**CONTRATO PGE 003/2022**

| Modalidade de Licitação | Número |
|---|---|
| Pregão Eletrônico | 010/2021 |

**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 010/2021, processo administrativo nº 006.0409.2021.0029638-21, 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 Segurança da Informação, desejando ampliar a segurança da rede e dos ativos da Procuradoria Geral do Estado – 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.

**[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 )** A garantia contratual será de 5% do valor do contrato, podendo recair sobre qualquer das modalidades previstas no §1º do art. 136 da Lei estadual nº 9.433/05.

**§1º** Sob pena da caracterização de inadimplemento contratual, a prova da garantia, na hipótese de opção pela modalidade caução em dinheiro ou títulos da dívida pública, deverá ser apresentada no prazo máximo de 05 (cinco) dias contados da data de assinatura do contrato, admitindo-se, para o seguro-garantia e a fiança bancária, que a comprovação seja feita no prazo máximo de 30 (trinta) dias daquela data, sem o que fica vedada, em qualquer caso, a realização de pagamento.

**§2º** A garantia responderá pelo inadimplemento das obrigações contratuais e pelas multas impostas, independentemente de outras cominações legais.

**§3º** A CONTRATADA ficará obrigada a repor o valor da garantia quando esta for utilizada, bem como a atualizar o seu valor nas mesmas condições do contrato.

**§4º** No caso de seguro-garantia ou fiança bancária, não será admitida a existência de cláusulas que restrinjam ou atenuem a responsabilidade do segurador ou fiador.

**§5º** A CONTRATADA deverá atualizar a garantia sempre que houver alteração contratual, no mesmo prazo deferido para a comprovação da garantia originária, visando assegurar a cobertura das modificações procedidas.

**§6º** Será recusada a garantia que não atender às especificações solicitadas, devendo ser notificada a CONTRATADA para que, no prazo de 05 (cinco) dias, sane a incorreção apontada ou, no caso de títulos da dívida pública, seguro-garantia ou fiança bancária, promova a substituição por caução em dinheiro.

**§7º** O retardamento, a falta da apresentação ou a não substituição da garantia impedirá a realização do pagamento das faturas apresentadas, sem prejuízo da incidência de multa moratória, da rescisão do contrato nos termos do art. 167, inc. III, da Lei nº 9.433/05 e das demais cominações legais.

**§8º** A devolução da garantia ocorrerá após o recebimento definitivo da totalidade do objeto do contrato, com a demonstração de cumprimento, pela CONTRATADA, das obrigações pactuadas.

**CLÁUSULA QUARTA – REGIME DE EXECUÇÃO**

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

**CLÁUSULA QUINTA – PREÇO**

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

**[SERVIÇOS]**

| ITEM | Código SIMPAS | Descrição | Unidade de Fornecimento (UF) | Quantitativo | Preço Unitário 36 (Trinta E Seis) Meses | Preço Global |
|---|---|---|---|---|---|---|
| 1 | 02.81.06.00000487-1 | LICENÇA DE USO DE SOFTWARE, appliance de monitoramento, log e relatoria, incluindo serviços de instalação, garantia e suporte. | Un. | 1,000 | R$ 70.000,00 | R$ 70.000,00 |
| 2 | 02.81.06.00000488-0 | LICENÇA DE USO DE SOFTWARE, firewalls UTM, incluindo serviços de instalação, garantia e suporte. | Un. | 2,000 | R$ 230.000,00 | R$ 460.000,000 |
| **VALOR GLOBAL** | | | | | | **R$ 530.000,00** |

**§1º** Estima-se para o contrato o valor global de **R$ 530.000,00 (quinhentos e trinta 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 consequência 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 empresa deverá apresentar as seguintes documentações dos produtos:

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

II - 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.

**§3º** A CONTRATADA deverá apresentar juntamente com a documentações dos produtos, certificado ou título, concedido pelo fabricante, que comprove o credenciamento da CONTRATADA como representante autorizada;

**§4º** A CONTRATADA deverá apresentar juntamente com as documentações dos produtos, as licenças dos produtos fornecidos necessários para a implantação e as mídias de instalação com 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(m) indicado(s) como fiscal(is) deste Contrato o(s) servidor(es): **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.

**§9º** O pagamento referente ao itens supracitados deste documento (serviço de suporte técnico, implantação, manutenção e atualização) será realizado em 36 (trinta e seis) parcelas mensais e de igual valor, devendo a fatura referente à primeira parcela ser emitida 10 (dez) dias após a entrega da solução e conclusão dos serviços de instalação e treinamento, de acordo com as especificações deste Termo de Referência;

**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 consequências 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 subsequente 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 subsequente 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 – 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 DÉCIMA OITAVA – 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 DÉCIMA NONA – 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.

_____

**PROCURADORIA GERAL DO ESTADO**

_____

**CENTRO DE PESQUISA EM INFORMÁTICA LTDA**

_____

TESTEMUNHA

_____

TESTEMUNHA

**ANEXO I**

*GOVERNO DO ESTADO DA BAHIA*
PROCURADORIA GERAL DO ESTADO-PGE

**TERMO DE REFERÊNCIA**

**Empresa especializada em fornecimento de serviços de Soluções de Segurança da Informação**

**1. OBJETO**

Constitui objeto desta Licitação a contratação de empresa especializada em fornecimento de serviços de soluções de Segurança da Informação, desejando ampliar a segurança da rede e dos ativos da Procuradoria Geral do Estado – PGE/BA, contemplados pelos itens abaixo discriminados a serem executados de forma continuada pelo período de 36 (trinta e seis) meses, para a PGE/BA, em Lote Único, nos moldes das especificações e quantitativos descritos nos Anexos a este instrumento convocatório, incluindo, instalação, garantia, manutenção e suporte técnico de acordo com as condições e especificações constante neste termo.

DOS ITENS

| ITEM | DESCRIÇÃO |
|---|---|
| 1 | Contratação de serviços de empresa especializada para o fornecimento de 02 (dois) Firewalls UTM, incluindo serviços de instalação, garantia e suporte por 36 (trinta e seis) meses. |
| 2 | Contratação de serviços de empresa especializada para o fornecimento de 01 (um) Appliance de monitoramento, log e relatoria, incluindo serviços de instalação, garantia e suporte por 36 (trinta e seis) meses. |

**2.JUSTIFICATIVA**

O firewall corporativo é um ativo de segurança da informação fundamental numa rede de dados, uma vez que ele regula/monitora todo o tráfego de entrada e saída na rede. Por meio da introspecção dos dados de rede, o firewall corporativo é capaz de bloquear acessos não autorizados, mediar o uso de internet, criar conexões seguras com unidades remotas e usuários, bem como oferecer atualizações automáticas para ameaças de dia zero (zero-day malware).

As Soluções de Firewall de Próxima Geração (Next Generation Firewall são tecnologias modernas de Firewall que representa um quesito de segurança fundamental, uma vez que

regula o tráfego de dados entre redes confiáveis e não confiáveis (Internet) e impede a transmissão e recepção de informações a partir de acessos nocivos ou não autorizados na rede. Isso é possível, através de um sistema de detecção de intrusões, Anti-Malware na camada de rede, filtragem de tráfego web malicioso e a inspeção de tráfego SSL na busca de ameaças camufladas sobre a camada de criptografia.

No contexto da Segurança da Informação, a Procuradoria Geral do Estado possui em sua infraestrutura soluções de segurança firewall Fortinet modelo Fortigate 300D, números de série FGT3HD3915806460 e FGT3HD3915806391; assim como, um sistema de armazenamento de logs e geração de relatórios que permite melhor visibilidade e gerenciamento dos recursos de Internet, FortiAnalyzer, modelo FAZ-200D, número de série: FL200D3A15001378. Estes equipamentos são responsáveis por controlar o tráfego de entrada e saída da rede da PGE/BA, protegendo-a contra ameaças, invasões e perdas de informação.

Cumpre salientar que a Procuradoria também possui em sua infraestrutura 18 (dezoito) Access Point Fortinet, modelo FortiAP Indoor FAP-223C, para prover acesso gerenciável e seguro à rede wireless aos usuários da Procuradoria na unidade administrativa situada no CAB.

Os equipamentos FortiGate 300D, são de suma importância para o funcionamento da rede de dados da instituição, visto que através deles é possível proteger, gerenciar, administrar e controlar todo o tráfego na rede da sede administrativa do CAB.

Cumpre destacar que durante o período de pandemia causada pelo novo coronavírus (Covid-19), esses equipamentos permitiram a continuidade das atividades da Procuradoria em sistema home office, conectando os colaboradores de forma segura à rede corporativa da PGE/BA através de VPN (*Virtual Private Network*).

Entretanto, os referidos equipamentos estão em uso por mais de cinco anos e tiveram o anúncio de fim de venda. Isto significa para necessidade de mudança de equipamentos, visto que a tecnologia passa a ser obsoleta e ter mais probabilidade de sofrer ataques cibernéticos.

Desta forma, poderá ser gerada uma exposição a possíveis ataques cibernéticos no ambiente da PGE. Além disto, todo o controle de conteúdo web será desabilitado permitindo que os usuários tenham acesso, inclusive à sites maliciosos e também utilizando todo link de banda, criando lentidão no ambiente operacional.

Considerando a utilização de firewalls Fortinet no ambiente tecnológico da PGE, assim como a concentração de logs e geração de relatórios através do FortiAnalyzer, modelo FAZ-200D, e os pontos de acesso a rede sem fio FAP-223C, estimamos que a compatibilidade e interoperabilidade entre a nova solução de segurança (firewall) objeto deste termo de referência com a infraestrutura já existente, é essencial para a continuidade dos negócios da PGE.

Ademais, a equipe de analistas da PGE possui experiência na administração e configuração de equipamentos Fortinet. A definição da marca padronizada preserva o investimento e aproveita o conhecimento adquirido, não sendo necessária a contratação de um novo treinamento.

Esta escolha fundamenta-se na Lei Estadual 9.433/05 que em seu Art. 31º Inciso I recomenda que as compras públicas deverão "*atender ao princípio da padronização e à compatibilidade de especificações técnicas e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas*".

Outrossim é o entendimento do Tribunal de Contas da União através da Súmula nº 270,

vejamos: *"Em licitações referentes a compras, inclusive de softwares, é possível a indicação de marca, desde que seja estritamente necessária para atender exigências de padronização e que haja prévia justificação".*

Assim posto, esta demanda implica na manutenção do padrão de equipamentos atualmente em uso, ou seja, a continuidade do produto da Fortinet, para solução de proteção de rede de Next Generation Firewall (NGFW). Cabe destacar, que essa manutenção pela marca não implica em inexigibilidade de licitação, pois, existe no mercado uma quantidade considerável de empresas – credenciadas pelo fabricante dos equipamentos – capaz de fornecer os novos equipamentos e prestar os serviços desejados.

Ressalta-se que a escolha das especificações do presente objeto está relacionada à necessidade deste Órgão e foram devidamente avaliadas por esta Coordenação, estando constatado, principalmente, que as características do item escolhido são comuns no mercado e não restringirão a competição. Ademais, é preciso destacar que o item se encontra devidamente cadastrado no catálogo do SIMPAS através do CÓDIGO SIMPAS **02.24.13.00001899-6,** o que atesta, também, a avaliação realizada pela Secretaria de Administração/SAEB.

**3. DAS ESPECIFICAÇÕES TÉCNICAS – ITEM 01**

**FIREWALL**

**3.1 Requisitos de desempenho**

3.1.1 Throughput de, no mínimo, 11 Gbps com a funcionalidade de *firewall* habilitada para tráfego IPv4 e IPv6, independentemente do tamanho do pacote;

3.1.2 Suporte a, no mínimo, 3 milhões de conexões simultâneas;

3.1.3 Suporte a, no mínimo, 280 mil novas conexões por segundo;

3.1.4 Throughput de, no mínimo, 13 Gbps de VPN IPSec;

3.1.5 Estar licenciado para, ou suportar sem o uso de licença, 2.500 túneis de *VPN IPSEC Site-to-Site* simultâneos;

3.1.6 Estar licenciado para, ou suportar sem o uso de licença, 16.000 túneis de clientes *VPN IPSEC* simultâneos;

3.1.7 Throughput de, no mínimo, 2 Gbps de VPN *SSL*;

3.1.8 Suporte a, no mínimo, 500 clientes de *VPN SSL* simultâneos;

3.1.9 Suportar no mínimo 5 Gbps de *Throughput* de IPS;

3.1.10 Suportar no mínimo 4 Gbps de *Throughput* de Inspeção SSL;

3.1.11 Possuir ao menos 16 interfaces RJ-45;

3.1.12 Possuir ao menos 08 interfaces SFP;

3.1.13 Possuir ao menos 01 porta de gerenciamento RJ-45;

3.1.14 Possuir ao menos 01 disco, no mínimo 480 GB SSD;

**3.2 Características Gerais**

3.2.1 A solução deve consistir em plataforma de proteção de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração. Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais podem instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris ou GNU/Linux;

3.2.2 Por funcionalidades de NGFW entende-se: firewall, reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;

3.2.3 As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que sejam do mesmo fabricante e obedeçam a todos os requisitos mínimos desta especificação;

3.2.4 A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;

3.2.5 Serão aceitos equipamentos para montagem em rack 19", ou de mesa, incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação, e não ser maior que 1U de espaçamento em rack;

3.2.6 O software deverá ser fornecido em sua versão mais atualizada;

3.2.7 O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;

3.2.8 Os dispositivos de proteção de rede devem possuir suporte a 4094 VLAN Tags 802.1q;

3.2.9 Os dispositivos de proteção de rede devem possuir suporte a agregação de links 8023ad e LACP;

3.2.10 Os dispositivos de proteção de rede devem possuir suporte a Policy based routing ou policy based forwarding;

3.2.11 Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);

3.2.12 Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay, DHCP Server, Jumbo Frames;

3.2.13 Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;

3.2.14 Deve suportar NAT dinâmico (N-para-1);

3.2.15 Deve suportar NAT dinâmico (N-para-N);

3.2.16 Deve suportar NAT estático (1-para-1);

3.2.17 Deve suportar NAT estático (N-para-N);

3.2.18 Deve suportar NAT estático bidirecional 1-to-1;

3.2.19 Deve suportar Tradução de porta (PAT);

3.2.20 Deve suportar NAT de Origem;

3.2.21 Deve suportar NAT de Destino;

3.2.22 Deve suportar NAT de Origem e NAT de Destino simultaneamente;

3.2.23 Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

3.2.24 Deve suportar NAT64 e NAT46;

3.2.25 Deve implementar o protocolo ECMP;

3.2.26 Deve implementar balanceamento de link por hash do IP de origem e por hash do IP de origem e destino;

3.2.27 Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links;

3.2.28 Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;

3.2.29 Deve permitir monitorar, via SNMP, falhas de hardware, uso de recursos por número elevado de sessões, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;

3.2.30 Enviar log para sistemas de monitoração externos, simultaneamente;

3.2.31 Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;

3.2.32 Implementar proteção anti-spoofing;

3.2.33 Implementar otimização do tráfego entre dois equipamentos;

3.2.34 Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

3.2.35 Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

3.2.36 Suportar OSPF graceful restart;

3.2.37 Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);

3.2.38 Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

3.2.39 Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;

3.2.40 Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha visibilidade do tráfego;

3.2.41 Deve suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;

3.2.42 Suporte à configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo transparente;

3.2.43 Suporte à configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3;

3.2.44 Suporte à configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3 e com no mínimo 3 equipamentos no cluster;

3.2.45 A configuração em alta disponibilidade deve sincronizar: sessões, configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede, Associações de Segurança das VPN's, Tabelas FIB;

3.2.46 O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;

3.2.47 Deve possuir suporte à criação de sistemas virtuais no mesmo appliance;

3.2.48 Em alta disponibilidade, deve ser possível o uso de clusters virtuais, seja ativo-ativo ou ativo-passivo, permitindo a distribuição de carga entre diferentes contextos;

3.2.49 Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas;

3.2.50 Controle, inspeção e descriptografia de SSL para tráfego de entrada (Inbound) e Saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);

**3.3 Controle por política de firewall**

3.3.1 Deverá suportar controles por zona de segurança;

3.3.2 Controles de políticas por porta e protocolo;

3.3.3 Controle de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;

3.3.4 Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

3.3.5 Controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS);

3.3.6 Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound);

3.3.7 Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound);

3.3.8 Deve descriptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2;

3.3.9 Controle de inspeção e descriptografia de SSH por política;

3.3.10 Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;

3.3.11 Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo);

3.3.12 QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações;

3.3.13 Suporte a objetos e regras IPV6;

3.3.14 Suporte a objetos e regras multicast;

3.3.15 Deve suportar no mínimo três tipos de resposta nas políticas de firewall: Drop sem notificação do bloqueio ao usuário, Drop com notificação do bloqueio ao usuário, Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão;

3.3.16 Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

**3.4 Controle de aplicações**

3.4.1 O dispositivo de proteção de rede deve possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

3.4.2 Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;

3.4.3 Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

3.4.4 Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, Skype, facebook, LinkedIn, twitter, Citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, WhatsApp, 4shared, dropbox, google drive, skydrive, db2, mysql, Oracle, Active Directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;

3.4.5 Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

3.4.6 Deve detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Bittorrent e aplicações VOIP que utilizam criptografia proprietária;

3.4.7 Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;

3.4.8 Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

3.4.9 Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex;

3.4.10 Identificar o uso de táticas evasivas via comunicações criptografadas;

3.4.11 Atualizar a base de assinaturas de aplicações automaticamente;

3.4.12 Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos;

3.4.13 Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Controlador de Domínio, nem nas estações dos usuários;

3.4.14 Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

3.4.15 Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;

3.4.16 Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;

3.4.17 Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;

3.4.18 A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS-SQL, IMAP, DNS, LDAP, RTSP e SSL;

3.4.19 O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

3.4.20 Deve alertar o usuário quando uma aplicação for bloqueada;

3.4.21 Deve possibilitar a diferenciação de tráfegos Peer2Peer (bittorrent, emule etc.) possuindo granularidade de controle/políticas para os mesmos;

3.4.22 Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat etc.) possuindo granularidade de controle/políticas para os mesmos;

3.4.23 Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo;

3.4.24 Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate etc.) possuindo granularidade de controle/políticas para os mesmos;

3.4.25 Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol etc.);

3.4.26 Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação;

3.4.27 Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;

3.4.28 Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;

3.4.29 Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

3.4.30 As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;

3.4.31 Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;

3.4.32 Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset;

3.4.33 As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

3.4.34 Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

3.4.35 Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;

3.4.36 Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

3.4.37 Deve permitir o bloqueio de vulnerabilidades;

3.4.38 Deve permitir o bloqueio de exploits conhecidos;

3.4.39 Deve incluir proteção contra-ataques de negação de serviços;

3.4.40 Deverá possuir os seguintes mecanismos de inspeção de IPS: Análise de padrões de estado de conexões, de decodificação de protocolo, de detecção de anomalias de protocolo, análise heurística, IP Defragmentation, remontagem de pacotes de TCP, bloqueio de pacotes malformados;

3.4.41 Ser imune e capaz de impedir ataques como: Syn flood, ICMP flood, UDP flood, etc;

3.4.42 Detectar e bloquear a origem de portscans;

3.4.43 Bloquear ataques efetuados por worms conhecidos;

3.4.44 Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

3.4.45 Possuir assinaturas para bloqueio de ataques de buffer overflow;

3.4.46 Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

3.4.47 Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou Anti-Spyware, permitindo a criação de exceções com granularidade nas configurações;

3.4.48 Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP,

FTP, SMB, SMTP e POP3;

3.4.49 Identificar e bloquear comunicação com botnets;

3.4.50 Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

3.4.51 Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;

3.4.52 Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;

3.4.53 Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;

3.4.54 Os eventos devem identificar o país de onde partiu a ameaça;

3.4.55 Deve incluir proteção contra vírus em conteúdo HTML e JavaScript, software espião (spyware) e worms;

3.4.56 Proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;

3.4.57 Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança etc., ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança;

**3.5 Filtro de URL**

3.5.1 Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

3.5.2 Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

3.5.3 Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;

3.5.4 Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

3.5.5 Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;

3.5.6 Possuir pelo menos 60 categorias de URLs;

3.5.7 Deve possuir a função de exclusão de URLs do bloqueio, por categoria;

3.5.8 Permitir a customização de página de bloqueio;

3.5.9 Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site);

**3.6 Identificação de usuários**

3.6.1 Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, Edirectory e base de dados local;

3.6.2 Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

3.6.3 Deve possuir integração e suporte a Microsoft Active Directory para os seguintes sistemas operacionais: Windows Server 2008, 2008 R2, 2012, 2012 R2, 2016;

3.6.4 Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso como, mas não limitado à utilização de sistemas virtuais, segmentos de rede, etc;

3.6.5 Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

3.6.6 Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;

3.6.7 Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);

3.6.8 Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

3.6.9 Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

3.6.10 Permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso à internet e gerenciamento da solução;

3.6.11 Prover no mínimo um token nativamente, possibilitando autenticação de duplo fator;

**3.7 QOS e Traffic Shaping**

3.7.1 Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, ustream etc.) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;

3.7.2 Suportar a criação de políticas de QoS e Traffic Shaping por: endereço de origem,

endereço de destino, por usuário e grupo, por aplicações (incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus), por porta,

3.7.3 O QoS deve possibilitar a definição de tráfego com: banda garantida, banda máxima e fila de prioridade;

3.7.4 Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype for Business;

3.7.5 Suportar marcação de pacotes Diffserv, inclusive por aplicação;

3.7.6 Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;

3.7.7 Deve suportar QOS (traffic-shapping), em interface agregadas ou redundantes;

**3.8 Filtro de dados**

3.8.1 Permitir identificar, e opcionalmente prevenir, a transferência de vários tipos de arquivos (MS Office, PDF etc.) identificados sobre aplicações (HTTP, FTP, SMTP etc.);

3.8.2 Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

3.8.3 Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

3.8.4 Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;

**3.9 GEO Localização**

3.9.1 Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;

3.9.2 Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

3.9.3 Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas;

**3.10 VPN**

3.10.1 Suportar VPN Site-to-Site e Cliente-To-Site;

3.10.2 Suportar IPSec VPN;

3.10.3 Suportar SSL VPN;

3.10.4 A VPN IPSEc deve suportar 3DES;

3.10.5 A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;

3.10.6 A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;

3.10.7 A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);

3.10.8 A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);

3.10.9 A VPN IPSEc deve suportar Autenticação via certificado IKE PKI

3.10.10 Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

3.10.11 Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting;

3.10.12 A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;

3.10.13 A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;

3.10.14 Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;

3.10.15 Atribuição de DNS nos clientes remotos de VPN;

3.10.16 Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

3.10.17 Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;

3.10.18 Suportar leitura e verificação de CRL (certificate revocation list);

3.10.19 Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;

3.10.20 O agente de VPN a ser instalado nos equipamentos desktop e laptops, dever ser capaz de ser distribuído de maneira automática via Microsoft SCCM, Active Directory e ser descarregado diretamente desde link existente no próprio portal, o qual residirá no centralizador de VPN;

3.10.21 Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Antes do usuário autenticar na estação;

3.10.22 Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Após autenticação do usuário na estação;

3.10.23 Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Sob demanda do usuário;

3.10.24 Deverá manter uma conexão segura com o portal durante a sessão;

3.10.25 O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bits), Windows 8 (32 e 64 bits), Windows 10 (32 e 64 bits) e Mac OS X (v10.10 ou superior);

3.10.26 Os equipamentos de NGFW deverão contar com a inclusão em autoridades certificadoras (enrollment) mediante SCEP (Simple Certificate Enrollment Protocol) e mediante arquivos; Certificação ICSA para o Firewall;

3.10.27 Certificação ICSA IPSEC (VPN IPSec); Certificação ICSA para Sistema de Detecção de Intrusão; Certificação ICSA para Antivírus; Certificação FIPS 140-2 para Firewall; Certificação Common Criteria como EAL4+.

**3.11 Recurso de controladora dos pontos de acesso sem fio**

3.11.1 Estar contido ou não no appliance do NGFW e, caso não esteja contido no appliance do NGFW, deverá ser compatível com montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação, e não ser maior que 1U de espaçamento em rack.

3.11.2 Suporte ao serviço de servidor DHCP por SSID para prover endereçamento IP automático para os clientes wireless;

3.11.3 Suportar IPv4 e IPv6 por SSID;

3.11.4 Permitir escolher se o tráfego de cada SSID será enviado à controladora ou comutado diretamente pela interface do Access Point em determinada VLAN;

3.11.5 Permitir definir quais redes serão acessadas através da controladora e quais redes serão comutadas diretamente pela interface do Access Point;

3.11.6 Suporte a monitoração e supressão de Ponto de Acesso indevido;

3.11.7 Prover autenticação para a rede wireless através de bases externas como LDAP ou RADIUS;

3.11.8 Permitir autenticar usuários da rede wireless de forma transparente em domínio Windows;

3.11.9 Deverá permitir a visualização dos clientes wireless conectados;

3.11.10 Deverá prover suporte a Fast Roaming;

3.11.11 Possuir Captive Portal por SSID;

3.11.12 Permitir configurar o bloqueio de tráfego entre SSIDs;

3.11.13 Deverá suportar Wi-Fi Protected Access (WPA) e WPA2 por SSID, utilizando-se de AES e/ou TKIP;

3.11.14 Deverá suportar 802.1x através de RADIUS na controladora wireless;

3.11.15 Permitir configurar parâmetros de rádio, como banda e canal, na controladora wireless;

3.11.16 Possuir método de descoberta de novos Pontos de Acesso baseados em Broadcast ou Multicast;

3.11.17 Possuir lista contendo Pontos de Acesso Aceitos e Pontos de Acesso Indevidos (Rogue);

3.11.18 Possuir proteção contra-ataques do tipo ARP Poisoning na controladora wireless;

3.11.19 Implementar Protected Management Frames de acordo com norma WiFi alliance para 802.11ac;

3.11.20 Possuir WIDS integrado com detecção de ataques de Broadcast De-authentication;

3.11.21 Possuir WIDS integrado com detecção de ataques de Spoofed De-authentication;

3.11.22 Possuir WIDS integrado com detecção de senha WEP fraca;

3.11.23 Possuir WIDS integrado com detecção de bridge wireless;

3.11.24 Implementar provisionamento automático de canais dos Access Points, de forma a minimizar interferência entre eles;

3.11.25 Permitir definir em quais horários determinados SSID estará disponível;

3.11.26 A controladora wireless deverá oferecer mecanismos de segurança e controle de acesso integrado, baseado em identidade do usuário;

3.11.27 Possibilitar definir número máximo de clientes permitidos por SSID;

3.11.28 Deve permitir criar, gerenciar e disponibilizar redes wireless mesh;

3.11.29 Possuir mecanismo de criação automática de usuários visitantes e senhas auto-geradas e/ou manual, que possam ser enviadas por email ou SMS aos usuários, e com capacidade de definição de horário da expiração da senha;

3.11.30 A comunicação entre o Access Point e a controladora wireless deve poder ser efetuada de forma criptografada;

3.11.31 Deve possuir mecanismo de ajuste de potência do sinal de forma a reduzir interferência entre canais entre dois access points gerenciados;

3.11.32 Possuir mecanismo de balanceamento de tráfego/usuários entre Access Points;

3.11.33 Possuir mecanismo de balanceamento de tráfego/usuários entre frequências e/ou radios dos Access Points;

3.11.34 Deve permitir a identificação do firmware utilizado por cada Access Point gerenciado e permitir o upgrade via interface gráfica;

3.11.35 Permitir que sejam desabilitados clientes wireless que possuam taxa de transmissão baixa;

3.11.36 Permitir bloquear clientes wireless que tenham sinal fraco, definindo um valor do sinal a partir do qual tais clientes serão ignorados;

3.11.37 Deve permitir suprimir Rogue APs detectados;

3.11.38 Deve permitir configurar o valor de Short Guard Interval para 802.11n e 802.11ac em 5GHz;

3.11.39 Deve permitir selecionar individualmente em cada Access Point quais os SSIDs que serão propagados;

3.11.40 Deve permitir bloquear tráfego interno entre usuários de um mesmo SSID;

3.11.41 Deve permitir associação dinâmica de VLANs aos usuários autenticados via RADIUS num SSID;

3.11.42 Deve indicar graficamente os dispositivos conectados em cada SSID, assim como a quantidade de banda consumida, tempo de conexão e login;

3.11.43 Deve permitir visualizar as aplicações e ameaças por dispositivo wireless;

3.11.44 Havendo licença para controle de aplicação, tal feature deve ser atualizada de forma automática;

3.11.45 Com a devida licença, a controladora deve dispor de, no mínimo, 1027 aplicações para reconhecimento do tráfego;

3.11.46 A controladora wireless deve possuir interface de gerência embarcada no próprio equipamento;

3.11.47 Prover autenticação através de TACACS+.

**4 DAS ESPECIFICAÇÕES TÉCNICAS – ITEM 02**

4.1.1 Deve possuir a capacidade de registrar até 500 eventos de log por segundo;

4.1.2 Deve possuir, no mínimo, 2x RJ45 GE interfaces Gigabit Ethernet;

4.1.3 Deve possuir disco interno de 4TB (2x 2TB), no mínimo;

4.1.4 Suportar log remoto no formato syslog;

4.1.5 O appliance deve poder funcionar como sistema de disco de rede (NFS - Network File System e Windows Network), com controle de permissões e cotas de utilização pelos dispositivos gerenciados;

4.1.6 Quanto ao armazenamento de dados de segurança:

4.1.7 Deve ser capaz de receber logs de pelo menos 50 dispositivos;

4.1.8 Possuir a visualização de log em tempo real de tráfegos de rede;

4.1.9 Permitir a visualização de logs de histórico dos acessos de tráfegos de rede;

4.1.10 Permitir a visualização dos eventos de auditoria;

4.1.11 Permitir realização de backup e restauração dos dados;

4.1.12 Permitir o envio dos logs a outro centralizador de log externo a solução;

4.1.13 Atuar como um NAS (Network Attached Storage).

4.1.14 Quanto aos relatórios - Possuir pelo menos 20 tipos de relatórios pré-definidos na solução;

4.1.15 Permitir geração de relatórios agendados ou sob demanda nos formatos HTML e PDF;

4.1.16 Permitir o envio dos relatórios, conforme item anterior, através de e-mail para usuários pré-definidos;

4.1.17 Disponibilizar relatórios através de FTP;

4.1.18 Possuir relatórios de acessos autorizados demonstrando a quantidade de acessos autorizados, bem como, a quantidade de bytes trafegados, sendo possível sua visualização detalhada por, IP de origem, URL acessada;

4.1.19 Possuir relatório de utilização da internet por protocolo;

4.1.20 Possuir relatório dos 10 (dez) sites web mais acessados;

4.1.21 Possuir relatório das 10 (dez) categorias de sites web mais acessados;

4.1.22 Possuir relatório dos 10 (dez) usuários mais ativos;

4.1.23 Permitir customização dos relatórios, incluindo logotipo da CONTRATANTE;

4.1.24 Possuir relatórios pre-configurados para os seguintes tipos:

4.1.25 Máquinas mais acessadas;

4.1.26 Serviços mais utilizados;

4.1.27 Usuários que mais utilizaram serviços;

4.1.28 URLs mais visualizadas;

4.1.29 Categorias Web mais acessadas;

4.1.30 Maiores emissores e receptores de e-mail.

4.1.31 O equipamento deve ser capaz de analisar e monitorar pelo menos 2.500 vulnerabilidades distintas dos principais ativos de rede;

4.1.32 O equipamento deve ser capaz de detectar as máquinas existentes na rede para que sejam realizados os testes de vulnerabilidade.

4.1.33 A detecção de grupos de máquinas dever ser possível por faixa de IP ou por nome de domínio, usando protocolos ICMP, DNS, Traceroute e portas UDP/TCP;

4.1.34 O appliance deve ser entregue em formato Desktop ou Rackmount.

4.1.35 Devem ser analisadas vulnerabilidades de sistemas operacionais, servidores e aplicações web, servidores ftp e de e-mail, no mínimo;

4.1.36 Deve ser possível selecionar os tipos de vulnerabilidades que se pretende analisar;

4.1.37 Deve ser possível agendar as verificações de vulnerabilidade nos ativos de rede e gerar relatórios por nível de severidade das vulnerabilidades;

4.1.38 O equipamento deve prover ferramenta de análise de tráfego de rede que permita ao administrador otimizar as regras de proteção da rede;

4.1.39 O sistema deve apresentar o log de atividade na rede em tempo real e também o histórico de tráfego;

4.1.40 O sistema deve permitir a filtragem dos logs para que sejam apresentadas as entradas que atendem ou não as condições estabelecidas pelo administrador;

4.1.41 O sistema deve permitir a realização de buscas nos logs baseado em filtros estabelecidos pelo administrador;

4.1.42 Deve incluir toda e qualquer licença de software necessária;

**5 CONDIÇÕES DO FORNECIMENTO**

5.1 A CONTRATADA deverá entregar, às suas expensas, todos os itens acessórios de hardware necessários à perfeita instalação e funcionamento dos equipamentos, incluindo conectores, cabos, suportes e demais itens necessários para instalação e funcionamento da solução contratada, em plena compatibilidade com as especificações constantes neste Termo de Referência e recomendadas pelo fabricante.

5.2 Todos os equipamentos fornecidos e seus componentes deverão ser novos, de primeiro uso e devem estar acondicionados adequadamente em caixa original lacrados de fábrica, de forma a propiciar completa segurança durante e transporte.

5.3 Toda a solução e suas implantações serão supervisionadas pela PGE Pública.

5.4 A CONTRATADA será responsável por projetar, instalar, configurar e dar suporte na solução ofertada durante todo o período de licenciamento e garantia das licenças.

5.5 A implementação das políticas de segurança será de responsabilidade exclusiva da CONTRATADA mediante determinações da CONTRATANTE.

**6 DA GARANTIA E DA ASSISTÊNCIA TÉCNICA**

6.1 Todos os componentes de hardware e software, deverão possuir garantia de, no mínimo, 36 (trinta e seis) meses, com suporte técnico de 8 (oito) horas por dia, 5 (cinco) dias por semana, na cidade de Salvador (BA). Ressalta-se que esta contração pela natureza do escopo é de praxe no mercado utilizar garantia de 36 meses, uma vez que envolve melhor custo benefício com os fabricante em relação as renovações de licenças.

6.2 O serviço deverá ser prestado por profissional de nível superior, devidamente certificado nas soluções tecnológicas utilizadas na prestação dos serviços contratados.

6.3 Durante o período de execução dos serviços, a CONTRATADA deverá garantir o funcionamento do software, com suporte técnico do FABRICANTE prestado em caso de falha.

6.4 Deverá ser garantida, neste prazo, a atualização de versões, releases, componentes (bibliotecas, filtros, dentre outros) e módulos dos softwares e equipamentos utilizados na prestação dos serviços.

**7 SUPORTE TÉCNICO E ACORDO DE NÍVEL DE SERVIÇO**

7.1 Atender às necessidades da PGE/BA para suporte técnico da Solução de Segurança da Informação, com o objetivo de proteger a rede corporativa e aumentar o nível de conformidade com a política de segurança.

7.2 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.

7.3 O suporte técnico ao produto fornecido deverá ser 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;

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

7.5 Deverão ser executados pela empresa CONTRATADA serviços de Instalação e configuração

para uso da solução CONTRATADA com supervisão da equipe técnica da PGE/BA;

7.6 Deverá ser executada pela empresa CONTRATADA uma análise da situação atual e elaborar, em conjunto com a equipe interna da PGE/BA, 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;

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

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

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

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

7.11 A empresa CONTRATADA deverá realizar duas avaliações on-site durante o período de vigência do contrato, perante solicitação da CONTRATANTE, do ambiente da PGE/BA, 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/BA;

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

7.13 Caberá a PGE/BA 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 6;

7.14 O suporte técnico deverá ser prestado nas seguintes formas:

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

7.14.2 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/BA. Neste caso a CONTRATADA deve possuir plantão de 8 (oito) horas por dia, 5 (cinco) dias por semana, para este tipo de atendimento;

7.15 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;

7.16 O encaminhamento de chamados deverá ser efetuado pelos técnicos responsáveis no prazo máximo conforme os níveis de severidade indicados no item 6. Após este prazo, em

caso de não solução, a CONTRATADA deverá acionar o atendimento, no local designado pela PGE/BA, de acordo com o nível de serviço acordado. O suporte prestado pela empresa terá chamados ilimitados;

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

7.18 A CONTRATADA deverá responder aos acionamentos, dentro dos prazos fixados no item 6, a partir da abertura do acionamento;

7.19 O término do atendimento deverá ocorrer dentro dos prazos fixados no item 6, a partir do contato do técnico da CONTRATADA, responsável pelo atendimento;

7.20 Entende-se por início do atendimento a hora do contato do técnico de suporte da CONTRATADA com a equipe da CONTRATANTE;

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

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

7.23 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;

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

7.25 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;

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

7.27 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.

7.28 Comprovação de Garantia: para assegurar a esta Instituição a garantia total solicitada e demais condições exigidas, será necessário comprovar por meio de documentação do FABRICANTE específica para este Processo licitatório, anexada à proposta comercial, que o equipamento ofertado terá garantia, mínima, de 5 (cinco) anos e tempo de atendimento exigidos no Edital.

**8 ACORDO DE NÍVEL DE SERVIÇO (ANS)**

8.1 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;

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

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

8.4 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.

8.5 A CONTRATADA deverá fazer análises dos chamados e enviar recomendações de possíveis treinamentos, necessários ao desenvolvimento da equipe, sem ônus para a CONTRATANTE.

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

8.7 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.

8.8 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;

8.9 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.

8.10 Níveis de Serviço e Tempo Esperados:

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

8.10.2 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.

8.10.3 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 |

8.10.4 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 Coordenação de Tecnologia da Informação e Comunicação – CTIC da PGE;

8.11 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.

8.12 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;

8.13 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;

8.14 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.

8.15 A CONTRATADA deverá ainda realizar os seguintes suportes proativos:

8.15.1 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.

8.15.2 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.

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

**9 CRITÉRIOS OBRIGATÓRIOS**

9.1 Atendimento da Assistência Técnica: Prazo de 36 (trinta e seis) meses com manutenção on-site fornecido pelo fabricante do equipamento em Salvador;

9.2 A empresa licitante deverá atender a todos os requisitos mínimos exigidos, e no caso da não comprovação acarretará na sua desclassificação.

9.3 Todo suporte deve ser prestado por técnicos certificados pelo fabricante.

9.4 A empresa proponente deverá apresentar obrigatoriamente, comprovação de que possui em seu quadro técnico no mínimo um profissional com a certificação técnica do fabricante no Lote em que ela for lograda vencedora.

9.5 A licitante deverá apresentar os certificados dos técnicos e comprovação de vínculo destes com a empresa.

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

9.7 As propostas deverão prever e especificar o período de garantia mínimo de 36 (trinta e seis) com atendimento ON-SITE em até 4 horas.

9.8 A Empresa licitante deve apresentar declaração de que dispõe de mão-de-obra adequada e disponível, local, para execução dos serviços.

9.9 A Empresa licitante, não poderá transferir a outrem os compromissos assumidos, no todo ou em parte, os serviços.

9.10 O não cumprimento destes requisitos implicará na desclassificação imediata da licitante.

9.11 Deverá ser apresentado prospecto com as características técnicas de todos os

componentes do equipamento, incluindo especificação de marca, modelo, e outros elementos que de forma inequívoca identifiquem e comprovem as configurações cotadas, possíveis expansões e upgrades, através de certificados, manuais técnicos, folders e demais literaturas técnicas editadas pelos fabricantes. Serão aceitas cópias das especificações obtidas em sítios dos fabricantes na Internet, em que constem o respectivo endereço eletrônico. O licitante deverá informar exatamente o Marca e modelo dos equipamentos e Software ofertado e os catálogos devem obrigatoriamente ser públicos, ou seja, devem estar publicados no website do fabricante.

**10 DA VISTORIA**

10.1 As licitantes que dispensarem a realização da visita técnica deverão apresentar, junto com os documentos de habilitação, sob pena de inabilitação, declaração formal de que estão cientes das condições para o cumprimento das obrigações objeto da licitação, não podendo se eximir, posteriormente, das obrigações assumidas ou reivindicar qualquer alteração contratual sob o argumento de desconhecer as peculiaridades do objeto.

10.2 Responsável pelo agendamento de visita técnica: Servidor responsável: Maurício de Cerqueira Pereira Telefone: (71) 3115-0431

Endereço: 3a Avenida, no 370 - Centro Administrativo da Bahia, CEP 41.745-005 - Salvador - Bahia Horário: : 9h às 16 h E-mail: mauricio.pereira@pge.ba.gov.br3 A vistoria será acompanhada por profissional designado pela PGE-BA.

10.3 As LICITANTES poderão realizar uma visita técnica, se assim optar, sendo propiciado o exame, a conferência e a constatação prévia de todos os detalhes e características técnicas do objeto, para que o mesmo tome conhecimento de tudo aquilo que possa, de alguma forma, influir sobre o custo, preparação da proposta e execução do objeto;

10.4 Entre outros aspectos, poderão verificar as instalações, normas, padrões, metodologias e configurações do ambiente de tecnologia da informação e comunicação da PGE e demais detalhes necessários à execução dos serviços;

10.5 Para realizar a vistoria, os representantes deverão apresentar documento comprovando estar credenciado pela empresa interessada;

10.6 O agendamento de visita poderá ocorrer até 48 (quarenta e oito) horas antes da data e horário de abertura do processo licitatório;

10.7 O atestado de visita técnica (Declaração de Ciência dos Requisitos Técnicos – edital) deverá ser assinado pelo representante da PGE, comprovando que a empresa realizou a vistoria técnica para conhecimento dos serviços necessários, do ambiente tecnológico da PGE e das condições técnicas para sua realização.

**11 DOCUMENTAÇÃO TÉCNICA**

11.1 A empresa deverá apresentar as seguintes documentações dos produtos:

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

11.1.2 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.

11.2 A CONTRATADA deverá apresentar juntamente com a documentações dos produtos, certificado ou título, concedido pelo fabricante, que comprove o credenciamento da CONTRATADA como representante autorizada;

11.3 A CONTRATADA deverá apresentar juntamente com as documentações dos produtos, as licenças dos produtos fornecidos necessários para a implantação e as mídias de instalação com toda documentação acessórias relativas aos produtos fornecidos.

**12 FORMA DE PAGAMENTO**

12.1 O pagamento referente ao itens supracitados deste documento (serviço de suporte técnico, implantação, manutenção e atualização) será realizado em 36 (trinta e seis) parcelas mensais e de igual valor, devendo a fatura referente à primeira parcela ser emitida 10 (dez) dias após a entrega da solução e conclusão dos serviços de instalação e treinamento, de acordo com as especificações deste Termo de Referência;

**13 TESTE E VERIFICAÇÃO PRELIMINAR**

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;

13.1 O processo de realização dos testes de verificação preliminar do software será desenvolvido de acordo com os eventos e atividades descritos a seguir:

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

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

13.4 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;

13.5 A verificação preliminar não implica em recebimento definitivo do software fornecido;

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

**14 PRAZO DE ENTREGA**

14.1 Os equipamentos deverão ser entregues no prazo máximo de 60 (sessenta) dias contados da assinatura da Autorização de Material de Serviço – AFM.

**15 ACEITE E INSTALAÇÃO**

15.1 O aceite do produto será feito pela PGE/BA, após a implantação e entrada em operação

das licenças fornecido;

15.2 A entrega e instalação das licenças será feita de acordo com plano de implantação, apresentado pela CONTRATADA e aprovado pela CONTRATANTE;

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

15.4 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.

**16 LOCAL DE EXECUÇÃO DOS SERVIÇOS**

16.1 3a Avenida Centro Administrativo da Bahia, 370 - Centro Administrativo da Bahia, Salvador - BA, 41745-005.

**17 UTILIZAÇÃO DE SOFTWARES**

17.1 A CONTRATADA entregará a CONTRATANTE toda e qualquer documentação gerada em função da prestação de serviços decorrente deste Termo de Referência.

17.2 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. 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.

17.3 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.

**18 PROPRIEDADE INTELECTUAL**

18.1 A CONTRATADA entregará a CONTRATANTE toda e qualquer documentação gerada em função da prestação de serviços decorrente deste Termo de Referência.

18.2 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. 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.

18.3 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.

**19 PRAZO DE VIGÊNCIA**

19.1 O prazo de contratação do objeto deste Termo de Referência será de 36 (trinta e seis) meses, contados a partir da publicação da assinatura do contrato.

**20 ANEXOS**

| | |
|---|---|
| ANEXO I | TERMO DE COMPROMISSO, SIGILO E CONFIDENCIALIDADE |
| ANEXO II | DECLARAÇÃO DE VISTORIA |
| ANEXO III | PROPOSTA DE PREÇOS |

**ANEXO I**

**TERMO DE COMPROMISSO, SIGILO E CONFIDENCIALIDADE**

Os abaixo-assinados, de um lado a _____, CNPJ nº _____/_____, situada na cidade de _____, à Rua: _____, bairro _____, doravante denominada CONTRATANTE, e de outro lado _____, CNPJ nº _____/_____, situada na cidade de _____, à Rua: _____, bairro _____, doravante denominada CONTRATADA, tem entre si justa e acertada, a celebração do presente TERMO DE COMPROMISSO, SIGILO E CONFIDENCIALIDADE, através do qual a CONTRATADA aceita não divulgar sem autorização prévia e formal segredos e informações sensíveis de propriedade da _____ e se compromete a praticar procedimentos de segurança da informação, em conformidade com as seguintes cláusulas e condições:

PRIMEIRA – A CONTRATADA reconhece que em razão das suas atividades profissionais, estabelece contato com informações sigilosas, que devem ser entendidas como segredo. Estas informações devem ser tratadas confidencialmente sob qualquer condição e não podem ser divulgadas a terceiros não autorizados, aí se incluindo os próprios Colaboradores da _____, sem a expressa e escrita autorização da _____.

SEGUNDA - As informações, exemplificadas abaixo, devem receber o tratamento de confidencialidade adequado, de acordo com o seu nível de classificação.

1. Programas de computador, suas listagens, documentação, artefatos diversos, código fonte e código objeto;

2. Toda a informação relacionada a programas existentes ou em fase de desenvolvimento no âmbito da, inclusive fluxogramas, estatísticas, especificações, avaliações, resultados de testes, arquivos de dados, artefatos diversos e versões “beta” de quaisquer programas;

3. Documentos, informações e dados armazenados de atuação consultiva e contenciosa, de estratégias ou demais dados e/ou informações de caráter sigiloso ou restrito à ;

4. Metodologia, projetos e serviços utilizados;

5. Números e valores financeiros.

TERCEIRA – A CONTRATADA reconhece que a lista acima é meramente exemplificativa e ilustrativa e que outras hipóteses de confidencialidade que já existam ou que venham a surgir no futuro devem ser mantidas sob segredo. Em caso de dúvida acerca da confidencialidade de determinada informação a CONTRATADA deve tratar a mesma sob sigilo até que seja autorizado, formalmente, a tratá-la de forma diferente pela CONTRATANTE.

QUARTA – A CONTRATADA reconhece que, no seu desligamento definitivo da _____, deverá entregar à CONTRATANTE todo e qualquer material de propriedade desta, inclusive notas pessoais envolvendo matérias sigilosas relacionadas com a _____, registros de documentos de qualquer natureza que tenham sido usados, criados ou estado sob seu controle. A CONTRATADA também assume o compromisso de não utilizar qualquer informação adquirida quando de suas atividades para a _____.

QUINTA – A CONTRATADA deve assegurar que todos os seus colaboradores guardarão sigilo sobre as informações que porventura tiverem acesso, mediante o ciente de seus colaboradores em Termo próprio a ser firmado entre a CONTRATADA e seus colaboradores, e que os mesmos comprometer-se-ão a informar, imediatamente, ao seu superior hierárquico, qualquer violação das regras de sigilo, por parte dele ou de qualquer pessoa, inclusive nos casos de violação não intencional.

Parágrafo Primeiro: A coleta dos Termos de Sigilo de seus colaboradores não exime a CONTRATADA das penalidades por violação das regras por parte de seus contratados.

Parágrafo Segundo: A CONTRATADA deverá fornecer cópia de todos os termos firmados com seus colaboradores à _____ no prazo de 10 dias após assinatura dos respectivos termos.

Parágrafo Terceiro: Sempre que um colaborador for admitido, A CONTRATADA deverá fornecer cópia dos novos termos firmados no prazo de 2 dias após assinatura dos respectivos termos.

SEXTA - O atendimento deste TERMO DE COMPROMISSO, SIGILO E CONFIDENCIALIDADE, bem como da das Diretrizes Básicas da Política de Segurança da Informação devem ser incorporados formalmente ao contrato de trabalho dos funcionários da CONTRATADA que prestarem serviços à _____.

SÉTIMA – A CONTRATADA deverá seguir a Política de Segurança da Informação definida pela CONTRATANTE.

OITAVA - O não cumprimento de quaisquer das cláusulas deste Termo implicará em responsabilização civil e criminal, de acordo com a legislação vigente.

Em, _____de _____de 20___.

_____

Responsável pelo Contrato - CONTRATANTE

_____

Responsável pelo Contrato - CONTRATADA

**ANEXO II**

**Declaração de Vistoria Expedida pela PGE/BA**

**OBSERVAÇÕES SOBRE A VISITA TÉCNICA**

Fica facultado as empresas licitantes a realização de visita técnica, para conhecer as instalações e condições para prestação dos serviços, saneando quaisquer dúvidas em relação ao processo de contratação dos serviços.

A visita deverá ser agendada previamente, com no mínimo 24 (vinte e quatro) horas de antecedência, junto à **Coordenação de Tecnologia da Informação e Comunicação - CTIC**, pelos telefone (71) 3115-0546.

A visita somente poderá ser realizada nos horários das 8:30h às 17:00h, em dias de expediente regular, no prazo de até 72 (setenta e duas) horas antes da licitação.

A visita deverá ser realizada por profissional pertencente ao quadro funcional ou sócio da licitante, portador de diploma de nível superior em informática, cuja comprovação deverá ocorrer no momento da realização da visita técnica, mediante carta de apresentação assinada pelo representante legal da empresa, constando as informações inerentes às qualificações exigidas. As informações apresentadas são de inteira responsabilidade da licitante.

DECLARAÇÃO DE VISTORIA EXPEDIDA PELA ADMINISTRAÇÃO

Atesto que o responsável técnico da _____ (indicar nome da Pessoa Jurídica licitante), CNPJ nº_____ (indicar CNPJ da licitante), Sr.(a) _____, CPF nº _____, interessado em participar da _____ (indicar modalidade de licitação: pregão/concorrência/tomada de preço/convite) nº _____, vistoriou _____ (indicar a Unidade Administrativa vistoriada) e tomou ciência do estado das condições locais para o cumprimento das obrigações relativas ao objeto licitado.

Salvador _____de _____ de 2021.

_____

(assinatura, identificação do servidor público e respectivo cadastro).

**ANEXO III – PREÇO MÉDIO**

| | | | | | |
|---|---|---|---|---|---|
| | | | | **VALOR UNITÁRIO** | **VALOR** |

| ITEM | DESCRIÇÃO | UNIDADE | QUANTIDADE | UNITÁRIO MENSAL (R$) | GLOBAL (R$) |
|---|---|---|---|---|---|
| 1 | Contratação de serviços de empresa especializada para o fornecimento de 02 (dois) Firewalls UTM, incluindo serviços de instalação, garantia e suporte por 36 meses. | MÊS | 36 | R$ | R$ |
| 2 | Contratação de serviços de empresa especializada para o fornecimento de 01 (um) Appliance de monitoramento, log e relatoria, incluindo serviços de instalação, garantia e suporte por 36 meses. | MÊS | 36 | R$ | R$ |

Documento assinado eletronicamente por **Mauricio de Cerqueira Pereira**, **Coordenador Técnico**, em 23/09/2021, às 11:08, 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 **00036219028** e o código CRC **7D63BEC1**.

**Referência:** Processo nº 006.0409.2021.0029638-21 SEI nº 00036219028



**ANEXO II**

# PROPOSTA COMERCIAL FORTINET – V 1.1 (Ajustada)

S·I·T·E

CONSULTORIA E TECNOLOGIA

Responsável:

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

FORTINET

28/12/2021

## *A PROCURADORIA GERAL DO ESTADO – PGE / BA*

**Att: Comissão de Licitação**

**REF: Proposta de fornecimento para serviços e soluções de Segurança da Informação, objetivando ampliar a segurança da rede e dos ativos da Procuradoria Geral do Estado da Bahia – PGE/BA, composta por: 02 (dois) Firewalls UTM em modo Alta-Disponibilidade (HA) do Fabricante Fortinet, marca/modelo: FortiGate 201F, assim como 01 (um) appliance de log e monitoramento, do Fabricante Fortinet, marca/modelo: FortiAnalyzer FAZ-150G, com garantia de 36 (trinta e seis) meses, serviço de instalação configuração e suporte on-site – Pregão Eletrônico n.º 10/2021 e Processo Administrativo n.º 006.0409.2021.0029638-21, conforme edital e seus respectivos anexos e Termo de referência.**

### APRESENTAÇÃO DA EMPRESA

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

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

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

### DOS PRODUTOS E SERVIÇOS

Fornecimento para serviços e soluções de Segurança da Informação, objetivando ampliar a segurança da rede e dos ativos da Procuradoria Geral do Estado da Bahia – PGE/BA, composta por: 02 (dois) Firewalls UTM em modo Alta-Disponibilidade (HA) do Fabricante Fortinet, marca/modelo: FortiGate 201F, assim como 01 (um) appliance de log e monitoramento, do Fabricante Fortinet, marca/modelo: FortiAnalyzer FAZ-150G, com garantia de 36 (trinta e seis) meses, serviço de instalação configuração e suporte on-site.

### DA FORTINET

A Fortinet é uma empresa fornecedora mundial de equipamentos de segurança de rede e líder de mercado no gerenciamento unificado de ameaças (UTM).

Seus produtos e serviços de assinaturas fornecem ampla, integrada e de alto desempenho contra ameaças de segurança dinâmica, simplificando a infraestrutura de segurança de TI.

Seus clientes incluem empresas, prestadores de serviços e entidades governamentais em todo o mundo. Principal produto da Fortinet's, FortiGate proporciona desempenho com acelerador ASIC e integra várias camadas de segurança projetadas para ajudar a proteger contra ameaças de aplicação e de rede, empregando tecnologias inovadoras para a segurança de redes e análise de conteúdo.

Os sistemas da Fortinet integram um amplo conjunto da indústria de tecnologias de segurança, incluindo firewall, VPN, antivírus, prevenção de intrusão (IPS), filtro de web, AntiSpam e traffic shaping, que pode ser implantado individualmente, para complementar as soluções legadas ou combinados para uma solução abrangente de



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

# Proposta Comercial

## *A PROCURADORIA GERAL DO ESTADO – PGE / BA*

**Att: Comissão de Licitação**

**REF: Proposta de fornecimento para serviços e soluções de Segurança da Informação, objetivando ampliar a segurança da rede e dos ativos da Procuradoria Geral do Estado da Bahia – PGE/BA, composta por: 02 (dois) Firewalls UTM em modo Alta-Disponibilidade (HA) do Fabricante Fortinet, marca/modelo: FortiGate 201F, assim como 01 (um) appliance de log e monitoramento, do Fabricante Fortinet, marca/modelo: FortiAnalyzer FAZ-150G, com garantia de 36 (trinta e seis) meses, serviço de instalação configuração e suporte on-site – Pregão Eletrônico n.º 10/2021 e Processo Administrativo n.º 006.0409.2021.0029638-21, conforme edital e seus respectivos anexos e Termo de referência.**

### APRESENTAÇÃO DA EMPRESA

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

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

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

### DOS PRODUTOS E SERVIÇOS

Fornecimento para serviços e soluções de Segurança da Informação, objetivando ampliar a segurança da rede e dos ativos da Procuradoria Geral do Estado da Bahia – PGE/BA, composta por: 02 (dois) Firewalls UTM em modo Alta-Disponibilidade (HA) do Fabricante Fortinet, marca/modelo: FortiGate 201F, assim como 01 (um) appliance de log e monitoramento, do Fabricante Fortinet, marca/modelo: FortiAnalyzer FAZ-150G, com garantia de 36 (trinta e seis) meses, serviço de instalação configuração e suporte on-site.

### DA FORTINET

A Fortinet é uma empresa fornecedora mundial de equipamentos de segurança de rede e líder de mercado no gerenciamento unificado de ameaças (UTM).

Seus produtos e serviços de assinaturas fornecem ampla, integrada e de alto desempenho contra ameaças de segurança dinâmica, simplificando a infraestrutura de segurança de TI.

Seus clientes incluem empresas, prestadores de serviços e entidades governamentais em todo o mundo. Principal produto da Fortinet's, FortiGate proporciona desempenho com acelerador ASIC e integra várias camadas de segurança projetadas para ajudar a proteger contra ameaças de aplicação e de rede, empregando tecnologias inovadoras para a segurança de redes e análise de conteúdo.

Os sistemas da Fortinet integram um amplo conjunto da indústria de tecnologias de segurança, incluindo firewall, VPN, antivírus, prevenção de intrusão (IPS), filtro de web, AntiSpam e traffic shaping, que pode ser implantado individualmente, para complementar as soluções legadas ou combinados para uma solução abrangente de



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

gerenciamento de ameaças.

Hoje a Fortinet, possui mais de 500.000 appliances e mais de 75.000 clientes espalhados por todo o mundo. Incluindo:

07 (sete) das 10(dez) maiores empresas da América
09 (nove) das 10(dez) maiores empresas de telecomunicações
09 (nove) das 10(dez) maiores empresas bancárias;
07 (sete) das 10(dez) maiores empresas de aviação;

A empresa complementa essas soluções com uma matriz de gestão, análise de e-mail, banco de dados e produtos de segurança de Endpoints.

A Fortinet possui sede em Sunnyvale, Califórnia, com parceiros por todo o mundo.
Reconhecimentos da empresa:

- ✓ Líder mundial em UTM (IDC; Frost & Sullivan);
- ✓ Uma das Top 04 (quatro) Network Security Appliance Vendedores WW (IDC);
- ✓ Classificado Tier 1 Enterprise Security Vendor (Current Analysis);
- ✓ Líder no Gartner Multi-Function Firewall Magic Quadrant.
- ✓ Classificado "Top Player" em Email Security Appliance Quadrant.
- ✓ Certificado ISO 9001:2000 para a Norma de qualidade Sistemas de Gestão;

## SUPORTE TÉCNICO E ACORDO DE NÍVEL DE SERVIÇO

Atender às necessidades da PGE/BA para suporte técnico da Solução de Segurança da Informação, com o objetivo de proteger a rede corporativa e aumentar o nível de conformidade com a política de segurança.

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.

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

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

Serão executados pela XSITE serviços de Instalação e configuração para uso da solução XSITE com supervisão da equipe técnica da PGE/BA;

Será executada pela XSITE uma análise da situação atual e elaborar, em conjunto com a equipe interna da PGE/BA, um plano de otimização de recursos, rotinas, procedimentos e processos para o novo ambiente de segurança. Essa documentação será entregue, pela XSITE, em formato digital, em no máximo 30 (trinta) dias consecutivos, a contar da data da entrega das licenças.

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

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

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



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

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

A XSITE realizará duas avaliações on-site durante o período de vigência do contrato, perante solicitação da CONTRATANTE, do ambiente da PGE/BA, 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/BA;

Todo suporte será prestado por técnicos certificados pelo fabricante;

Caberá a PGE/BA requisitar o suporte técnico, ficando a XSITE obrigada a realizá-lo, de acordo com o nível de severidade e nos prazos máximos assim definidos no item 3.1;

O suporte técnico será prestado nas seguintes formas:

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

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

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

O encaminhamento de chamados será efetuado pelos técnicos responsáveis no prazo máximo conforme os níveis de severidade indicados no item 6. Após este prazo, em caso de não solução, a XSITE acionará o atendimento, no local designado pela PGE/BA, de acordo com o nível de serviço acordado. O suporte prestado pela empresa terá chamados ilimitados;

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

A XSITE responderá aos acionamentos, dentro dos prazos fixados no item 3.1, a partir da abertura do acionamento;

O término do atendimento ocorrerá dentro dos prazos fixados no item 3.1, a partir do contato do técnico da XSITE, responsável pelo atendimento;

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

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

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

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

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



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

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

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

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

Comprovação de Garantia: para assegurar a esta Instituição a garantia total solicitada e demais condições exigidas, comprovamos por meio de documentação da Fortinet (ANEXO I) específica para este Processo licitatório, anexada à proposta comercial, que o equipamento ofertado terá garantia, mínima, de 5 (cinco) anos e tempo de atendimento exigidos no Edital.

## ACORDO DE NÍVEL DE SERVIÇOS (ANS)

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

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

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

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

A XSITE fará análises dos chamados e enviar recomendações de possíveis treinamentos, necessários ao desenvolvimento da equipe, sem ônus para a CONTRATANTE.

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

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

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

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

**Níveis de Serviço e Tempo Esperados:**

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

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



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

segurança e à performance do software e do ambiente; atualização simultânea nos ambientes dos órgãos e entidades da CONTRATANTE.

Para efeito dos atendimentos técnicos, a XSITE observará os níveis de severidade e respectivos prazos máximos fixados no edital.

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

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.

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

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

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

A XSITE realizará os seguintes suportes proativos:

- Duas avaliações on-site por ano do ambiente da CONTRATANTE, mediante verificação de instalações e configurações de toda a solução, adequando-as às melhores práticas de segurança, essa atividade deve gerar relatório para posterior melhoria pela equipe da CONTRATANTE.
- Uma avaliação on-site por ano do ambiente da CONTRATANTE, mediante verificação de instalações e configurações de toda a solução de gerência centralizada, adequando-as às melhores práticas de segurança, essa atividade deve gerar relatório para posterior melhoria pela equipe da CONTRATANTE.
- Quatro visitas técnicas on-site durante o ano de profissionais certificados pelo fabricante para apoiar nas implementações e nos controles gerados pelas ações proativas.

## CRITÉRIOS OBRIGATÓRIOS

Atendimento da Assistência Técnica: Prazo de 36 (trinta e seis) meses com manutenção on-site fornecido pelo fabricante do equipamento em Salvador;

A XSITE atende a todos os requisitos mínimos exigidos, e no caso da não comprovação acarretará na sua desclassificação.

Todo suporte será prestado por técnicos certificados pelo fabricante.

A XSITE apresentará declaração de que dispõe de mão-de-obra adequada e disponível, local, para execução dos serviços.

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

O não cumprimento destes requisitos implicará na desclassificação imediata da licitante.

## ACEITE E INSTALAÇÃO

O aceite do produto será feito pela PGE/BA, após a implantação e entrada em operação das licenças fornecido;



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

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

A instalação seguirá cronograma previsto no plano de implantação;

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

## LOCAL DE EXECUÇÃO DOS SERVIÇOS

A prestação dos serviços ocorrerá na sede da PGE situada na 3ª Avenida Centro Administrativo da Bahia, nº 370. Salvador/BA. CEP: 41745-005.

## UTILIZAÇÃO DE SOFTWARES

A XSITE entregará a CONTRATANTE toda e qualquer documentação gerada em função da prestação de serviços decorrente deste Termo de Referência.

A XSITE 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. 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.

A XSITE 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.

## PROPRIEDADE INTELECTUAL

A XSITE entregará a CONTRATANTE toda e qualquer documentação gerada em função da prestação de serviços decorrente deste Termo de Referência.

A XSITE 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. 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.

A XSITE 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.

## DA CONFIDENCIALIDADE

A XSITE será expressamente responsabilizada quanto à manutenção de sigilo absoluto sobre quaisquer dados, informações, artefatos, contidos em quaisquer documentos e em quaisquer mídias, de que venha a ter conhecimento durante a execução dos trabalhos, não podendo, sob qualquer pretexto divulgar, reproduzir ou utilizar, sob pena de sanções legais, independentemente da classificação de sigilo conferida pela PGE a tais documentos, mesmo após a conclusão do vínculo contratual. Será mantido em rigoroso sigilo e confidencialidade das informações, e não divulgará a qualquer terceiro, por quaisquer meios, qualquer informação, documento e material produzido a que tiver ou venha a ter acesso durante a vigência deste contrato, e em razão do serviço objeto do presente contrato, que não seja conhecida do público em geral;



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

A XSITE não divulgará quaisquer informações a que tenha acesso em virtude dos trabalhos ou de que tenha tomado conhecimento em decorrência da execução do objeto, sem autorização da Autoridade Competente da PGE, por escrito, sob pena de aplicação das sanções cabíveis, além do pagamento de indenização por perdas e danos. Toda a produção intelectual, inovações e de toda e qualquer documentação, dados, relatórios, além de materiais e outros gerados em razão da prestação de serviços é de propriedade da PGE;

A XSITE assinará termo de compromisso e sigilo, conforme ANEXO I - MINUTA DO TERMO DE RESPONSABILIDADE E SIGILO PARA A EMPRESA deste TDR, se comprometendo a não divulgar, sem expressa autorização da PGE, as informações com as quais tiverem contato durante e após a vigência do contrato;

Além disso, a XSITE garante que todos os colaboradores da LICITANTE envolvidos com a prestação de serviços objeto deste edital apresentem termo de confidencialidade assinado junto à empresa com a qual mantêm vínculo, conforme ANEXO II - MINUTA DO TERMO DE RESPONSABILIDADE E SIGILO PARA O PROFISSIONAL deste TDR, também se comprometendo a não divulgar, sob hipótese alguma, as informações com as quais tiverem contato dentro do ambiente computacional da PGE;

A PGE se reserva o direito de, a qualquer tempo, promover modificações no termo de confidencialidade, ou até mesmo substituí-lo por outro modelo, de modo a refletir as políticas e diretrizes adotadas pela área de segurança;

O descumprimento da obrigação de sigilo e confidencialidade sujeitará a XSITE ao pagamento, ou recomposição, de todas as perdas e danos resultantes do descumprimento, bem como a sua responsabilização civil e criminal respectivas, as quais serão apuradas em regular processo judicial ou administrativo.

Durante o período de execução dos serviços, a XSITE garantirá o funcionamento do software, com suporte técnico do FABRICANTE 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 terão o mesmo período de licenciamento.

O serviço será prestado por profissional devidamente certificado nas soluções tecnológicas utilizadas na prestação dos serviços contratados.

## CONDIÇÕES DE FORNECIMENTO:

A XSITE entregará, às suas expensas, todos os itens acessórios de hardware necessários à perfeita instalação e funcionamento dos equipamentos, incluindo conectores, cabos, suportes e demais itens necessários para instalação e funcionamento da solução XSITE, em plena compatibilidade com as especificações constantes neste Termo de Referência e recomendadas pelo fabricante.

Todos os equipamentos fornecidos e seus componentes serão novos, de primeiro uso e devem estar acondicionados adequadamente em caixa original lacrados de fábrica, de forma a propiciar completa segurança durante e transporte.

Toda a solução e suas implantações serão supervisionadas pela PGE.

A XSITE será responsável por projetar, instalar, configurar e dar suporte na solução ofertada durante todo o período de licenciamento e garantia das licenças.

A implementação das políticas de segurança será de responsabilidade exclusiva da XSITE mediante determinações da CONTRATANTE.



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

## DOS INVESTIMENTOS

| LOTE ÚNICO | | | | |
|---|---|---|---|---|
| ITEM | DESCRIÇÃO/CÓDIGO SIMPAS | QUANTIDADE (UNIDADE) | PREÇO UNITÁRIO POR SOLUÇÃO PARA 36 (TRINTA E SEIS) MESES | PREÇO GLOBAL |
| 1 | Fornecimento para 02 (dois) Firewalls UTM em modo Alta-Disponibilidade (HA) do Fabricante Fortinet, marca/modelo: FortiGate 201F, com garantia de 36 (trinta e seis) meses, serviço de instalação configuração e suporte on-site - Código SIMPAS: 02.81.06.00000488-0. | 02 | R$ 230.000,00 | R$ 460.000,00 |
| 2 | Fornecimento para 01 (um) appliance de log e monitoramento, do Fabricante Fortinet, marca/modelo: FortiAnalyzer FAZ-150G, com garantia de 36 (trinta e seis) meses, serviço de instalação configuração e suporte on-site - Código SIMPAS: 02.81.06.00000487-1. | 01 | R$ 70.000,00 | R$ 70.000,00 |

O valor total da proposta é de R$ 530.000,00 (quinhentos e trinta mil reais).

A validade da proposta é de 60 (sessenta) dias.

O prazo de entrega dos equipamentos: até 60 (sessenta) dias, contados a partir da assinatura do contrato ou instrumento equivalente;

Os equipamentos ofertados acima, terão garantia, mínima, de 5 (cinco) anos e tempo de atendimento exigidos no Edital, conforme documento (*End of Order Fortinet*).

Prazo de instalação e configuração: até 30 (trinta) dias consecutivos, contados da data da entrega das licenças.

Período do licenciamento e prazo contratual: 36 (trinta e seis) meses.

Esta proposta prevê e especifica o período de garantia mínimo de 36 (trinta e seis) com atendimento ONSITE em até 4 horas.

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.



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

ANEXO II

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/dhvl6ydp9cm22dz/AAA1LgSzJR-LV1LMwFpvWxzYa?dl=0

Atenciosamente

João Gualberto Rizzo Araújo
jgra@xsite.com.br
Razão Social: Centro de Pesquisas em Informática LTDA
CNPJ: 40.584.096/0001-05
Tel. (71) 3018-7284 / Cel (71) 98182-5862 / 0800.600.7274
Endereço – Salvador: Rua Edístio Pondé, nº 353, sala 807 / 808, 8º andar, Ed. Empresarial Tancredo Neves - CEP: 41.770-395.
Insc. Municipal: 94.249/001-25 | Insc. Estadual: 053.342.364ME
Banco Bradesco, Agência 0592, Conta Corrente: 50.654-0
Nome fantasia: XSITE Consultoria e Tecnologia.

JOAO GUALBERTO RIZZO ARAUJO:50690124520 Assinado de forma digital por JOAO GUALBERTO RIZZO ARAUJO:50690124520 Dados: 2021.12.28 10:25:01 -03'00'





Documento assinado eletronicamente por **João Gualberto Rizzo Araújo**, **Representante Legal da Empresa**, em 20/01/2022, às 08:35, 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 21/01/2022, às 12:40, 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 **Lucas Silva do Couto**, **Coordenador IV**, em 21/01/2022, às 14:32, 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 21/01/2022, às 14:38, 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 **00041559447** e o código CRC **900318EA**.

**Referência:** Processo nº 006.7550.2022.0000615-40 SEI nº 00041559447

DIÁRIO OFICIAL
República Federativa do Brasil - Estado da Bahia
SALVADOR, TERÇA-FEIRA, 25 DE JANEIRO DE 2022 - ANO CVI - Nº 23.339

o objeto adjudicado conforme publicado no DOE de 28/12/2021 - ANO CVI - Nº 23.320 - SEÇÃO 7 - PG. 47. BA, 19/01/2021. Adson Marchesini - CEL BM - Comandante Geral.

# RECURSOS

# SECRETARIA DA ADMINISTRAÇÃO

**DECISÃO DE RECURSO - CONVITE Nº 002/2021 - SAEB/CCL**
A Comissão de Licitação para Obras e Serviços de Engenharia, Arquitetura e Urbanismo, no uso de suas atribuições, e, com fundamento no art. 202, § 4º da Lei Estadual n° 9.433/2005 e disposições do Edital da Licitação, decide **DAR PROVIMENTO** ao recurso interposto pela empresa Freitas Guimarães Engenharia Eireli (processo SEI nº 009.0187.2022.0000962-43), com a consequente reforma da decisão para habilitá-la na licitação acima referenciada, cujo objeto é: Contratação dos serviços para execução de obra civil para acessibilidade da Biblioteca Central Julieta Carteado- BCJC da UEFS, 24/01/2022. Ana Cláudia Dôto Mônaco - Presidente da Comissão em exercício.

# SECRETARIA DE DESENVOLVIMENTO URBANO

## Companhia de Desenvolvimento Urbano do Estado da Bahia – CONDER

COMPANHIA DE DESENVOLVIMENTO URBANO DO ESTADO DA BAHIA - CONDER

**NOTIFICAÇÃO DE RECURSO DA LICITAÇÃO PRESENCIAL Nº 056/21 - CONDER**
A Comissão Permanente de Licitação - COPEL, em conformidade com a Lei Federal n° 13.303/2016, o RILC da CONDER e as disposições do Edital da Licitação, comunica aos interessados que o licitante **CONSORCIO ENGETEC SIAN (ENGETEC CONSTRUÇÕES E MONTAGENS S.A. / SIAN ENGENHARIA LTDA)** interpôs recurso contra a decisão da Comissão no julgamento da Fase de Habilitação da licitação supracitada, que tem por objeto a **CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA ELABORAÇÃO DOS PROJETOS BÁSICO E EXECUTIVO DE ENGENHARIA E EXECUÇÃO DE OBRAS DE INFRAESTRUTURA, PARA IMPLANTAÇÃO DO SISTEMA VIÁRIO DO NOVO COMPLEXO METRÔ RODOVIÁRIO, INCLUSIVE DA INTERSEÇÃO DA BA 528 X BR 324, NO MUNICÍPIO DE SALVADOR - BAHIA.** O texto do referido Recurso encontra-se à disposição dos interessados, no Site da CONDER, no campo da licitação em questão, para fins de direito. Salvador, 24 de janeiro de 2022. Janilton Santos Pereira - Presidente da Comissão Permanente de Licitação, em exercício.

**NOTIFICAÇÃO DE RECURSO DA LICITAÇÃO PRESENCIAL Nº 102/21 - CONDER**
A Comissão Permanente de Licitação - COPEL, em conformidade com a Lei Federal n° 13.303/2016, o RILC da CONDER e as disposições do Edital da Licitação, comunica aos interessados que o licitante **AGSERVICE ENGENHARIA LTDA** interpôs recurso contra a decisão da Comissão no julgamento da Fase de Proposta de Preços da licitação supracitada, que tem por objeto a **CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA EXECUÇÃO DE OBRAS DE CONSTRUÇÃO E ADEQUAÇÃO FÍSICA DE 04 (QUATRO) UNIDADES ESCOLARES ESTADUAIS DE TEMPO INTEGRAL, LOCALIZADAS NOS MUNICÍPIOS DE FEIRA DE SANTANA, ITAPARICA E TAPEROÁ - BAHIA.** O texto do referido Recurso encontra-se à disposição dos interessados, no Site da CONDER, no campo da licitação em questão, para fins de direito. Salvador, 24 de janeiro de 2022. Janilton Santos Pereira - Presidente da Comissão Permanente de Licitação, em exercício.

# CONTRATOS

# CASA CIVIL

**CASA CIVIL**
**RESUMO DO TERMO ADITIVO Nº 02/2022 - CONTRATO Nº 02/2021**
Processo: Nº 014.1517.2021.0004531-06. Contratante: O Estado da Bahia, através da Casa Civil - Contratada: 2W COMÉRCIO DISTRIBUIÇÃO E SERVIÇOS EIRELI. Objeto: Prorrogação do prazo da vigência por mais 12 (doze) meses de 25/01/2022 a 24/01/2023 e renúncia expressa ao Reajustamento INPC/IBGE do período de 2021-2022. Valor global estimado: R$138.393,80(cento e trinta e oito mil trezentos e noventa e três reais e oitenta centavos). Unidade Orçamentária/ Gestora: 14.101/0004 - Fonte: 100 - Projeto/ Atividade: 4304 - Elemento de Despesa: 33.90.30 e 33.90.39. Salvador 24/01/2022.

**CASA CIVIL**
**RESUMO DO TERMO ADITIVO Nº 03/2022 - CONTRATO Nº 01/2021**
Processo: Nº 014.1517.2021.0004466-65. Contratante: O Estado da Bahia, através da Casa Civil - Contratada: 2W COMÉRCIO DISTRIBUIÇÃO E SERVIÇOS EIRELI. Objeto: Prorrogação do prazo da vigência por mais 12 (doze) meses de 26/01/2022 a 25/01/2023 e renúncia expressa ao Reajustamento INPC/IBGE do período de 2021-2022. Valor global estimado: R$45.997,75 (quarenta e cinco mil novecentos e noventa e sete reais e setenta e cinco centavos). Unidade Orçamentária/ Gestora: 14.101/0004 - Fonte: 100 - Projeto/ Atividade: 4304 - Elemento de Despesa: 33.90.30 e 33.90.39. Salvador 24/01/2022.

# PROCURADORIA GERAL DO ESTADO

**RESUMO DE CONTRATO**
Processo SEI nº 006.0409.2021.0029638-21
Contrato nº PGE 003/2022 - Pregão Eletrônico nº 010/2021
Contratante: ESTADO DA BAHIA/PROCURADORIA GERAL DO ESTADO
Contratada: **CENTRO DE PESQUISAS EM INFORMÁTICA LTDA**
Objeto: Serviços de Solução de Segurança da Informação, no valor global estimado de R$ 530.000,00 (quinhentos e trinta mil reais). Unidade Orçamentária - 06.601, Fonte - 154, Projeto/ Atividade - 5121, Elemento da Despesa - 33.90.40. Prazo: 36 (trinta e seis) meses, a partir da data da assinatura (21/01/2022). Regime de Execução/Forma de Pagamento: Serviço com empreitada por preço - unitário.
Setor Responsável pela Gestão Contratual: Coordenação de Gestão Estratégica - CGE.
Gestor: Eduardo Jorge Rodrigues Brandão.
Fiscal: Mauricio de Cerqueira Pereira.

# SECRETARIA DA ADMINISTRAÇÃO

**RESUMO DO CONTRATO COELBA**
**Processo SEI n°**: 009.0231.2021.0036874-71. **Modalidade**: Inexigibilidade de Licitação nº 002/2022. **Contratante:** Estado da Bahia, através da Secretaria da Administração. **Contratada:** Companhia de Eletricidade do Estado da Bahia - COELBA. **Objeto:** Fornecimento de energia elétrica, atendida em Alta Tensão, Estrutura Tarifária Horosazonal Verde, para a unidade consumidora da Secretaria da Educação, conforme tabela a seguir. **Vigência:** 24 (vinte e quatro) meses, a contar da data da assinatura do contrato. **Unidade Orçamentária**: 11.101, **Unidade Gestora:** 0001, **Ação (Projeto/Atividade):** 12.122.306.4514, **Natureza da Despesa**: 33.90.39.00, **Destinação de Recurso**: 0.107.000000. **Assinatura:** 21.01.2022.

| CONTA CONTRATO | NÚMERO DO CONTRATO / TIPO | REGIME TARIFÁRIO | ESTIMATIVA ORÇAMENTÁRIA CONTRATUAL |
|---|---|---|---|
| 24749851 | 5057673/CCER 5057673/CUSD | Horosazonal Verde | R$ 210.777,84 |

**RESUMO DO CONTRATO COELBA**
**Processo SEI n°**: 009.0231.2021.0046849-12. **Modalidade**: Inexigibilidade de Licitação nº 001/2022. **Contratante:** Estado da Bahia, através da Secretaria da Administração. **Contratada:** Companhia de Eletricidade do Estado da Bahia - COELBA. **Objeto:** Fornecimento de energia elétrica, atendida em Alta Tensão, Estrutura Tarifária Horosazonal Verde, para a unidade consumidora da Secretaria da Educação, conforme tabela a seguir. **Vigência:** 24 (vinte e quatro) meses, a contar da data da assinatura do contrato. **Unidade Orçamentária**: 11.101, **Unidade Gestora:** 0001, **Ação (Projeto/Atividade):** 12.122.306.4514, **Natureza da Despesa**: 33.90.39.00, **Destinação de Recurso**: 0.107.000000. **Assinatura:** 21.01.2022.

| CONTA CONTRATO | NÚMERO DO CONTRATO / TIPO | REGIME TARIFÁRIO | ESTIMATIVA ORÇAMENTÁRIA CONTRATUAL |
|---|---|---|---|
| 7065078591 | 5056604/CCER 5056604/CUSD | Horosazonal Verde | R$ 215.280,00 |

**RESUMO DO TERMO ADITIVO Nº 04 AO CONTRATO Nº 019/2018**
**Processo SEI nº:** 009.0216.2021.0049544-33. **Contratante**: Estado da Bahia, através da Secretaria da Administração. **Contratada:** Rótula Car Transporte Ltda. **Objeto:** Prorrogação do prazo de vigência do referido contrato por 365 (trezentos e sessenta e cinco) dias, contados a partir de 26.01.2022 e término em 25.01.2023, mantendo-se o valor global estimado em R$ 175.380,00 (cento e setenta e cinco mil, trezentos e oitenta reais). **Unidade Orçamentária:** 09.101; **Unidade Gestora:** 0015; **Projeto/Atividade**: 04.122.502.2067; **Natureza da Despesa**: 3.3.90.39; **Destinação de Recurso**: 0100.000000. **Assinatura:** 21.01.2022.

## Departamento Estadual de Trânsito – DETRAN

**RESUMO DE CONTRATO Nº. 002/2022**
PROCESSO SEI Nº 049.3047.2021.0017971-08. Pregão Eletrônico nº 005/2021; **Contratante**: Departamento Estadual de Trânsito da Bahia - DETRAN/BA; **Contratada**: C M LEMOS