CONTRATO PGE 024/2021

Modalidade de Licitação	Número
Pregão eletrônico	02/2021

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

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, nº 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, doravante denominado **CONTRATANTE**, e a **CENTRO DE PESQUISA EM INFORMÁTICA LTDA.**, CNPJ nº 40.584.096/0001-05, situada na rua Edístio Pondé, Empresarial Tancredo Neves, 353, salas 807 e 808, STIEP, Salvador/BA, neste ato representada pelo **SR. JOÃO GUALBERTO RIZZO ARAUJO**, portador da cédula de identidade nº 03.688.884-28, emitida por SSP-BA, inscrito no CPF/MF sob o nº 506.901.245-20, adjudicatária do pregão nº 02/2021, processo administrativo nº 006.0409.2021.0007522-03, 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 prestação de serviços de Solução de Endpoint Visibility Access Security - EVAS, doravante denominada Solução de EVAS, contemplando licença de uso com manutenção e suporte técnico de softwares à sua operacionalização, visando garantir o controle, políticas de conformidade, a visibilidade e a segurança no acesso à rede da Procuradoria Geral do Estado da Bahia – PGE/BA 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. **[NOTA: subcontratação vedada]**

[SERVIÇOS NÃO-CONTÍNUOS]

CLÁUSULA SEGUNDA – PRAZO

O prazo de vigência do contrato, a contar da data da sua assinatura, será de 36 (trinta e seis) 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:

ITEM	Código SIMPAS	Descrição	Unidade de Fornecimento (UF)	Quantitativo	PREÇO UNITÁRIO	PREÇO TOTAL
1	02.24.13.00001974-7	Fornecimento, instalação e configuração de Licenca de software do fabricante: Forescout, marca/modelo ForeScout CounterACT See + Control License for 100 endpoints + ActiveCare Basic 3 years - ForeScout CounterACT See + Control for 100 endpoints + ForeScout Open Integration Module, license for 100 endpoints + ActiveCare Basic 3 years - ForeScout Open Integration Module for 100 endpoints, com os respectivos Part Number's: o 10 x FS-LICSEECONTROL-100 o 10 x FS-AC-BSEECONTROL-100-3 o 10 x FS-LIC-MOD-OIM-100 o 10 x FS-AC-B-MOD-OIM100-3 A solução será fornecida para até 1.000 (um mil) dispositivos de acesso, em unidades mínimas de 100 (cem) dispositivos.	100 Devices	10	R$ 32.500,00	R$ 325.000,00
				VALOR ESTIMADO GLOBAL		R$ 325.000,00

§1º Estima-se para o contrato o valor global de R$ 325.000,00 (trezentos e vinte e cinco mil 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
06.601	03	126	315	5121
Região/planejamento	Natureza da despesa	Destinação do recurso	Tipo de recurso orçamentário	
7800	33.90.40	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:

[SERVIÇOS EM GERAL]

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.

§1º. 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.

§2º A contratada deverá apresentar documentação técnica nos termos a seguir.

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

- Documentação das Funcionalidades: Este documento conterá as características técnicas do produto e suas funções, procedimentos e parâmetros de configuração, tabelas, ilustrações etc.;
- 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.

II. A Contratada deverá apresentar juntamente com a documentação dos produtos, certificado ou título, concedido pelo fabricante, que comprove o credenciamento da Contratada como representante autorizada;

III. A Contratada deverá apresentar juntamente com a documentação do produto, as licenças dos produtos fornecidos necessários para a implantação;

IV. A documentação dos produtos abrange: manuais operacionais dos produtos, documento com as especificações técnicas dos produtos e seus recursos, as licenças dos produtos, mídias contendo os produtos para instalação fornecidos e toda documentação acessórias relativas aos produtos fornecidos.

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 a 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:

[AQUISIÇÕES OU SERVIÇOS (EXCETO ENGENHARIA)]

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.

§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

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

§1º A Contratada concorda que os direitos patrimoniais autorais relativos aos resultados produzidos durante a vigência do Contrato são de propriedade exclusiva da Contratante, devidamente amparada pela Lei nº 9.610/1998, de Diretos Autorais, respeitados os direitos morais do autor.

§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 licitatório, 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 12.290, 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.

ANEXO I

SEÇÃO SEÇÃO II

TERMO DE REFERÊNCIA DO OBJETO DA LICITAÇÃO

1. Descritivo: A presente licitação tem por objeto a contratação de empresa para prestação de serviços de Solução de Endpoint Visibility Access Security – EVAS, doravante denominada Solução de EVAS, contemplando licença de uso com manutenção e suporte técnico de softwares necessários à sua operacionalização, visando garantir o controle, políticas de conformidade, a visibilidade e a segurança no acesso à rede da Procuradoria Geral do Estado da Bahia – PGE/BA, conforme características, quantitativos, condições e especificações disciplinadas nesta Seção.

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

LOTE ÚNICO – AMPLA PARTICIPAÇÃO				
ITEM	**Descrição**	**Unidade de Fornecimento (UF)**	**Quantitativo**	**Cronograma/Prazo**
1	INSTALAÇÃO E CONFIGURAÇÃO de *software ForeScout* EVAS - *CounterACT*. Deve ser realizado por profissional certificado pelo fabricante do produto. Descrição complementar: Conforme item 3.3 do Termo de Referência **ATENÇÃO! A solução deve ser fornecida para até 1.000 (um mil) dispositivos de acesso, em unidades mínimas de 100 (cem) dispositivos.** Código SIMPAS: 02.24.13.00001974-7 **Descrição completa vide anexo deste Termo de Referência, constante do anexo da Seção II, Parte I.**	**UN**	**10**	Prazo de entrega: até 30 (trinta) dias, contados a partir da assinatura do contrato ou instrumento equivalente; Período do licenciamento: 36 (trinta e seis) 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 A contratação visa atender às necessidades da CONTRATANTE para suporte técnico da Solução de EVAS, com o objetivo de proteger a rede corporativa (Controle de Acesso à Rede) além de aumentar o nível de conformidade, segurança e visibilidade

2.2.2 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;

2.2.3 O produto deverá estar licenciado em nome da Procuradoria Geral do Estado da Bahia - PGE, sendo que o suporte, a manutenção e suas atualizações (upgrade e update) deverão ocorrer sem ônus para este Órgão;

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

2.2.5 Treinamento Hands on de atualização tecnológica da solução para pelo menos 02 (dois) técnicos nas instalações da Contratante;

2.2.6 Suporte técnico ao produto fornecido em língua portuguesa.

2.3 Suporte Técnico:

2.3.1 O suporte técnico ao produto fornecido deverá ser prestado 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;

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

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

2.3.4 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;

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

2.3.6 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 7 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;

2.3.8 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 2 (dois) técnicos da PGE;

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

2.3.10 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;

2.3.11 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;

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

2.3.13 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 5.4

2.3.14 O suporte técnico deverá ser prestado nas seguintes formas:

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

2.3.14.2 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;

2.3.14.3 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;

2.3.14.4 O encaminhamento de chamados deverá ser efetuado pelos técnicos responsáveis no prazo máximo conforme os níveis de severidade indicados no item 5.4. 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;

2.3.14.5 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

2.3.14.6 A Contratada deverá responder aos acionamentos, dentro dos prazos fixados no item 5.4, a partir da abertura do acionamento;

2.3.14.7 O término do atendimento deverá ocorrer dentro dos prazos fixados no item 5.4, a partir do contato do técnico da Contratada, responsável pelo atendimento;

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

2.3.14.9 Entende-se por término de atendimento a disponibilidade do produto para uso em perfeitas condições de funcionamento no local onde está instalado;

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

2.3.14.11 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;

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

2.3.14.13 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;

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

2.3.14.15 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.

2.3.15 Equipe Técnica: Composta de técnicos certificados pelo fabricante do software fornecido, e preparada para dar todo o suporte técnico e ajuda necessária para maximizar os benefícios oferecidos pelo software, aumentando a sua performance.

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 a 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:

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

2.4.10.2 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: 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.

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

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

2.4.10.4 -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 e Gestão da Informação. Todo o chamado somente será caracterizado como “encerrado” mediante concordância da Coordenador de Tecnologia da

Informação e Comunicação - CTIC;

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

2.4.12 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;

2.4.13 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;

2.4.14 A CONTRATADA deverá prestar suporte a todos os componentes de software fornecidos que forem necessários para a implementação e utilização da solução, sem ônus para a CONTRATANTE durante 36 (trinta e seis) meses.

2.4.15 A contratada deverá ainda realizar os seguintes suportes proativos:

2.4.15.1 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.

2.4.15.2 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.

2.4.15.3 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 VERIFICAÇAÕ 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 do software 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 do software, 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 do software fornecido;

2.5.4 O relatório gerado em função dos Testes de Verificação Preliminar será documento integrante do Termo de Recebimento e Aceitação do software fornecido.

2.6 ENTREGA, ACEITE E INSTALAÇÃO

2.6.1 O aceite do software será feito pela PGE, após a implantação e entrada em operação das licenças fornecido;

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 do software fornecido, 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 ao produto 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 do produto 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 dos produtos, 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 do produto, as licenças dos produtos fornecidos necessários para a implantação;

2.7.4 A documentação dos produtos abrange: manuais operacionais dos produtos, documento com as especificações técnicas dos produtos e seus recursos, as licenças dos produtos, mídias contendo os produtos para instalação fornecidos e toda documentação acessórias relativas aos produtos fornecidos.

3 Especificações

3.1 Garantia Técnica

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 36 (trinta e seis) meses com suporte técnico de 08 (oito) horas por dia, 05 (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).

3.2 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 do equipamento e software, com suporte técnico prestado em caso de falha. Deverá ser garantida neste prazo a atualização de versões, releases, componentes (bibliotecas, filtros etc.) e módulos dos produtos. Todos os produtos deverão ter o mesmo período de licenciamento

4. Responsável pelas informações constantes do termo de referência:	
Servidor responsável:	Eduardo Jorge Brandão
Lotação:	Coordenação de Gestão Estratégica

ANEXO I DO TERMO DE REFERÊNCIA – ESPECIFICAÇÕES TÉCNICAS

Solução de Visibilidade, Gestão de Acesso à Rede, Segurança e Conformidade de Dispositivos Conectados (EVAS – Endpoint Visibility, Access and Security)

3.1 A solução deverá ser fornecida conforme necessidade da CONTRATANTE, em unidade mínima de gerenciamento de 100 dispositivos. O fornecimento deve contemplar o gerenciamento central de múltiplos appliances virtuais, bem como integração com soluções de terceiros a partir de protocolos abertos, tais como SQL, LDAP e Web Services, conforme especificações;

3. 2 As licenças poderão ser distribuídas em múltiplos appliances virtuais, gerenciados centralmente, em unidades de 100 licenças, conforme a necessidade do CONTRATANTE. Não deverá haver limitação no número de appliances virtuais gerenciados;
3. 3 A solução deverá ser fornecida para até 1.000 (um mil) dispositivos de acesso, em unidades mínimas de 100 dispositivos;
3. 4 A solução dever ser fornecida na modalidade de licenciamento perpétuo sem prejuízo de nenhuma das funcionalidades existentes ao final do período de suporte e atualizações;
3. 5 NA solução ofertada deverá atender às seguintes características técnicas:
3. 6 A solução deverá ser fornecida em formato de appliance virtual compatível com o VMware ESXi v6.0 ou superior, Microsoft HyperV Server 2012, 2012 R2, 2016 e KVM on Red Hat Enterprise Linux (RHEL)/CentOS 7;
3. 7 Deve monitorar todo o tráfego da rede através de uma porta espelhada no switch core (porta SPAN);
3. 8 Deve realizar todas as suas funções sem a utilização de agentes (AGENTLESS) instalados nas máquinas corporativas (estações de trabalho, servidores, dispositivos móveis, dentre outros);
3. 9Deve criar e manter atualizada, em tempo real, a lista de todos os elementos da rede, incluindo equipamentos de rede, impressoras, dispositivos de usuários finais, servidores, sistemas operacionais, aplicações, processos, portas abertas, dispositivos periféricos, vulnerabilidades e usuários, permitindo o agrupamento automático baseado em condições, e a aplicação automática de ações de controle de acesso, garantia de conformidade (remediação) e orquestração de segurança;
3. 10 Deve ser capaz de classificar automaticamente impressoras, dispositivos de rede, máquinas Windows, Linux e Macintosh, Dispositivos Móveis e dispositivos que estejam realizando tradução de endereços (NAT);
3. 11 Deve ser capaz de diferenciar máquinas corporativas de máquinas não corporativas;
3. 12 Deve ser capaz de classificar os dispositivos de IT (Information Technology) e OT (Operational Technology) por função em subcategorias, no mínimo:

- IT: Computador, Mobile, Networking, Storage, Acessórios (ex: impressoras);
- OT: Sistema de Aquisição de Dados, Monitoramento Ambiental, Sistema de Controle Industrial, Segurança Física (ex: Câmeras IP), Monitoramento e Controle Remoto, Saúde.
    3. 13 Deve ser capaz de classificar dispositivos por sistema operacional contendo, no mínimo as seguintes categorias: Alcatel-Lucent, Android, Avaya, Chrome OS, Cisco IOS, Cisco ASA-OS, Cisco Access Points, ExtremeXOS, FortiOS, Huawei VRP, iOS, LG Web OS, Linux, Macintosh, UNIX, Windows;
    3. 14 Deve ser capaz de classificar dispositivos por fabricante e modelo para dispositivos IoT (Internet of Things), tais como wearables e dispositivos móveis, e OT (Operational Technology), tais como sistemas de controle industrial;
    3. 15 Deve ser capaz de realizar a classificação passiva de dispositivos para que a classificação seja realizada sem contato ativo direto com o dispositivo (ex: para dispositivos que controlam processos operacionais de tempo real);
    3. 16 Deve ser capaz de criar inventário das informações da rede e dos dispositivos catalogando, pelo menos, sistemas operacionais e respectivas versões, máquinas e respectivas versões dos sistemas operacionais Windows, Linux e Mac, processos em execução (Windows, Linux e Mac), portas de comunicação abertas nos dispositivos, aplicações instaladas em Windows, dispositivos externos conectados, usuários registrados como visitantes, dentre outras;
    3. 17 Deve permitir o controle de acesso à rede baseado em perfis e regras de conformidade;
    3. 18 Deve prover funções de visibilidade e controle para ambientes de nuvem nas seguintes plataformas: AWS, Azure, VMWare vCenter, VMWare NSX e VMWare vSphere;
    3. 19 Deve possuir autenticação de usuários com LDAP, RADIUS, Active Directory e 802.1x, possuindo, ainda, um servidor RADIUS e RADIUS Proxy integrado para facilitar o deployment baseado em 802.1x;
    3. 20 Deve suportar segurança 802.1x pre-connect e controle 802.1x post-connect tanto para rede cabeada como rede sem fio tanto de usuários corporativos como visitantes.
    3. 21 Deve suportar RADIUS authentication, authorization e accounting;
    3. 22 Deve possuir catálogo de MAC Addresses para suportar Mac Address Bypass para dispositivos que não suportam 802.1x;
    3. 23 Deve permitir que a autenticação 802.1x seja realizada através de servidor Microsoft Active Directory e servidor RADIUS externo (RADIUS Proxy);
    3. 24 Deve ser capaz de atribuir labels aos dispositivos baseados em listas de MAC Addresses mantidos em servidores FTP ou LDAP;
    3. 25 Deve permitir a automação do registro de convidados, tanto na rede cabeada como na rede sem fio, através de captive portal, sem necessidade de configuração/reconfiguração de equipamentos de acesso (switches);
    3. 26 Deve identificar automaticamente os servidores de DNS da rede;
    3. 27 Deve garantir a conformidade das configurações das máquinas corporativas (estações de trabalho, servidores, dispositivos móveis, dentre outros) com as políticas de segurança da organização, incluindo controle das soluções baseadas

em agentes, tais como antivírus, patches de sistema operacional e bloqueio de software não-autorizado;

3. 28 Deve realizar a detecção de ameaças baseada em análise do comportamento dos dispositivos (pós-admissão) não baseada em assinaturas (ex: Port Scan (TCP/UDP), Ping Sweep Scan, SNMP Scan, User Scan, Tentativa de Infecção via rede) e permitir o monitoramento e bloqueio do dispositivo;
3. 29 Deve detectar dispositivos não-autorizados, tais como switches e access points (APs), identificando ainda se é um dispositivo que realiza tradução de endereços (NAT) e se está ou não autorizado a utilizar a rede;
3. 30 Deve detectar portas de switches com múltiplos hosts conectados;
3. 31 Deve detectar dispositivos sem endereço IP (tais como stealthy packet capture devices projetados para furto de informações) e executar ações de bloqueio de porta do switch e mudança de VLAN;
3. 32 Deve controlar os dispositivos móveis conectados à rede em tempo real;
3. 33 Deve possuir inventário e controle da rede em tempo real, permitindo rastrear e controlar usuários, aplicações, processos, portas e dispositivos externos;
3. 34 Deve ser capaz de definir segmentos de rede baseados em endereços IP e filtrar os dados apresentados baseados em segmentos;
3. 35 Deve permitir a criação de subsegmentos para diferenciar os setores e poder aplicar as políticas em diferentes segmentos;
3. 36 Deve ser capaz de definir unidades organizacionais baseadas em segmentos de rede e filtrar os dados baseados em unidades organizacionais;
3. 37 Deve ser capaz de realizar avaliação de postura de segurança de dispositivos IoT (Internet of Things) através da avaliação do uso de credenciais (SNMP, SSH e Telnet):

- Padrão/Default de fábrica;
- Base do fabricante de credenciais fracas/comuns;
- Credenciais fornecidas manualmente pelo administrador.

3. 38 Deve possuir módulo de relatórios e dashboard para monitoramento do nível de conformidade (compliance);
3. 39 Deve possuir mecanismo para scanear máquinas Windows em busca de IOC's (Indicators of Compromise) e executar ações em resposta à identificação de máquinas comprometidas;
3. 40 Cada IoC deverá poder ser composto, pelo menos, dos seguintes atributos: Nome da Ameaça, Nome do Arquivo, Tamanho do Arquivo, Hash do Arquivo, Tipo de Função Hash Utilizada, Severidade, Endereço de Central de Comando & Controle (CnC);
3. 41 Deve possuir mecanismo automático de remoção de IoC's da base de dados da solução de acordo com a severidade e tempo de existência do IoC.
3. 42 Deve permitir a automação e orquestração de soluções de terceiros a partir de eventos detectados pela solução, utilizando-se das capacidades de integração em ações definidas nas políticas da solução.
3. 43 As ações devem poder ser encadeadas através de agendamento da sua execução permitindo a orquestração de resposta a incidentes através de comunicação com soluções de terceiros via protocolos abertos (LDAP, SQL e Web Services);
3. 44 Deve ser capaz de detectar novos dispositivos de rede a partir de traps SNMP v1, v2c e v3 enviados pelos switches;
3. 45 Deve ser capaz de executar ações e consultar informações em switches de diversos fabricantes e switches genéricos através de protocolo SNMP;
3. 46 Deve suportar SNMP v1, v2c e v3 para permitir o monitoramento do appliance através de sistemas externos de monitoramento de rede;
3. 47 Deve ser capaz de enviar traps SNMP para sistemas de monitoramento de rede quando ocorrerem modificações de configuração e quando os limites de utilização do sistema forem ultrapassados (ex: número de dispositivos gerenciados, utilização de CPU, utilização de memória, perda de pacotes etc.);
3. 48 Deve ser capaz de enviar e receber mensagens via SYSLOG;
3. 49 Deve ser capaz de usar informações do tráfego DHCP para classificar os dispositivos sem a necessidade de utilização de IP Helper Address para redirecionamento das requisições DHCP;
3. 50 Deve ser capaz de analisar o tráfego de rede e calcular estatísticas como tamanho médio de pacote, número médio de pacotes por segundo e resoluções de nomes via DNS;
3. 51 Deve ser capaz de receber e processar informações de Flow (NetFlow v9, IPFIX e sFlow) para identificação de dispositivos e propriedades de dispositivos;
3. 52 Deve ser capaz de identificar, aplicar políticas, manter a segurança e garantir a conformidade de dispositivos na nuvem pública da Amazon – AWS, inclusive identificando e controlando instâncias Elastic Compute Cloud (EC2), usuários Identity and Access Management (IAM) e Virtual Private Clouds (VPCs), permitindo:
3. 53 Ver instâncias EC2, usuários IAM e VPCs;
3. 54 Criar e aplicar políticas nestas entidades AWS;
3. 55 Manter a segurança e conformidade das instâncias de nuvem, usuários IAM e VPCs.
3. 56 Deve ser capaz de identificar, aplicar políticas, manter a segurança e garantir a conformidade de dispositivos na nuvem pública da Microsoft – Azure, inclusive identificando e controlando instâncias de Virtual Machines (VM) e Virtual Networks (VNET), permitindo:

- Ver instâncias VM e redes VNETs;
- Criar e aplicar políticas nestas entidades Azure;
- Manter a segurança e conformidade das instâncias de VM's e VNET's.

3. 57 Deve suportar a descoberta e gerenciamento de dispositivos em máquinas virtuais VMWare vSphere;
3. 58 Deve ser capaz de aplicar funcionalidades de controle em máquinas virtuais de ambientes VMWare vCenter;
3. 59 Deve ser capaz de aplicar micro-segmentação em máquinas virtuais de ambientes VMWare NSX;
3. 60 Deve ser capaz de identificar dispositivos e servidores configurados com o uso de credenciais comuns da empresa e que devem ser considerados inseguros;
3. 61 Deve possuir trilha de auditoria acessível pela interface gráfica que registre todas as operações de modificação nas configurações da solução (adições, edições e remoções).
3. 62 A solução ofertada deverá possuir os seguintes atributos e propriedades:
3. 63 Deve ser capaz de identificar atributos e propriedades dos dispositivos para permitir a criação de políticas baseadas em condições, no mínimo:
3. 64 Autenticação: Identificar autenticação via HTTP(80/TCP), Telnet(23/TCP), NetBIOS(139/TCP), FTP(21/TCP) IMAP (143/TCP), POP3(110/TCP), rlogin(513/TCP) e Active Directory;
3. 65 Dispositivo: banners de serviço, endereço IP, nome DNS, se está realizando NAT, usuário logado, interfaces de rede, resultados de scripts, portas abertas, número de endereços IPv4 e IPv6, NIC Vendor, NetBIOS Hostname, NetBIOS Domain, qualquer atributo SNMP do dispositivo, resultado de comando via SSH;
3. 66 Usuário: nome, status da autenticação e grupo de trabalho;
3. 67 Windows Active Directory: conta desabilitada, conta expirada, Display Name, Member Of, Email, Initials etc.
3. 68 Sistema Operacional (Windows/Linux/Mac): tipo e versão do SO; processos em execução; existência, data e tamanho de arquivos; resultado de execução de scripts, usuário logado;
3. 69 Detalhes de Máquinas Windows: domínio, último evento de login, existência e valores de chaves de registro, serviços instalados, serviços em execução, vulnerabilidades, dispositivos externos;
3. 70 Detalhes de máquinas virtuais: Health Status de máquinas Guest VMWARE e tipo de instância Amazon EC2;

3. 71 Segurança: agente de antivírus instalado, nível de atualização e status de firewall, IoC's (Indicators of Compromise), ARP Spoofing, sessões abertas como cliente, sessões abertas como servidor, traps SNMP recebidas da porta onde o dispositivo está conectado;
3. 72 Aplicações Windows: aplicações instaladas, incluindo versão, aplicações de Cloud Storage, Instant Messaging, Criptografia de Disco e Peer to Peer instaladas e em execução; Periféricos: tipo do dispositivo, fabricante e tipo de conexão;
3. 73 Rede: segmento de rede, switch e porta ao qual o dispositivo está conectado, VLAN.
3. 74 Deve ser capaz de criar novas propriedades/atributos para os dispositivos usando o resultado de scripts executados nos dispositivos (ex: quantidade de instâncias de um determinado processo em execução em servidores Linux);
3. 75 Deve ser capaz de criar novas propriedades/atributos para os dispositivos baseado em valores consultados em bases de dados externas via SQL, Web Services e LDAP.
3. 76 Deve ser capaz de criar novas propriedades baseado na comparação entre propriedades já existentes;
3. 77 Deve ser possível criar listas de valores de propriedades para serem usadas como operandos em regras de políticas (Ex: Listas de Endereços IP, Listas de Nomes de Máquinas, Listas de Processos etc.);
3. 78 Deve ser possível detectar mudanças de valores em propriedades tais como: Aplicações Windows Instaladas e/ou Removidas, Novas Interfaces de Rede, Mudança de Data, Tamanho e Versão de Arquivos Windows, Criação/Remoção de Arquivos Windows, Mudança de Endereço IP, Mudança de Nome no DNS, Alterações no Windows Registry, Mudança de Porta no Switch, dentre outras, e utilizá-las como condições nas regras das políticas para execução de ações;
3. 79 Deve ser possível utilizar atributos e propriedades para organizar os dispositivos em grupos, de forma a permitir melhor controle sobre a aplicação de políticas.

Ações

3.79.1 Deve ser possível definir os seguintes tipos de ações automáticas nas políticas:

3.79.2 Restringir o acesso através de modificação de VLAN, desabilitar porta de switch e TCP Resets (Firewall Virtual);

3.79.3 As ações de Firewall Virtual (TCP Resets) devem poder ser realizadas no tráfego originado pelo dispositivo e no tráfego destinado ao dispositivo;

3.79.4 Bloquear acesso de e para hosts e portas específicas;

3.79.5 Deve ser possível especificar o segmento de rede/faixa de IP e portas que estão impedidos de se comunicar com o dispositivo bloqueado;

3.79.6 Deve ser possível criar exceções à regra para permitir o acesso de administradores ao dispositivo.

3. 80 Notificar o usuário através de redirecionamento de tráfego HTTP inclusive em ambientes que utilizam Web Proxy;
3. 81 Deve ser possível redirecionar o tráfego para qualquer URL definida pelo administrador;
3. 82 Deve ser possível criar exceções para impedir o redirecionamento de tráfego direcionado a URL's específicas;
3. 83 Deve ser possível criar exceções para impedir o redirecionamento de tráfego para segmentos de rede e faixas de IP específicas.
3. 84 Redirecionar tráfego usando HTTPS;
3. 85 Bloquear tráfego HTTPS passando através de servidor Proxy;
3. 86 Permitir redirecionar os usuários para páginas de autenticação e de ações de remediação;
3. 87 Permitir definir exceções para URL's específicas;
3. 88 Registrar convidados através de formulário de registro (captive portal) para máquinas não corporativas (terceiros, visitantes, BYOD), tanto para acessos via rede cabeada como rede sem fio, sem necessidade de configuração/reconfiguração de equipamentos de acesso (ex: switches), com as seguintes capacidades:
3. 89 Permitir definir a validade de tempo de acesso do usuário;
3. 90 Capacidade de definir diversos tipos de convidados com privilégios diferenciados;
3. 91 Atribuir limitações de rede de acordo com o usuário;
3. 92 Formulário de auto registro com acesso automático, sem necessidade de aprovação;
3. 93 Formulário de auto registro com envio de códigos de verificação via e-mail para permitir o acesso (one time password);
3. 94 Formulário de auto registro com aprovação de acesso por "sponsor" devidamente autorizado;
3. 95 Controlar o acesso do convidado até que o seu acesso seja aprovado pelo "sponsor" indicado;
3. 96 Possuir Dissovable Agent para levantamento de informações e aplicação de políticas de conformidade em máquinas não-corporativas, sem necessidade de permissões de administrador para execução e sem processo de instalação, não deixando nenhum rastro após o reboot.
3. 97 Redirecionamento de tráfego via DNS (DNS Enforcement);
3. 98 Comunicação: enviar e-mail de alertas aos usuários e administradores, notificar de usuário através de redirecionamento HTTP, enviar traps SMP, envio de registros para SYSLOG.
3. 99 Remediação de sistema operacional Windows: instalar patch de sistema operacional; criar e modificar chaves de registro; iniciar agente de segurança e atualizar assinaturas; desabilitar dispositivo externo, encerrar processos de Cloud Storage, P2P e IM;
3. 100 Iniciar e encerrar processos e scripts em Windows, Linux e Mac;
3. 101 Executar scripts no dispositivo com passagem de parâmetros para o script com valores dos atributos disponíveis sobre o dispositivo;
3. 102 Deve ser possível executar scripts como "root" em dispositivos Linux usando "sudo".
3. 103 Executar scripts no servidor da solução com passagem de parâmetros para o script com valores de atributos disponíveis do dispositivo;
3. 104 Bloquear tráfego malicioso e colocar em quarentena dispositivo malicioso.
3. 105 Atribuir dispositivos a grupos para utilização como critério de filtragem em políticas;
3. 106 Enviar comandos para soluções de terceiros, através de protocolo aberto (SQL, LDAP e Web Services).
3. 107 Iniciar atualizações de segurança do Windows, via Microsoft Web site ou WSUS;
3. 108 Deve permitir escolher um dos três métodos de atualização disponíveis na plataforma: Download e Instalação Automáticas, Download Automático e Notificação do Usuário, Usando as Configurações de "Automatic Update" do Dispositivo.
3. 109 Deve possuir um assistente, via WEB, que permita aos próprios usuários aplicarem ações de remediação de vulnerabilidades do sistema operacional Windows que tenham sido detectadas no dispositivo;
3. 110 Todas as ações executadas sobre um dispositivo devem ser registradas (log) nas informações detalhadas do dispositivo;

Políticas

3. 111 As políticas devem ser compostas por regras de condição e execução de ações em um escopo específico;
3. 112 Deve permitir a limitação de escopo de aplicação da política baseado em faixas de endereço IP, segmentos de rede e grupos de dispositivos.
3. 113 Deve permitir criar exceções para escopo de políticas baseado em endereço IP, MAC Address, NetBIOS Hostname; Username e grupos de dispositivos;
3. 114 As regras de cada política devem ser criadas com base em condições lógicas (AND,

OR, NOT) sobre quaisquer propriedades/atributos e informações levantadas sobre cada dispositivo;

3. 115 Deve ser possível definir se o resultado da avaliação de uma condição será verdadeiro ou falso em caso de ausência de informações sobre a propriedade/atributo que está sendo avaliado;
3. 116 Cada regra deve suportar a execução de múltiplas ações e o agendamento das mesmas para permitir flexibilidade na implementação de ações de controle de acesso, remediação e orquestração de segurança.
3. 117 O agendamento de ações deve suportar pelo menos as seguintes opções:

3.117.1 Imediatamente;

3.117.2 Após um intervalo de tempo definido pelo administrador;

3.117.3 Data e hora específica.

3. Deve ser possível estabelecer a duração da aplicação das ações com as seguintes opções:

3.118.1 Sem data final;

3.118.2 Após um intervalo de tempo definido pelo administrador;

3.118.3 Data e hora específica.

3. 119 Deve ser possível atribuir labels aos dispositivos e criar contadores para implementar lógicas de políticas complexas, capazes de reter o estado do dispositivo durante os processos de reverificação das condições lógicas.
3. 120 Deve permitir a criação de um catálogo de condições customizadas para serem reutilizadas em regras de diferentes políticas;
3. 121 Deve ser possível definir novas propriedades do dispositivo baseado na comparação ente outras propriedades já existentes;
3. 122 As políticas criadas pelo administrador deverão permitir estabelecer condições de classificação e conformidade (compliance) de dispositivos, bem como definir ações automáticas de remediação, tais como:
3. 123 Identificar hosts e colocar em quarentena quando não houver o software de antivírus instalado ou não estiver com os patches de sistema atualizados;
3. 124 Limitar acesso à rede para convidados;
3. 125 Ativar detecção automática para hosts que estão faltando service pack e integrar com ferramenta de correção (WSUS);
3. 126 Verificar todos os servidores que não estão em conformidade (compliance) com as políticas;
3. 127 Automaticamente deverá descobrir e colocar em quarentena os access points (APs) wireless desconhecidos.
3. 128 Deve possuir capacidade de atualizar bases de dados externas via comandos SQL parametrizados com dados dos dispositivos disponíveis na solução;
3. 129 Deve ser capaz de executar comandos em soluções de terceiros através de chamadas de Web Services parametrizados com dados dos dispositivos disponíveis na solução.
3. 130 Deve possuir capacidade de buscar informações em soluções de terceiros, através de LDAP, SQL e Web Services, para aplicação de políticas de segurança, controle de acesso e conformidade de dispositivos.
3. 131 Deve possibilitar a importação e exportação de políticas;
3. 132 Deve fornecer as informações sobre os dispositivos em tempo real;
3. 133 Deve possuir templates de políticas pré-definidas e assistente gráfico para permitir a criação rápida de políticas padrão.
3. 134 Deve permitir detectar usuários e dispositivos que estão fora de conformidade com a política de segurança, informando na console a razão da não-conformidade e detalhes completos do usuário/dispositivo, permitindo ainda a aplicação de ações automáticas de remediação;
3. 135 Deve executar envio de alertas, restrições de acesso e ações de remediação automáticas, incluindo:
3. 136 Atribuição de um dispositivo a VLANs específicas para controle de acesso;
3. 137 Migração do dispositivo automaticamente para rede de convidados;
3. 138 Migração de um dispositivo da rede de produção para uma rede de quarentena;
3. 139 Finalização de aplicações não-autorizadas nas estações de trabalho e servidores corporativos.

Inventário em Tempo Real

3. 140 Deve possuir inventário de usuários, dispositivos, software, hardware e rede com, no mínimo, as seguintes categorias:
3. 141 Inventário de usuários da rede;
3. 142 Inventário de convidados registrados incluindo status da aprovação de acesso, identificação do aprovador e da pessoa de contato indicada durante o processo de registro;
3. 143 Inventário de portas de comunicação abertas associadas aos respectivos dispositivos;
3. 144 Inventário de vulnerabilidades Microsoft associadas aos respectivos dispositivos;
3. 145 Inventário de Hardware de máquinas Windows contendo:
3. 146 Informações gerais do equipamento: número de processadores, total de memória física, fabricante, modelo, time zone;
3. 147 Discos: tipo do drive, nome do volume, tamanho, espaço disponível;
3. 148 Monitores: tipo e fabricante;
3. 149 Placa mãe: fabricante e modelo;
3. 150 Adaptadores de rede: índice, endereço MAC, endereço IP, Subrede IP e default gateway;
3. 151 Memória física: capacidade, tipo, velocidade e fabricante;
3. 152 Dispositivos Plug-and-Play: Class GUID, Device ID e fabricante;
3. 153 Processador: fabricante, arquitetura, família, max clock speed, número de cores, percentual de carga e status.
3. 154 Inventário de dispositivos externos conectados em máquinas Windows (wireless, impressoras, adaptadores de rede, modems, dispositivos de imagem, dirves de disco externo, DVD/CDROM, bluetooth);
3. 155 Inventário de aplicações instaladas em ambientes Windows e Mac;
3. 156 Inventário de switches com informação de número de dispositivos conectados por porta.
3. 157 Deve permitir integrar-se com bases de dados e soluções externas para atualização imediata de informações de inventário de dispositivos existentes e de novos dispositivos que se conectarem à rede usando SQL e Web Services.
3. 158 Deve permitir a criação de listas baseadas no inventário, tais como listas de aplicações autorizadas e não-autorizadas.

Console de Gerenciamento

3. 159 Toda informação detectada deverá ser unificada em uma única console de gerenciamento central oferecida pelo próprio fabricante capaz de gerenciar múltiplos appliances;
3. 160 A Console de Gerenciamento Central deve ser capaz de atribuir a cada appliance o conjunto de segmentos de rede a ser monitorado/controlado por cada um.
3. 161 Deverá possuir painéis/telas que apresentem:
3. 162 Políticas, regras e detalhes dos dispositivos que caíram no escopo e nas regras estabelecidas com capacidade de filtragem por segmento, unidade organizacional e grupos e mecanismo de busca baseado em texto;
3. 163 A tela/painel deverá mostrar tabela customizável com detalhes dos dispositivos, como:

• Endereço Mac;

• Endereço IP;

• Segmento de rede;

• Nome DNS e NetBIOS;

• Switch, porta e VLAN de conexão do dispositivo;

• Nome/Login do usuário;

• Ações executadas sobre o dispositivo.

3. 164 Deve ser possível customizar as propriedades dos dispositivos a serem apresentados na tabela;
3. 165 Para cada máquina selecionada na tela/painel deverá ser possível:

• Visualizar as políticas e regras em que o dispositivo foi enquadrado, informando data e hora, e as políticas e regras em que o dispositivo não foi enquadrado informando a razão de o mesmo não ter sido avaliado;

• Exibir todos os detalhes (atributos e propriedades) do dispositivo selecionado;

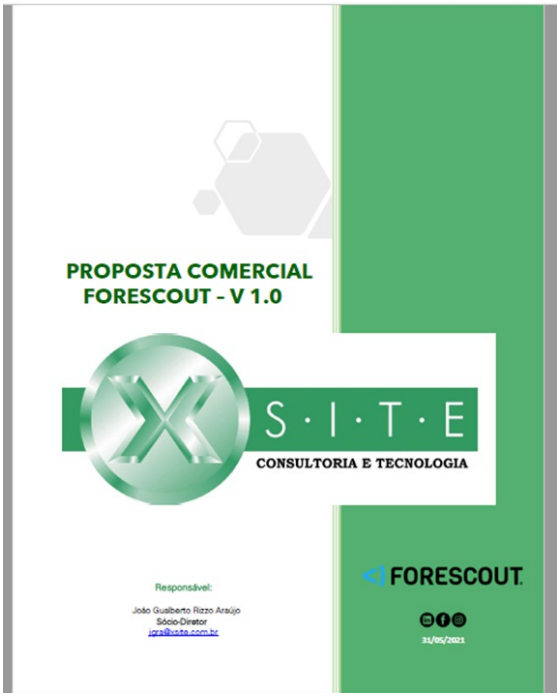
• Informações de compliance do dispositivo selecionado.

3. 166 Inventário de usuários, dispositivos, aplicações e informações de rede com capacidade de filtragem por segmento, unidade organizacional e grupos e mecanismo de busca baseado em texto;
3. 167 Criação, modificação e configuração de políticas;
3. 168 Ameaças detectadas com capacidade de filtragem por segmento, unidade organizacional e grupos e mecanismo de busca baseado em texto.
3. 169 Deve possuir assistente web de customização de aparência das telas de notificação e login via HTTP e do portal de gerenciamento de convidados;
3. 170 Deve permitir que aplicações de terceiros consultem e atualizem propriedades/atributos dos dispositivos através de chamadas de Web Services disponíveis na solução.
3. 171 Deve possuir portal WEB para consulta rápida de todos os detalhes dos dispositivos com facilidade de busca baseada em atributos do dispositivo, no mínimo por endereço IPv4, endereço IPv6, login do usuário, nome DNS, IP do switch onde o dispositivo está conectado, NetBIOS Domain, NetBIOS Hostname, e VMWare ESXi Server Name;
3. 172 Deve permitir a visualização de registro de auditoria, contendo informações sobre as atividades dos administradores da solução em um período de tempo específico;
3. 173 Deve permitir a visualização log de eventos detectados pelas políticas da solução, atualizado em tempo real e filtrado por faixa de endereços IP e período de tempo, para permitir a investigação das atividades de dispositivos específicos;
3. 174 Deve permitir a visualização dos logs de sistema (system logs) e envio dos mesmos para um servidor Syslog externo;
3. 175 Deve fornecer opção de remediação, restrição de acesso e comunicação com o usuário final diretamente a partir da console, no mínimo:
3. 176 Criar exceções para dispositivo;
3. 177 Reverificar status do dispositivo;
3. 178 Bloquear ou colocar em quarentena máquina em uma VLAN;
3. 179 Bloquear acesso à internet;
3. 180 Finalizar um processo;
3. 181 Forçar autenticação na rede;
3. 182 Possibilitar realizar a reverificação do dispositivo, por demanda, para todas as políticas ou apenas as selecionadas;
3. 183 Possibilitar filtrar dispositivos baseado em segmentos de rede, unidades organizacionais e grupos;
3. 184 Possibilitar visualizar apenas os dispositivos submetidos à classificação passiva;
3. 185 Deve possuir mecanismos de limitação (threshold) de aplicação de ações de bloqueio e limitação de acesso baseado em percentual do número de dispositivos controlados, incluindo, pelo menos, as ações de desabilitar porta de switch, modificação de VLAN, TCP Reset (Firewall Virtual), notificação via HTTP, redirecionamento via HTTP e matar processos em máquinas Windows.

Relatórios e Dashboard

3. 186 Deve possuir facilidade para geração e agendamento de relatórios com informações de tempo real sobre políticas, compliance de dispositivos, vulnerabilidades de máquinas Windows, informações do inventário, detalhes de dispositivos, ativos de rede e usuários visitantes;
3. 187 Deve possuir relatório/gráfico de tendência de políticas ao longo do tempo para permitir a avaliação da evolução de questões de classificação e compliance de dispositivos;
3. 188 Todos os relatórios devem poder ser filtrados, pelo menos, por segmento de rede.
3. 189 Todos os relatórios devem permitir agendamento e envio por e-mail;
3. 190 Os relatórios que apresentem detalhes dos dispositivos devem permitir ao administrador selecionar, dentre todos os atributos dos dispositivos, aqueles que devem ser apresentados no relatório;
3. 191 Deve possuir dashboard customizável que apresente de forma gráfica e dinâmica informações de classificação, conformidade e estado de gerenciamento dos dispositivos;
3. 192 O dashboard deve ser composto por Widgets customizáveis que apresentem gráficos com dados estatísticos coletados das políticas e regras de classificação/compliance criadas pelo administrador;
3. 193 Os Widgets devem permitir modificar dinamicamente o período de tempo apresentado no gráfico;
3. 194 Os Widgets que apresentem gráficos de tendência de regras de compliance devem possuir setas indicativas de tendências de melhoria ou piora nos níveis de compliance;
3. 195 Deve ser possível customizar o sentido das setas indicativas para indicar qual das direções (cima/baixo) indica melhoria do nível de compliance;
3. 196 Deve possibilitar a geração de relatórios das detecções de ameaças realizadas pela solução incluindo, pelo menos:
3. 197 Resumo executivo de máquinas infectadas e máquinas alvo dos ataques
3. 198 Máquinas infectadas por segmento de rede
3. 199 Máquinas origem de escaneamentos de rede
3. 200 Tentativas de infecção ao longo do tempo
3. 201 Tentativas de scan ao longo do tempo;
3. 202 Tentativas de infecção de domínios fora da rede da organização;

ANEXO II



S·I·T·E
CONSULTORIA E TECNOLOGIA

Proposta Comercial

À Procuradoria Geral do Estado – PGE / BA

Att: Comissão de Licitação

REF: Proposta de fornecimento de solução de Endpoint Visibility Access Security – EVAS, doravante denominada solução de EVAS, contemplando licença de uso com manutenção e suporte técnico de softwares necessários à sua operacionalização – Pregão Eletrônico nº 02/2021 – Processo Administrativo nº 006.0409.2021.0007522-03.

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.

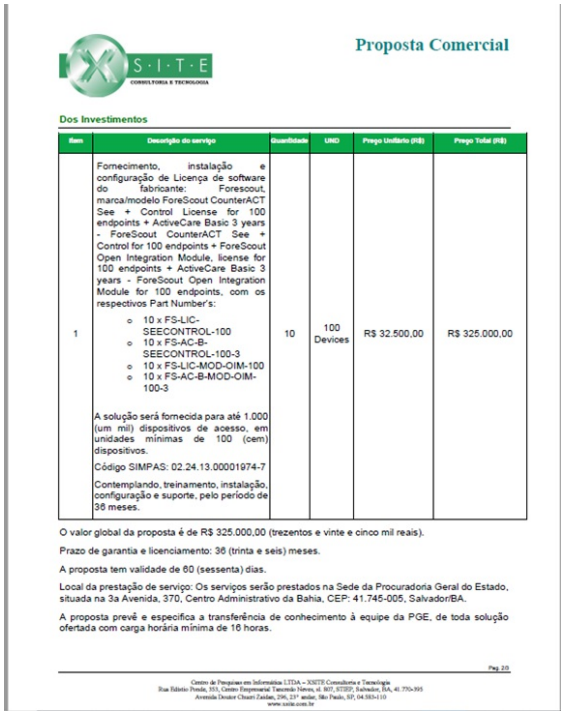
Dos Produtos, Serviços e Software

Proposta de fornecimento de solução de Endpoint Visibility Access Security – EVAS, doravante denominada solução de EVAS para 1.000 (um mil) dispositivos de acesso, em unidades mínimas de 100 (cem) dispositivos, Forescout, marca/modelo ForeScout CounterACT See + Control License for 100 endpoints + ActiveCare Basic 3 years - ForeScout CounterACT See + Control for 100 endpoints + ForeScout Open Integration Module, license for 100 endpoints + ActiveCare Basic 3 years - ForeScout Open Integration Module for 100 endpoints, com os respectivos Part Number's: 10x FS-LIC-SEECONTROL-100 + 10x FS-AC-B-SEECONTROL-100-3 + 10x FS-LIC-MOD-OIM-100 e 10x FS-AC-B-MOD-OIM-100-3, assim como, licença de uso com manutenção e suporte técnico de softwares necessários à sua operacionalização, além de instalação, treinamento, configurações e suporte pelo período de 36 meses.

Da Forescout

Forescout Technologies é um fornecedor líder de soluções de controle de segurança de rede generalizada de empresas Global 2000 e organizações governamentais. Com a Forescout, as organizações podem monitorar continuamente e mitigar exposições de segurança e ataques cibernéticos que melhor aproveita seus investimentos existentes, otimiza seus recursos de TI e aumenta a sua postura geral de segurança. O Forescout é uma plataforma de segurança de rede que fornece visibilidade e controle dinâmico de todos os dispositivos em sua rede. Com ele é possível identificar automaticamente quem e o que está em sua rede, além de também controlar o acesso com políticas de segurança, bloqueando ameaças e corrigindo violações de segurança em estações e servidores.

Centro de Pesquisas em Informática LTDA – XSITE Consultoria e Tecnologia
Rua Edelzio Penda, 353, Centro Empresarial Tancredo Neves, cl. 807, STIEP, Salvador, BA, 41.770-395
Avenida Doutor Chucri Zaidan, 296, 23º andar, São Paulo, SP, 04.583-110



Proposta Comercial

Dos Investimentos

Item	Descrição do serviço	Quantidade	UNID	Preço Unitário (R$)	Preço Total (R$)
1	Fornecimento, instalação e configuração de Licença de software do fabricante: Forescout, marca/modelo ForeScout CounterACT See + Control License for 100 endpoints + ActiveCare Basic 3 years - ForeScout CounterACT See + Control for 100 endpoints + ForeScout Open Integration Module, license for 100 endpoints + ActiveCare Basic 3 years - ForeScout Open Integration Module for 100 endpoints, com os respectivos Part Number's: o 10 x FS-LIC-SEECONTROL-100 o 10 x FS-AC-B-SEECONTROL-100-3 o 10 x FS-LIC-MOD-OIM-100 o 10 x FS-AC-B-MOD-OIM-100-3 A solução será fornecida para até 1.000 (um mil) dispositivos de acesso, em unidades mínimas de 100 (cem) dispositivos. Código SIMPAS: 02.24.13.00001974-7 Contemplando, treinamento, instalação, configuração e suporte, pelo período de 36 meses.	10	100 Devices	R$ 32.500,00	R$ 325.000,00

O valor global da proposta é de R$ 325.000,00 (trezentos e vinte e cinco mil reais).

Prazo de garantia e licenciamento: 36 (trinta e seis) meses.

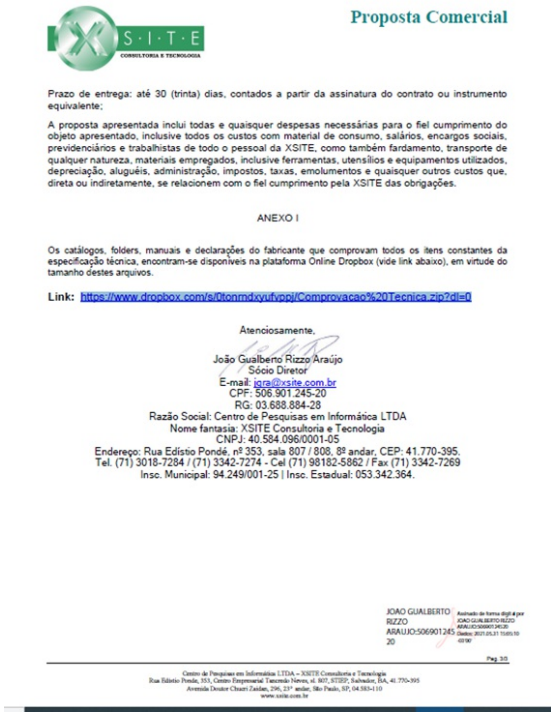
A proposta tem validade de 60 (sessenta) dias.

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

Pag. 2/3

Centro de Pesquisas em Informática LTDA – XSITE Consultoria e Tecnologia
Rua Edistio Pondé, 353, Centro Empresarial Tancredo Neves, sl. 807, STIEP, Salvador, BA, 41.770-395
Avenida Doutor Chucri Zaidan, 296, 23º andar, São Paulo, SP, 04.583-110
www.xsite.com.br



Proposta Comercial

Prazo de entrega: até 30 (trinta) dias, contados a partir da assinatura do contrato ou instrumento equivalente;

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 XSITE, 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 XSITE das obrigações.

ANEXO I

Os catálogos, folders, manuais e declarações do fabricante que comprovam todos os itens constantes da especificação técnica, encontram-se disponíveis na plataforma Online Dropbox (vide link abaixo), em virtude do tamanho destes arquivos.

Link: https://www.dropbox.com/sh/0tonmdxyufvppjl/Comprovacao%20Tecnica.zip?dl=0

Atenciosamente,

João Gualberto Rizzo Araújo
Sócio Diretor
E-mail: jgra@xsite.com.br
CPF: 506.901.245-20
RG: 03.688.884-28
Razão Social: Centro de Pesquisas em Informática LTDA
Nome fantasia: XSITE Consultoria e Tecnologia
CNPJ: 40.584.096/0001-05
Endereço: Rua Edístio Pondé, nº 353, sala 807 / 808, 8º andar, CEP: 41.770-395.
Tel. (71) 3018-7284 / (71) 3342-7274 - Cel (71) 98182-5862 / Fax (71) 3342-7269
Insc. Municipal: 94.249/001-25 | Insc. Estadual: 053.342.364.

JOAO GUALBERTO RIZZO ARAUJO:50690124520

Pag. 3/3

Centro de Pesquisas em Informática LTDA – XSITE Consultoria e Tecnologia
Rua Edístio Pondé, 353, Centro Empresarial Tancredo Neves, sl. 807, STIEP, Salvador, BA, 41.770-395
Avenida Doutor Chucri Zaidan, 296, 23º andar, São Paulo, SP, 04.583-110
www.xsite.com.br

Documento assinado eletronicamente por **João Gualberto Rizzo Araújo**, **Representante Legal da Empresa**, em 14/06/2021, às 12:04, 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 15/06/2021, às 15:16, 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 **Vinicius Do Nascimento Miguel**, **Assistente de Procuradoria**, em 15/06/2021, às 15:23, 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 **Jef de Almeida Borges**, **Coordenador III**, em 15/06/2021, às 15:25, 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 **00031631889** e o código CRC **F5AF7DD4**.

PROCURADORIA GERAL DO ESTADO

RESUMO DE CONTRATO
Processo SEI nº 006.7548.2020.0010856-39
Contrato n°. PGE 004/2021 - Dispensa nº 058/2020
Contratante: ESTADO DA BAHIA/PROCURADORIA GERAL DO ESTADO
Contratada: **EMPRESA GRÁFICA DA BAHIA - EGBA**
Objeto: Serviços especializados e continuados de Arquivamento e Movimentação de Documentos para a PGE, no valor global estimado de R$ 322.860,00 (trezentos e vinte e dois mil oitocentos e sessenta reais), Unidade Orçamentária - 06.601, Fontes - 154/354, Projeto/Atividade - 4704, Elemento de Despesa - 33.90.39. Prazo: 12 (doze) meses, a partir de 08/06/2021. Regime de Execução/Forma de Pagamento: Empreitada por preço unitário.
Setor Responsável pela Gestão Contratual: Coordenação de Arquivo e Documentação
Gestora: Celidalva Alves Ribeiro Bastos
Fiscal: Fabiana Priscilla Senna Ferreira

RESUMO DE CONTRATO
Processo: SEI 006.0409.2021.0007522-03
Contrato: n° PGE 024/2021- Pregão Eletrônico nº 002/2021
Contratante: ESTADO DA BAHIA/PROCURADORIA GERAL DO ESTADO
Contratada: **CENTRO DE PESQUISA EM INFORMÁTICA LTDA.**
Objeto: Serviços de Solução de Endpoint Visibility Access Security - EVAS, doravante denominada Solução de EVAS, contemplando licença de uso com manutenção e suporte técnico de softwares à sua operacionalização, visando garantir o controle, políticas de conformidade, a visibilidade e a segurança no acesso à rede da Procuradoria Geral do Estado da Bahia - PGE/BA, no valor global estimado de R$ 325.000,00 (trezentos e vinte e cinco mil reais), Unidade Orçamentária - 06.601, Fonte - 154, Projeto/Atividade - 5121, Elemento de Despesa - 33.90.40. Prazo: 36 (trinta e seis) meses, a partir da data da assinatura (15/06/2021). 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: Maurício de Cerqueira Pereira

RESUMO DE ADITIVO CONTRATUAL
Termo Aditivo 02 (Contrato PGE 020/2019)
Processo nº 006.7550.2019.0009274-54
Contratante: ESTADO DA BAHIA/PROCURADORIA GERAL DO ESTADO
Contratada: **PEDRO REFRIGERAÇÃO COMÉRCIO E SERVIÇO LTDA-ME**
Objeto: Prorrogar o contrato por 12 (doze) meses, com início em 18/06/2021 e término em 17/06/2022, cujas despesas serão atendidas pela Unidade Orçamentária - 06.601, Fontes - 154/354, Projeto/Atividade - 2000, Elemento de Despesa - 33.90.39, retificadas as cláusulas em desacordo com as modificações ora inseridas e ratificadas as demais.

RESUMO DE ADITIVO CONTRATUAL
Termo Aditivo 02 (Contrato PGE 021/2019)
Processo nº 006.7550.2019.0009285-15
Contratante: ESTADO DA BAHIA/PROCURADORIA GERAL DO ESTADO
Contratada: **PEDRO REFRIGERAÇÃO COMÉRCIO E SERVIÇO LTDA-ME**
Objeto: Prorrogar o contrato por 12 (doze) meses, com início em 18/06/2021 e término em 17/06/2022, cujas despesas serão atendidas pela Unidade Orçamentária - 06.601, Fontes - 154/354, Projeto/Atividade - 2000, Elemento de Despesa - 33.90.39, retificadas as cláusulas em desacordo com as modificações ora inseridas e ratificadas as demais.

RESUMO DE ADITIVO CONTRATUAL
Termo Aditivo 02 (Contrato PGE 026/2019)
Processo nº 006.7550.2019.0010056-07
Contratante: ESTADO DA BAHIA/PROCURADORIA GERAL DO ESTADO
Contratada: **FLORICULTURA PARAISO LTDA - EPP**
Objeto: Prorrogar o contrato por 12 (doze) meses, com início em 03/07/2021 e término em 02/07/2022, cujas despesas serão atendidas pela Unidade Orçamentária - 06.601, Fonte - 154, Projeto/Atividade - 2000, Elemento de Despesa - 33.90.30, retificadas as cláusulas em desacordo com as modificações ora inseridas e ratificadas as demais.

ALTERAÇÃO DE DESIGNAÇÃO GESTOR/FISCAL - Conforme art. 3º da Portaria PGE nº 041 de 30 de abril de 2019

Setor Responsável pela Gestão Contratual: Assessoria de Comunicação Social
Instrumento: Contrato PGE 013/2021
Objeto: Serviços de Design Gráfico
Empresa: MONICA DE LIMA SANTIAGO
Gestora: Waldimara Silva Santana
Fiscal: Thais Ribeiro dos Santos Bahia

Setor Responsável pela Gestão Contratual: Procuradoria Judicial
Instrumento: Contrato PGE 041/2019
Objeto: Serviço de seleção e recorte eletrônico de publicações de decisões e despachos judiciais através de integração automatizada de sistemas, proferidos em ações em que o Estado da Bahia figure como parte no Diário do Poder Judiciário(capital e interior), no Diário da Justiça Federal - Seção Bahia, no Diário da Justiça do Trabalho - TRT 5ª Região (Capital e Interior) e nos Diários do Tribunal Regional Federal, do Superior Tribunal de Justiça, do Superior Tribunal do Trabalho e do Supremo Tribunal Federal.
Empresa: AUTOCLIP SERVIÇOS PESQUISA E DESENVOLVIMENTO DE TECNOLOGIA DA INFORMAÇÃO - LTDA.
Gestora: Kariny Queiroz de Souza
Fiscal: Rafaela Marques Vieira Nery

Setor Responsável pela Gestão Contratual: Coordenação de Gestão Estratégica
Instrumento: Contrato PGE 011/2017
Objeto: Serviços de sustentação, garantia de evolução tecnológica e funcional, suporte técnico personalizado e serviços sob demanda, visando a manutenção, para o Sistema SAJ/Procuradorias, da Procuradoria Geral do Estado da Bahia.
Empresa: SOFTPLAN PLANEJAMENTO E SISTEMAS LTDA.
Gestor: Eduardo Jorge Rodrigues Brandão
Fiscal: Vito Magarão
Obs. Designação retroativa à 10/05/2021

Setor Responsável pela Gestão Contratual: Coordenação de Gestão Estratégica
Instrumento: Contrato PGE 018/2018
Objeto: Serviços técnicos especializados em tecnologia da informação e comunicação relativos a Desenvolvimento e Manutenção de Sistemas (Especificação de Requisitos e Codificação de Sistemas de Informação, Serviços de Administração de Dados, Serviços de Pesquisa e Desenvolvimento de Solução de TIC e Serviço de Gestão Eletrônica de Documentos por sistemas), sob demanda, com o objetivo de atender as demandas da Procuradoria Geral do Estado da Bahia.
Empresa: AVANSYS TECNOLOGIA LTDA
Gestor: Eduardo Jorge Rodrigues Brandão
Fiscais: Vito Magarão / Vera Lucia Vieira Bacelar
Obs. Designação retroativa à 10/05/2021

Setor Responsável pela Gestão Contratual: Coordenação de Gestão Estratégica
Instrumento: Contrato PGE 043/2018
Objeto: Serviços técnicos especializados em Análise, Modelagem, Implementação, Monitoramento, Controle e Melhoria dos Processos de Negócio da Procuradoria Geral do Estado da Bahia.
Empresa: UNION INFORMÁTICA LTDA - EPP
Gestor: Eduardo Jorge Rodrigues Brandão
Fiscal: Vera Lucia Vieira Bacelar
Obs. Designação retroativa à 10/05/2021

Setor Responsável pela Gestão Contratual: Coordenação de Gestão Estratégica
Instrumento: Contrato SAEB 058/2018
Objeto: Serviços de Suporte, Manutenção, Integração e Customização do Sistema de Gestão de Ações Prioritárias, Projetos, Programas e Portfólios - SG, oriundo de customização do Sistema Channel.
Empresa: JEXPERTS TECNOLOGIA S/A
Gestor: Eduardo Jorge Rodrigues Brandão
Fiscal: Lucimário Ramos Oliveira
Obs. Designação retroativa à 10/05/2021

Setor Responsável pela Gestão Contratual: Coordenação de Gestão Estratégica
Instrumento: Contrato PGE 032/2019
Objeto: Serviço de manutenção e suporte das licenças, bem como a administração e execução de atividades rotineiras para sustentação dos ambientes da solução de ECM [Enterprise Content Management] da Procuradoria Geral do Estado.
Empresa: INETUM BRASIL LTDA
Gestor: Eduardo Jorge Rodrigues Brandão
Fiscal: Lucimário Ramos Oliveira
Obs. Designação retroativa à 10/05/2021

RESUMO DE ADITIVO CONTRATUAL
Termo Aditivo 05 (Contrato PGE 029/2016)
Processo nº 006.7550.2019.0018046-66
Contratante: ESTADO DA BAHIA/PROCURADORIA GERAL DO ESTADO
Contratada: **FERLY COMERCIO E SERVIÇOS LTDA. ME**
Objeto: Prorrogar o contrato, em caráter excepcional, por 06 (seis) meses, com início em 27/06/2021 e término em 26/12/2021, cujas despesas serão atendidas pela Unidade Orçamentária - 06.601, Fontes - 154/354, Projeto/Atividade - 2000, Elemento de Despesa - 33.90.39, retificadas as cláusulas em desacordo com as modificações ora inseridas e ratificadas as demais.

SECRETARIA DA ADMINISTRAÇÃO

RESUMO DO CONTRATO Nº 030/2021
Processo SEI nº: 009.0210.2020.0034232-86. **Contratante:** Estado da Bahia, através da Secretaria da Administração. **Contratada**: Realiza Construções Eireli. **Objeto:** execução de obra de acessibilidade externa do prédio TCE / TCM, de acordo com as especificações do instrumento convocatório e da proposta apresentada. **Valor Global Estimado:** R$ 713.273,79 (setecentos e treze mil, duzentos e setenta e três reais e setenta e nove centavos). **Modalidade de Licitação:** Tomada de Preço n° 002/2021. **Vigência:** 150 (cento e cinquenta) dias corridos, contados da emissão da ordem de serviço. **Regime de Execução:** Empreitada por Preço