preços dos insumos básicos utilizados no contrato, conforme o art. 143, inc. II, alínea "e", da Lei estadual nº 9.433/05.

CLÁUSULA DÉCIMA-TERCEIRA – ALTERAÇÕES CONTRATUAIS

A prorrogação, suspensão ou rescisão sujeitar-se-ão às mesmas formalidades exigidas para a validade deste contrato.

§1º A admissão da fusão, cisão ou incorporação da CONTRATADA está condicionada à manutenção das condições de habilitação e à demonstração, perante o CONTRATANTE, da inexistência de comprometimento das condições originariamente pactuadas para a adequada e perfeita execução do contrato.

§2º Independem de termo contratual aditivo, podendo ser registrado por simples apostila:

I. a simples alteração na indicação dos recursos orçamentários ou adicionais custeadores da despesa, sem modificação dos respectivos valores;

II. reajustamento de preços previsto no edital e neste contrato, bem como as atualizações, compensações ou apenações financeiras decorrentes das condições de pagamento dos mesmos constantes;

III. o empenho de dotações orçamentárias suplementares até o limite do seu valor corrigido.

CLÁUSULA DÉCIMA-QUARTA - INEXECUÇÃO E RESCISÃO

A inexecução total ou parcial do contrato ensejará a sua rescisão, com as conseqüências contratuais e as previstas na Lei estadual nº 9.433/05.

§1º A rescisão poderá ser determinada por ato unilateral e escrito do CONTRATANTE nos casos enumerados nos incisos I a XV, XX e XXI do art. 167 da Lei estadual nº 9.433/05

§2º Quando a rescisão ocorrer com base nos incisos I e XVI a XX do art. 167 da Lei estadual nº 9.433/05, sem que haja culpa da CONTRATADA, será este ressarcido dos prejuízos regularmente comprovados que houver sofrido, na forma do §2º do art. 168 do mesmo diploma.

CLÁUSULA DÉCIMA-QUINTA – PENALIDADES

Constituem ilícitos administrativos as condutas previstas nos arts. 184, 185 e 199 da Lei estadual nº 9.433/05, sujeitando-se os infratores às cominações legais, especialmente as definidas no art. 186 do mesmo diploma, garantida a prévia e ampla defesa em processo administrativo.

§1º Para a aplicação das penalidades serão levados em conta a natureza e a gravidade da falta, os prejuízos dela advindos para a Administração Pública e a reincidência na prática do ato, observando-se os critérios de dosimetria estabelecidos pelo Decreto estadual nº 13.967/12.

§2º Serão punidos com a pena de declaração de inidoneidade para licitar e contratar com a Administração, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a autoridade competente para aplicar a punição, os que incorram nos ilícitos previstos nos incisos I a V do art. 184, nos incisos II, III e V do art. 185 e no art. 199 da Lei estadual nº 9.433/05.

§3º Serão punidos com a pena de suspensão temporária do direito de cadastrar e licitar e impedimento de contratar com a Administração os que incorram nos ilícitos previstos nos incisos VI e VII do art. 184 e nos incisos I, IV, VI e VII do art. 185 da Lei estadual nº 9.433/05.

§4º A CONTRATADA será descredenciada do Sistema de Registro Cadastral quando, em razão da ocorrência das faltas previstas na Lei estadual nº 9.433/05, deixar de satisfazer as exigências relativas à habilitação jurídica, qualificação técnica, qualificação econômico-financeira, regularidade fiscal e trabalhista exigidas para cadastramento.

§5º A inexecução contratual, inclusive por atraso injustificado na execução do contrato, sujeitará a CONTRATADA à multa de mora, na forma prevista na cláusula seguinte, que será graduada de acordo com a gravidade da infração, observado o disposto na Lei estadual nº 9.433/05 e no Decreto estadual nº 13.967/12.

CLÁUSULA DÉCIMA-SEXTA – SANÇÃO DE MULTA

A pena de multa será aplicada em função de inexecução contratual, inclusive por atraso injustificado na execução do contrato, sem prejuízo da rescisão unilateral do contrato, a qualquer tempo, e a aplicação das demais sanções previstas na Lei estadual nº 9.433/05.

§1º Quanto à obrigação principal, será observado o que se segue:

I. Em caso de descumprimento total da obrigação principal, será aplicada multa no percentual de 10% (dez por cento) incidente sobre o valor global do contrato.

II. Caso o cumprimento da obrigação principal, uma vez iniciado, seja descontinuado, será aplicado o percentual de 10% (dez por cento) sobre o saldo do contrato, isto é, sobre a diferença entre o valor global do contrato e o valor da parte do fornecimento ou do serviço já realizado.

III. O atraso no cumprimento da obrigação principal ensejará a aplicação de multa no percentual de 0,3% (três décimos por cento) ao dia, até o trigésimo dia de atraso, e de 0,7% (sete décimos por cento) por cada dia subseqüente ao trigésimo, calculados sobre o valor da parcela do fornecimento ou do serviço em mora.

§2º Quanto à obrigação acessória, assim considerada aquela que coadjuva a principal, será observado o que se segue:

I. Em caso de descumprimento total da obrigação acessória, será aplicada multa no percentual de 10% (dez por cento) incidente sobre o valor ou custo da obrigação descumprida.

II. Caso o cumprimento da obrigação acessória, uma vez iniciado, seja descontinuado, será aplicado o percentual de 5% (cinco por cento) sobre o valor ou custo da obrigação descumprida.

III. O atraso no cumprimento da obrigação acessória ensejará a aplicação de multa no percentual de 0,2% (dois décimos por cento) ao dia, até o trigésimo dia de atraso, e de 0,6% (seis décimos por cento) por cada dia subseqüente ao trigésimo, calculados sobre o valor ou custo da obrigação descumprida.

IV. Caso não seja possível identificar o valor ou custo da obrigação acessória descumprida, a multa será arbitrada pelo CONTRANTE, em valor que não supere 1% da sanção pecuniária que seria cabível pelo descumprimento da obrigação principal.

§3º Se a multa moratória atingir o patamar de 10% (dez por cento) do valor global do contrato, deverá, salvo justificativa escrita devidamente fundamentada, ser recusado o recebimento do objeto, sem prejuízo da aplicação das demais sanções previstas em lei.

§4º Na hipótese de o contratado se negar a efetuar o reforço da caução, dentro de 10 (dez) dias contados da data de sua convocação, será aplicada multa no percentual de 2,5% (dois e meio por cento) incidente sobre o valor global do contrato.

§5º As multas previstas nesta cláusula não têm caráter compensatório e o seu pagamento não eximirá a CONTRATADA da responsabilidade por perdas e danos decorrentes das infrações cometidas.

§6º A multa, aplicada após regular processo administrativo, será descontada da garantia do contratado faltoso.

§7º Se o valor da multa exceder ao da garantia prestada, além da perda desta, a CONTRATADA responderá pela sua diferença, que será descontada dos pagamentos eventualmente devidos pela Administração ou, ainda, se for o caso, cobrada judicialmente.

§8º Caso não tenha sido exigida garantia, à Administração se reserva o direito de descontar diretamente do pagamento devido à CONTRATADA o valor de qualquer multa porventura imposta.

CLÁUSULA DÉCIMA-SÉTIMA - UTILIZAÇÃO DE SOFTWARES

§1º A CONTRATADA fornecerá, por sua conta, a instalação, configuração e licenças de todos os softwares que se fizerem necessários para a execução contratual da prestação de serviços decorrentes deste Termo de Referência.

§2º Qualquer instalação de software em ambiente da CONTRATADA será precedida de justificativa, e somente será autorizado se for compatível com as exigências da CONTRATANTE e de seu provedor. Necessidades outras, além das descritas acima, serão arcadas pela própria CONTRATADA, as quais não serão passíveis de cobranças adicionais.

CLÁUSULA DÉCIMA-OITAVA - PROPRIEDADE INTELECTUAL

§1º A Contratada entregará a Contratante toda e qualquer documentação gerada em função da prestação de serviços decorrente do quanto estabelecido no Termo de Referência.

§2º Entendem-se por resultados quaisquer estudos, relatórios, especificações, descrições técnicas, protótipos, dados, esquemas, plantas, desenhos, diagramas, páginas na Intranet e Internet e documentação didática em papel ou em mídia eletrônica

§3º A Contratada fica proibida de veicular e comercializar todos e quaisquer produtos e informações geradas ou conhecidas relativas ao objeto da prestação dos serviços, salvo se houver a prévia autorização por escrito da Contratante.

CLÁUSULA DÉCIMA-NONA - VINCULAÇÃO AO INSTRUMENTO CONVOCATÓRIO

Integram o presente contrato, como se nele estivessem transcritas, as cláusulas e condições estabelecidas no processo de contratação, referido no preâmbulo deste instrumento, inclusive anexos e adendos, e na proposta da licitante vencedora.

CLÁUSULA VIGÉSIMA - COMUNICAÇÃO ELETRÔNICA

Fica pactuado que os atos de comunicação processual com a CONTRATADA poderão ser realizados por meio eletrônico, na forma do disposto na Lei nº 12.209, de 20 de abril de 2011, e do Decreto nº 15.805, de 30 de dezembro de 2014.

Parágrafo único. A CONTRATADA deverá manter atualizado o endereço eletrônico cadastrado no Sistema Eletrônico de Informações - SEI, para efeito do recebimento de notificação e intimação de atos processuais.

CLÁUSULA VIGÉSIMA-PRIMEIRA – FORO

As partes elegem o Foro da Cidade do Salvador, Estado da Bahia, que prevalecerá sobre qualquer outro, por mais privilegiado que seja, para dirimir quaisquer dúvidas oriundas deste contrato.

E, por estarem assim justos e contratados, firmam o presente contrato em 02 (duas) vias de igual teor e forma na presença das testemunhas que subscrevem depois de lido e achado conforme.

Salvador, ____ de _____de 2022.

PROCURADORIA GERAL DO ESTADO DA BAHIA | **CENTRO DE PESQUISAS EM INFORMÁTICA LTDA**

Testemunha | **Testemunha**

ANEXO I

SEÇÃO II
TERMO DE REFERÊNCIA DO OBJETO DA LICITAÇÃO

1. Descritivo: A presente licitação tem por objeto a contratação de empresa especializada para fornecimento de licença de uso de Software de Gestão de Vulnerabilidades, objetivando ampliar a segurança da rede e dos ativos da Procuradoria Geral do Estado da Bahia – PGE/BA, com garantia de 24 (vinte e quatro) meses, serviço de instalação, treinamento (Hands on), configuração e suporte on-site,, conforme características, quantitativos, condições e especificações disciplinadas nesta Seção.

2. Características, quantitativos, cronograma/prazo de entrega e local de entrega:

Descrição	Unidade de Fornecimento (UF)	Quantitativo	Cronograma/Prazo
LICENÇA DE USO DE SOFTWARE Software de Gestão de Vulnerabilidades, Contratação de solução unificada de gestão de vulnerabilidade e conformidade de configurações para Ativos e Aplicações Web, em modelo de subscrição, incluindo instalação, implantação, suporte técnico e treinamento, pelo período de 24 meses. Código SIMPAS: 02.81.06.00000493-6 **Descrição completa vide anexo deste Termo de Referência.**	**UN**	**2.000**	Prazo de entrega: até 15 (quinze) dias, contados a partir da assinatura do contrato ou instrumento equivalente; Período do licenciamento: 24 (vinte e quatro) meses

2.1 Local da prestação de serviço: Os serviços serão prestados na Sede da Procuradoria Geral do Estado, situada na 3a Avenida, 370, Centro Administrativo da Bahia, CEP: 41.745-005, Salvador/BA.

2.2 Disposições gerais:

2.2.1 O contrato prevê a contratação de empresa especializada para fornecimento e serviços de soluções de Segurança da Informação, contemplando manutenção e suporte técnico de necessários à sua operacionalização, visando garantir as políticas de Segurança da Informação da Procuradoria Geral do Estado da Bahia – PGE/BA, de acordo com as características abaixo:

2.2.1.1 O objeto descrito neste Termo de Referência deverá ser entregue e instalado pelos técnicos da empresa fornecedora, na quantidade e características especificadas e dentro do prazo fixado e respeitando os termos estabelecidos neste termo de referência;

2.2.1.2 Acesso telefônico 08h/dia, 5 dias da semana;

2.2.1.3 Treinamento de atualização tecnológica da solução para pelo menos 05 (cinco) técnicos nas instalações da Contratante;

2.2.1.4 Suporte técnico da Solução de Segurança fornecida em língua portuguesa

2.3 SUPORTE TÉCNICO E ACORDO DE NÍVEL DE SERVIÇO

2.3.1 A equipe técnica deverá ser composta de técnicos certificados pelo fabricante da solução de segurança fornecida, e preparada para dar todo o suporte técnico e ajuda necessária para maximizar os benefícios oferecidos pela solução de segurança, aumentando a sua performance.

2.3.2 O suporte técnico da Solução de Segurança fornecida deverá ser prestado pelo através de contato Telefônico (telefone 0800 do fabricante ou telefone com numeração comum do fornecedor), Sitio de Internet (website do fabricante ou do fornecedor), Correio Eletrônico (e-mail do fabricante ou do fornecedor) ou no Local (provido pelo fabricante ou pelo fornecedor), em casos de grande emergência;

2.3.3 O suporte técnico deverá ser fornecido pelo fornecedor da solução de segurança ou pelo fabricante, no Brasil e na língua portuguesa;

2.3.4 Deverão ser executados pela empresa contratada serviços de Instalação e Configuração para uso da solução contratada com supervisão da equipe técnica da PGE;

2.3.5 Deverá ser executada pela empresa contratada uma análise da situação atual e elaborar, em conjunto com a equipe interna da PGE, um plano de otimização de recursos, rotinas, procedimentos e processos para o novo ambiente de segurança. Essa documentação deverá ser entregue, pela empresa contratada, em formato digital;

2.3.6 A empresa contratada deverá preservar todo ambiente computacional existente, de forma a manter a integridade dos dados, aplicativos e sistemas operacionais em funcionamento;

2.3.7 A empresa contratada deverá preparar o ambiente de modo a operar conforme o estabelecido no plano de otimização de recursos, rotinas, procedimentos e processos;

2.3.8 A instalação e configuração da solução deverá ser realizada de acordo com o horário de funcionamento da PGE, de segunda à sexta-feira, das 8:30 às 18:00h, em horário e dias a serem combinados entre a PGE e a contratada;

2.3.9 Deverá ser oferecido treinamento hands-on de atualização tecnológica da solução implantada, com o mínimo de 16 (dezesseis) horas, em dias úteis, nas instalações da contratante, para no mínimo 5 (cinco) técnicos da PGE;

2.3.10 O treinamento ou hands-on deverá ser iniciado imediatamente após a instalação e configuração das licenças;

2.3.11 O prazo de execução dos serviços de Instalação, Configuração e Treinamento para uso da solução de segurança no parque computacional da PGE deverá ser concluído em no máximo 30 (trinta) dias consecutivos, a contar da data da entrega das licenças;

2.3.12 A empresa contratada deverá realizar duas avaliações on-site durante o período de vigência do contrato, perante solicitação da contratante, do ambiente da PGE, mediante verificação de instalações e configurações de toda a solução de segurança, adequando-as às melhores práticas, essa atividade deve gerar relatório para posterior melhoria pela equipe da PGE;

2.3.13 Todo suporte deve ser prestado por técnicos certificados pelo fabricante;

2.3.14 Caberá a PGE requisitar o suporte técnico, ficando a Contratada obrigada a realizá-lo, de acordo com o nível de severidade e nos prazos máximos assim definidos no item 2.4;

2.3.15 O suporte técnico deverá ser prestado nas seguintes formas:

2.3.15.1 Plantão Telefônico, Website e E-mail - Serviço de uso ilimitado, no período de 8 (oito) horas por dia, 5 (cinco) dias por semana;

2.3.15.2 No Local (on site) - Serviço de uso ilimitado, prestado em caso de emergência, ou outra necessidade maior e também compreendendo os seguintes tipos de atendimento local previstos: suporte para upgrade de versões e releases do software; solução de problemas detectados (troubleshoot); análise e correção de eventos relacionados à segurança e à performance do software e do ambiente; integração dos ambientes da configuração do software na rede da PGE. Neste caso a contratada deve possuir plantão de 8 (oito) horas por dia, 5 (cinco) dias por semana, para este tipo de atendimento;

2.3.15.3 Para a execução do suporte técnico, a Contratada deverá contar com equipe técnica certificada pelo fabricante e com suporte ilimitado (quantidade de chamados) ao centro de suporte mundial do fabricante a nível internacional, a fim de garantir transferência diretamente ao fabricante dos problemas de maior complexidade que não tenham sido resolvidos em seu próprio laboratório;

2.3.15.4 O encaminhamento de chamados deverá ser efetuado pelos técnicos responsáveis no prazo máximo conforme os níveis de severidade indicados no item 2.4. Após este prazo, em caso de não solução, a Contratada deverá acionar o atendimento, no local designado pela PGE, de acordo com o nível de serviço acordado. O suporte prestado pela empresa terá chamados ilimitados;

2.3.15.5 O atendimento No Local (on site) deve ser provido na PGE, no seguinte endereço: 3ª Av. Centro Administrativo da Bahia, 370 - CAB, Salvador - BA, 41745-005

2.3.15.6 A Contratada deverá responder aos acionamentos, dentro dos prazos fixados no item 2.4, a partir da abertura do acionamento;

2.3.15.7 O término do atendimento deverá ocorrer dentro dos prazos fixados no item 2.4, a partir do contato do técnico da Contratada, responsável pelo atendimento;

2.3.15.8 Entende-se por início do atendimento a hora do contato do técnico de suporte da Contratada com a equipe da Contratante;

2.3.15.9 Entende-se por término de atendimento a disponibilidade da Solução de Segurança para uso em perfeitas condições de funcionamento no local onde está instalado;

2.3.15.10 O nível de severidade será informado pela Contratante no momento da abertura de cada chamado;

2.3.15.11 O nível de severidade poderá ser reclassificado a critério da Contratante. Caso isso ocorra haverá o início de nova contagem de prazo, conforme o novo nível de severidade;

2.3.15.12 Todas as solicitações de suporte técnico devem ser registradas pela Contratada, para acompanhamento e controle da execução do serviço;

2.3.15.13 A Contratada deverá apresentar relatório de atendimento para cada solicitação de suporte, contendo data e hora da solicitação de suporte técnico, do início e do término do atendimento, identificação do problema, providências adotadas e demais informações pertinentes;

2.3.15.14 O relatório de atendimento deverá ser assinado pelo servidor da Contratante que solicitou o suporte técnico;

2.3.15.15 Para a execução do atendimento, é necessária a autorização da Contratante para instalação ou desinstalação de quaisquer softwares ou equipamentos que não façam parte da solução de segurança fornecida.

2.4 Acordo de Nível de Serviço (ANS):

2.4.1 A Contratada deverá possuir Central de Atendimento (contato telefônico, sítio na Internet e e-mail) para consultas, aberturas de chamados técnicos e envio de arquivos para análise, durante 8 (oito) horas por dia, 5 (cinco) dias por semana;

2.4.2 A Contratada deverá prestar serviços de suporte técnico 8 horas por dia, 5 dias por semana, na cidade de Salvador (BA), relativos à prestação do serviço objeto deste Termo de Referência, sem ônus para a Contratante;

2.4.3 Para efeito dos atendimentos técnicos, a Contratada deverá observar os níveis de severidade e respectivos prazos máximos fixados abaixo;

2.4.4 Todos os chamados, inclusive os que podem resultar em manutenção de natureza corretiva, bem como o fluxo de resolução de problemas, deverão ser documentados. Esta documentação, bem como outras geradas em processos de atendimento, auditorias, manutenção ou configurações, deverá ser entregue à CONTRATANTE através de relatórios (impressos ou em mídia digital) mediante solicitação.

2.4.5 A CONTRATADA deverá fazer análises dos chamados e enviar recomendações de possíveis treinamentos necessários ao desenvolvimento da equipe da CONTRATANTE.

2.4.6 A CONTRATADA deverá apresentar relatório contendo as ações adotadas para a solução do problema.

2.4.7 A CONTRATADA deverá disponibilizar à CONTRATANTE serviço de atendimento de um Gestor do contrato de Suporte, responsável este que será o ponto focal de todas as necessidades de suporte da CONTRATANTE para casos de escalações ou problemas de atendimento do Suporte Técnico. Caso a CONTRATADA tenha seus laboratórios em outros países que não seja o território nacional, o Gestor deverá ter fluência na língua para facilitar a comunicação entre as partes.

2.4.8 A CONTRATANTE permitirá o acesso dos técnicos credenciados pela CONTRATADA às instalações onde se encontrarem os equipamentos para a prestação dos serviços de manutenção. Entretanto, tais técnicos ficarão sujeitos às normas internas de segurança da CONTRATANTE, notadamente àquelas atinentes à identificação, trânsito e permanência nas dependências;

2.4.9 Mesmo se permitido pela CONTRATANTE, a permanência do técnico além do tempo de resolução do problema, para a continuidade de solução de um problema, não deverá representar qualquer ônus adicional à CONTRATANTE.

2.4.10 Níveis de Serviço e Tempo Esperados:

2.4.11 Plantão Telefônico por número 0800 como serviço de uso ilimitado, no período de 8 (oito) horas por dia, 5 (cinco) dias por semana;

2.4.12 No Local (on site) – Serviço de uso ilimitado, prestado em caso de emergência, ou outra necessidade maior e também compreendendo os seguintes tipos de atendimento local: suporte para upgrade de versões e releases do software; solução de problemas detectados (troubleshoot); análise e correção de eventos relacionados à segurança e à performance do software e do ambiente; atualização simultânea nos ambientes dos órgãos e entidades da CONTRATANTE.

2.4.13 Para efeito dos atendimentos técnicos, a Contratada deverá observar os níveis de severidade e respectivos prazos máximos fixados abaixo:

3 NÍVEIS DE SEVERIDADE DOS CHAMADOS	
Nível	**Descrição**
1	Serviços totalmente indisponíveis.
2	Serviços parcialmente indisponíveis ou com degradação de tempo de resposta no acesso aos aplicativos.
3	Serviços disponíveis com ocorrência de alarmes de avisos, consultas sobre problemas, dúvidas gerais sobre o equipamento fornecido.

Tabela de Prazos de Atendimento ao Software				
Modalidade	**Prazos**	**Níveis de Severidade**		
		1	**2**	**3**
On Site	Início atendimento	1 hora	2 horas	24 horas
	Término atendimento	2 horas	4 horas	72 horas
Telefone, e-mail e web	Início atendimento	-	-	24 horas
	Término atendimento	-	-	72 horas

2.4.14 Para o Nível 1, caso o atendimento não seja finalizado até as 20h00min, o técnico não poderá interrompê-lo, devendo continuar até sua finalização, ou a interrupção do mesmo pela Coordenação de Tecnologia da Informação e Comunicação - CTIC. Todo o chamado somente será caracterizado como "encerrado" mediante concordância da Coordenação de Tecnologia da Informação e Comunicação - CTIC;

2.4.15 Para as situações em que a solução definitiva de problemas no ambiente demande reimplantação, reestruturação ou reinstalação da solução, este deverá ser programado e planejado, com a antecedência necessária, de modo a não prejudicar a operação dos demais sistemas da CONTRATANTE.

2.4.16 A CONTRATADA deverá disponibilizar à CONTRATANTE um serviço preventivo de verificação e atualização de versões ou correções (patches) que se fizerem necessários, específicos para a solução ofertada, sem ônus para a CONTRATANTE;

2.4.17 No caso de necessidade de ações preventivas ou corretivas a CONTRATANTE agendará com antecedência junto a CONTRATADA as implementações das correções, fora do horário comercial, preferencialmente em feriados e finais de semana, sem ônus para a CONTRATANTE;

2.4.18 A CONTRATADA deverá prestar suporte a todos os componentes da solução de segurança fornecidos que forem necessários para a implementação e utilização da solução, sem ônus para a CONTRATANTE durante 24 (vinte e quatro) meses.

2.4.19 A contratada deverá ainda realizar os seguintes suportes proativos:

2.4.19.1 Duas avaliações on-site por ano do ambiente da CONTRATANTE, mediante verificação de instalações e configurações de toda a solução, adequando-as às melhores práticas de segurança, essa atividade deve gerar relatório para posterior melhoria pela equipe da CONTRATANTE.

2.4.19.2 Uma avaliação on-site por ano do ambiente da CONTRATANTE, mediante verificação de instalações e configurações de toda a solução de gerência centralizada, adequando-as às melhores práticas de segurança, essa atividade deve gerar relatório para posterior melhoria pela equipe da CONTRATANTE.

2.4.19.3 Quatro visitas técnicas on-site durante o ano de profissionais certificados pelo fabricante para apoiar nas implementações e nos controles gerados pelas ações proativas.

2.5 TESTE E VERIFICAÇÃO PRELIMINAR

2.5.1 Todos os componentes disponíveis nas licenças fornecidas serão testados por meio de procedimentos designados pela Contratante, findo os quais será elaborado relatório técnico com a análise dos resultados;

2.5.2 O processo de realização dos testes de verificação preliminar da solução de segurança será desenvolvido de acordo com os eventos e atividades descritos a seguir:

2.5.2.1 Conferência da Entrega: consiste na identificação e conferência das licenças fornecidas;

2.5.2.2 Teste de Instalação: consiste na verificação da instalação e da configuração das funcionalidades instaladas;

2.5.2.3 Testes de Ativação: consiste na operacionalização da solução de segurança, após a conclusão dos testes de instalação, com a verificação de suas características, de suas funcionalidades e de sua compatibilidade;

2.5.3 A verificação preliminar não implica em recebimento definitivo da solução de segurança fornecida;

2.5.4 O relatório gerado em função dos Testes de Verificação Preliminar será documento integrante do Termo de Recebimento e Aceitação da solução de segurança fornecida.

2.6 ENTREGA, ACEITE E INSTALAÇÃO

2.6.1 O aceite da solução de segurança será feito pela PGE, após a implantação e entrada em operação das licenças fornecidas;

2.6.2 O aceite das licenças será feito mediante emissão pela "Comissão de Recebimento", nomeada pela PGE, do "Termo de Recebimento e Aceitação";

2.6.3 A entrega e instalação das licenças será feita de acordo com plano de implantação, apresentado pela Contratada e aprovado pela Contratante;

2.6.4 A instalação deverá seguir cronograma previsto no plano de implantação;

2.6.5 Como parte dos documentos de aceite da solução de segurança fornecida, a Contratada deverá apresentar "Tabela de Comprovação Técnica " das especificações exigidas neste Termo de Referência (apresentar na Tabela a correlação das especificações com a respectiva comprovação técnica, exemplo, página, item, documento etc.). A comprovação técnica deverá ser efetuada através de documentos oficiais referentes a Solução de Segurança fornecido, bem como referente aos módulos complementares.

2.7 DOCUMENTAÇÃO TÉCNICA

2.7.1 A documentação técnica a ser fornecida deverá conter no mínimo os módulos descritos a seguir:

2.7.1.1 Documentação das Funcionalidades: Este documento conterá as características técnicas da Solução de Segurança e suas funções, procedimentos e parâmetros de configuração, tabelas, ilustrações etc.;

2.7.1.2 Documentação de Instalação e Operação: Este documento conterá informações quanto aos procedimentos de instalação e operação, comandos e teste aplicáveis, procedimentos de inicialização, de configuração e gerência de desempenho, de falhas e de segurança pertinentes.

2.7.2 A Contratada deverá apresentar juntamente com a documentação da Solução de Segurança, certificado ou título, concedido pelo fabricante, que comprove o credenciamento da Contratada como representante autorizada;

2.7.3 A Contratada deverá apresentar juntamente com a documentação da Solução de Segurança, as licenças necessárias para a implantação;

2.7.4 A documentação abrange: manuais operacionais da Solução de Segurança, documento com as especificações técnicas das soluções e seus recursos, as licenças, mídias contendo as informações necessárias para instalação, fornecidos e toda documentação acessórias relativas a solução fornecidos.

3. Especificações:

3.1 Garantia Técnica:

(x) 3.1 O prazo legal de garantia técnica será de 30 (trinta) dias, tratando-se de fornecimento de serviço não durável, e de 90 (noventa) dias, tratando-se de fornecimento de serviço durável (art. 26, I e II do CDC).

3.1.1 Deverá ser acrescido ao prazo da garantia legal, o prazo de licenciamento do software de 24 (vinte e quatro) meses, com suporte técnico de 8 (oito) horas por dia, 5 (cinco) dias por semana, na cidade de Salvador (BA).

3.1.2 A garantia contratual é complementar à legal e será conferida mediante termo escrito (art. 50 do CDC).

3.1.3 A licitante deverá comprovar, através de atestado/certificado expedido pelo fabricante do objeto desta licitação, ser revenda credenciada.

3.2 O termo de garantia ou equivalente deve ser padronizado e esclarecer, de maneira adequada, em que consiste, a forma, o prazo e o lugar em que pode ser exercitada, bem como os ônus a cargo do Contratante, devendo ser entregue devidamente preenchido, pela Contratada, no ato do fornecimento, acompanhada de manual de instrução e, quando for o caso, do manual de instalação e uso do produto, em linguagem didática, com ilustrações (art. 50, parágrafo único, do CDC).

3.3 Durante o período de licenciamento o fabricante vai garantir o funcionamento da solução de segurança, com suporte técnico prestado em caso de falha. Deverá ser garantida neste prazo a atualização de versões, releases, componentes (bibliotecas, filtros etc.) e módulos da Solução de Seguranças. Todos as soluções deverão ter o mesmo período de licenciamento.

3.4 A empresa deverá demonstrar na declaração formal de disponibilidade (Parte II – Seção III) citada no item d.1 do 1.3 – Qualificação Técnica (Parte II – Seção I) que possui em seu quadro técnico no mínimo um profissional com a certificação técnica do fabricante, apresentando certificado que comprove tal condição, além das comprovações de vínculo deste com a empresa no momento oportuno, nas formas previstas no item d.2 da citada Seção (1.3 – Qualificação Técnica (Parte II – Seção I).

4. Responsável pelas informações constantes do termo de referência:

Servidor responsável:	Maurício de Cerqueira Pereira
Lotação:	PGE/CGE/CTIC

ANEXO I DO TERMO DE REFERÊNCIA – ESPECIFICAÇÕES TÉCNICAS

1. **DAS ESPECIFICAÇÕES TÉCNICAS**

1.1 Solução de Gestão de Vulnerabilidade e Auditoria de Configurações de Ativos

1.1.1 A solução deve realizar varreduras (scans) de vulnerabilidades, avaliação de configuração e conformidade (baseline e compliance);

1.1.2 A solução deve possuir recurso de varredura ativa, onde o scanner comunica-se com os alvos (ativos) através da rede;

1.1.3 A solução de gestão de vulnerabilidades deve suportar varreduras de dispositivos de IoT;

1.1.4 A solução deve ser licenciada pelo número de endereços IP ou dispositivos (assets);

1.1.5 A solução deve fornecer um modelo de armazenamento integrado que não dependa de um banco de dados externos ou de terceiros;

1.1.5.1 Caso a solução dependa de banco de dados de terceiros, todas as licenças deverão ser fornecidas pela CONTRATADA.

1.1.6 A solução deverá suportar API (Application Programming Interface) baseada em REST (Representatonal State Transfer) para automação de processos e integração com aplicações terceiras.

1.1.7 A solução deve possuir integração via API no mínimo as seguintes linguagens: Python, Powershell, Ruby, javascript, Java, Swift e PHP;

1.1.8 A solução deve possuir métodos de consulta via api e envio, tais como: HTTP METHOD (POST, GET, PUT AND DELETE)

1.1.9 A solução deve incluir a opção para agentes instalados e licenciados em estações de trabalho e servidores, para varredura diretamente no sistema operacional;

1.1.9.1 Tais agentes devem ser gerenciados pela mesma interface/console da plataforma de gestão de vulnerabilidades;

1.1.10 A solução deve permitir o agrupamento de scanners para facilitar o gerenciamento e aplicação de políticas.

1.1.11 A solução deve realizar a varredura tanto de dispositivos na rede interna, dispositivos expostos a demais redes externas, tanto quanto dispositivos em nuvens públicas como Azure, AWS ou GCP.

1.1.11.1 O escaneamento para os dispositivos expostos deve sem realizados através de SCANS (ENGINE) do próprio fabricante alocados no Brasil;

1.1.12 Os scanners e sensores agentes deverão ser gerenciados por uma única plataforma, de maneira centralizada;

1.1.13 O acesso a console de gerenciamento deve ser fornecida para pelo menos 10 usuários simultâneos;

1.1.14 A solução deve ser capaz de se integrar e disponibilizar insumos para soluções de correlação de eventos externa (SIEM);

1.1.15 A solução deve apresentar, para cada vulnerabilidade encontrada, a descrição e passos que devem ser tomados para correção;

1.1.16 A solução deve apresentar, para cada vulnerabilidade encontrada, evidências da vulnerabilidade através de saídas das verificações (outputs);

1.1.17 A solução deve fornecer controle de acesso baseado em função (*RBAC- Role Based Access Control*) para controlar o acesso do usuário a conjuntos de dados e funcionalidades;

1.1.18 A solução deve ser capaz de definir e gerenciar grupos de usuários, incluindo limitação de funções de varreduras e acesso a relatórios e dashboards;

1.1.19 A solução deve ter a capacidade de excluir determinados endereços IP do escopo de qualquer varredura ou scan;

1.1.20 A solução deve criptografar todos resultados de varreduras obtidos e informações inseridas tanto em descanso quanto em trânsito;

1.1.21 A solução deve suportar métodos de autenticação usando bases de autenticação local, e SAML (Security Assertion Markup Language) para uso de SSO (Single Sign-On);

1.1.22 A solução deve ser capaz de orquestrar scanners ilimitados dentro da infraestrutura;

1.1.23 A solução não deve impor nenhum limite de quantidade de scanners implementados dentro da infraestrutura;

1.1.24 A solução deverá possuir sistema de alertas para informar a disponibilidade de resultados dos escaneamentos através de email e SMS;

1.1.25 A solução deve oferecer capacidade de configuração dinâmica de grupos de ativos através de no mínimo as seguintes características:

2. Sistema Operacional, Endereço IP, DNS, NetBIOS Host, MAC, AWS Instance Type, AWS EC2 Name, Software instalado, Azure VM ID, AWS Region, Google Cloud Instance ID, Azure Resource ID, Ativos avaliados;

2.1 Dos requisitos e relatórios e painéis gerenciais

2.1.1 A solução deverá possuir painéis gerenciais (dashboards) pré-definidos para rápida visualização dos resultados, permitindo ainda a criação de painéis personalizados.

2.1.2 Os painéis gerenciais deverão ser apresentados em diversos formatos, incluindo gráficos e tabelas, possibilitando a exibição de informações em diferentes níveis de detalhamento.

2.1.3 Os relatórios devem ser disponibilizados sob demanda no console de gerência da solução;

2.1.4 Os relatórios devem conter informações da vulnerabilidade, severidade, se existe um *exploit* disponível e informações do ativo.

2.1.5 A solução deve permitir a customização de dashboards/relatórios.

2.1.6 A solução deve concentrar todos os relatórios na plataforma central de gerenciamento, não sendo aceitas soluções fragmentadas;

2.1.7 A solução deve ser capaz de produzir relatórios, pelo menos, nos seguintes formatos: HTML, PDF e CSV;

2.1.8 A solução deve possibilitar a criação de relatórios baseado nos seguintes alvos: Todos os ativos e Alvos específicos;

2.1.9 Deve suportar a criação de relatórios criptografados (protegidos por senha configurável);

2.1.10 A solução deve suportar o envio automático de relatórios para destinatários específicos;

2.1.11 Deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual;

2.1.12 Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos;

2.2 Das varreduras

2.2.1 A solução deve realizar varreduras em uma variedade de sistemas operacionais, incluindo no mínimo Windows, Linux e Mac OS, bem como appliances virtuais;

2.2.2 A solução deve suportar varredura com e sem agente, de maneira ativa e passiva, distribuídas em diferentes localidades e regiões e gerenciar todos por uma console central;

2.2.3 A solução deve fornecer agentes instaláveis em sistemas operacionais distintos para monitoramento contínuo de vulnerabilidades;

2.2.4 Tais agentes devem realizar conexões para o sistema gerenciamento através de protocolo seguro;

2.2.5 A solução deve ser configurável para permitir a otimização das configurações de varredura.

2.2.6 A solução 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;

2.2.7 A solução deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até acesso de sistema ou administrativo;

2.2.8 A solução deve se integrar com solução de gerenciamento de acessos privilegiados para autenticação nos dispositivos, no mínimo, os seguintes:

2.2.8.1 CyberArk;

2.2.8.2 BeyondTrust

2.2.8.3 Thycotic

2.2.8.4 Centrify

2.2.9 A solução deve suportar o agendamento de scans personalizados, incluindo a capacidade de executar varreduras em tempos designados, com frequência pré-determinada;

2.2.10 A solução deve ser capaz de identificar novos hosts no ambiente sem a necessidade de scan;

2.2.11 solução deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados;

2.2.12 A solução deve ser capaz de realizar em tempo real a descoberta de vulnerabilidades nas seguintes tecnologias:

2.2.12.1 Cloud Services;

2.2.12.2 Data Leakage;

2.2.12.3 Database;

2.2.12.4 IoT;

2.2.12.5 Mobile Devices;

2.2.12.6 Operating System;

2.2.12.7 Peer-To-Peer;

2.2.12.8 SCADA;

2.2.12.9 Web Servers;

2.2.12.10 Web Clients;

2.2.13 A solução deve ser capaz de identificar a comunicação de malwares na rede de forma passiva;

2.2.14 A solução deve em tempo real, detectar logins e downloads de arquivos em um compartilhamento de rede;

2.3 Da análise e priorização de vulnerabilidades

2.3.1 A solução deve ser capaz de exibir ambos severidade e pontuação, com base em CVSS (Common Vulnerability Scoring System) e inteligência

de ameaças;

2.3.2 A solução deve utilizar sistema de pontuação e priorização das vulnerabilidades que utilize no mínimo:

2.3.2.1 CVSS Impact Score;

2.3.2.2 Idade da Vulnerabilidade;

2.3.2.3 Maturidade de códigos de exploração da vulnerabilidade encontrada;

2.3.2.4 Frequência de uso da vulnerabilidade em ataques e campanhas atuais;

2.3.2.5 Disponibilidade do código de exploração da vulnerabilidade;

2.3.2.6 Presença de módulos de exploração de vulnerabilidade em frameworks automatizados de exploração de vulnerabilidades como CANVAS, Metasploit e Core Impact;

2.3.2.7 Popularidade da vulnerabilidade em fóruns e comunicações na Darkweb;

2.3.3 O mecanismo de priorização deve ser sujeito a modificações e atualizações diárias com base em inteligência de ameaças e observação de tendências na Internet;

2.4 Da Análise de Risco do Ambiente

2.4.1 A solução deve gerar um score que combine dados de vulnerabilidades com a criticidade dos ativos do ambiente computacional;

2.4.2 O score deve ser gerado automaticamente por meio de algoritmos de inteligência artificial (Machine Learning) e deve calcular a probabilidade de exploração de uma determinada vulnerabilidade;

2.4.3 Deve ser capaz de calcular a criticidade dos ativos da organização;

2.4.4 A solução deve ser capaz de realizar um benchmark no ambiente da CONTRATANTE comparando sua maturidade com outras organizações do mesmo setor;

2.4.5 A solução deve prover visão sobre quais ações de remediação reduzem o maior nível de risco do ambiente;

2.4.6 A solução deve também permitir a visualização de ações de remediação agregadas para visão consolidada de redução de risco;

2.4.7 Deve permitir modificar a qualquer momento o tipo de indústria para comparação. Ex: Mudar de Setor Público para Mercado Financeiro

2.4.8 Deve fornecer uma lista com as principais recomendações para o ambiente com foco na redução da exposição cibernética da organização;

2.4.9 A solução deve gerar uma pontuação para cada um dos ativos onde é levado em conta as vulnerabilidades presentes naquele ativo assim como a classificação do ativo na rede (peso do ativo).

2.4.10 A solução deve gerar uma pontuação global referente a exposição cibernética da organização baseado nas pontuações de cada um dos ativos.

2.4.11 A solução deve oferecer uma capacidade de comparação (benchmarking) da pontuação referente a exposição cibernética com outros players da mesma indústria assim como outras empresas do mercado.

2.4.12 A solução deve permitir um acompanhamento histórico do nível de exposição da organização;

2.4.13 Permitir realizar alterações na classificação dos ativos (atribuição de pesos diferentes) podendo sobrescrever a classificação atribuída automaticamente pela solução.

2.4.14 A solução deverá apresentar indicadores específicos referentes a remediação, possuindo no mínimo informações referentes ao tempo entre remediação e o tempo o qual a vulnerabilidade foi descoberta no ambiente, tempo entre a remediação e a data de publicação da vulnerabilidade, quantidade média de vulnerabilidades críticas por ativo e a comparação da quantidade de vulnerabilidades corrigidas por criticidade.

2.4.15 A solução deve permitir a segregação lógica entre áreas distintas da empresa afim de obter a pontuação referente exposição cibernética por área.

2.5 Da descoberta de ativos

2.5.1 A solução deve ser capaz de realizar escaneamento de descoberta de rede utilizando os seguintes critérios como alvo: IP, CIRD e Range;

2.5.2 A solução deve disponibilizar modelos de escaneamento de descoberta, ajustável, com os seguintes tipos de scan:

2.5.2.1 Enumeração de Hosts;

2.5.2.2 Identificação de Sistema Operacional (SO);

2.5.2.3 Port Scan (Portas comuns);

2.5.2.4 Port Scan (Todas as portas);

2.5.2.5 Customizado;

2.5.3 A solução deve permitir realizar escaneamento de descoberta customizado podendo ser parametrizado de acordo com a necessidade.

2.5.4 A parametrização do escaneamento de descoberta deve, no mínimo, conter os seguintes requisitos:

2.5.5 Descoberta de Host:

2.5.5.1 Ping o host remoto;

2.5.5.2 Usar descoberta rápida;

2.5.5.3 Métodos de ping;

a. ARP;

b. TCP;

c. ICMP;

d. UDP;

2.5.5.4 Escaneamento de descoberta de dispositivos de OT;

2.5.5.5 Escaneamento de descoberta em redes de impressora;

2.5.5.6 Escaneamento em redes Novell;

2.5.5.7 Tecnologia de Wake-on-LAN;

2.5.6 Port Scanning

2.5.6.1 Portas

a. Considerar portas não escaneadas como fechadas;

b. Range de portas a serem escaneadas;

2.5.6.2 Enumerar Portas locais:

a) SSH (netstat);

b) WMI (netstat);

c) SNMP

2.5.7 Descoberta de Serviços;

2.5.7.1 Sondar todas as portas para encontrar serviços;

2.5.7.2 Procurar por serviços baseado em SSL/TLS;

2.5.7.3 Enumerar todas as cifras SSL/TLS;

2.5.8 A solução deve realizar descoberta de ativo de forma passiva e adicionado automaticamente na console de gerenciamento.

2.5.9 A solução deve descobrir passivamente quando um host é adicionado na rede.

2.6 Da avaliação de vulnerabilidade

2.6.1 A solução deve ser capaz de realizar testes sem a necessidade de agentes instalados no dispositivo destino para detecção de vulnerabilidades.

2.6.2 A solução deve detectar e classificar através de severidades, riscos e vulnerabilidades;

2.6.3 A solução deve também fornecer informações detalhadas sobre a natureza da vulnerabilidade, evidências da existência da vulnerabilidade e recomendações para mitigá-los;

2.6.4 A solução deve incluir uma saída detalhada das vulnerabilidades descobertas como versões de DLL esperadas e encontradas;

2.6.5 A solução deve ser compatível com CVE e fornecer pelo menos 10 anos de cobertura CVE;

2.6.6 A solução deve identificar vulnerabilidades especificas para o Active Directory com os seguintes padrões de verificação;

2.6.6.1 Contas administrativas vulneráveis a Kerberoasting attack;

2.6.6.2 Utilização de criptografia vulnerável com autenticação Kerberos;

2.6.6.3 Contas com pré-autenticação do Kerberos desabilitada;

2.6.6.4 Verificação de usuários com a opção de nunca expirar a senha com a opção habilitada;

2.6.6.5 Verificar validação de fragilidades do tipo “Unconstrained Delegation”;

2.6.6.6 Verificação de “Pre-Windows 2000 Compatible Access”;

2.6.6.7 Verificação de validade de chaves mestras "Kerberos KRBTGT”;

2.6.6.8 Verificação de “SID History Injection”;

2.6.6.9 Verificação de “Printer Bug Exploit”;

2.6.6.10 Verificação de “Primary Group ID”;

2.6.6.11 Verificação de usuários com Passwords em branco;

2.6.7 A solução deve suportar o uso de SMB e WMI para verificação de sistemas Microsoft Windows;

2.6.8 A solução deve ser capaz de iniciar automaticamente serviços de registro remoto em sistemas Windows ao executar uma varredura credenciada;

2.6.9 A solução deve ser capaz de parar automaticamente o serviço de registro remoto em sistemas Windows novamente assim que a varredura estiver completa.

2.6.10 O scanner deve oferecer suporte a shell seguro (SSH) com a capacidade de escalar privilégios para varredura de vulnerabilidades e auditorias de configuração em sistemas Unix.

2.6.11 A solução deve suportar o uso do netstat (Linux) e WMI (Windows) para uma enumeração rápida e precisa de portas em um sistema quando as credenciais são fornecidas;

2.6.11.1 A solução deve possibilitar a verificação remota de portas, além da enumeração local de portas, para ajudar a determinar se algum mecanismo de controle de acesso está sendo utilizado.

2.6.12 A solução deve fornecer auditoria de patch (MS Bulletins) para as principais versões de Windows

2.6.13 A solução deve fornecer auditoria de patch para todos os principais sistemas operacionais Unix incluindo Mac OS, Linux, Solaris e IBM AIX.

2.6.14 A solução deve fornecer varredura para aplicativos comerciais diversos e proprietários, incluindo, mas não limitando-se a: Java, Adobe, Oracle, Apple, Microsoft, Check Point, Palo Alto Networks, Cisco, Fortinet, Fireeye, McAfee, etc.;

2.6.15 A solução deve incluir classificação de severidades de acordo com o padrão Sistema Comum de Pontuação de Vulnerabilidade Versão (CVSS2 e CSVSS 3);

2.6.16 A solução deve fornecer informações acerca da disponibilidade de códigos de exploração das vulnerabilidades encontradas em frameworks de exploração para as plataformas mais populares: Core, Metasploit e Canvas;

2.6.17 A solução deve informar se a vulnerabilidade pode e está sendo ativamente explorada por código malicioso (malware);

2.6.18 A solução deve possuir importação de arquivos.YARA;

2.6.19 Deve ser capaz de identificar e classificar vulnerabilidades de máquinas virtuais em nuvem pública em infraestruturas como serviço nas plataformas AWS, Microsoft Azure e Google Cloud.

2.7 Da auditoria de Configuração

2.7.1 A solução deve ser capaz de realizar auditoria de conformidade sem a necessidade de agente instalado no dispositivo de destino;

2.7.2 A solução deve fornecer benchmarks de auditoria de segurança e configuração para conformidade regulatória e outros padrões de práticas recomendadas pela área ou fabricantes.

2.7.3 A solução deve realizar verificações de auditoria contendo as de segurança, com indicação de sucesso ou falha, baseado nos principais frameworks reconhecidos pela indústria, pelo menos os seguintes:

2.7.3.1 Center for Internet Security Benchmarks (CIS)

2.7.3.2 Defense Information Systems Agency (DISA) STIGs

2.7.3.3 Health Insurance Portability and Accountability Act (HIPAA)

2.7.3.4 Payment Card Industry Data Security Standards (PCI DSS)

2.7.4 A solução deve fornecer auditoria de programas antivírus para determinação de presença e status de inicialização para no mínimo as seguintes soluções: TrendMicro Office Scan, McAfee VirusScan, Microsoft Endpoint Protection e Kaspersky;

2.7.5 A solução deve fornecer auditorias de configuração com base benchmarks em CIS (Center for Internet Security) L1 e L2, para ambos os sistemas operacionais Microsoft Windows e Linux;

2.7.6 A solução deve permitir auditoria de conformidade em servidores Windows, Linux, Bancos de Dados SQL Server, a fim de determinar se estão configurados de acordo com os principais Framework de segurança como, por exemplo, CIS e DISA;

2.7.7 A solução deve oferecer validação e suporte a SCAP (Security Content Automation Protocol);

Solução de análise dinâmica de vulnerabilidades para aplicações Web

2.8 A solução deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações Web como parte dos ativos a serem inspecionados;

2.9 A solução deve ser capaz de executar varreduras em sistemas web através de seus endereços IP ou FQDN (DNS);

2.10 A solução deve avaliar no mínimo os padrões de segurança OWASP Top 10 e PCI (payment card industry data security standard);

2.11 A solução deve suportar as diretivas PCI ASV 5.5 para definição de escopo de análise da aplicação;

2.12 A solução deve suportar as diretivas PCI ASV 6.1 para definição de balanceadores de carga das aplicações bem como suas configurações para inclusão no relatório de resultados;

2.13 A solução deve possuir templates prontos de varreduras entre simples e extensos;

2.14 Para varreduras extensas e detalhadas, deve varrer e auditar no mínimo os seguintes elementos:

2.14.1 Cookies, Headers, Formulários e Links;

2.14.2 Nomes e valores de parâmetros da aplicação;

2.14.3 Elementos JSON e XML;

2.14.4 Elementos DOM;

2.15 A solução deve permitir somente a execução da função crawler, que consiste na navegação para descoberta das URLs existentes na aplicação;

2.16 A solução deve ser capaz de utilizar scripts customizados de crawl com parâmetros definidos pelo usuário;

2.17 A solução deve excluir determinadas URLs da varredura através de expressões regulares;

2.18 A solução deve excluir determinados tipos de arquivos através de suas extensões;

2.19 A solução deve instituir no mínimo os seguintes limites:

2.19.1 Número máximo de URLs para crawl e navegação;

2.19.2 Número máximo de diretórios para varreduras;

2.19.3 Número máximo de elementos DOM;

2.19.4 Tamanho máximo de respostas;

2.19.5 Limite de requisições de redirecionamentos;

2.19.6 Tempo máximo para a varredura;

2.19.7 Número máximo de conexões HTTP ao servidor hospedando a aplicação Web;

2.19.8 Número máximo de requisições HTTP por segundo;

2.20 A solução deve detectar congestionamento de rede e limitar os seguintes aspectos da varredura:

2.20.1 Limite em segundos para timeout de requisições de rede;

2.20.2 Número máximo de timeouts antes que a varredura seja abortada;

2.21 A solução deve agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual;

2.22 A solução deve enviar notificações através de no mínimo E-mail e SMS;

2.23 A solução deve possuir a flexibilidade de selecionar quais testes serão realizados de forma granular, através da seleção de testes, plug-ins ou ataques;

2.24 A solução deve avaliar sistemas web utilizando protocolos HTTP e HTTPs;

2.25 A solução deve possibilitar a definição de atributos no cabeçalho (HEADER) da requisição HTTP de forma personalizado a ser enviada durante os testes;

2.26 A solução deve ser compatível com avaliação de web services REST e SOAP;

2.26.1 Deverá suportar no mínimo os seguintes esquemas de autenticação:

2.26.2 Autenticação básica (digest);

2.26.3 NTLM;

2.26.4 Form de login;

2.26.5 Autenticação de Cookies;

2.26.6 Autenticação através de Selenium;

2.27 A solução deve importar scripts de autenticação selenium previamente configurados pelo usuário;

2.28 A solução deve customizar parâmetros Selenium como delay de exibição da página, delay de execução de comandos e delay de comandos para recepção de novos comandos;

2.29 A solução deve exibir os resultados das varreduras em tendência temporal para acompanhamento de correções e introdução de novas vulnerabilidades;

2.30 A solução deve exibir os resultados agregados de acordo com as categorias do OWASP Top 10 (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project).

2.31 Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações;

2.32 Para cada vulnerabilidade encontrada, deve ser exibido evidências da mesma em seus detalhes;

2.33 Para vulnerabilidades de injeção de código (SQL, XSS, XSRF, etc), deve evidenciar nos detalhes do evento encontrado:

2.33.1 Payload injetado;

2.33.2 Evidência em forma de resposta da aplicação;

2.33.3 Detalhes da requisição HTTP;

2.33.4 Detalhes da resposta HTTP;

2.34 Os detalhes das vulnerabilidades devem conter descrição da falha e referências didáticas para a revisão dos analistas;

2.35 Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação das mesmas;

2.36 A solução deve possuir suporte a varreduras de componentes para no mínimo:

2.36.1 Wordpress, Blog Designer Plugin for Wordpress, Event Calendar Plugin for Wordpress, Convert Plus Plugin for Wordpress, AngularJS, Apache, Apache Tomcat, Apache Tomcat JK connecto, Apache Spark e Apache Struts, Atlassian Confluence, Atlassian Crowd e Atlassian Jira, Backbone.js, ASP.NET, Bootstrap, Drupal, Joomla!, jQuery, Lighttpd, Magento, Modernizr, Nginx, PHP, AJAX, Sitefinity, Telerik, ThinkPHP, Webmin e YUI;

Solução de análise em imagens de ambientes Containers

2.37 A solução deve ser licenciada contabilizando o número de imagens únicas, não sendo contabilizadas novas versões de uma mesma imagem;

2.38 A solução deve analisar, testar e reportar falhas de segurança em aplicações em Containers Docker como parte dos ativos a serem inspecionados;

2.39 A solução deve ser capaz de analisar imagens preparadas pelos desenvolvedores na esteira DevOps em busca de imagens com vulnerabilidades identificadas e malware residente no sistema de arquivos;

2.40 A solução deve integrar a esteira DevOps através de API, invocando o envio da imagem para análise em repositório próprio da solução ou utilizando scanner implementado em infraestrutura proprietária do órgão com a finalidade de evitar o envio de imagens e propriedade intelectual da contratante;

2.41 A documentação de API da solução deverá ter acesso público através de website ou documentação do próprio fabricante;

2.42 A console de administração deverá possuir controle de acesso no mínimo permitindo usuários com capacidade de somente visualizar as informações, e usuários com capacidade para efetuar análise das imagens;

2.43 A solução deve inventariar o sistema operacional de cada imagem analisada e suas vulnerabilidades encontradas;

2.44 A solução deve identificar containers que não foram analisados antes de sua implementação em produção;

2.45 A solução deve analisar as camadas (layers) de um container;

2.46 A solução deve identificar containers que tiveram mudanças de arquivos entre a análise e a sua implementação em produção;

2.47 A solução deve informar os CVEs para cada vulnerabilidade encontrada nos pacotes e bibliotecas residentes na imagem;

2.48 A solução deve ter a capacidade de testar automaticamente todas as imagens armazenadas, ou previamente testadas, sempre que uma nova vulnerabilidade for publicada e atualizada no banco de dados de vulnerabilidade da solução, sem qualquer tipo intervenção manual;

2.49 A solução deve inventariar os pacotes e bibliotecas e suas respectivas versões e listar as mesmas dentro do relatório de resultados de análise de cada imagem;

2.50 A solução deve possuir conectores e permitir importação de imagens dos seguintes repositórios:

2.51 Docker;

2.52 Docker EE;

2.53 AWS ECR;

2.54 JFrog Artifactory;

2.55 A solução deve possuir integração com Microsoft Azure Container, Vmware Harbor e Sonatype Nexus para importar e analisar imagens;

2.56 A solução deve fornecer scanner em formato Docker para implementação local e análise de imagens sem a necessidade de envio destas para repositório remoto, fora do ambiente da contratante;

2.57 A solução ser capaz de configurar políticas usando como condições: CVSS Score, CVEs específicos e Malware identificado;

2.58 A solução deve permitir a criação de políticas especificas por repositório;

2.59 A solução deve prover integração com as seguintes plataformas de integração contínua: Bamboo, CircleCI, Codeship, Distelli, Drone.io, Jenkins, Shippable, Solano Labs, Travis CI, Wrecker e Kubernets;

Solução de análise de condigo em ambiente DevOps

2.60 A solução deve detectar e configurações incorretas da infraestrutura de nuvem em fases de design, construção e tempo de execução do seu ciclo de vida de desenvolvimento de software;

2.61 A solução deve prevenir problemas de segurança identifique e remova falhas na nuvem durante desenvolvimento antes de chegarem à produção;

2.62 A solução deve ser possível avaliar modelos de infraestrutura como código (IaC), com integrações em:

2.62.1 Terraform;

2.62.2 AWS CloudFormation;

2.62.3 Azure Resource Manager;

2.63 A solução deve prevenir o desvio de postura na nuvem identifique discrepâncias entre o IaC e sua nuvem em execução ambiente;

2.64 A solução deve fornecer sugestões de correção automaticamente por meio de pull ou mesclagem;

2.65 A solução deve contextualizar riscos compreender as vulnerabilidades de aplicativos no contexto de suas configurações de infraestrutura para obter uma imagem real do risco que eles presente;

2.66 A solução deve prover integração no mínimo com as seguintes plataformas abaixo:

2.66.1 Jira

2.66.2 Slack

2.66.3 AWS SNS

2.66.4 Jenkin

2.66.5 Terraform Cloud

2.66.6 CircleCI

2.66.7 Splunk

2.66.8 AWS CloudTrail

2.67 A solução deve possuir integração com no m´nimo os seguintes Repositórios:

2.67.1 Bitbucket

2.67.2 GitHub

2.67.3 GitLab

2.67.4 Azure DevOps

2.68 A solução deve possuir funcionalidade de monitoramento dos repositórios sempre que houver alteração de código uma verificação automática via IaC deve apresentar a diferença;

2.69 solução deve possuir políticas de análise em ambiente de nuvem para no mínimo as seguintes plataformas:

2.69.1 AWS

2.69.2 Azure

2.69.3 GCP

2.69.4 Kubernetes

2.70 A solução deve possuir análise por benchmarks e compliance para os seguintes padrões em formato de Dashboard

2.70.1 CIS

2.70.2 NIST

2.70.3 ISO-27001

2.70.4 PCI-DSS

2.70.6 CCM

2.70.7 GDPR

Solução de análise em ambiente Microsoft Active Directory

2.7 1A solução deve identificar fraquezas ocultas em configurações do dedicadas ao Active Directory;

2.72 A solução deve possuir ações preventivas de hardening para o Active Directory;

2.73 A solução deve identificar ataque específicos para a estrutura do Active Directory

2.74 A solução deve possuir funcionalidade para analisar em detalhes cada configuração incorreta que acarreta riscos de segurança – com uma linguagem simples, contextualizando tal risco para os times envolvidos;

2.75 A solução deve possuir recomendações de correção para cada configuração incorreta no Active Directory;

2.76 A solução deve avaliar relações de confiança perigosas entre florestas e domínios;

2.77 A solução deve capturar as mudanças que ocorrem no AD e demostrar na console de administração;

2.78 A solução deve possuir dashboard com os principais ataques e vulnerabilidades por domínio;

2.79 A solução deve permitir a correlação de mudanças no Active Directory e desvios de segurança;

2.80 A solução deve analisar em detalhes um ataque explorando as descrições através do framework MITRE ATT&CK;

2.81 A solução deve prover interface web para gerenciamento de todas as funcionalidades;

2.82 A solução deve possuir capacidade nativa de criação de dashboards customizados;

2.83 A solução deve suportar um modelo de controle de acesso baseado em funções (RBAC) flexível;

2.84 A solução deve realizar alterações no Active Directory, seus objetos e atributos;

2.85 A solução deve armazenar ou sincronizar nenhuma credencial de objetos do Active Directory;

2.86 A solução deve suportar ambientes com múltiplas florestas e domínios;

2.87 A solução deve suportar monitoramento contínuo de ambientes com Active Directory com o nível funcional de floresta e domínio a partir do 2003;

2.88 A solução deve suportar reter os eventos coletados por no mínimo um ano;

2.89 A solução deve descobrir e mapear a superfície de ataque do Active Directory e seus domínios monitorados com os seguintes padrões:

2.89.1 Não depender de agentes ou sensores para coleta de informações do AD;

2.89.2 A solução deve seguir as boas práticas de *menor privilégio*, a conta de serviço utilizada para conexão com o Active Directory, sendo o menor nível de acesso esperado para a conta de serviço como parte do grupo *Domain User*;

2.89.3 Interface web que consolida e apresenta de maneira unificada os domínios monitorados e as possíveis relações de confiança estabelecidas entre eles;

2.90 A solução deve analisar continuamente a postura de segurança do AD, minimamente avaliando:

2.90.1 Validação de GPOs desvinculadas, desabilitadas ou órfãs;

2.90.2 Validação de contas desativadas em grupos privilegiados;

2.90.3 Domínio usando uma configuração perigosa de compatibilidade com versões anteriores por meio de alterações no atributo *dSHeuristics*;

2.90.4 Validação de atributos relacionados a roaming de credenciais vulneráveis (*ms-PKI-DPAPIMasterKeys*) gerenciados por um usuário sem privilégios;

2.90.5 Validação de domínio sem GPOs de proteção de computador, desativando protocolos vulneráveis antigos, como *NTLMv1;*

2.90.6 Validação de contas com senhas que nunca expiram;

2.90.7 Validação de senhas reversíveis em GPOs;

2.90.8 Validação de uso de senhas reversíveis em contas de usuário;

2.90.9 Validação de utilização de protocolo criptográfico fraco (Ex. DES) em contas de usuário;

2.90.10 Validação de uso do LAPS (Solução de senha de administrador local) para gerenciar senhas de contas locais com privilégios;

2.90.11 Validação se o domínio possui um nível funcional desatualizado;

2.90.12 Validação de contas de usuário utilizando senha antiga;

2.90.13 Validação se o atributo *AdminCount* está definido em usuários padrão;

2.90.14 Validação do uso recente da conta de administrador padrão;

2.90.15 Validação de usuários com permissão para ingressar computadores no domínio;

2.90.16 Validação de contas dormentes;

2.90.17 Validação de computadores executando um sistema operacional obsoleto;

2.90.18 Validação de restrições de *logon* para usuários privilegiados em ambiente com múltiplos tiers (1, 2 e 3) de segregação de ativos;

2.90.19 Validação de direitos perigosos configurados no *Schema* do AD;

2.90.20 Validação de relação de confiança perigosa com outras *Florestas* e *Domínios*;

2.90.21 Validação de contas que possuem um atributo perigoso de histórico SID (*SID History*);

2.90.22 Validação de contas utilizando controle de acesso compatível com versões anteriores ao Windows 2000;

2.90.23 Validação da última alteração de senha do KDC;

2.90.24 Validação da última alteração da senha da conta SSO do *Azure AD*;

2.90.25 Validação de contas que podem ter senha em branco/vazia;

2.90.26 Validação de utilização do grupo nativo *Protected Users*;

2.90.27 Validação de privilégios sensíveis (Ex. *Debug a program, Replace a process level token, etc.)* perigosos atribuídos aos usuários;

2.90.28 Validação de possível senha em *clear-text*;

2.90.29 Validação de sanidade das GPOs e componentes CSEs (*Client-Side Extension*);

2.90.30 Validação de uso de algoritmos de criptografia fracos na PKI do Active Directory;

2.90.31 Validação de contas de serviço com SPN (*Service Principal Name*) que fazem parte de grupos privilegiados;

2.90.32 Validação de contas anormais nos grupos administrativos padrão do AD;

2.90.33 Validação de consistência no *container adminSDHolder*;

2.90.34 Validação de delegação *Kerberos* perigosa;

2.90.35 Validação em permissões de objetos raiz que permitem ataques do tipo DCSync;

2.90.36 Validação de políticas de senha fracas aplicadas aos usuários;

2.90.37 Validação das permissões relacionadas às contas do *Azure AD Connect*;

2.90.38 Validação do ID do grupo primário do usuário (*Primary Group ID*);

2.90.39 Validação de permissões em GPOs sensíveis associadas aos *Containers Configuration*, *Sites*, *Root Partition* e *OUs* sensíveis como *Domain Controllers;*

2.90.40 Controladores de domínio gerenciados por usuários ilegítimos;

2.90.41 Validação de certificado mapeado através de atributo *altSecurityIdentities* em contas privilegiadas;

2.90.42 Validação de uso de protocolo *Netlogon* inseguro (Zerologon/CVE-2020-1472);

2.91 A solução deve identificar vulnerabilidades e configurações incorretas do AD à medida que são introduzidas sendo:

2.91.1 Identificar todas as vulnerabilidades e configurações incorretas no AD;

2.91.2 Monitorar relações de confiança perigosas em toda a estrutura AD;

2.91.3 Apresentar ameaças e alterações sem a necessidade de scans estáticos e programados no Active Directory e sua infraestrutura;

2.91.4 Apresentar as ameaças e alterações em tempo real ou em menos de cinco minutos;

2.92 Detecção e resposta a ataques:

2.92.1 Monitorar continuamente os indicadores de possíveis ataque como DCSync, DCShadow, Password Spraying, Password Guessing/Brute Force, Lsaas Injecton nos controladores de domínio, Golden Ticket, NTLM Relay, entre outros;

2.92.2 Detecção de ataques ao AD em tempo real ou em menos de um minuto;

2.92.3 Análise detalhada do ataque, apresentando ativo de origem, vetor de ataque, controlador de domínio afetado, técnica aplicada;

2.92.4 Apresentação de ataques em uma linha do tempo;

2.92.5 Investigar ameaças, reproduzir ataques e procurar por backdoors;

2.92.6 Permitir busca ágil de eventos específicos na base da solução através de queries customizadas;

2.93 A solução deve ser capaz de enviar alertas por e-mail;

2.94 A solução nativamente deve ser capaz de se integrar com SIEM através de protocolo SYSLOG;

2.95 A solução deve ser capaz de filtrar e enriquecer os eventos que serão enviados para o SIEM;

2..96 A solução deve produzir regras YARA na detecção de ataques (Ex. DCSync, Golden Ticket) identificados pela ferramenta;

2.97 A solução deve possuir conjunto de APIs REST, todas as chamadas disponíveis devem estar contidas na documentação;

2.98 A solução deve permitir a criação de listas de exclusões, suportando minimamente Exclusão por domínios do AD monitorados e por itens analisados;

2.99 A solução deve ser licenciada pelo número de usuários habilitados;

ANEXO II

PROPOSTA COMERCIAL TENABLE – V 1.0 (Ajustada)

S·I·T·E

CONSULTORIA E TECNOLOGIA

Responsável:

João Gualberto Rizzo Araújo
Sócio-Diretor
jgra@xsite.com.br

tenable

29/07/2022

Proposta Comercial

A Procuradoria Geral do Estado da Bahia – PGE/BA

Att: Comissão Permanente de Licitação

REF: Proposta para fornecimento de licença de uso de software de gestão de vulnerabilidade objetivando ampliar a segurança da rede e dos ativos da Procuradoria Geral do Estado da Bahia – PGE/BA, com garantia de 24 (vinte e quatro) meses, serviço de instalação, treinamento (Hands on), configuração e suporte onsite, do fabricante: Tenable, marca/modelo: Tenable EP – Pregão Eletrônico n.º 007/2022 – Processo Administrativo n.º 006.0409.2022.0008208-20.

Apresentação da Empresa

A XSITE é uma empresa com mais de 15 anos de experiência em Segurança da Informação. Nossa missão é transformar as organizações em ambientes mais seguros, produtivos e sustentáveis, através da aplicação de Tecnologias de Gestão e Segurança Informação, atuando de forma segura e com responsabilidade social e ambiental.

A empresa tem demonstrado aos seus clientes que é possível elevar o nível de proteção das suas informações e reduzir os custos de operação de segurança através de automação. Aliando qualidade de produtos, custos acessíveis, profissionais qualificados e serviços de excelência temos sido capazes de ofertar elevados níveis de qualidade com os preços mais competitivos do mercado.

A XSITE realiza a integração segura, rápida, automatizada e inteligente de soluções de segurança, computação em nuvem e infraestrutura. A larga experiência em Segurança da Informação, transformaram comprometimento e estudo em respeito, credibilidade e confiança de centenas de clientes, agregando valor para as organizações e desenvolvendo importantes casos de sucesso.

Dos Produtos e Serviços

Proposta para fornecimento de solução de Gestão de Vulnerabilidades, Contratação de solução unificada de gestão de vulnerabilidade e conformidade de configurações para Ativos e Aplicações Web, em modelo de subscrição, do fabricante: Tenable, marca/modelo: Tenable EP, incluindo instalação, implantação, suporte técnico e treinamento, pelo período de 24 meses.

Disposições gerais:

O contrato prevê a contratação de empresa especializada para fornecimento e serviços de soluções de Segurança da Informação, contemplando manutenção e suporte técnico de softwares necessários à sua operacionalização, visando garantir as políticas de Segurança da Informação da Procuradoria Geral do Estado da Bahia - PGE/BA, de acordo com as características abaixo:

O objeto descrito neste Termo de Referência será entregue e instalado pelos técnicos da empresa fornecedora, na quantidade e características especificadas e dentro do prazo fixado e respeitando os termos estabelecidos neste termo de referência;

Acesso telefônico 08h/dia, 5 dias da semana;

Treinamento Hands on de atualização tecnológica da solução para pelo menos 05 (cinco) técnicos nas instalações da Contratante;

Suporte técnico da Solução de Segurança fornecida em língua portuguesa.

Centro de Pesquisas em Informática LTDA – XSITE Consultoria e Tecnologia
Rua Edistio Ponde, 353, Centro Empresarial Tancredo Neves, sl. 807, STIEP, Salvador, BA, 41.770-395
www.xsite.com.br

Suporte Técnico e Acordo de Nível de Serviço:

A equipe técnica será composta de técnicos certificados pelo fabricante da solução de segurança fornecida, e preparada para dar todo o suporte técnico e ajuda necessária para maximizar os benefícios oferecidos pela solução de segurança, aumentando a sua performance.

O suporte técnico da Solução de Segurança fornecida será prestado pelo através de contato Telefônico (telefone 0800 do fabricante ou telefone com numeração comum do fornecedor), Sitio de Internet (website do fabricante ou do fornecedor), Correio Eletrônico (e-mail do fabricante ou do fornecedor) ou no Local (provido pelo fabricante ou pelo fornecedor), em casos de grande emergência;

O suporte técnico será fornecido pelo fornecedor da solução de segurança ou pelo fabricante, no Brasil e na língua portuguesa;

Serão executados pela XSITE serviços de Instalação e Configuração para uso da solução contratada com supervisão da equipe técnica da PGE;

Será executada pela XSITE uma análise da situação atual e elaborar, em conjunto com a equipe interna da PGE, um plano de otimização de recursos, rotinas, procedimentos e processos para o novo ambiente de segurança. Essa documentação deverá ser entregue, pela XSITE, em formato digital;

A XSITE preservará todo ambiente computacional existente, de forma a manter a integridade dos dados, aplicativos e sistemas operacionais em funcionamento;

A XSITE preparará o ambiente de modo a operar conforme o estabelecido no plano de otimização de recursos, rotinas, procedimentos e processos;

A instalação e configuração da solução será realizada de acordo com o horário de funcionamento da PGE, de segunda à sexta-feira, das 8:30 às 18:00h, em horário e dia a serem combinados entre a PGE e a XSITE;

Será oferecido treinamento hands-on de atualização tecnológica da solução implantada, com o mínimo de 16 (dezesseis) horas, em dias úteis, nas instalações da contratante, para no mínimo 5 (cinco) técnicos da PGE;

O treinamento ou hands-on será iniciado imediatamente após a instalação e configuração das licenças;

O prazo de execução dos serviços de Instalação, Configuração e Treinamento para uso da solução de segurança no parque computacional da PGE deverá ser concluído em no máximo 30 (trinta) dias consecutivos, a contar da data da entrega das licenças;

A XSITE realizará duas avaliações on-site durante o período de vigência do contrato, perante solicitação da contratante, do ambiente da PGE, mediante verificação de instalações e configurações de toda a solução de segurança, adequando-as às melhores práticas, essa atividade deve gerar relatório para posterior melhoria pela equipe da PGE;

Todo suporte será prestado por técnicos certificados pelo fabricante;

Caberá a PGE requisitar o suporte técnico, ficando a XSITE obrigada a realizá-lo, de acordo com o nível de severidade e nos prazos máximos assim definidos no item 2.4;

O suporte técnico será prestado nas seguintes formas:

Plantão Telefônico, Website e E-mail - Serviço de uso ilimitado, no período de 8 (oito) horas por dia, 5 (cinco) dias por semana;

No Local (on site) - Serviço de uso ilimitado, prestado em caso de emergência, ou outra necessidade maior e também compreendendo os seguintes tipos de atendimento local previstos: suporte para upgrade de versões e releases do software; solução de problemas detectados (troubleshoot); análise e

correção de eventos relacionados à segurança e à performance do software e do ambiente; integração dos ambientes da configuração do software na rede da PGE. Neste caso a XSITE possui plantão de 8 (oito) horas por dia, 5 (cinco) dias por semana, para este tipo de atendimento;

Centro de Pesquisas em Informática LTDA – XSITE Consultoria e Tecnologia
Rua Edistio Ponde, 353, Centro Empresarial Tancredo Neves, sl. 807, STIEP, Salvador, BA, 41.770-395
www.xsite.com.br

Para a execução do suporte técnico, a XSITE contará com equipe técnica certificada pelo fabricante e com suporte ilimitado (quantidade de chamados) ao centro de suporte mundial do fabricante a nível internacional, a fim de garantir transferência diretamente ao fabricante dos problemas de maior complexidade que não tenham sido resolvidos em seu próprio laboratório;

O encaminhamento de chamados será efetuado pelos técnicos responsáveis no prazo máximo conforme os níveis de severidade indicados no item 2.4. Após este prazo, em caso de não solução, a XSITE acionará o atendimento, no local designado pela PGE, de acordo com o nível de serviço acordado. O suporte prestado pela empresa terá chamados ilimitados;

O atendimento No Local (on site) será provido na PGE, no seguinte endereço: 3ª Av. Centro Administrativo da Bahia, 370 - CAB, Salvador - BA, 41745-005.

A XSITE responderá aos acionamentos, dentro dos prazos fixados no item 2.4, a partir da abertura do acionamento;

O término do atendimento ocorrerá dentro dos prazos fixados no item 2.4, a partir do contato do técnico da XSITE, responsável pelo atendimento;

Entende-se por início do atendimento a hora do contato do técnico de suporte da XSITE com a equipe da Contratante;

Entende-se por término de atendimento a disponibilidade da Solução de Segurança para uso em perfeitas condições de funcionamento no local onde está instalado;

O nível de severidade será informado pela Contratante no momento da abertura de cada chamado;

O nível de severidade poderá ser reclassificado a critério da Contratante. Caso isso ocorra haverá o início de nova contagem de prazo, conforme o novo nível de severidade;

Todas as solicitações de suporte técnico devem ser registradas pela XSITE, para acompanhamento e controle da execução do serviço;

A XSITE apresentará relatório de atendimento para cada solicitação de suporte, contendo data e hora da solicitação de suporte técnico, do início e do término do atendimento, identificação do problema, providências adotadas e demais informações pertinentes;

O relatório de atendimento será assinado pelo servidor da Contratante que solicitou o suporte técnico;

Para a execução do atendimento, é necessária a autorização da Contratante para instalação ou desinstalação de quaisquer softwares ou equipamentos que não façam parte da solução de segurança fornecida.

Acordo de Nível de Serviço (ANS):

A XSITE possui Central de Atendimento (contato telefônico, sítio na Internet e e-mail) para consultas, aberturas de chamados técnicos e envio de arquivos para análise, durante 8 (oito) horas por dia, 5 (cinco) dias por semana;

A XSITE prestará serviços de suporte técnico 8 horas por dia, 5 dias por semana, na cidade de Salvador (BA), relativos à prestação do serviço objeto deste Termo de Referência, sem ônus para a Contratante;

Para efeito dos atendimentos técnicos, a XSITE observará os níveis de severidade e respectivos prazos máximos fixados abaixo;

Todos os chamados, inclusive os que podem resultar em manutenção de natureza corretiva, bem como o fluxo de resolução de problemas, deverão ser documentados. Esta documentação, bem como outras geradas em processos de atendimento, auditorias, manutenção ou configurações, deverá ser entregue à

CONTRATANTE através de relatórios (impressos ou em mídia digital) mediante solicitação.

A XSITE fará análises dos chamados e enviar recomendações de possíveis treinamentos necessários ao desenvolvimento da equipe da CONTRATANTE.

A XSITE apresentará relatório contendo as ações adotadas para a solução do problema.

Centro de Pesquisas em Informática LTDA – XSITE Consultoria e Tecnologia
Rua Edístio Ponde, 353, Centro Empresarial Tancredo Neves, sl. 807, STIEP, Salvador, BA, 41.770-395
www.xsite.com.br

A XSITE disponibilizará à CONTRATANTE serviço de atendimento de um Gestor do contrato de Suporte, responsável este que será o ponto focal de todas as necessidades de suporte da CONTRATANTE

para casos de escalações ou problemas de atendimento do Suporte Técnico. Caso a XSITE tenha seus laboratórios em outros países que não seja o território nacional, o Gestor deverá ter fluência na língua para facilitar a comunicação entre as partes.

A CONTRATANTE permitirá o acesso dos técnicos credenciados pela XSITE às instalações onde se encontrarem os equipamentos para a prestação dos serviços de manutenção. Entretanto, tais técnicos ficarão sujeitos às normas internas de segurança da CONTRATANTE, notadamente àquelas atinentes à identificação, trânsito e permanência nas dependências;

Mesmo se permitido pela CONTRATANTE, a permanência do técnico além do tempo de resolução do problema, para a continuidade de solução de um problema, não deverá representar qualquer ônus adicional à CONTRATANTE.

Níveis de Serviço e Tempo Esperados:

Plantão Telefônico por número 0800 como serviço de uso ilimitado, no período de 8 (oito) horas por dia, 5 (cinco) dias por semana;

No Local (on site) - Serviço de uso ilimitado, prestado em caso de emergência, ou outra necessidade maior e também compreendendo os seguintes tipos de atendimento local: suporte para upgrade de

versões e releases do software; solução de problemas detectados (troubleshoot); análise e correção de eventos relacionados à segurança e à performance do software e do ambiente; atualização simultânea

nos ambientes dos órgãos e entidades da CONTRATANTE.

Para efeito dos atendimentos técnicos, a XSITE observará os níveis de severidade e respectivos prazos máximos fixados no edital Para o Nível 1, caso o atendimento não seja finalizado até as 20h00min, o técnico não poderá interrompê-lo, devendo continuar até sua finalização, ou a interrupção do mesmo pela Coordenação de Tecnologia da Informação e Comunicação - CTIC. Todo o chamado somente será caracterizado como "encerrado" mediante concordância da Coordenação de Tecnologia da Informação e Comunicação - CTIC;

Para as situações em que a solução definitiva de problemas no ambiente demande reimplantação, reestruturação ou reinstalação da solução, este deverá ser programado e planejado, com a antecedência necessária, de modo a não prejudicar a operação dos demais sistemas da CONTRATANTE.

A XSITE disponibilizará à CONTRATANTE um serviço preventivo de verificação e atualização de versões ou correções (patches) que se fizerem necessários, específicos para a solução ofertada, sem ônus para a CONTRATANTE;

No caso de necessidade de ações preventivas ou corretivas a CONTRATANTE agendará com antecedência junto a XSITE as implementações das correções, fora do horário comercial, preferencialmente em feriados e finais de semana, sem ônus para a CONTRATANTE;

A XSITE prestará suporte a todos os componentes da solução de segurança fornecidos que forem necessários para a implementação e utilização da solução, sem ônus para a CONTRATANTE durante 24 (vinte e quatro) meses.

A XSITE realizará os seguintes suportes proativos:

- Duas avaliações on-site por ano do ambiente da CONTRATANTE, mediante verificação de instalações e configurações de toda a solução, adequando-as às melhores práticas de segurança, essa atividade deve gerar relatório para posterior melhoria pela equipe da CONTRATANTE.
- Uma avaliação on-site por ano do ambiente da CONTRATANTE, mediante verificação de instalações e configurações de toda a solução de gerência centralizada, adequando-as às melhores práticas de segurança, essa atividade deve gerar relatório para posterior melhoria pela equipe da CONTRATANTE.

Centro de Pesquisas em Informática LTDA – XSITE Consultoria e Tecnologia
Rua Edistio Ponde, 353, Centro Empresarial Tancredo Neves, sl. 807, STIEP, Salvador, BA, 41.770-395
www.xsite.com.br

- Quatro visitas técnicas on-site durante o ano de profissionais certificados pelo fabricante para apoiar nas implementações e nos controles gerados pelas ações proativas.

Entrega, Aceite e Instalação

Aceite da solução de segurança será feito pela PGE, após a implantação e entrada em operação das licenças fornecidas;

O aceite das licenças será feito mediante emissão pela "Comissão de Recebimento", nomeada pela PGE, do "Termo de Recebimento e Aceitação";

A entrega e instalação das licenças será feita de acordo com plano de implantação, apresentado pela XSITE e aprovado pela Contratante;

A instalação seguirá cronograma previsto no plano de implantação;

Como parte dos documentos de aceite da solução de segurança fornecida, a XSITE apresentará "Tabela de Comprovação Técnica " das especificações exigidas neste Termo de Referência (apresentar na Tabela a correlação das especificações com a respectiva comprovação técnica, exemplo, página, item, documento etc.). A comprovação técnica deverá ser efetuada através de documentos oficiais referentes a Solução de Segurança fornecido, bem como referente aos módulos complementares.

Da Garantia Técnica

O prazo legal de garantia técnica será de 30 (trinta) dias, tratando-se de fornecimento de serviço não durável, e de 90 (noventa) dias, tratando-se de fornecimento de serviço durável (art. 26, I e II do CDC).

Será acrescido ao prazo da garantia legal, o prazo de licenciamento do software de 24 (vinte e quatro) meses, com suporte técnico de 8 (oito) horas por dia, 5 (cinco) dias por semana, na cidade de Salvador (BA).

A garantia contratual é complementar à legal e será conferida mediante termo escrito (art. 50 do CDC).

A XSITE comprovará, através de atestado/certificado expedido pelo fabricante do objeto desta licitação, ser revenda credenciada.

O termo de garantia ou equivalente deve ser padronizado e esclarecer, de maneira adequada, em que consiste, a forma, o prazo e o lugar em que pode ser exercitada, bem como os ônus a cargo do Contratante, devendo ser entregue devidamente preenchido, pela Contratada, no ato do fornecimento, acompanhada de manual de instrução e, quando for o caso, do manual de instalação e uso do produto, em linguagem didática, com ilustrações (art. 50, parágrafo único, do CDC).

Durante o período de licenciamento o fabricante vai garantir o funcionamento da solução de segurança, com suporte técnico prestado em caso de falha. Será garantida neste prazo a atualização de versões, releases, componentes (bibliotecas, filtros etc.) e módulos da Solução de Seguranças. Todos as soluções deverão ter o mesmo período de licenciamento.

A XSITE demonstrará na declaração formal de disponibilidade (Parte II - Seção III) citada no item d.1 do 1.3 - Qualificação Técnica (Parte II - Seção I) que possui em seu quadro técnico no mínimo um profissional com a certificação técnica do fabricante, apresentando certificado que comprove tal condição, além das comprovações de vínculo deste com a empresa no momento oportuno, nas formas previstas no item d.2 da citada Seção (1.3 - Qualificação Técnica (Parte II - Seção I).

Centro de Pesquisas em Informática LTDA – XSITE Consultoria e Tecnologia
Rua Edistio Ponde, 353, Centro Empresarial Tancredo Neves, sl. 807, STIEP, Salvador, BA, 41.770-395
www.xsite.com.br

Proposta Comercial

Dos Investimentos

ITEM	DESCRIÇÃO / CÓDIGO SIMPAS	Quantidade	PREÇO UNITÁRIO (R$)	PREÇO TOTAL (R$)
01	LICENCA DE USO DE SOFTWARE de Gestão de Vulnerabilidades, Contratação de solução unificada de gestão de vulnerabilidade e conformidade de configurações para Ativos e Aplicações Web, em modelo de subscrição, incluindo instalação, implantação, suporte técnico e treinamento, pelo período de 24 meses – Fabricante: Tenable, marca/modelo: Tenable EP. Código SIMPAS: 02.81.06.00000493-6.	2000	R$ 597,49	R$ 1.194.980,00

O valor total da proposta é de R$ 1.194.980,00 (um milhão, cento e noventa e quatro mil novecentos e oitenta reais).

A validade da proposta é de 60 (sessenta) dias; O prazo de entrega será de até 15 (quinze) dias, contados a partir da assinatura do contrato ou instrumento equivalente;

O prazo de garantia/licenciamento é de 24 (vinte e quatro) meses.

Esta proposta prevê e especifica a transferência de conhecimento à equipe da PGE, de toda solução ofertada com carga horária mínima de 16 horas;

A XSITE, não transferirá a outrem os compromissos assumidos, no todo ou em parte, os serviços.

Local da prestação de serviço: Os serviços serão prestados na Sede da Procuradoria Geral do Estado, situada na 3a Avenida, 370, Centro Administrativo da Bahia, CEP: 41.745-005, Salvador/BA.

A proposta apresentada inclui todas e quaisquer despesas necessárias para o fiel cumprimento do objeto apresentado, inclusive todos os custos com material de consumo, salários, encargos sociais, previdenciários e trabalhistas de todo o pessoal da contratada, como também fardamento, transporte de qualquer natureza, materiais empregados, inclusive ferramentas, utensílios e equipamentos utilizados, depreciação, aluguéis, administração, impostos, taxas, emolumentos e quaisquer outros custos que, direta ou indiretamente, se relacionem com o fiel cumprimento pela contratada das obrigações.

Atenciosamente

João Gualberto Rizzo Araújo
jgra@xsite.com.br
Razão Social: Centro de Pesquisas em Informática LTDA - CNPJ: 40.584.096/0001-05
Tel. (71) 3018-7284 / Cel (71) 98182-5682
Endereço - Salvador: Rua Edístio Pondé, nº 353, sala 807 / 808, 8º andar, Ed. Empresarial Tancredo Neves - CEP: 41.770-395.
Insc. Municipal: 94.249/001-25 | Insc. Estadual: 053.342.364ME
Banco Bradesco, Agência 0592, Conta Corrente: 50.654-0
Nome fantasia: XSITE Consultoria e Tecnologia.

JOAO GUALBERTO RIZZO ARAUJO:50690124520 Assinado de forma digital por JOAO GUALBERTO RIZZO ARAUJO:50690124520 Dados: 2022.07.29 15:20:37 -03'00'

Documento assinado eletronicamente por **João Gualberto Rizzo Araújo**, **Representante Legal da Empresa**, em 25/08/2022, às 15:43, conforme horário oficial de Brasília, com fundamento no art. 13º, Incisos I e II, do Decreto nº 15.805, de 30 de dezembro de 2014.

Documento assinado eletronicamente por **Paulo Moreno Carvalho**, **Procurador Geral do Estado**, em 30/08/2022, às 17:43, conforme horário oficial de Brasília, com fundamento no art. 13º, Incisos I e II, do Decreto nº 15.805, de 30 de dezembro de 2014.

Documento assinado eletronicamente por **Inês Maria Nascimento Santos**, **Analista Procurador Área Ap Adm**, em 31/08/2022, às 09:30, conforme horário oficial de Brasília, com fundamento no art. 13º, Incisos I e II, do Decreto nº 15.805, de 30 de dezembro de 2014.

Documento assinado eletronicamente por **Jucilene Meneses do Sacramento Bispo**, **Assistente de Procuradoria**, em 31/08/2022, às 09:31, conforme horário oficial de Brasília, com fundamento no art. 13º, Incisos I e II, do Decreto nº 15.805, de 30 de dezembro de 2014.

A autenticidade deste documento pode ser conferida no site https://seibahia.ba.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **00052626346** e o código CRC **5E846EED**.

Referência: Processo nº 006.7550.2022.0032203-04 SEI nº 00052626346

SECRETARIA DA EDUCAÇÃO

NOTIFICAÇÃO ADMINISTRATIVA Nº 69/2022
A Comissão Processante Local, instituída pela Portaria nº 1540/2022, de 10 de agosto de 2022, com fulcro no art. 123 da Lei Estadual n° 12.209/11, resolve NOTIFICAR a empresa Delta Locação de Serviços e Empreendimentos Ltda, inscrita sob CNPJ n° 04.370.972/0001-29, para que, no prazo de 30 (trinta) dias, contados a partir da publicação deste ato, efetue o pagamento do valor de R$ 59.756,24 (cinquenta e nove mil setecentos e cinquenta e seis reais e vinte e quatro centavos), respectivo a penalidade de multa imputada no Processo sancionatório SEI nº 011.5558.2019.0063320-22. Advertimos que o prazo para impugnação dos cálculos, relativos ao valor da multa acima indicado, é de 10 (dez) dias, contados a partir da publicação deste ato. Informamos a possibilidade de solicitação de parcelamento da dívida, que deverá ser encaminhada via e-mail ao endereço eletrônico: comissaoprocessante.sec@educacao.ba.gov.br, para apreciação nos termos do art. 50 do Decreto Estadual n° 15.805/14. Salientamos que o não pagamento, no prazo acima referido, importará em inscrição do débito em Divida Ativa Não Tributária - DANT, pela Procuradoria Geral do Estado - PGE, nos termos da Lei Estadual n° 13.446/15. Fica franqueada vistas ao Processo SEI nº 011.5558.2019.0063320-22, mediante solicitação prévia, a qual deverá ser remetida para o endereço eletrônico: comissaoprocessante.sec@educacao.ba.gov.br. Salvador, 29 de agosto de 2022. Lívia Fortuna - Presidente da Comissão Processante Local - SEC

Universidade Estadual de Santa Cruz – UESC

COMUNICADO RECURSO
(Pregão Eletrônico nº 019/2022)
O PREGOEIRO OFICIAL DA UNIVERSIDADE ESTADUAL DE SANTA CRUZ - UESC comunica aos interessados no processo em referência, tendo como objeto a Aquisição de aparelho de Raios X, que por motivo de recurso impetrado pela Sociedade Empresária **LOTUS INDUSTRIA E COMERCIO LTDA.**, contra a decisão do Pregoeiro e Equipe que, com arrimo no parecer técnico declarou vencedora a Sociedade Empresária **VMI TECNOLOGIAS LTDA.**, fica a licitação SUSPENSA, até ulterior deliberação. Ilhéus, 31 de agosto de 2022 - Emanuel F. Neto - Pregoeiro.

SECRETARIA DE INFRAESTRUTURA

JULGAMENTO DE RECURSO - CONCORRÊNCIA Nº 122/2022 - SEINFRA
O Secretário de Infraestrutura do Estado da Bahia - SEINFRA, no uso de suas atribuições, com fundamento no art. 202 da Lei Estadual nº 9.433/2005, decide dar provimento ao recurso interposto pela licitante Prosseguir Construções e Empreendimentos Ltda-EPP, na licitação acima referenciada. Salvador-BA, 31/08/2022. Marcus Cavalcanti/Secretário de Infraestrutura.

SECRETARIA DA SAÚDE

DECISÃO DE RECURSO - TOMADA DE PREÇOS Nº 002/2022 - SECRETARIA DA SAÚDE DO ESTADO DA BAHIA / DIRETORIA DE LICITAÇÃO. A Secretária da Saúde do Estado da Bahia, no uso de suas atribuições, em conformidade com o art. 203 da Lei Estadual n° 9.433/2005, de acordo com o decisum inserido no evento 00053195956 decide "conhecer do recurso interposto pela CONSTRUTORA SANTA RITA LTDA, CNPJ nº 27.529.241/0001-89, recepcionado como direito de petição, haja vista a tempestividade, e quanto ao mérito, JULGAR IMPROCEDENTE", com base na manifestação da Comissão de Licitação do certame constante nos autos do Processo n° 019.5043.2021.0151039-54, na licitação acima referenciada, cujo objeto é a **contratação de empresa para execução das obras de finalização da construção, reforma e ampliação de imóvel para implantação da sede do Núcleo Regional de Brumado - Bahia**. Salvador - BA, 30/08/2022. Adélia Maria Carvalho de Melo Pinheiro. Secretária da Saúde do Estado da Bahia.

CONTRATOS

CASA CIVIL

Empresa Gráfica da Bahia – EGBA

INSTRUMENTO DE ADITAMENTO AO CONTRATO Nº 035/2017

PROCESSO SEI Nº 052.2973.2022.0002792-20. **CONTRATANTE**: Empresa Gráfica da Bahia - EGBA. **CONTRATADA**: Papa-Léguas Serviços de Motoboy Eireli. **OBJETO**: Prorrogação de prazo. **PRAZO**: 06 (seis) meses, a partir de 31 de agosto de 2022. **DATA DA ASSINATURA**: 30/08/2022.

CASA MILITAR

RESUMO DO TERMO ADITIVO n.º 034/2022

PROCESSO: Pregão Eletrônico n.º CMG/017/2021 - **PRIMEIRO TERMO ADITIVO AO CONTRATO** nº CMG/028/2021 - **CONTRATANTE:** Estado da Bahia / Casa Militar do Governador - **CONTRATADA**: **ATA - AEROTÁXI ABAETÉ LTDA**, CNPJ n.º 14.674.451/0001-19 - **OBJETO**: Reequilíbrio econômico-financeiro no percentual de 19,72% (dezenove vírgula setenta e dois por cento) - **VALOR ESTIMADO**: R$ 1.284.553,90 (um milhão, duzentos e oitenta e quatro mil quinhentos e cinquenta e três reais e noventa centavos) - **DOTAÇÃO ORÇAMENTÁRIA**: Atividade: 2116 - Elemento de Despesa: 3.3.90.33.00 - Fonte: 0.100.000000 - **PRAZO DE DURAÇÃO**: a contar de 08/03/2022 - **REGIME DE EXECUÇÃO:** Empreitada por preço unitário - **FORMA DE PAGAMENTO**: Ordem Bancária.

PROCURADORIA GERAL DO ESTADO

RESUMO DE CONTRATO
Processo SEI nº 006.0409.2022.0008208-20
Contrato nº PGE 034/2022 - Pregão Eletrônico 007/2022
Contratante: ESTADO DA BAHIA/PROCURADORIA GERAL DO ESTADO
Contratada: **CENTRO DE PESQUISAS EM INFORMÁTICA LTDA**
Objeto: Fornecimento de licença de uso de Software de Gestão de Vulnerabilidades, objetivando ampliar a segurança da rede e dos ativos da Procuradoria Geral do Estado da Bahia - PGE/BA, com garantia de 24 (vinte e quatro) meses, serviço de instalação, treinamento (Hands on), configuração e suporte on-site, no valor global estimado de R$ 1.194.980,00 (um milhão cento e noventa e quatro mil novecentos e oitenta reais). Unidade Orçamentária - 06.601, Fontes - 300/154, Projeto/Atividade - 5121, Elemento da Despesa - 33.90.40. Prazo: 24 (vinte e quatro) meses, a partir de 30/08/2022. Regime de Execução/Forma de Pagamento: Empreitada por preço unitário.
Setor Responsável pela Gestão Contratual: Coordenação de Gestão Estratégica - CGE.
Gestor: Eduardo Jorge Rodrigues Brandão.
Fiscal: Mauricio de Cerqueira Pereira

SECRETARIA DA ADMINISTRAÇÃO

RESUMO DO CONTRATO Nº 078/2022
Processo SEI nº: 009.0206.2022.0011589-16. **Contratante:** Estado da Bahia, através da Secretaria da Administração. **Contratada**: Marcos Costa Salomão Ltda. **Objeto:** Prestação de serviços técnicos de pessoa jurídica especializada em treinamento para capacitar servidores públicos, na área de regularização do patrimônio imobiliário, com o objetivo de promover e ampliar os conhecimentos práticos e teóricos nesta área. **Valor Total Estimado:** R$ 40.000,00 (quarenta mil reais). **Vigência**: 02 (dois) meses, a contar da data da assinatura do contrato a ser firmado. **Modalidade de Licitação:** Inexigibilidade nº 066/2022. **Unidade Orçamentária:** 09.101; **Unidade Gestora**: 0002, **Ação**: 04.122.502.2000, **Natureza da Despesa**: 3.3.90.39, **Destinação de Recurso**: 0.100.000000. **Assinatura do contrato**: 30.08.2022.

RESUMO DO CONTRATO Nº 072/2022
Processo SEI: 009.1494.2022.0018241-24. **Contratante:** Estado da Bahia, através da Secretaria da Administração. **Contratada**: Creta Comércio e Serviços Ltda. **Objeto:** Prestação de serviços terceirizados de Suporte Administrativo e Operacional a Prédios Públicos. **Valor Mensal Estimado:** 6.724,16 (seis mil, setecentos e vinte e quatro reais e dezesseis centavos). **Vigência**: A partir de 18.08.2022 e término em 02.02.2023. **Modalidade:** Dispensa de Licitação nº 009/2022. **Regime de Execução:** Empreitada por preço unitário. **Forma de Pagamento:** Através de ordem bancária ou crédito em conta corrente. As despesas decorrentes desta contratação correrão por conta das dotações orçamentárias das diversas Unidades Gestoras devidamente consignadas nos Termos de Cooperação firmados com os demais Órgãos participes. **Assinatura**: 17.08.2022.

RESUMO DO CONTRATO Nº 075/2022
Processo SEI: 009.1494.2022.0018241-24. **Contratante:** Estado da Bahia, através da Secretaria da Administração. **Contratada**: Creta Comércio e Serviços Ltda. **Objeto:** Prestação de serviços terceirizados de Suporte Administrativo e Operacional a Prédios Públicos. **Valor Mensal Estimado:** 479.375,01 (quatrocentos e setenta e nove mil trezentos e setenta e cinco reais e um centavo). **Vigência**: A partir de 18.08.2022 e término em 03.03.2023. **Modalidade:** Dispensa de Licitação nº 009/2022. **Regime de Execução:** Empreitada por preço unitário. **Forma de Pagamento:** Através de ordem bancária ou crédito em conta corrente. As despesas decorrentes desta contratação correrão por conta das dotações orçamentárias das diversas Unidades Gestoras devidamente consignadas nos Termos de Cooperação firmados com os demais Órgãos participes. **Assinatura**: 17.08.2022.

RESUMO DO TERMO ADITIVO Nº 01 AO CONTRATO Nº 034/2021
Processo SEI nº: 009.0281.2022.0001739-08. **Contratante:** Estado da Bahia, através da Secretaria da Administração. **Contratada.** Ellu Terceirização Eireli. **Objeto**: Prorrogação do