Governo do Estado do Rio de Janeiro
Companhia Estadual de Águas e Esgotos do Rio de Janeiro
Diretoria Jurídica

CONTRATO Nº 079/2025 (DFI)

CONTRATO CEDAE Nº 079/2025 (DFI) que entre si celebram a **COMPANHIA ESTADUAL DE ÁGUAS E ESGOTOS (CEDAE)** e a **2R DATATEL TELEINFORMÁTICA LTDA.**

A **COMPANHIA ESTADUAL DE ÁGUAS E ESGOTOS,** sociedade de economia mista, com sede nesta Cidade, na Av. Presidente Vargas, 2655 – Cidade Nova – CEP 20.210-030, registrada na JUCERJA sob n.º 5.000, em 14 de agosto de 1975, inscrita no CNPJ/MF sob o n.º 33.352.394/0001-04, neste ato por meio de seu Diretor Presidente, Sr. AGUINALDO BALLON, e de seu Diretor Administrativo Financeiro e de Relações com Investidores, Sr. ANTONIO CAROS DOS SANTOS, doravante denominada **CEDAE,** e a **2R DATATEL TELEINFORMÁTICA LTDA.** sediada na Praça XV de Novembro, 20, grupo 401-B, Centro, Rio de Janeiro, Cep. 20.010-010, inscrita no CNPJ sob o n.º 73.514.382/0001-45, neste ato por meio de seu sócio administrador, Sr. ROBSON PINTO BOTELHO, daqui por diante denominada **CONTRATADA,** resolvem celebrar o presente Contrato autuado no **Processo Administrativo SEI-150017/008939/2024**, mediante **ADESÃO À ATA DE REGISTRO DE PREÇOS N. 007/2024 DO PRODERJ,** realizada através do Pregão Eletrônico para Registro de Preços n. 007/2024, o que se faz com fundamento no art. 21 do Regulamento Interno de Licitações e Contratos da CEDAE (RILC), bem como na Lei nº 13.303, de 30 de junho de 2016, pelos quais se regerá, assim como pelos preceitos de direito privado, cláusulas e condições seguintes:

CLÁUSULA PRIMEIRA - DO OBJETO

A presente contratação é decorrente da adesão à Ata de Registro de Preços **N. 007/2024,** realizada para a **"CONTRATAÇÃO DE EMPRESA DO RAMO DE TECNOLOGIA I INFORMAÇÃO PARA O FORNECIMENTO DE SOLUÇÃO DE FIREWALL, COM GARANTIA DE 60 MESES, CONTEMPLANDO HARDWARE E SOFTWARE, COM INSTA CONFIGURAÇÃO, NAS DEPENDÊNCIAS DO CONTRATANTE E CURSO DE TREINAMENTO OFICIAL DA SOLUÇÃO", para os itens 1 a 5 do LOTE 1 e item 1 do LOTE 3 do licitado**, conforme quantidades aprovadas em Resolução de Diretoria autuada sob o index 100194944 do processo administrativo de referência.

Parágrafo Primeiro - O **Termo de Referência do PRODERJ e seus anexos** (index 98355550), o **Termo de Referência da CEDAE** (index 98143181), a **Proposta** da contratada (index 98905102), o **Cronograma físico-Financeiro** (index 100549512) e o **Acordo de Nível de Serviço** (index 98233337) autuados no processo administrativo de referência obrigam as partes e complementam o presente ajuste, embora não transcritos.

Parágrafo Segundo – Estão inseridos no escopo da contratação os **itens 1 a 5 do LOTE I e o item 1 do LOTE 3** do Registro de Preços, conforme quantidades detalhadas abaixo:

EQUIPAMENTOS					
Item	**Item da ATA**	**IFS**	**Descrição**	**Unidade**	**QTD sol**
1	1 - Lote 1		APPLIANCE FIREWALL TIPO 1 - INCLUSOS: HARDWARE, LICENCIAMENTO E GARANTIA POR 60 MESES	Unidade	4
2	2 - Lote 1		CONSOLE DE GERENCIAMENTO CENTRALIZADO PARA O FIREWALL TIPO 1 COM GARANTIA DE 60 MESES	Unidade	2
3	3 - Lote 1		CONSOLE DE GERENCIAMENTO DE LOGS PARA O FIREWALL TIPO 1 COM GARANTIA DE 60 MESES	Unidade	2
4	4 - Lote 1		CONSOLE DE RELATORIA CENTRALIZADA PARA O FIREWALL TIPO 1 COM GARANTIA DE 60 MESES	Unidade	2
5	1 - Lote 3		APPLIANCE FIREWALL TIPO 3 - INCLUSOS: HARDWARE, LICENCIAMENTO E GARANTIA POR 60 MESES	Unidade	12
SERVIÇOS					
6	5 - Lote 1		SERVIÇO DE TREINAMENTO OPERACIONAL PARA A SOLUÇÃO DOS ITENS 1, 2, 3 e 4	Aluno	13

(i) O treinamento referente ao item 5 do LOTE 1 terá duração mínima de 40 (quarenta) horas, conforme previsto n o item III da cláusula 3.3.8 do termo de referência do Proderj. O treinamento será em português, ministrado na modalidade remota, em plataforma virtual disponibilizada pela contratada.

Parágrafo Terceiro – Em caso de eventual divergência entre o Termo de Referência do Proderj, ou da CEDAE, com as disposições deste contrato, pervalecerá o que houver sido previsto nesse último, uma vez que decorrente da negociação obtida junto à **CONTRATADA**. Já em caso de eventual divergência entre os Termo de Referência do PRODERJ e da CEDAE, referente às especificações técnicas, prevalecerá sempre o que houver sido previsto no Termo de Referência do PRODERJ.

CLÁUSULA SEGUNDA - DO PRAZO

O prazo da contratação será de **90 (noventa) dias** contados da data indicada na Ordem de Fornecimento, que poderá ser emitida após a assinatura do contrato.

(i) Todas as etapas da contratação encontram-se inseridas nesse prazo, conforme cronograma físico-financeiro autuado sob o index 100549512.

Parágrafo Primeiro - O decurso do prazo estipulado não acarretará, por si só, a resolução do ajuste, continuando as partes contratualmente obrigadas até que se opere o aceite definitivo do objeto, respondendo a **CONTRATADA** pela mora a que der causa.

Parágrafo Segundo - O prazo ora previsto poderá ser alterado por acordo entre as partes, por meio de termo aditivo, devendo ser observado, neste caso, o disposto no art.

205 do RILC.

Parágrafo Terceiro - Ocorrendo impedimento, paralisação ou sustação do contrato por ordem da CEDAE, o prazo de execução será automaticamente prorrogado por igual período, bastando o registro formal de interrupção no processo administrativo, conforme art. 206 do RILC.

Parágrafo Quarto - A prorrogação de prazo formalizada **por culpa da CONTRATADA** impedirá que o período acrescido à execução seja considerado para a recomposição dos preços contratados, conforme previsto no art. 205, parágrafo único, do RILC.

Parágrafo Quinto - A prorrogação de prazo por motivos alheios à vontade das partes não justificará, por si só, a alteração dos preços pactuados a não ser que fique demonstrado o desequilíbrio econômico-financeiro decorrente de fatos imprevisíveis, ou previsíveis de consequências incalculáveis, que importem no retardamento ou na inexecução do contrato, ficando vedada, desde já, a revisão dos preços após o encerramento do contrato pela conclusão do seu objeto.

CLÁUSULA TERCEIRA - DAS OBRIGAÇÕES DA CEDAE

3..1 Exigir o cumprimento de todas as obrigações assumidas pelo CONTRATADO, de acordo com o Termo de Referência do PRODERJ, Contrato e seus Anexos.
3.2 Receber o objeto no prazo e condições estabelecidas.
3.3 Notificar o CONTRATADO, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto fornecido, para que seja por ele substituído, reparado ou corrigido, no total ou em parte, às suas expensas.
3.4 Acompanhar e fiscalizar a execução do Contrato e o cumprimento das obrigações pelo CONTRATADO.
3.5 Comunicar ao CONTRATADO para que emita Nota Fiscal relativa à parcela incontroversa da execução do objeto, com vistas à liquidação e pagamento, no caso de divergência acerca do cumprimento das obrigações assumidas, quanto à dimensão, qualidade e quantidade.
3.6 Efetuar o pagamento ao CONTRATADO do valor correspondente ao fornecimento do objeto, no prazo, forma e condições estabelecidos no presente Contrato.
3.7 Aplicar ao CONTRATADO sanções motivadas pela inexecução total ou parcial das obrigações contratuais, na forma prevista na lei e neste Contrato.
3.8 Dar ciência à Assessoria Jurídica CEDAE para as providências relacionadas à adoção de eventuais medidas judiciais, em caso de descumprimento de obrigações pelo CONTRATADO.
3.9 Emitir decisão fundamentada sobre todas as solicitações e reclamações relacionadas à execução do presente Contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste.
3.9.1 A CEDAE terá o prazo de 1 (um) mês, a contar da data do protocolo do requerimento, para decidir, admitida a prorrogação motivada, por igual período.
3.10 Responder aos eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pelo CONTRATADO no prazo máximo de 45 (quarenta e cinco) dias, admitida a prorrogação motivada, por uma única vez, por igual período.
3.11 Notificar os emitentes das garantias quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais
3.12 A CEDAE não responderá por quaisquer compromissos assumidos pelo CONTRATADO perante terceiros, ainda que vinculados à execução do Contrato, bem como por qualquer dano causado a terceiros em decorrência de ato do CONTRATADO, de seus empregados, prepostos ou subordinados.
3.13 O presente Contrato não configura vínculo empregatício entre os trabalhadores ou sócios do CONTRATADO com a CEDAE.
3.14 Atender as demais obrigações estabelecidas no Subitem 3.23.1 do Termo de Referência do PRODERJ.

CLÁUSULA QUARTA - DAS OBRIGAÇÕES DA CONTRATADA

4.1 O CONTRATADO deverá cumprir todas as obrigações constantes deste Contrato e em seus Anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas:
4.1.1 Entregar o objeto acompanhado, se for o caso, do manual do usuário, com uma versão em português, e da relação da rede de assistência técnica autorizada.
4.1.2 Comunicar a CEDAE, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação.
4.1.3 Atender às determinações regulares emitidas pelo fiscal ou gestor do Contrato ou autoridade superior (art. 137, II, da Lei nº 14.133/2021) e prestar todo esclarecimento ou informação por eles solicitados.
4.1.4 Alocar os empregados necessários, com habilitação e conhecimento adequados, ao perfeito cumprimento das cláusulas deste Contrato, fornecendo os materiais, equipamentos, ferramentas e utensílios demandados, cuja quantidade, qualidade e tecnologia deverão atender às recomendações de boa técnica e a legislação de regência.
4.1.5 Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do Contrato, os bens nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados.
4.1.6 Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com o Código de Defesa do Consumidor (Lei nº 8.078/1990), bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa responsabilidade à fiscalização ou ao acompanhamento da execução contratual pela CEDAE, que ficará autorizada a descontar dos pagamentos devidos ou da garantia o valor correspondente aos danos sofridos. 4.1.7 Não contratar, durante a vigência do Contrato, cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente da CEDAE ou de agente público que atue na fiscalização ou na gestão do Contrato.
4.1.8 Manter a regularidade junto ao SICAF.
4.1.8.1 Quando não for possível a verificação da regularidade no Sistema de Cadastro de Fornecedores – SICAF, o CONTRATADO deverá entregar ao setor responsável pela fiscalização do Contrato, junto com a Nota Fiscal para fins de pagamento, os seguintes documentos: a) prova de regularidade relativa à Seguridade Social; b) certidão conjunta relativa aos tributos federais e à Dívida Ativa da União; c) certidões que comprovem a regularidade perante a Fazenda Municipal, Estadual ou Distrital do domicílio ou sede do contratado; d) Certificado de Regularidade do FGTS; e e) Certidão Negativa de Débitos Trabalhistas – CNDT.
4.1.9 Responsabilizar-se pelo cumprimento de todas as obrigações trabalhistas, previdenciárias, fiscais, comerciais e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade para a CEDAE e não poderá onerar o objeto do Contrato.
4.1.10 Comunicar ao Fiscal do Contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local da execução do objeto contratual.
4.1.11 Paralisar, por determinação da CEDAE, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros.
4.1.12 Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local de execução do objeto e nas melhores condições de segurança, higiene e disciplina.
4.1.13 Submeter previamente, por escrito, da CEDAE, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo ou instrumento congênere.
4.1.14 Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos, nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre, na forma do art. 7º, XXXIII, da Constituição Federal.
4.1.15 Manter durante toda a vigência do Contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação na licitação.
4.1.16 Cumprir, durante todo o período de execução do Contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas na legislação (art. 116 da Lei nº 14.133/2021).
4.1.16.1 Comprovar a reserva de cargos a que se refere a cláusula acima, no prazo fixado pelo Fiscal do Contrato, com a indicação dos empregados que preencheram as referidas vagas (art. 116, parágrafo único, da Lei nº 14.133/2021).
4.1.17 Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do Contrato.
4.1.18 Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto do Contrato, exceto quando o equivoco decorrer de fatos imprevisíveis ou previsíveis de consequências incalculáveis que invibializem a eecução do contrato como pactuado.
4.1.19 Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança da CEDAE.
4.1.20 Prestar esclarecimentos ou informações solicitadas pela CEDAE ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do empreendimento.
4.1.21 Caso o valor do Contrato se enquadre no limite previsto no art. 1º da Lei estadual nº 7.753, de 17 de outubro de 2017, manter Programa de Integridade nos termos da referida Lei e eventuais modificações e regulamentos subsequentes, consistindo tal programa no conjunto de mecanismos e procedimentos internos de integridade, auditoria e incentivo à denúncia de irregularidades e na aplicação efetiva de códigos de ética e de conduta, políticas e diretrizes com o objetivo de detectar e sanar desvios, fraudes, irregularidades e atos ilícitos praticados contra a Administração Pública.
4.1.22 Orientar e treinar seus empregados sobre os deveres previstos na Lei nº 13.709, de 14 de agosto de 2018 (LGPD), adotando medidas eficazes para proteção de dados pessoais a que tenha acesso por força da execução deste Contrato.

4.1.23 Observar integralmente as demais obrigações previstas no Subitem 3.23.2 do Termo de Referência do Proderj.

CLÁUSULA QUINTA – DO VALOR DO CONTRATO

A **CONTRATADA** se obriga a executar o objeto de forma integral, pelo preço de R$ **27.327.625,00 (vinte e sete milhões, trezentos e vinte e sete mil, seiscentos e vinte e cinco reais)**, conforme proposta autuada sob o index 98905102 do processo administrativo de referência, abaixo reproduzida:

LOTE 1 - FIREWALL TIPO 1						
Item	**IDSIGA**	**Descrição**	**Unidade de Fornecimento**	**QTD solicitada**	**Valor Unitário (R$)**	**Valor Total (R$)**
1	168256	AQUISIÇÃO DE APPLIANCE FIREWALL TIPO 1 -INCLUSOS: HARDWARE, LICENCIAMENTO, INSTALAÇÃO, CONFIGURAÇÃO E GARANTIA POR 60 MESES	Unidade	4	R$ 6.090.000,00	R$ 24.360.000,00
2	172443	AQUISIÇÃO DE CONSOLE DE GERENCIAMENTO CENTRALIZADO PARA O FIREWALL TIPO 1 COM GARANTIA DE 60 MESES	Unidade	2	R$ 74.000,00	R$ 148.000,00
3	172442	AQUISIÇÃO DE CONSOLE DE GERENCIAMENTODE LOGS PARA O FIREWALL TIPO 1 COM GARANTIA DE 60 MESES	Unidade	2	R$ 74.000,00	R$ 148.000,00
4	172444	AQUISIÇÃO DE CONSOLE DE RELATORIACENTRALIZADA PARA O FIREWALL TIPO 1 COM GARANTIA DE 60 MESES	Unidade	2	R$ 74.000,00	R$ 148.000,00
5	180944	SERVIÇO DE TREINAMENTO OPERACIONAL PARAA SOLUÇÃO DO LOTE 1	Aluno/vaga	13	R$ 5.500,00	R$ 71.500,00
					Total LOTE 1	R$ 24.875.500,00

LOTE 3 - FIREWALL TIPO 3						
Item	**IDSIGA**	**Descrição**	**Unidade de Fornecimento**	**QTD solicitada**	**Valor Unitário (R$)**	**Valor Total (R$)**
1	168258	AQUISIÇÃO DE APPLIANCE FIREWALL TIPO 3 -INCLUSOS: HARDWARE, LICENCIAMENTO, INSTALAÇÃO, CONFIGURAÇÃO E GARANTIA POR 60 MESES	Unidade	12	R$ 204.343,75	R$ 2.452.125,00
					Total LOTE 3	2.452.125,00

Parágrafo Primeiro - O preço ajustado inclui o lucro e todos os custos e tributos (inclusive ICMS, conforme registrado pela CONTRATADA em sua manifestação autuada sob o index 100083429), sejam diretos ou indiretos, responsabilizando-se a **CONTRATADA** por toda e qualquer despesa ainda que não prevista textualmente neste Contrato, inclusive a que decorrer de ato ou fato que implique em transgressão ou inobservância de qualquer dispositivo legal ou regulamentar, federal, estadual ou municipal.

Parágrafo Segundo - As despesas com a execução do presente contrato correrão à conta das seguintes dotações orçamentárias, para o corrente exercício de 2025, assim classificados:

Programa de Trabalho: 2200022016
Conta Contábil: 151110013, 151110014 e 411110158
Fonte de Recursos: 10
Código Orçamentário: 44905238, 44904052 e 33903921
Centro de Custos: DF21000000
ID da Reserva Orçamentária: 2025000761 e 2025000762

Parágrafo Terceiro - Eventuais despesas relativas a exercícios futuros correrão por conta das respectivas dotações orçamentárias, e serão empenhadas no início de cada exercício financeiro.

CLÁUSULA SEXTA – CONDIÇÕES PARA PAGAMENTO

O(s) pagamento(s) à **CONTRATADA** será(ão) realizado(s) no prazo de até 30 (trinta) dias contados de cada recebimento provisório previsto na cláusula décima quinta, o que será feito observando o calendário previsto na Ordem de Serviço n. 16.088-00 de 2022, bem como os limites estabelecidos no cronograma físico- financeiro autuado sob o index 100549512 do processo administrativo de referência.

Parágrafo Primeiro - Quando houver glosa parcial do objeto, a CEDAE deverá comunicar ao CONTRATADO para que emita Nota Fiscal ou Fatura com o valor exato dimensionado.

Parágrafo Segundo - Recebida a Nota Fiscal ou Fatura, a CEDAE deverá realizar consulta ao SICAF para verificar: a) a manutenção das condições de habilitação exigidas pelo instrumento convocatório; b) se o CONTRATADO foi penalizado com as sanções de declaração de inidoneidade ou impedimento de licitar e contratar com o Poder Público, observadas as abrangências de aplicação; e c) eventuais ocorrências impeditivas indiretas, hipótese na qual o gestor deverá verificar se houve fraude por parte das empresas

apontadas no Relatório de Ocorrências Impeditivas Indiretas.

Parágrafo Terceiro - Constatando-se a situação de irregularidade do CONTRATADO, será providenciada sua notificação, por escrito, para que, no prazo de 15 (quinze) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa e especifique as provas que pretende produzir.

Parágrafo Quarto - O prazo poderá ser prorrogado uma vez, por igual período, a critério da CEDAE.

Parágrafo Quinto - Não havendo regularização ou sendo a defesa considerada improcedente, caberá à CEDAE comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do CONTRATADO, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

Parágrafo Sexto - Persistindo a irregularidade, a CEDAE deverá adotar as medidas necessárias à rescisão do Contrato nos autos do processo administrativo correspondente, assegurada ao CONTRATADO a ampla defesa.

Parágrafo Sétimo - Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do Contrato, caso o CONTRATADO não regularize sua situação.

Parágrafo Oitavo - O pagamento será efetuado no prazo máximo de até 30 (trinta) dias, contado do recebimento da Nota Fiscal ou Fatura.

Parágrafo Nono - Havendo erro na apresentação da Nota Fiscal ou Fatura, ou circunstância que impeça à liquidação da despesa, o pagamento ficará sobrestado até que o CONTRATADO providencie as medidas saneadoras. Nessa hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a CEDAE.

Parágrafo Décimo - Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

Parágrafo Décimo-Primeiro - Independentemente do percentual de tributo inserido na planilha, no pagamento serão retidos na fonte os percentuais estabelecidos na legislação vigente.

Parágrafo Décimo-Segundo - O CONTRATADO regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123/2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele Regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar nº 123/2006.

Parágrafo Décimo-Terceiro - Os pagamentos eventualmente realizados com atraso, desde que não decorram de ato ou fato atribuível ao CONTRATADO, sofrerão a incidência de atualização monetária e juros de mora pelo IPCA-E, calculado pro rata die, e aqueles pagos em prazo inferior ao estabelecido no instrumento convocatório serão feitos mediante desconto de 0,5% (um meio por cento) ao mês, calculado pro rata die.

Parágrafo Décimo-Quarto - O CONTRATADO deverá emitir a Nota Fiscal Eletrônica – NF-e, consoante o Protocolo ICMS nº 42/2009, com a redação conferida pelo Protocolo ICMS nº 85/2010, e caso seu estabelecimento esteja localizado no Estado do Rio de Janeiro, deverá observar a forma prescrita nas alíneas "a", "b", "c", "d" e "e" do parágrafo 1º do artigo 2º da Resolução SEFAZ nº 971/2016.

Parágrafo Décimo-Quinto - No caso de o CONTRATADO estar estabelecido em localidade que não possua agência da instituição financeira contratada pelo Estado do Rio de Janeiro ou, caso verificada pela CEDAE a impossibilidade de o CONTRATADO, em razão de recusa expressa da instituição financeira contratada pelo Estado do Rio de Janeiro, abrir ou manter conta corrente naquela instituição financeira, o pagamento poderá ser feito mediante crédito em conta corrente de outra instituição financeira. Nesse caso, eventuais ônus financeiros e/ou contratuais adicionais serão suportados exclusivamente pelo CONTRATADO.

CLÁUSULA SÉTIMA – DA SUBCONTRATAÇÃO

Não será admitida a subcontratação na execução deste contrato.

CLÁUSULA OITAVA – DA IMPOSSIBILIDADE DE MODIFICAÇÃO DO CONTRATO PELA SUPPRESSIO

O atraso, a tolerância ou a omissão da **CEDAE** no exercício de suas prerrogativas jamais ensejará a modificação automática das cláusulas avençadas, não sugerindo qualquer renúncia de direitos por parte desta, que poderá exercê-los a qualquer tempo.

CLÁUSULA NONA – DA ALTERAÇÃO DO CONTRATO

Este contrato poderá ser alterado por acordo entre as partes, formalizado por meio de Termo Aditivo, com observância do disposto nos arts. 208 a 211 do RILC.

Parágrafo Único – As alterações que se fizerem necessárias nas quantidades ou qualidade do serviço contratado deverão observar os limites do §§1º e 2º do art. 81 da Lei 13.303/2016.

CLÁUSULA DÉCIMA – DO REAJUSTE

Os preços contratados serão reajustados após o interregno de 1 (um) ano, mediante solicitação do CONTRATADO.

Parágrafo Primeiro - O interregno mínimo de 1 (um) para o primeiro reajuste será contado da data do orçamento estimado no Registro de Preços do qual decorre esta contratação.

Parágrafo Segundo - Nos reajustes subsequentes ao primeiro, o interregno mínimo de 1 (um) ano será contado a partir do fato gerador que deu ensejo ao último reajuste.

Parágrafo Terceiro - Os preços iniciais serão reajustados, mediante a aplicação, pela CEDAE, **do índice ICTI**, exclusivamente para as obrigações que se iniciem após a anualidade.

Parágrafo Quarto - No caso de atraso ou não divulgação do(s) índice(s) de reajustamento, a CEDAE pagará ao CONTRATADO a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo.

Parágrafo Quinto - Fica o CONTRATADO obrigado a apresentar memória de cálculo referente ao reajustamento de preços do valor remanescente, sempre que este ocorrer, sendo adotado na aferição final o índice definitivo.

Parágrafo Sexto - Caso o índice estabelecido para reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação então em vigor.

Parágrafo Sétimo - Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de Termo Aditivo.

Parágrao Oitavo - O pedido de reajuste deverá ser formulado durante a vigência do Contrato e antes de eventual prorrogação contratual, sob pena de preclusão.

Parágrafo Nono - Os efeitos financeiros do pedido de reajuste serão contados:

a) da data-base prevista no Contrato, desde que requerido o reajuste no prazo de 60 (sessenta) dias da data de publicação do índice ajustado contratualmente;

b) a partir da data do requerimento do CONTRATADO, caso o pedido seja formulado após o prazo fixado na alínea a, acima, o que não acarretará a alteração do marco para cômputo da anualidade do reajustamento, já adotado no Edital e no Contrato.

Parágrafo Décimo - Caso, na data de eventual prorrogação contratual, ainda não tenha sido divulgado o índice de reajuste, deverá, a requerimento do CONTRATADO, ser inserida cláusula no Termo Aditivo de prorrogação para resguardar o direito futuro do CONTRATADO, a ser exercido tão logo se disponha dos valores reajustados, sob pena de preclusão.

Parágrafo Décimo-Primeiro - A extinção do Contrato não configurará óbice para o deferimento do reajuste solicitado tempestivamente, hipótese em que será concedido por meio de termo indenizatório.

Parágrafo Décimo-Segundo - O reajuste será realizado por apostilamento, se esta for a única alteração contratual a ser realizada.

Parágrafo Décimo-Terceiro - O reajuste de preços não interfere no direito das partes de solicitar, a qualquer momento, a manutenção do equilíbrio econômico dos contratos com base no disposto no art. 81, inciso VI da Lei 13.303/2016.

CLÁUSULA DÉCIMA-PRIMEIRA – DAS SANÇÕES ADMINISTRATIVAS E DEMAIS PENALIDADES

A inexecução dos serviços, total ou parcial, a execução imperfeita, a mora na execução ou qualquer inadimplemento ou infração contratual, sujeitarão a **CONTRATADA**, sem prejuízo da responsabilidade civil ou criminal que lhe couber, às penalidades seguintes:

a) advertência;

b) multa de mora e multa administrativa, previstas no art. 4º, §§1º e 2º do Procedimento de Aplicação de Sanções; e

c) suspensão temporária da participação em licitação e impedimento de contratar com a CEDAE por prazo não superior a 2 (dois) anos.

Parágrafo Primeiro - A sanção administrativa deve ser determinada de acordo com a natureza e a gravidade da falta cometida.

Parágrafo Segundo - Todas as sanções previstas no caput desta cláusula serão impostas pelo Diretor responsável, na forma do art. 22, §1º, do Procedimento de aplicação de sanções da CEDAE.

Parágrafo Terceiro- A **multa administrativa**, prevista na alínea "b" do caput, será aplicada à CONTRATADA pelo descumprimento de suas obrigações acessórias, observando o que segue:

i) corresponderá ao valor de até 5% (cinco por cento), aplicada de acordo com a gravidade da infração e proporcionalmente às parcelas não executadas, a contar da data da infração, com observância do previsto no art. 5-A do Procedimento de Aplicação de Sanções (PAS);

i.1.) Nas infrações cometidas após o encerramento do contrato, a base de cálculo será o valor da contratação.

ii) nas reincidências específicas, deverá corresponder, no mínimo, ao dobro do valor da que tiver sido inicialmente imposta;

iii) O somatório das multas administrativas deverá observar o limite de 20% (vinte por cento) do valor do contrato ou do empenho.

iv) poderá ser aplicada cumulativamente a qualquer outra penalidade; e

v) não tem caráter compensatório, não se confundindo, portanto, com as multas por atraso, com a multa rescisória e com a multa prevista na cláusula décima oitava, que poderão ser aplicadas cumulativamente à multa administrativa.

Parágrafo Quarto - A suspensão temporária da participação em licitação e impedimento de contratar, prevista na alínea "c", caput, desta cláusula, será aplicada nos casos descritos pelo art. 9º do Procedimento de Aplicação de Sanções da CEDAE, e não poderá exceder a 2 (dois) anos.

Parágrafo Quinto - A aplicação das penalidades acima referidas, em virtude das infrações contratuais retro mencionadas, não importará em renúncia, por parte da **CEDAE,** da faculdade de declarar rescindido o contrato, se assim entender conveniente ao interesse público.

Parágrafo Sexto - O atraso injustificado no cumprimento das obrigações contratuais sujeitará a **CONTRATADA** à **multa de mora** por dia útil que exceder ao prazo estipulado, conforme percentuais abaixo:

a) 0,33% (trinta e três centésimos por cento) por dia de atraso, calculado sobre o valor correspondente à parte inadimplente, até o limite de 9,9%, correspondente a até 30 (trinta) dias de atraso; e

b) 0,66 % (sessenta e seis centésimos por cento) por dia de atraso, calculado sobre o valor correspondente à parte inadimplente, quando o atraso ultrapassar 30 (trinta) dias, até o limite máximo de 20%.

Parágrafo Sétimo - As multas porventura aplicadas serão consideradas dívidas líquidas e certas, ficando a **CEDAE** autorizada a descontá-las das garantias prestadas, e caso estas sejam insuficientes, dos pagamentos devidos à **CONTRATADA;** ou ainda, quando for o caso, cobrá-las judicialmente, servindo para tanto, o instrumento contratual como título executivo extrajudicial.

Parágrafo Oitavo - A intimação do interessado deverá indicar o prazo e o local para a apresentação de defesa.

I) A defesa prévia do interessado será exercida no prazo de 10 (dez) dias úteis, na forma prevista no art. 26, §§ 3º e 5º do Procedimento de Aplicação de Sanções da CEDAE.

Parágrafo Nono - Será emitida decisão conclusiva sobre a aplicação ou não da sanção, pela autoridade competente, devendo ser apresentada a devida motivação, com a demonstração dos fatos e dos respectivos fundamentos jurídicos.

Parágrafo Décimo - Todas as multas previstas neste contrato, incluindo a rescisória e a prevista na cláusula décima oitava, serão somadas quando aplicadas cumulativamente, e terão como limite seus respectivos percentuais máximos.

Parágrafo Décimo-Primeiro - O Procedimento de Aplicação das Sanções (PAS) da CEDAE encontra-se disponível para consulta no link https://cedae.com.br/regulamento.

CLÁUSULA DÉCIMA-SEGUNDA - DA RESCISÃO CONTRATUAL

A inexecução total ou parcial do contrato poderá ensejar a sua rescisão com as consequências cabíveis.

Parágrafo Primeiro - A rescisão contratual poderá ocorrer por:

I - ato unilateral e escrito, quando verificada a ocorrência de qualquer das situações descritas no art. 222 do RILC;
II- acordo entre as partes, reduzido a termo no processo de contratação, desde que seja vantajoso à CEDAE; ou
III – decisão judicial ou arbitral.

Parágrafo Segundo - Os casos de rescisão contratual deverão ser formalmente motivados nos autos do processo administrativo que ensejou a contratação, sendo assegurado à **CONTRATADA** o direito ao contraditório e ampla defesa.

Parágrafo Terceiro - Quando a rescisão ocorrer por interesse exclusivo da **CEDAE**, sem que haja culpa da **CONTRATADA**, esta será ressarcida dos prejuízos que houver sofrido.

Parágrafo Quarto - A rescisão por ato unilateral da **CEDAE**, quando justificada no descumprimento de obrigações contratuais por parte da **CONTRATADA**, acarretará a aplicação de multa rescisória, no percentual de 10% (dez por cento) calculada sobre o saldo reajustado do contrato, bem como a execução da garantia contratual e/ou a utilização dos créditos decorrentes do próprio contrato.

Parágrafo Quinto - A **CEDAE** se reserva o direito de cobrar indenização suplementar em juízo se ficar constatado que o prejuízo causado foi superior ao valor da multa rescisória aplicada, conforme autorização contida no art. 416, parágrafo único, *in fine,* do Código Civil.

Parágrafo Sexto - A rescisão contratual por acordo entre as partes será da competência das mesmas autoridades referidas no art. 25 do RILC; enquanto a rescisão unilateral ficará a cargo do Diretor responsável pela contratação, conforme art. 15 do Procedimento Interno de Sanções da CEDAE.

Parágrafo Sétimo - A CONTRATADA concorda previamente em aceitar eventual redução qualitativa ou quantitativa de itens, ou a rescisão unilateral do contrato, fundamentada na redução das operações da CEDAE que decorram de processos de concessão dos serviços de saneamento à iniciativa privada pelos municípios remanescentes, renunciando, desde já, a qualquer indenização ou compensação por perdas e danos, devendo ser observada a antecedência mínima de 30 (trinta) dias para comunicação por parte da CEDAE.

CLÁUSULA DÉCIMA-TERCEIRA – DA GARANTIA

A CONTRATADA deverá prestar garantia contratual, optando por uma das modalidades previstas no §1º do art. 70 da Lei 13.303/16.

Parágrafo Primeiro - O comprovante deverá ser apresentado na Tesouraria da CEDAE, no 6º andar do prédio Sede, no prazo máximo de 10 (dez) dias úteis contados da assinatura do instrumento.

Parágrafo Segundo - A garantia deverá ser prestada em percentual correspondente a 5% (cinco por cento) do valor do contrato, com exceção apenas da caução em dinheiro, que poderá ser prestada em percentual inferior, correspondente a 1,5% (um e meio por cento).

Parágrafo Terceiro - A garantia prestada não poderá se vincular a outras contratações, salvo após sua liberação.

Parágrafo Quarto - A garantia que vier a ser prestada na modalidade de seguro ou de fiança bancária deverá ser firmada de modo a abranger todos os prejuízos resultantes da execução deste contrato, decorrentes de conduta dolosa ou culposa da CONTRATADA, incluindo as multas pecuniárias aplicadas pela CEDAE.

Parágrafo Quinto - Se da contratação resultar a transferência da posse direta de bens da CEDAE à CONTRATADA, em valor total superior a **R$ 1.000,000,00 (um milhão de reais),** será exigido, ainda, o ***seguro multirriscos básico***, que conterá as seguintes coberturas adicionais mínimas: Danos Elétricos, Subtração de Bens e Mercadorias, Responsabilidade Civil de Operações, Responsabilidade Civil do Empregador, Equipamentos Estacionários e Móveis, cuja cobertura alcançará o valor total destes bens.

Parágrafo Sexto - A garantia somente poderá ser liberada após o recebimento definitivo do objeto, cabendo à CONTRATADA formular tal solicitação.

Parágrafo Sétimo - A garantia que não for prestada em dinheiro deverá ser firmada com prazo de validade superior à vigência do contrato administrativo em, no mínimo, 90 (noventa) dias.

Parágrafo Oitavo - A **CONTRATADA** se declara ciente de que as alterações de valor e/ou de prazo efetuadas no contrato importarão na necessidade de reforço e/ou prorrogação da garantia prestada, não se eximindo desta responsabilidade mesmo quando silente o aditivo formalizado.

Parágrafo Nono - Nos casos em que os valores das multas vierem a ser descontados da garantia, seu valor original será recomposto no prazo de até 72 (setenta e duas) horas, sob pena de multa e/ou de rescisão administrativa do contrato.

Parágrafo Décimo - A garantia que for prestada na modalidade fiança bancária deverá ser apresentada conforme modelo constante do Anexo VII da OS n. 14.927/2017.

Parágrafo Décimo-Primeiro - O atraso da **CONTRATADA** em prestar ou revalidar a garantia autorizará a CEDAE a promover o bloqueio dos pagamentos devidos até o limite

máximo de 5% (cinco por cento) do valor do contrato. Uma vez prestada a garantia, esta substituirá o bloqueio.

Parágrafo Décimo-Segundo - O bloqueio efetuado com base no parágrafo anterior não gerará direito a nenhum tipo de compensação financeira à **CONTRATADA**.

Parágrafo Décimo-Terceiro - A **CEDAE** se ressalva o direito de pleitear em juízo as perdas e danos que não puderem ser reparados através da garantia prestada.

CLÁUSULA DÉCIMA-QUARTA – DO RECURSO AO JUDICIÁRIO

As importâncias decorrentes de quaisquer penalidades impostas à **CONTRATADA**, inclusive as perdas e danos ou prejuízos que a execução do contrato tenha acarretado, quando superiores à garantia prestada ou aos créditos que a **CONTRATADA** tenha em face da **CEDAE**, que não comportarem cobrança amigável, serão cobrados judicialmente.

Parágrafo Único – Caso a **CEDAE** tenha de recorrer ou comparecer a Juízo para haver o que lhe for devido, a **CONTRATADA** ficará sujeita ao pagamento, além do principal do débito, da pena convencional de 10% (dez por cento) sobre o valor do litígio, dos juros de mora de 1% (um por cento) ao mês, despesas de processo e honorários de advogado, estes fixados, desde logo, em 20% (vinte por cento) sobre o valor em litígio.

CLÁUSULA DÉCIMA-QUINTA – DA ACEITAÇÃO PROVISÓRIA DO OBJETO

A aceitação provisória nos contratos de aquisição ocorrerá conforme o número de parcelas de fornecimento, mediante o recebimento do material no almoxarifado da Companhia ou fora deste, observando-se os seguintes procedimentos:

Parágrafo Primeiro - Os materiais e equipamentos entregues no almoxarifado serão recepcionados e devidamente conferidos pelo Chefe do Almoxarifado. Em seguida, deverão sofrer inspeção técnica por parte do Departamento de Pesquisa de Material e, posteriormente, pela Comissão de Fiscalização do Contrato, que os aceitarão provisoriamente pela emissão do TERMO DE RECEBIMENTO E INSPEÇÃO DE MATERIAL (doc. Ref. ANEXO III da Ordem de Serviço "E" n. 16.107-00 de 2024).

Parágrafo Segundo - Os materiais e equipamentos entregues fora do almoxarifado serão recepcionados por pelo menos um dos membros da Comissão de Fiscalização do Contrato, que será responsável pela verificação das conformidades, validando a aceitação destes, pela emissão do TERMO DE ACEITAÇÃO PARA RECEBIMENTO DE MATERIAL FORA DO ALMOXARIFADO (doc. Ref. ANEXO V da Ordem de Serviço "E" n. 16.107-00 de 2024).

Parágrafo Terceiro - A documentação acessória aos Termos de Recebimento será a estabelecida pela Gerência de Suprimento, bem como os demais procedimentos e prazos implicados nesse processo.

Parágrafo Quarto - Para o pagamento de cada nota fiscal será obrigatória a apresentação dos citados Termos aprovados.

Parágrafo Quinto - Em se tratando de fornecimento contínuo, cada entrega obedecerá o procedimento descrito acima, inclusive quanto aos signatários previstos nos itens 3.1 da OS n. 16.107-00 de 2024. No entanto, nestes casos, na liberação do último pagamento deverá ser observado, no que couber, o procedimento descrito nos itens 2.1 a 25, 2.8 a 2.9 da OS n. 16.107-00 de 2024, conforme previsto no art. 186 RILC

Parágrafo Sexto - A aceitação provisória poderá ser dispensada nas hipóteses mencionadas no item 5 da OS n. 16.107-00 de 2024, caso em que será substituída pela emissão de simples "recibo".

Parágrafo Sétimo - Todos os documentos mencionados nesta cláusula ficarão autuados no processo administrativo referente à contratação, bem como no processo de prestação de contas que deverá ser aberto em virtude da OS "E" nº 14.695/2017.

CLÁUSULA DÉCIMA-SEXTA – DA ACEITAÇÃO DEFINITIVA DO OBJETO

Parágrafo Primeiro - Nos contratos de compras, a emissão do Termo de Aceitação Definitiva ocorrerá mediante a verificação da qualidade e quantidade do material entregue no Almoxarifado da Companhia ou fora deste, observando as seguintes etapas:

Parágrafo Segundo - O Gerente do Contrato solicitará à Comissão de Fiscalização designada o FORMULÁRIO DE ACOMPANHAMENTO DA EXECUÇÃO DO CONTRATO (ANEXO VII), devidamente preenchido e assinado.

Parágrafo Terceiro - Em seguida, procederá à verificação dos Aceites Provisórios emitidos.

Parágrafo Quarto - Inexistindo impropriedades, nos casos até R$ 300.000,00, o Termo de Aceitação Definitiva deverá ser emitido e assinado pelo Gerente do Contrato e Comissão de Fiscalização.

Parágrafo Quinto - Os contratos com valores superiores a R$ 300.000,00, deverão ser assinados conforme descrito no item 9.1 da OS n. 16.107-00 de 2024.

Parágrafo Sexto - A emissão do Termo de Aceitação Definitiva, assinado pelas partes, ocorrerá em até 90 (noventa dias) dias do recebimento da comunicação da Contratada e implicará na liberação da garantia contratual, se houver.

CLÁUSULA DÉCIMA SÉTIMA– DA PUBLICAÇÃO

O extrato desta contratação será publicado no Diário Oficial do Estado, para fins de mera publicidade, e posteriormente divulgado no sítio eletrônico da **CEDAE**.

Parágrafo Único - Após a publicação no Diário Oficial, deverá ser observado o disposto na Deliberação TCE-RJ n. 312/2020 para o envio das informações nos casos exigidos.

CLÁUSULA DÉCIMA OITAVA– DAS MEDIDAS DE INTEGRIDADE – LEI ESTADUAL 7.753/2017

Parágrafo Primeiro - Na execução do presente Contrato é vedado às partes, dentre outras condutas:

a) prometer, oferecer ou dar, direta ou indiretamente, vantagem indevida a agente público ou a quem quer que seja;
b) criar, de modo fraudulento ou irregular, pessoa jurídica para celebrar o presente Contrato;
c) obter vantagem ou benefício indevido, de modo fraudulento, de modificações ou prorrogações do presente Contrato, sem autorização em lei, no ato convocatório da

licitação pública ou nos respectivos instrumentos contratuais;
d) manipular ou fraudar o equilíbrio econômico-financeiro do presente Contrato; ou
e) de qualquer maneira fraudar o presente Contrato; assim como realizar quaisquer ações ou omissões que constituam prática ilegal ou de corrupção, nos termos da Lei nº 12.846/2013 (conforme alterada) ou de quaisquer outras leis ou regulamentos aplicáveis ("Leis Anticorrupção"), ainda que não relacionadas com o presente Contrato.

Parágrafo Segundo - A **CONTRATADA** compromete-se a respeitar, cumprir e fazer cumprir, no que couber, o **Código de Ética e Conduta da CEDAE, presente no link www.cedae.com.br/governancacorporativa.**

Parágrafo Terceiro - A violação aos parágrafos primeiro e segundo pelos administradores, empregados ou prestadores de serviços da **CONTRATADA**, a depender da gravidade da infração e dos danos causados à CEDAE, acarretará na aplicação das sanções administrativas previstas no contrato, rescisão unilateral e/ou ressarcimento de perdas e danos apurados.

Parágrafo Quarto - A comunicação imediata à CEDAE de eventual violação aos parágrafos primeiro e segundo, acompanhada das medidas tomadas pela **CONTRATADA,** suficientes para sanar a violação, desde que preservados os negócios da CEDAE, sua imagem e reputação, serão consideradas como atenuantes para o fim previsto no parágrafo anterior.

Parágrafo Quinto - A **CONTRATADA** se obriga a possuir e manter programa de integridade nos termos da disciplina conferida pela Lei Estadual n.° 7.753/2017 e eventuais modificações e regulamentos subsequentes, consistindo tal programa no "*conjunto de mecanismos e procedimentos internos de integridade, auditoria e incentivo à denúncia de irregularidades e na aplicação efetiva de códigos de ética e de conduta, políticas e diretrizes com o objetivo de detectar e sanar desvios, fraudes, irregularidades e atos ilícitos praticados contra a Administração Pública*".

Parágrafo Sexto - O programa de integridade será obrigatório nos contratos com prazo de vigência igual ou superior a 180 (cento e oitenta) dias cujo valor ultrapasse R$ 885.000,00 (oitocentos e oitenta e cinco mil reais), para compras e serviços, ou R$ 1.973.000,00 (um milhão novecentos e setenta e três mil reais), para obras e serviços de engenharia; sendo facultativo nos demais casos.

Parágrafo Sétimo - A **CONTRATADA** que não possuir o programa de integridade já implantado deverá constituí-lo no prazo de até 180 (cento e oitenta) dias contados da assinatura deste contrato.

Parágrafo Oitavo - O não atendimento ao disposto no parágrafo sétimo implicará na aplicação de multa moratória de 0,02%, por dia, incidente sobre o valor do contrato.

Parágrafo Nono - O montante correspondente à soma dos valores básicos das multas moratórias será limitado a 10% do valor do contrato.

Parágrafo Décimo - O não cumprimento da exigência durante o período contratual acarretará na impossibilidade da contratação da empresa com a Administração Direta e Indireta do Estado do Rio de Janeiro até a sua regular situação.

Parágrafo Décimo-Primeiro - O cumprimento da exigência da implantação não implicará ressarcimento das multas aplicadas.

Parágrafo Décimo-Segundo - Caberá ao Gerente do Contrato, sem prejuízo de suas demais atribuições, conforme estabelecido no artigo 11 da Lei Estadual 7.753 de 02/10/2017, fiscalizar a aplicabilidade de seus dispositivos.

Parágrafo Décimo-Terceiro - As ações e deliberações do Gerente do Contrato não poderão implicar interferência na gestão das empresas nem ingerência de suas competências, devendo ater-se a responsabilidade de aferir a implantação do Programa de Integridade por meio de prova documental emitida pela **CONTRATADA**."

Parágrafo Décimo-Quarto - A prática de atos de contra a Administração Pública Estadual sujeitará a **CONTRATADA** às sanções previstas na Lei Federal nº 12.846/2013, na forma do Decreto Estadual n. 46.366/2018.

CLÁUSULA DÉCIMA NONA – DO SIGILO E DA PROTEÇÃO A DADOS PESSOAIS, COM BASE NA LGPD

9.1 A CONTRATADA deverá manter sigilo sobre toda e qualquer informação confidencial, reservada ou exclusiva, incluindo informações técnicas, de negócio ou financeira, comunicada pela CEDAE, ou obtida em função da execução do objeto contratado, exceto as informações que: a- Sejam de domínio público à época da comunicação; b- Seja conhecida pela parte receptora antes da comunicação ou caia no domínio público sem culpa da parte receptora; c- Seja desenvolvida, de modo independente, pela parte receptora, sem uso de informação confidencial.

9.2 Na forma do disposto no Termo de Referência – Anexo I ao instrumento convocatório, a CEDAE, e a CONTRATADA, devem cumprir a Lei Federal nº 13.709/2018, no âmbito da fiscalização, da guarda dos dados e da execução do objeto deste Contrato.

9.3 A CONTRATADA deve assegurar que o acesso a dados pessoais seja limitado aos empregados, prepostos ou colaboradores que necessitem conhecer/acessar os dados de guarda e responsabilidade da CEDAE, na medida em que sejam estritamente necessários para as finalidades deste Contrato, e cumprir a legislação aplicável, assegurando que todos esses indivíduos estejam sujeitos a compromissos de confidencialidade ou obrigações profissionais de confidencialidade.

9.4 Considerando a natureza dos dados tratados, pertinentes ao objeto desta contratação, a CEDAE e a CONTRATADA deverão adotar, em relação aos dados pessoais, medidas de segurança, técnicas e administrativas, aptas a proteger os dados e informações de acessos, não autorizados, e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

9.5 A CONTRATADA deve notificar imediatamente, à CEDAE, a ocorrência de incidente de segurança, relacionado a dados pessoais, por ela tratados, fornecendo informações suficientes para que a CEDAE cumpra quaisquer obrigações de comunicação da ocorrência, à autoridade nacional, e aos titulares dos dados.

9.6 A CEDAE e a CONTRATADA devem adotar as medidas cabíveis para auxiliar na investigação, mitigação e reparação de cada um dos incidentes de segurança, quando identificada a responsabilização exclusiva, de uma parte e/ou outra.

9.7 A CONTRATADA, na execução dos serviços de plataforma de serviços digitais, deve auxiliar a CEDAE, na elaboração de relatórios de impacto à proteção de dados pessoais, observado o disposto no artigo 38 da Lei Federal nº 13.709/2018, no âmbito da execução deste Contrato.

9.8 Por ocasião do encerramento deste Contrato, a CONTRATADA deve, imediatamente, ou, mediante justificativa, em até 10 (dez) dias úteis da data de seu encerramento, fornecer, a CEDAE, a base de dados do atendimento, inclusive eventuais cópias de dados pessoais tratados no âmbito do Contrato, certificando por escrito, ao CEDAE, o cumprimento desta obrigação.

9.9 A CONTRATADA deve colocar à disposição do CEDAE, conforme solicitado, toda informação necessária para demonstrar o cumprimento do disposto nesta CLÁUSULA, e deve permitir auditorias e contribuir com elas, incluindo inspeções, pelo CEDAE, ou auditor por ele indicado, em relação ao tratamento de dados pessoais do cidadão, que acessar na base de dados da CEDAE.

9.10 Todas as notificações e comunicações, realizadas nos termos desta cláusula, devem se dar por escrito e serem entregues pessoalmente, encaminhadas pelo correio ou por e-mail para os endereços físicos ou eletrônicos informados em documento escrito emitido por ambas as partes por ocasião da assinatura deste Instrumento Contratual, ou outro endereço informado em notificação posterior.

9.11 A CONTRATADA poderá responder por quaisquer danos, perdas ou prejuízos causados a CEDAE, ou a terceiros, decorrentes do descumprimento da Lei Federal nº 13.709/2018, não excluindo ou reduzindo essa responsabilidade a fiscalização do CEDAE em seu acompanhamento.

9.12 Considerando que, o acesso aos dados pessoais, por meio da plataforma digital de serviços, se dará por meio de consulta a base de dados, controlada pela CEDAE, a CONTRATADA deverá obter o consentimento do titular, no momento da interação na plataforma de que trata o inciso I do artigo 7º da Lei nº 13.709/2018, devendo ser observadas pela CONTRATADA ao longo de toda a vigência do contrato todas as obrigações específicas vinculadas a essa hipótese legal de tratamento de dados pessoais.

9.13 É vedada a transferência de dados pessoais, pela CONTRATADA, para fora do território do Brasil sem o prévio consentimento, por escrito, do CEDAE, e demonstração da observância, pela CONTRATADA, da adequada proteção desses dados, cabendo à CONTRATADA o cumprimento de toda a legislação de proteção de dados ou de privacidade de outro (s) país (es) que for aplicável.

9.14 A CONTRATADA não poderá realizar subcontratação.

9.15 A CONTRATADA deve tomar medidas razoáveis para assegurar que empregados, prepostos ou colaboradores de qualquer subcontratado, que necessitem conhecer/acessar dados pessoais relacionados à execução do contrato, estejam sujeitos a compromissos de confidencialidade ou obrigações profissionais de confidencialidade, e cumprir, no tocante à subcontratação, todas as disposições aplicáveis da Lei Federal nº 13.709/2018.

9.16 A subcontratação, mesmo quando autorizada pela CEDAE, não exime a CONTRATADA das obrigações decorrentes deste contrato, de modo que a CONTRATADA permanecerá por elas integralmente responsável perante a CEDAE, inclusive na hipótese de descumprimento dessas obrigações pela subcontratada.

9.17 A CEDAE é a controladora dos dados gerados na prestação dos serviços públicos de atendimento ao cidadão, realizada pela CONTRATADA, cabendo, por meio de normas e regras a serem definidas pela CEDAE, à delegação a CONTRATADA para o tratamento dos dados obtidos.

CLÁUSULA VIGÉSIMA - FORO

Para dirimir quaisquer questões porventura decorrentes deste Contrato, as partes elegem o foro da Comarca da Capital do Rio de Janeiro, com renúncia a qualquer outro, por mais privilegiado que seja.

E, por estarem assim acordes em todas as condições e cláusulas estabelecidas neste contrato, as partes assinam eletronicamente o presente instrumento elaborado em formato digital depois de lido e achado conforme, razão pela qual dispensam a presença de testemunhas.

Pela **CEDAE**:

AGUINALDO BALLON
Diretor Presidente

ANTONIO CARLOS DOS SANTOS
Diretor Administrativo-Financeiro e de Relações com Investidores

Pela **CONTRATADA**:

ROBSON PINTO BOTELHO
Representante

Rio de Janeiro, 20 maio de 2025

Documento assinado eletronicamente por **ROBSON PINTO BOTELHO**, **Usuário Externo**, em 20/05/2025, às 19:22, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Antonio Carlos dos Santos**, **Diretor Financeiro**, em 20/05/2025, às 19:37, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Aguinaldo Ballon**, **Diretor-Presidente**, em 21/05/2025, às 11:26, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **100575173** e o código CRC **6B373517**.

Avenida Presidente Vargas, 2655 - Bairro Cidade Nova, Rio de Janeiro/RJ, CEP 20210-030
Telefone:

Governo do Estado do Rio de Janeiro
Companhia Estadual de Águas e Esgotos do Rio de Janeiro
Diretoria Administrativa

TERMO DE REFERÊNCIA

1. OBJETO

1.1. Aquisição de uma solução integrada de NEXT GENERATION FIREWALL (NGFW) composta de Hardware e Software de segurança da informação do tipo UTM (Unified Threat Management) entendendo-se como tais o conjunto de serviços e recursos de: Filtro de pacotes com controle de estado, Filtro de conteúdo web, Interceptação SSL, Filtro de aplicações, Controle da web 2.0, Inspeção com proteção contra ataques de Malwares, vírus, worm, aplicativos maliciosos, WAF e Sandbox, integrar soluções do tipo (IPS, ATP, QoS, Balanceamento de serviços, Redundância de links, SD-WAN, VPN, DHCP e DNS). Com a capacidade de integrar todos os recursos em um único dispositivo.

2. JUSTIFICATIVA.

2.1. Atualmente já não é mais possível pensar em estruturas de TI, sem levar em consideração ataques de hackers, ataques cibernéticos, que crescem exponencialmente. Devemos proteger os dados e as informações para que não seja utilizada de maneira indevida, obtendo principalmente informações estratégicas.

2.2. Em um ambiente institucional como é o caso da CEDAE, os cuidados devem ser redobrados, tendo em vista a quantidade de dados dos mais diversos tipos, que oferecem um vasto campo para ações de criminosos, seja capturando, fraudando ou simplesmente analisando esses dados e vendendo informações privilegiadas para fornecedores;

2.3. Visando aumentar o nível de segurança do ambiente, a Gerência de Tecnologia da Informação através do seu Departamento de Suporte, Infraestrutura e Segurança da Informação, vem aprimorando e aperfeiçoando a utilização dos recursos de Segurança da Informação, evidenciando a necessidade de investimento em tecnologia, com o intuito de aumentar a disponibilidade, integridade, confidencialidade e segurança das informações institucionais, assim como garantir a boa utilização de todos os serviços;

2.4. Para que seja possível manter adequado nível de segurança da rede corporativa de dados e, assim, preservar os ativos corporativos (hardware, software e dados), torna-se imprescindível a adoção de soluções que gerenciem o acesso a cada um desses recursos, de forma a minimizar os riscos e evitar prejuízos, não só em relação as questões que envolvem tecnologia, mas também de ordem financeira e de imagem institucional;

2.5. Desta forma, torna-se imprescindível a aquisição do objeto.

3. QUANTIDADES

EQUIPAMENTOS					
Item	**Item da ATA**	**IFS**	**Descrição**	**Unidade**	**QT solici**
1	1 - Lote 1		APPLIANCE FIREWALL TIPO 1 - INCLUSOS: HARDWARE, LICENCIAMENTO E GARANTIA POR 60 MESES	Unidade	4
2	2 - Lote 1		CONSOLE DE GERENCIAMENTO CENTRALIZADO PARA O FIREWALL TIPO 1 COM GARANTIA DE 60 MESES	Unidade	2
3	3 - Lote 1		CONSOLE DE GERENCIAMENTO DE LOGS PARA O FIREWALL TIPO 1 COM GARANTIA DE 60 MESES	Unidade	2
4	4 - Lote 1		CONSOLE DE RELATORIA CENTRALIZADA PARA O FIREWALL TIPO 1 COM GARANTIA DE 60 MESES	Unidade	2
5	1 - Lote 3		APPLIANCE FIREWALL TIPO 3 - INCLUSOS: HARDWARE, LICENCIAMENTO E GARANTIA POR 60 MESES	Unidade	1
SERVIÇOS					
6	5 - Lote 1		SERVIÇO DE TREINAMENTO OPERACIONAL PARA A SOLUÇÃO DOS ITENS 1, 2, 3 e 4	Aluno	1

4. CARACTERISTICAS DO OBJETO

4.1. **Características Gerais das Soluções de Firewalls tipos 1 e 3**

4.1.1. **Arquitetura**

4.1.1.1. As soluções de Firewall dos tipos 1 e 3, deverão ser compostas por equipamento do tipo appliance, o software complementar para gerenciamento, logs e relatórios, bem como os treinamentos operacionais para as soluções;

4.1.1.2. Os firewalls gerenciados dos tipos 1 e 3, devem ser capazes de encaminhar pacotes para serem analisados por um sistema e/ou equipamento concentrador;

4.1.2. **Licenciamento**

4.1.2.1. Licença Padrão

4.1.2.2. Entende-se por Licença Padrão a licença de uso do fabricante em caráter permanente e perpétuo para todas as funcionalidades e quantidades mencionadas neste documento, com exceção aos itens relacionados à Atualização de Assinaturas de Proteção.

4.1.2.3. Entende-se por Atualização de Assinaturas de Proteção todas as funcionalidades, manuais ou automatizadas, necessárias para manter a solução em seu nível de identificação e proteção mais atualizado, tais como: atualização de assinaturas de prevenção de intrusão, assinaturas de identificação de vírus, assinaturas de identificação de aplicações, listas de classificação de URLs, listas de geolocalização, listas de endereços IPs utilizados por botnets, listas de endereços IPs de reputação duvidosa etc.

4.1.2.4. Todos os equipamentos firewall devem possuir esta licença ativada.

4.1.3. **Licença de Atualização de Segurança**

4.1.3.1. Entende-se por Licença de Atualização de Segurança a licença de uso do fabricante que permita a utilização das funcionalidades e quantidades mencionadas neste documento para os itens relacionados à Atualização de Assinaturas de Proteção (item 1.1.2.1.).

4.1.3.2. A licença deve permitir que todas as assinaturas, listas e demais métodos de detecção e prevenção de ameaças e de filtros de conteúdo e aplicação empregados pela solução sejam atualizados até suas últimas versões disponíveis.

4.1.3.3. As Licenças de Atualização de Segurança devem ter prazo de vigência de 60 (sessenta) meses, contados a partir da aplicação destas nos produtos.

4.1.4. **Hardware**

4.1.4.1. Deve ser fornecido em formato appliance físico;

4.1.4.2. Deve ser novo, sem uso, entregue em perfeito estado de funcionamento, sem marcas, amassados, arranhões ou outros problemas físicos, acondicionados em suas embalagens originais;

4.1.4.3. Nenhum dos equipamentos fornecidos pode estar em modo End of Life, End of Sale e End of Support no dia do Pregão Eletrônico;

4.1.4.4. Deve ser apropriado para o uso em ambiente tropical com umidade relativa na faixa de 10 a 90% (sem condensação) e temperatura ambiente na faixa de 0 a 40°C;

4.1.4.5. Deve possuir fonte com alimentação nominal de 100~120VAC e 210~230VAC e frequência de 50 ou 60 Hz ou auto-ranging. Deve vir acompanhado de cabo de alimentação com, no mínimo, 1,80m (6 pés), com plug tripolar 2P+T no padrão ABNT NBR 14136;

4.1.4.6. Deve possuir, no mínimo, 1 (uma) interface Ethernet dedicada para gerenciamento;

4.1.4.7. Deve ser fornecido em sua capacidade máxima de processamento, memória e armazenamento interno;

4.1.4.8. Deve ser fornecido com todas as suas portas de comunicação, interfaces e afins habilitadas, operacionais e prontas para operação, inclusive com seus respectivos transceivers instalados, sem custos adicionais;

4.1.4.9. Deve possuir certificação de conformidade sustentável de acordo com os padrões EPA (Environmental Protection Agency) ou similares, tais como EnergyStar, RoHS (Restriction on Harzardous Substances) ou WEEE (Waste Electrical and Eletronic Equipment).

4.1.5. **Funcionalidades Básicas**

4.1.5.1. Deve possuir MIB própria contemplando, no mínimo, indicadores de estado do hardware e de performance do equipamento;

4.1.5.2. Deve suportar o envio de notificações via e-mail, SNMP traps e mensagens de log;

4.1.5.3. Deve permitir o acesso ao equipamento via SSH e interface web HTTPS;

4.1.5.4. A comunicação entre a estação de trabalho do administrador e o firewall deve ser autenticada e criptografada;

4.1.5.5. Deve informar a utilização dos recursos de CPU, memória e atividade de rede;

4.1.5.6. Deve possuir visualização mínima sumarizada de aplicações, ameaças, URLs, endereços de origem, endereços de destino, levando-se em conta o quantitativo de sessões, de consumo de banda e categorização;

4.1.5.7. Deve possuir a funcionalidade de exportação automática dos logs para servidor syslog e para a solução de gerenciamento de logs;

4.1.5.8. Desejável possuir plano de gerenciamento segregado do plano de dados, inclusive com CPU e interfaces dedicadas;

4.1.5.9. Deve permitir a importação, criação e edição de regras SNORT;

4.1.5.10. Os Firewalls de segurança físico ou virtualizados, devem possuir mecanismo para dedicar processamento no equipamento de segurança para funções e ações de Gerenciamento, mesmo que o equipamento esteja com alto processamento de CPU. Assim evitando a falta de acesso do administrador para qualquer mitigação de problema e aplicação de política para solução de problemas. Entre as funções, deve suportar no mínimo: acesso SSH, acesso WEB, alterações de política, comunicação SNMP; 1.6. Console de Gerenciamento centralizado;

4.1.5.11. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7.

4.1.6. **Rede**

4.1.6.1. Deve suportar os protocolos IPv4 e IPv6;

4.1.6.2. Deve suportar VLAN no padrão 802.1q;

4.1.6.3. Deve suportar os protocolos DHCP e DHCPv6 e suas funcionalidades como cliente, servidor e relay;

4.1.6.4. Deve suportar Jumbo Frames;

4.1.6.5. Deve suportar sub interfaces Ethernet lógicas;

4.1.6.6. Deve suportar o protocolo NTP;

4.1.6.7. Deve implementar mecanismo de conversão de endereços NAT (Network Address Translation), de forma a possibilitar a realização de NAT estático (1-1), dinâmico (N-1), NAT pool (N-N) e NAT condicional (possibilitando que um endereço tenha mais de um NAT dependendo da origem, destino ou porta);

4.1.6.8. Deve permitir o registro de eventos de NAT com as informações de endereço interno, endereço público, data e hora do evento, portas de origem e destino;

4.1.6.9. Deve suportar tradução de porta (PAT);

4.1.6.10. Deve suportar as funcionalidades de roteamento estático e dinâmico em IPv4 e IPv6;

4.1.6.11. Deve suportar os protocolos RIP, OSPF v2, OSPF v3 e BGP v4;

4.1.6.12. Deve suportar os protocolos IGMP v2, IGMP v3, PIM-SM;

4.1.6.13. Deve suportar Virtual Routing Redundancy Protocol (VRRP) ou equivalente;

4.1.6.14. Deve suportar os protocolos SNMP v2 e SNMP v3;

4.1.6.15. Deve permitir monitorar, via SNMP, falhas de hardware, uso de recursos por número elevado de sessões, número de túneis estabelecidos na VPN, CPU, memória, status do cluster de Alta Disponibilidade e estatísticas de uso das interfaces de rede;

4.1.6.16. Deve suportar Policy Based Routing (PBR), possibilitando políticas de roteamento condicionado ao endereço IP de origem, endereço IP de destino e porta de comunicação;

4.1.6.17. Deve suportar no mínimo as seguintes funcionalidades em IPv6: SLAAC (address auto configuration), NAT64, Identificação de usuários a partir do LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Regras de proteção contra DoS (Denial of Service), De-criptografia SSL e SSH, PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, IPSEc, VPN SSL, Ativo/Ativo, Ativo/Passivo, SNMP, NTP, SYSLOG, DNS, Neighbor Discovery (ND), Recursive DNS Server (RDNSS), DNS Search List (DNSSL) e controle de aplicação.

4.1.7. **Autenticação e Identificação de Usuários**

4.1.7.1. Deve promover a integração com serviços de diretório LDAP e Active Directory, baseados em caracteres da língua portuguesa, para a identificação, autenticação, autorização e registro de eventos de acessos ou ameaças;

4.1.7.2. Deve identificar de forma transparente os usuários autenticados por meio de serviço de diretório LDAP ou Active Directory;

4.1.7.3. Não será permitida a utilização de agentes instalados nos servidores LDAP, Active Directory, proxies internos e equipamentos dos usuários, nem configuração adicional no navegador;

4.1.7.4. Não será permitida a interceptação ou espelhamento do tráfego destinado aos servidores LDAP, Active Directory e proxies internos;

4.1.7.5. Deve possuir portal de autenticação (captive portal) para a identificação e autenticação de usuários não registrados ou não reconhecidos;

4.1.7.6. O portal de autenticação deve ser capaz de identificar e autenticar usuários cadastrados em serviço de diretório LDAP e Active Directory;

4.1.7.7. Deve permitir a criação de políticas de segurança baseadas em usuários e grupos de usuários pertencentes a um diretório LDAP ou ao Active Directory;

4.1.7.8. Deve registrar a identificação do usuário em todos os logs de eventos de acesso ou de ameaças gerados pelo equipamento;

4.1.7.9. Deve registrar os eventos dos usuários em tempo real, sem a utilização de processos em lote (batches) ou processos de correlação após a ocorrência do evento em questão;

4.1.7.10. Deve possuir a capacidade de definir administradores com diferentes perfis de acesso. Os perfis de acesso devem ser, no mínimo, de leitura/escrita e somente leitura;

4.1.7.11. Desejável possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente, mesmo que não sejam servidores Windows;

4.1.7.12. Desejável identificar usuários através de leitura do campo x-fowarded-for, populando nos logs do firewall o endereço IP, bem como o usuário de rede responsável pelo acesso.

4.1.8. **Geolocalização**

4.1.8.1. Deve identificar os países de origem e destino de todas as conexões estabelecidas através do equipamento;

4.1.8.2. Deve identificar, no mínimo, 180 países;

4.1.8.3. Deve armazenar as listas de geolocalização no próprio equipamento;

4.1.8.4. Deve permitir a criação de políticas de segurança baseadas em geolocalização, permitindo o bloqueio de tráfego com origem ou destino a determinado país ou grupo de países;

4.1.8.5. Deve possibilitar a visualização dos países de origem e destino nos logs de eventos de acessos e ameaças.

4.1.9. **VPN**

4.1.9.1. Deve suportar VPN site-to-site em topologia Full Meshed (todos os gateways possuem links específicos para todos os demais gateways) e Estrela (gateways satélites se comunicam somente com um único gateway central);

4.1.9.2. Deve suportar criptografia 3DES, AES-128, AES-256;

4.1.9.3. Deve suportar integridade de dados com MD5, SHA-1 e SHA-256;

4.1.9.4. Deve suportar o protocolo IKE, fases I e II;

4.1.9.5. Deve suportar os algoritmos RSA e Dif ie-He lman groups 1, 2, 5 e 14;

4.1.9.6. Deve suportar Certificado Digital X.509;

4.1.9.7. Deve suportar NAT-T (NAT Transversal);

4.1.9.8. Deve permitir a criação de túneis VPN SSL/TLS e IPSec;

4.1.9.9. Deve suportar VPN IPSec client-to-site (acesso remoto);

4.1.9.10. Deve possuir cliente próprio para instalação nos dispositivos móveis dos usuários, sem custo adicional;

4.1.9.11. Deve permitir que o usuário realize a conexão VPN por meio de cliente instalado nos sistemas operacionais: Windows, Mac OS ou Linux do seu equipamento ou então por meio de interface web do tipo portal;

4.1.9.12. Caso o acesso seja feito por meio da interface Web, deverá ser compatível com, no mínimo, as versões atualizadas dos seguintes navegadores: Microsoft Edge, Mozilla Firefox e Google Chrome;

4.1.9.13. Deve suportar atribuição de endereço IP nos clientes remotos de VPN;

4.1.9.14. Deve suportar atribuição de DNS nos clientes remotos de VPN;

4.1.9.15. Deve suportar, no mínimo, os protocolos de roteamento estático e dinâmico OSPF e BGP;

4.1.9.16. O túnel IPSec VPN do cliente ao gateway (client-to-site) deve fornecer uma solução de autenticação única (single-sign-on) aos usuários, integrando-se com as ferramentas de Windows login;

4.1.9.17. O túnel IPSec VPN client-to-site deve também possuir autenticação em fator duplo (2FA) aos usuários;

4.1.9.18. Deve permitir criar políticas por usuário e grupos para tráfego de VPN client-to-site;

4.1.9.19. Deve suportar autoridade certificadora integrada ao gateway VPN ou à solução de gerenciamento centralizado;

4.1.9.20. Deve promover a integração com diretórios LDAP e Active Directory para a autenticação de usuários de VPN e regras de acesso;

4.1.9.21. Deve suportar os métodos de autenticação de VPN: usuário e senha de base interna do próprio equipamento, usuário e senha de diretório LDAP, usuário e senha do Active Directory, certificação digital por meio de certificados emitidos por autoridade certificadora integrada ao equipamento ou à solução de gerenciamento centralizado, certificação digital por meio de certificados emitidos por autoridade certificadora integrada ao Active Directory, certificação digital por meio de certificados emitidos por autoridade certificadora no padrão ICP-Brasil;

4.1.9.22. Deve suportar a integração com autoridades certificadoras de terceiros que possam gerar certificados no formato PKCS#12;

4.1.9.23. Deve suportar a solicitação de emissão de certificados à uma autoridade certificadora de confiança (enro lment) via SCEP (Simple Certificate Enro lment Protocol) ou CSR (Certificate Signing Requests);

4.1.9.24. Deve suportar a leitura e verificação de CRLs (Certification Revogation Lists);

4.1.9.25. Deve permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis de SSL;

4.1.9.26. Deve possuir mecanismos de checagem de conformidade do dispositivo remoto;

4.1.9.27. A checagem de conformidade deve permitir verificar, no mínimo, as seguintes informações no cliente remoto: sistema operacional e patches instalados, antivírus e versão instalada, firewall no host.

4.1.10. **Qualidade de Serviço (QoS)**

4.1.10.1. Deve permitir o controle de políticas de uso com base nas aplicações: permitir, negar, agendar, inspecionar e controlar o uso da largura de banda que utilizam cada aplicação ou usuário;

4.1.10.2. Deve suportar a criação de políticas de controle de uso de largura de banda baseadas em: porta ou protocolo, endereço IP de origem ou destino, usuário ou grupo de usuários, aplicações (por exemplo, Youtube e WhatsApp);

4.1.10.3. Deve suportar a priorização em tempo real de protocolos de voz (VoIP) como H.323, SIP;

4.1.10.4. Deve suportar a marcação de pacotes Dif Serv;

4.1.10.5. Deve permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.

4.1.11. **Balanceamento de Links**

4.1.11.1. 1.1.10.1. Deve implementar balanceamento de links utilizando as seguintes métricas e critérios para a escolha do caminho: aplicações, jitter, latência e perda de pacotes, permitindo que administradores configurem os valores de tais parâmetros para definir por qual interface certo tipo de tráfego será enviado;

4.1.11.2. 1.1.10.2. Caso o item acima não seja atendido em sua totalidade, será aceita composição com outro equipamento, do tipo appliance físico, desde que a configuração seja realizada através da interface de gerenciamento do firewall e da Solução de Gerenciamento Centralizada, sem nenhum ônus para a Contratante, garantindo o pleno atendimento das métricas e critérios para a escolha do caminho, segundo o item acima.

4.1.11.3. O appliance físico do item anterior deve possuir throughput igual ou superior à discriminada no throughput das “funcionalidades de Filtro de Pacotes, IPS, Filtro de Conteúdo e Proteção contra Malwares habilitadas simultaneamente” do respectivo firewall.

4.1.11.4. O appliance físico do item anterior deve possuir os mesmos requisitos de fontes de alimentação e de afixação em rack, quando exigidos, do respectivo firewall.

4.1.11.5. Os valores dos parâmetros jitter e latência devem poder ser configurados em unidade mínima de milissegundos (ms);

4.1.11.6. A interface virtual de balanceamento deve suportar agregar no mínimo 4 (quatro) interfaces, podendo ser do tipo: física, sub interface e VPN;

4.1.11.7. Deve suportar balanceamento de link por hash do IP de origem e destino;

4.1.11.8. 1.1.10.6. Deve suportar balanceamento de link por peso. Nesta opção deve ser possível definir o peso de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, 4 (quatro) links WAN;

4.1.11.9. Deve permitir a configuração da funcionalidade de balanceamento em qualquer interface WAN, seja ela MPLS, Internet, 4G/LTE etc;

4.1.11.10. Deve possuir roteamento baseado em políticas e múltiplas saídas (e tipos de saídas) WANs;

4.1.11.11. Deve permitir a configuração de failover entre links principais e secundários, caso os links utilizados ultrapassem os limites previamente

definidos de jitter, latência e perda de pacotes. Estes limites podem ser configurados para forçar o failover caso apenas um ou todos os limites sejam atingidos simultaneamente;

4.1.11.12. Deve suportar a configuração de regras que permita o failback imediato;

4.1.11.13. Deve ser compatível com a solução de VPN, permitindo que suas características e análises sejam realizadas nas VPNs, assim como em links WAN;

4.1.11.14. Deve ser compatível com VPNs montadas em interfaces virtuais com roteamento dinâmico;

4.1.11.15. Deve realizar o gerenciamento de tráfego por tipo de aplicação;

4.1.11.16. Deve selecionar o melhor caminho baseado em tipo de tráfego e do host de origem;

4.1.11.17. Deve suportar o monitoramento de link com ping e TCP echo; 1.1.10.16. Deve suportar o monitoramento de links VPN (interfaces virtuais);

4.1.11.18. Deve permitir a exportação de informações via netflow.

4.1.12. **Recursos de Segurança**

4.1.12.1. Deve possuir, no mínimo, funcionalidades Anti-Vírus, Anti-Bot, Anti-Malware, AntiSpyware, Sistema de Prevenção de Intrusão (IPS), Filtro de Conteúdo Web, Controle de Aplicação, Prevenção de Perdas de Dados (DLP). E sistemas de prevenção de ameaças de ZeroDay;

4.1.12.2. Deve suportar o funcionamento nos modos snifer (para inspeção de tráfego gerado por uma porta de rede espelhada), layer-2, layer-3, de forma simultânea em uma única instância de firewall;

4.1.12.3. Deve aplicar novas políticas de segurança sem provocar indisponibilidade de serviço ou descontinuidade das conexões ativas;

4.1.12.4. Deve suportar as atualizações automáticas das bases de assinaturas utilizadas na identificação de vírus, intrusões (IPS) e aplicações sem a necessidade de intervenção manual pelo administrador, sem perda das conexões ativas e sem reinicialização do equipamento;

4.1.12.5. Deve suportar as atualizações automáticas das listas de geolocalização e das listas e categorias de URLs sem a necessidade de intervenção manual pelo administrador, sem perda das conexões ativas e sem reinicialização do equipamento;

4.1.12.6. Deve possuir proteção contra ataques, no mínimo, dos tipos: IP Spoofing, Negação de Serviço (DoS e DDoS), SYN Flood Attack, ICMP Flood Attack e UDP Flood Attack, Buffer Overflow, Port Scanning, Man-in-the-Middle;

4.1.12.7. Deve identificar, decriptografar e analisar o tráfego SSL tanto em conexões de entrada (inbound) quanto de saída (outbound), com suporte a HTTP/2 e TLS 1.2 e 1.3;

4.1.12.8. Deve permitir a decriptografia da área útil do pacote de dados (payload) para fins de controle de acesso à Internet e proteção contra ameaças;

4.1.12.9. Deve permitir a diferenciação de conexões pessoais (bancos, shopping etc) e conexões não pessoais por meio de classificação automática;

4.1.12.10. Deve possuir funcionalidade de backup e restore da configuração e das políticas de segurança;

4.1.12.11. Deve armazenar os backups localmente, ou na solução de gerenciamento centralizado, e permitir que sejam transferidos para equipamentos externos por meio dos protocolos FTP ou SCP;

4.1.12.12. Deve possuir a capacidade de identificar ataques de Advanced Persistent Threat (APT) ou Zero-Day;

4.1.12.13. Deve possuir a capacidade de emular um ambiente operacional isolado e seguro (Sandbox), na nuvem do fabricante, para execução e observação de código malicioso, sem a utilização de assinaturas, com base na atividade, como, por exemplo, operações de arquivo, alterações de registro e sistema etc.;

4.1.12.14. Deve suportar a análise em pelo menos dois dos seguintes sistemas operacionais: Windows, Linux, MacOS e Android;

4.1.12.15. Deve suportar a análise dos tipos de arquivos: documentos Microsoft Office, dll, exe, pdf, gzip, tar, zip;

4.1.12.16. Deve suportar a análise dos protocolos HTTP/HTTPS, FTP e SMTP;

4.1.12.17. Desejável que a análise de links em sandbox seja capaz de classificar sites falsos na categoria de phishing e atualizar a base de filtro de URL da solução;

4.1.12.18. Para ameaças trafegadas em protocolo SMTP e POP3, é desejável que a solução seja capaz de mostrar nos relatórios o remetente, destinatário e assunto dos e-mails, permitindo identificação ágil do usuário vítima do ataque;

4.1.12.19. Deve permitir visualizar os resultados das análises de malwares de dia zero nos diferentes sistemas operacionais suportados;

4.1.12.20. Deve permitir informar ao fabricante quanto a suspeita de ocorrências de falso-positivo e falso- negativo na análise de malwares de dia zero;

4.1.12.21. Deve atualizar a base com assinaturas para bloqueio dos malwares identificados em sandbox de maneira automática;

4.1.12.22. Desejável permitir o envio para análise em sandbox de malwares bloqueados pelo antivírus;

4.1.12.23. Para ameaças trafegadas em protocolo SMTP e POP3, a solução deve ter a capacidade de mostrar nos relatórios o remetente, destinatário e assunto dos e-mails permitindo identificação ágil do usuário vítima do ataque;

4.1.12.24. O sistema de análise “In Cloud” ou local deve prover informações sobre as ações do Malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo Malware, gerar assinaturas de Antivírus e Anti-spyware automaticamente, definir URLs não confiáveis utilizadas pelo novo Malware e prover informações sobre o usuário infectado (seu endereço IP e seu login de rede);

4.1.12.25. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e class), Android APKs MacOS (mach-O, DMG e PKG), Linux (ELF), RAR e 7-ZIP no ambiente de sandbox;

4.1.12.26. A solução deve analisar os arquivos do tipo malware em bare metal para evitar técnicas de evasão. Caso não possua essa funcionalidade será permitido a integração com ferramentas que executem esta função;

4.1.12.27. A solução deve possuir a capacidade de analisar em sand-box os links (http e https) presentes no corpo de e-mails trafegados em SMTP e POP3.

4.1.12.28.

4.1.13. **Filtro de Pacotes**

4.1.13.1. Não deve possuir restrições ao número de máquinas ou usuários protegidos;

4.1.13.2. Deve informar o número de sessões simultâneas;

4.1.13.3. Deve suportar a implementação tanto em modo transparente (layer-2) quanto em modo gateway (layer-3);

4.1.13.4. Deve suportar Statefull Packet Inspection de tráfego IPv4 e IPv6;

4.1.13.5. Deve suportar controle de acesso para serviços e protocolos pré-definidos, bem como possibilitar a adição de novos serviços e protocolos;

4.1.13.6. Deve suportar os protocolos H.323, SIP;

4.1.13.7. Deve implementar mecanismo de proteção contra ataques de falsificação de endereços IP (anti-spoofing);

4.1.13.8. Deve implementar mecanismo de captura de pacotes, de forma manual ou automática, quando uma ameaça for detectada;

4.1.13.9. Deve identificar os usuários para qualquer protocolo ou aplicação baseada em TCP, UDP e ICMP;

4.1.13.10. Deve suportar a utilização simultânea de políticas de segurança em IPv4 e IPv6;

4.1.13.11. Deve suportar a implementação de políticas de segurança baseadas em: portas, protocolos, usuários, grupos de usuários, endereços IP, redes CIDR/VLSM, horário ou período de tempo, e suas combinações;

4.1.13.12. Deve suportar a consulta a fontes externas de endereços IP, domínios e URL's podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego;

4.1.13.13. Desejável possuir mecanismos de otimização de regras. De forma que com base na análise de tráfego o sistema automaticamente faça sugestões e melhorias nas regras existentes;

4.1.13.14. 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.

4.1.14. **Filtro de Conteúdo**

4.1.14.1. Deve prover o controle e proteção de acesso à Internet por meio do reconhecimento de aplicações, independente de porta e protocolo, e da classificação de URLs;

4.1.14.2. Deve ser capaz de identificar aplicações, independentemente das portas e protocolos, bem como das técnicas de evasão utilizadas;

4.1.14.3. Deve ser capaz de identificar se as aplicações estão utilizando sua porta padrão;

4.1.14.4. Deve ser capaz de identificar aplicações encapsuladas dentro de protocolos, como HTTP e HTTPS;

4.1.14.5. Deve ser capaz de identificar aplicações criptografadas usando SSL;

4.1.14.6. Deve ser capaz de identificar um mínimo de 1.400 (mil e quatrocentas) aplicações, incluindo, mas não se limitando a: peer-to-peer, streaming e download de áudio, streaming e download de vídeo, update de software, instant messaging, redes sociais, proxies, anonymizers, acesso e controle remoto, VOIP e email;

4.1.14.7. Deve ser capaz de identificar, no mínimo, as seguintes aplicações: Bittorrent, Youtube, Livestream, Skype, Viber, WhatsApp, Snapchat, Facebook, Facebook Messenger, Instagram, Twitter, Linkedin, Dropbox, Google Drive, One Drive, Logmein, Teamviewer, MS-RDP, VNC, Ultrasurf, TOR, Webex;

4.1.14.8. Deve armazenar a base de assinaturas no próprio equipamento;

4.1.14.9. Deve classificar as aplicações em categorias;

4.1.14.10. Deve permitir o agrupamento de aplicações em grupos personalizados;

4.1.14.11. Deve identificar os usuários que estão utilizando as aplicações;

4.1.14.12. Deve permitir o bloqueio de aplicações que não estejam utilizando suas portas padrão;

4.1.14.13. Deve suportar a implementação de políticas de segurança baseadas em: aplicações, categorias de aplicações, endereço IP de origem ou destino, rede CIDR/VLSM de origem ou destino, usuário ou grupo de usuários, horário ou período de tempo, e suas combinações;

4.1.14.14. Deve permitir a utilização ou bloqueio individualizado das aplicações, como BitTorrent e Skype, para determinados usuários ou grupos de usuários;

4.1.14.15. Deve permitir o registro de todos os fluxos autorizados/bloqueados das aplicações, incluindo o usuário identificado;

4.1.14.16. Deve permitir o controle de uso de banda de download ou upload utilizada pelas aplicações (traffic shaping) baseado em: endereço IP ou rede CIDR/VLSM de origem ou destino, usuário ou grupo de usuários, horário ou período de tempo, e suas combinações;

4.1.14.17. Deve ser capaz de efetuar a classificação de conteúdo de páginas web em HTTP e HTTPS, baseado em listas de categoria;

4.1.14.18. Deve possuir funcionalidades de tratamento de conteúdo web, devendo sua base de dados conter, no mínimo, 10 (dez) milhões de sites internet web já registrados e classificados, distribuídos em, no mínimo, 60 (sessenta) categorias ou subcategorias pré-definidas ou suas semelhantes: conteúdo adulto, chat, drogas ilegais, jogos de azar, jogos, pirataria, proxy remoto, redes sociais, streaming media, violência, pornografia, racismo, malware;

4.1.14.19. Deve permitir a inclusão de URLs customizadas por política (whitelist);

4.1.14.20. Deve armazenar as listas de categoria no próprio equipamento;

4.1.14.21. Deve identificar os usuários que estão acessando as páginas web;

4.1.14.22. Deve suportar a implementação de políticas de segurança baseadas em: URLs, categorias de URLs, endereço IP de origem ou destino, rede CIDR/VLSM de origem ou destino, usuário ou grupo de usuários, horário ou período de tempo, e suas combinações;

4.1.14.23. Deve alertar o usuário quando uma URL for bloqueada, por meio de página de bloqueio que possa ser customizada, e que informe, no mínimo, o motivo do bloqueio e a categoria na qual a URL foi classificada;

4.1.14.24. Deve 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 possibilitar o usuário continuar acessando o site);

4.1.14.25. Deve permitir registrar todos os acessos autorizados ou bloqueados às páginas web, incluindo sua classificação e o usuário identificado;

4.1.14.26. Desejável permitir habilitar aplicações SaaS apenas no modo corporativo e bloqueá-las quando usadas no modo pessoal;

4.1.14.27. Desejável identificar o uso de táticas evasivas, ou seja, ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas;

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

4.1.14.29. Deve permitir bloquear o acesso a sites de busca (Google, Bing, Yahoo), caso a opção Safe Search esteja desabilitada;

4.1.14.30. Deve suportar base ou cache de URL's local no appliance, evitando delay de comunicação/validação das URL's;

4.1.14.31. Desejável que a categorização de URL's analise a URL ao menos até o nível de diretório;

4.1.14.32. Desejável que a solução proteja contra o roubo de credenciais, usuários e senhas identificadas através da integração com Active Directory submetidos em sites não corporativos. Desejável ainda que permita a criação de regras onde usuários do Active Directory só possam enviar informações de login para sites autorizados;

4.1.14.33. Deve prover análise em tempo real de páginas maliciosas e dessa forma permitir a proteção em tempo real antes mesmo da atualização das bases de dados de URLs. Caso o fabricante não possua esta funcionalidade em sua plataforma será permitida a composição da solução, sem ônus a este órgão.

4.1.15. **Prevenção de Intrusão (IPS)**

4.1.15.1. Deve possuir tecnologia de detecção e prevenção de ataques e intrusões baseada em assinatura;

4.1.15.2. Possuir, no mínimo, um conjunto de 10.000 (dez mil) assinaturas de detecção e prevenção de ataques;

4.1.15.3. Detectar protocolos independentemente da porta utilizada, identificando aplicações conhecidas em portas não-padrão;

4.1.15.4. 1.1.14.4. Deve possuir, no mínimo, os seguintes mecanismos de detecção e prevenção: assinaturas de vulnerabilidades e exploits, assinaturas de ataques, validação de protocolos, detecção de anomalias, IP defragmentation, remontagem de pacotes TCP, nível de severidade do ataque;

4.1.15.5. Deve ser capaz de inspecionar tráfego criptografado usando SSL;

4.1.15.6. Deve ser capaz de inspecionar integralmente todos os pacotes de dados, independentemente de seus tamanhos;

4.1.15.7. Deve identificar os usuários relacionados aos eventos de intrusão;

4.1.15.8. Deve identificar os usuários relacionados aos eventos de bloqueio;

4.1.15.9. Deve permitir a criação de políticas de segurança que alertem, sem bloquear, sobre a ocorrência de um determinado ataque ou ameaça;

4.1.15.10. Deve permitir a criação de políticas de segurança que bloqueiem uma determinada ameaça;

4.1.15.11. Deve permitir a criação de políticas de segurança que bloqueiem um determinado ataque por meio de uma ação de DROP/RESET;

4.1.15.12. Deve permitir registrar todos os eventos de IPS, incluindo o usuário identificado;

4.1.15.13. Deve identificar e bloquear a comunicação com botnets

4.1.15.14. Deve bloquear malwares e spywares;

4.1.15.15. Deve inspecionar e bloquear vírus nos seguintes tipos de tráfego, no mínimo: HTTP, HTTPS, SMTP, POP3, FTP e SMB;

4.1.15.16. Deve suportar proteção contra vírus em conteúdo HTML e javascrip, software espião (spyware) e worms;

4.1.15.17. Deve suportar a inspeção de vírus em arquivos comprimidos utilizando o algoritmo deflate (zip, gzip etc);

4.1.15.18. Deve suportar bloqueio de download de pelo menos 45 tipos de arquivos;

4.1.15.19. Deve armazenar as bases de assinaturas no próprio equipamento;

4.1.15.20. Deve possuir a capacidade de detectar e prevenir contra ameaças em tráfego HTTP/2.

4.1.16. **Características Gerais das Consoles**

4.1.16.1. **Console de Gerenciamento Centralizado**

4.1.16.1.1. Deve ser fornecida em appliance virtual, compatível VMware vSphere ESXi 6.0 ou superior, ou baseado em software, compatível com Windows Server 2012 R2 ou superior, ou em appliance físico com suporte à fixação em bastidor (rack) padrãoEIA-310 com largura de 19' (dezenove polegadas) e altura de até duas unidades de rack (2U), acompanhado de todos os acessórios necessários (cabos, suportes, gavetas, braços, trilhos etc.);

4.1.16.1.2. Deve ser acessada via interface web ou através de um software cliente, com interface gráfica, instalado no Windows ou Linux;

4.1.16.1.3. Deve estar licenciada em caráter permanente/perpétuo para todas as funcionalidades e quantidades mencionadas;

4.1.16.1.4. Deve estar licenciada e permitir a gerência centralizada de, no mínimo, 15 equipamentos;

4.1.16.1.5. Deve estar licenciada para o limite máximo de usuários, objetos, regras de segurança, NAT e endereços IP suportados pela solução;

4.1.16.1.6. As comunicações entre a CGC e os firewalls e entre a CGC e as estações dos administradores do sistema devem ser criptografadas e autenticadas;

4.1.16.1.7. Deve ser capaz de realizar todas as configurações nos firewalls descritas nesta ata;

4.1.16.1.8. Deve possibilitar a aplicação simultânea de configurações em todos os firewalls gerenciados pela solução;

4.1.16.1.9. Deve permitir a criação e distribuição de políticas de segurança de forma centralizada, suportando organização hierárquica de regras;

4.1.16.1.10. Deve suportar, por meio da interface gráfica de gerenciamento, a criação e administração de políticas de filtro de pacotes, prevenção de intrusão, controle de aplicação, filtragem de URLs, monitoração de logs, debugging, troubleshooting e captura de pacotes;

4.1.16.1.11. Deve ser capaz de gerenciar os firewa ls em unidades remotas, fora da rede local;

4.1.16.1.12. Deve permitir a autenticação dos administradores através de contas locais e bases externas LDAP ou Active Directory;

4.1.16.1.13. Será permitido que a solução de gerenciamento centralizado possua um “appliance virtual” específico para atendimento às necessidades de identificação e autenticação de usuários;

4.1.16.1.14. Deve possuir a capacidade de definir administradores com diferentes perfis de acesso. Os perfis de acesso devem ser, no mínimo, de leitura/escrita e somente leitura;

4.1.16.1.15. Deve permitir a criação de perfis customizados;

4.1.16.1.16. Deve permitir, de forma granular, assinalar permissões para os administradores criarem outros usuários, alterarem e ler configurações etc.;

4.1.16.1.17. Deve permitir múltiplos administradores acessando o equipamento simultaneamente, sem restrição para leitura e escrita;

4.1.16.1.18. Deve suportar o bloqueio de alterações, evitando o conflito de configurações entre diferentes administradores efetuando alterações simultaneamente;

4.1.16.1.19. Deve registrar, em log de auditoria, as ações dos usuários administradores com o horário da alteração;

4.1.16.1.20. Deve suportar a identificação e utilização de usuários nas políticas de segurança;

4.1.16.1.21. Deve suportar agrupamento lógico de objetos ("object grouping") para criação de regras;

4.1.16.1.22. Deve possibilitar o gerenciamento (incluindo a criação, alteração, monitoração e exclusão) de objetos de rede. Deve ainda permitir detectar se e onde, na base de regras, está sendo utilizado determinado objeto de rede. Os tipos de objetos deverão permitir especificar de forma distinta grupos e objetos de rede e serviços, diferenciando-os e agrupando-os conforme suas características ou descrição de maneira a permitir o reaproveitamento dos mesmos em diferentes políticas;

4.1.16.1.23. Deve possibilitar a especificação de política por tempo, ou seja, permitir a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

4.1.16.1.24. Deve garantir que quando houver novas versões de software dos equipamentos, seja realizada a distribuição e atualização remota, de maneira centralizada;

4.1.16.1.25. Deve ser capaz de testar a conectividade dos equipamentos gerenciados;

4.1.16.1.26. Deve suportar configuração das funcionalidades de alta disponibilidade dos dispositivos físicos;

4.1.16.1.27. Deve permitir localizar em quais regras um objeto está sendo utilizado;

4.1.16.1.28. Deve permitir a identificação e exclusão de regras e objetos que estão aplicadas nos dispositivos, mas não afetam o desempenho e a segurança da rede (regras e objetos em desuso sob o ponto de vista lógico);

4.1.16.1.29. Deve suportar a geração de alertas automáticos via SNMP e syslog;

4.1.16.1.30. Deve informar a utilização dos recursos de CPU, memória e atividade de rede dos equipamentos gerenciados;

4.1.16.1.31. Deve informar o número de conexões simultâneas dos equipamentos gerenciados;

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

4.1.16.1.33. As consoles de gerenciamento centralizado, gerenciamento de logs, relatoria centralizada, poderão ser entregues em um único appliance, desde que atenda a todas as exigências deste documento.

4.1.16.2. **Console de Gerenciamento de Logs**

4.1.16.2.1. Deve ser fornecida em appliance virtual, compatível VMware vSphere ESXi 6.0 ou superior, ou baseado em software, compatível com Windows Server 2012 R2 ou superior, ou em appliance físico com suporte à fixação em bastidor (rack) padrãoEIA-310 com largura de 19’ (dezenove polegadas) e altura de até duas unidades de rack (2U), acompanhado de todos os acessórios necessários (cabos, suportes, gavetas, braços, trilhos etc);

4.1.16.2.2. Deve possuir relatórios de utilização dos recursos por aplicação, URLs, ameaças e etc;

4.1.16.2.3. Deve possuir visualização sumarizada de todas as aplicações, ameaças e URLs que foram identificadas e controladas pela solução; 1.2.2.4. Deve permitir a criação de relatórios customizados;

4.1.16.2.4. Deve ser capaz de receber logs de todos os firewa ls especificados nesta ATA;

4.1.16.2.5. Deve possibilitar a filtragem dos logs do equipamento por, no mínimo: aplicação, endereço IP de origem e destino, país de origem e destino, usuário e horário;

4.1.16.2.6. Deve possibilitar o registro dos fluxos de dados relativos a cada sessão, armazenando: endereços IP de origem e destino dos pacotes, traduções NAT, portas e protocolos de origem e destino, usuário identificado, ação sobre o pacote (permitido ou negado);

4.1.16.2.7. Deve possuir relatórios com informações consolidadas sobre: as mais frequentes fontes de conexões bloqueadas com seus destinos e serviços; os mais frequentes ataques e ameaças de segurança detectados com suas origens e destinos; os serviços de rede mais utilizados,

as aplicações maiores consumidoras de banda de Internet; os usuários maiores consumidores de banda de Internet; e os sítios na Internet mais visitados;

4.1.16.2.8. Deve possuir funcionalidade de exportação de relatórios e logs para o computador local ou via FTP, SFTP ou SCP;

4.1.16.2.9. Deve permitir a geração automática e agendada dos relatórios;

4.1.16.2.10. Deve estar licenciada em caráter permanente/perpétuo para todas as funcionalidades e quantidades mencionadas;

4.1.16.2.11. Deve estar licenciada e permitir a correlação de todos os eventos gerados por todos os equipamentos e contextos virtuais que compõem a solução;

4.1.16.2.12. Deve ser capaz de armazenar, no mínimo, 150 GB de logs diários;

4.1.16.2.13. O appliance virtual deve ser capaz de armazenar, no mínimo 4 TB de logs em disco disponibilizado para o mesmo;

4.1.16.2.14. Deve ser acessada via interface web ou através de um software cliente, com interface gráfica, instalado no Windows ou Linux;

4.1.16.2.15. Será permitida a entrega do "Console de Gerenciamento de Logs" como software agregado ao "Console de Gerenciamento Centralizado" ou ao "Console de Relatoria Centralizada".

4.1.16.3. **Console de Relatoria Centralizada**

4.1.16.3.1. Deve ser fornecida em appliance virtual, compatível com VMware vSphere ESXi 6.5 ou superior, ou baseado em software, compatível com Windows Server 2012 R2 ou superior;

4.1.16.3.2. Deve ser acessada via interface web ou através de um software cliente, com interface gráfica, instalado no Windows ou no Linux;

4.1.16.3.3. Deve estar licenciada em caráter permanente/perpétuo para todas as funcionalidades e quantidades mencionadas;

4.1.16.3.4. Deve estar licenciada e permitir a gerência centralizada de relatórios, para no mínimo, 15 equipamentos;

4.1.16.3.5. As comunicações entre a Console de Relatoria e os firewalls e entre a Console de Relatoria e as estações dos administradores do sistema devem ser criptografadas e autenticadas;

4.1.16.3.6. Deve ser capaz de gerar relatórios de equipamentos em unidades remotas, fora da rede local;

4.1.16.3.7. Deve permitir a autenticação dos administradores através de contas locais e bases externas LDAP ou Active Directory;

4.1.16.3.8. A console deve suportar acesso via SSH, cliente e WEB (HTTPS);

4.1.16.3.9. Coletar logs dos Firewalls, do "Console de Gerenciamento Centralizado" e do "Console de Gerenciamento de Logs";

4.1.16.3.10. Garantir a geração de relatórios com mapas geográficos, ou modo tabela, gerados em tempo real, para a visualização de origens e destinos do tráfego;

4.1.16.3.11. Permitir a extração de relatórios;

4.1.16.3.12. Possuir relatórios pré-definidos;

4.1.16.3.13. Permitir a geração de relatórios de logs de tráfego de dados;

4.1.16.3.14. Permitir a geração de relatórios de logs para auditoria das configurações de regras, objetos e acessos;

4.1.16.3.15. Possibilitar o envio de maneira automática de relatórios por e-mail;

4.1.16.3.16. Permitir o agendamento da geração de relatórios;

4.1.16.3.17. Ter a capacidade de definir filtros nos relatórios;

4.1.16.3.18. Gerar alertas automáticos via e-mail, snmp e syslog baseados em eventos de ocorrência como log, severidade de log, entre outros;

4.1.16.3.19. Permitir a criação de painéis (dashboards) customizados para visibilidades do tráfego de aplicativos, categorias de url, ameaças, serviços, países, origem e destino;

4.1.16.3.20. Possibilitar a visualização na interface gráfica de usuário (gui) da "console de relatoria centralizada as seguintes informações do sistema: logs diários recebidos, alertas gerados, entre outros;

4.1.16.3.21. Será permitida a entrega do "Console de Relatoria Centralizada" como software agregado ao "Console de Gerenciamento Centralizado" ou ao "Console de Gerenciamento de Logs".

4.1.17. **Características Específicas do Firewall Tipo 1**

4.1.17.1. Throughput de 40 Gbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito;

4.1.17.2. Em relação ao filtro de pacotes, deve possuir o Throughput de no mínimo 60 Gbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir;

4.1.17.3. Em relação ao túnel IPSec VPN, o throughput mínimo deverá ser de no mínimo 40 Gbps, com a inspeção e controle de aplicação e usuários ativada;

4.1.17.4. Deve permitir, no mínimo, 12.000.000 de conexões simultâneas;

4.1.17.5. Deve permitir, no mínimo, 600.000 novas conexões por segundo;

4.1.17.6. Deve permitir, no mínimo, 4000 VLANs;

4.1.17.7. Deve permitir, no mínimo, 12.000 túneis VPN site-to-site simultâneos;

4.1.17.8. Deve permitir, no mínimo, 25.000 túneis VPN client-to-site simultâneos;

4.1.17.9. Deve suportar afixação em bastidor (rack) padrão EIA-310 com largura de 19’ (dezenove polegadas) e altura de até quatro unidades de rack(4U), acompanhado de todos os acessórios necessários (cabos, suportes, gavetas, braços, trilhos etc);

4.1.17.10. Deve possuir 2 (duas) fontes de alimentação independentes, redundantes e hotswappable;

4.1.17.11. 2.1.11. O appliance deve possuir, no mínimo, 8 (oito) portas 100/1000/10000 BASE-T ou SFP podendo ser uma composição entre os dois tipos, acompanhadas de seus respectivos transceivers 1G BASE- T;

4.1.17.12. Deve possuir, no mínimo, 10 (dez) interfaces SFP/SFP+, com transceivers SFP+ 10GB-SR, para conexão ao meio via cabo de fibra ótica;

4.1.17.13. Deve possuir, no mínimo, 4 (quatro) interfaces 25 Gbps para utilização de transceivers padrão SFP28;

4.1.17.14. Deve possuir, no mínimo, 4 (quatro) interfaces 40/100 Gbps para utilização de transceivers padrão QSFP+/QSFP28;

4.1.17.15. Deve possuir, disco Solid State Drive (SSD) de, no mínimo, 400 GB;

4.1.17.16. Deve possuir, no mínimo, 20 sistemas virtuais lógicos (Contextos) no firewall Físico.

4.1.18. **Alta Disponibilidade**

4.1.18.1. Deve possibilitar a operação em alta disponibilidade (HA) no equipamento, permitindo uma arquitetura ativo/ativo e ativo/passivo com no mínimo 2 (dois) membros, com sincronismo de estados integrado;

4.1.18.2. Deve suportar o balanceamento de carga na arquitetura ativo/ativo;

4.1.18.3. Deve sincronizar sessões TCP/IP, tabelas NAT, tabelas FIB, associações de segurança das VPNs e todas as configurações necessárias para a manutenção da continuidade dos serviços;

4.1.18.4. Deve monitorar a falha dos links de comunicação;

4.1.18.5. Deve ser capaz de identificar e iniciar automaticamente um procedimento de failover sempre que ocorrer: a falha de um dos membros do cluster, a falha de qualquer componente ou processo crítico de um dos membros do cluster, a falha de um dos links de comunicação monitorados;

4.1.18.6. Deve ser capaz de realizar os procedimentos de failover sem perda das conexões ativas e sessões estabelecidas de forma transparente para o usuário;

4.1.18.7. Deve suportar a operação em cluster com no mínimo 2 equipamentos;

4.1.18.8. Desejável possuir 2 fans independentes, redundantes e hot swappable;

4.1.18.9. Deve possuir discos de sistema e de logs independentes e redundantes (RAID).

4.1.19. Características Específicas do Firewall Tipo 3

4.1.19.1. Throughput de 2 Gbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito.

4.1.19.2. Em relação ao filtro de pacotes, deve possuir o throughput mínimo de 4 Gbps.

4.1.19.3. Em relação ao túnel IPSec VPN, deve possuir o throughput mínimo de 3 Gbps.

4.1.19.4. Deve permitir, no mínimo, 350.000 conexões simultâneas.

4.1.19.5. Deve permitir, no mínimo, 65.000 novas conexões por segundo.

4.1.19.6. Deve permitir, no mínimo, 4000 VLANs.

4.1.19.7. Deve permitir, e estar licenciado para utilização de 2000 túneis VPN site-to-site simultâneos.

4.1.19.8. Deve permitir, e estar licenciado para utilização de 1500 túneis VPN client-to-site simultâneos.

4.1.19.9. Deve suportar a fixação em bastidor (rack) padrão EIA-310 com largura de 19’ (dezenove polegadas) e altura de no máximo uma unidade de rack (1U), acompanhado de todos os acessórios necessários (cabos, suportes, gavetas, braços, trilhos etc).

4.1.19.10. O appliance deve possuir, no mínimo, 08 (oito) portas de rede 1G RJ-45.

4.1.19.11. O appliance deve possuir uma porta 10/100/1000 para gerenciamento “out-of-band”.

4.1.19.12. Deve possuir, disco Solid State Drive (SSD) ou cartão eMMC de, no mínimo, 128GB.

5. Garantia técnica do produto fornecido

5.1.1. A Garantia dos itens 1, 2, 3, 4 de todos os lotes, obedecerá às seguintes regras:

5.1.2. Considera-se “garantia” a obrigação da CONTRATADA em reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, o objeto do contrato (e quaisquer de seus componentes) em que se verificarem vícios de produto, defeitos ou incorreções, durante o prazo de garantia especificado neste documento;

5.1.3. A garantia terá duração de 60 (sessenta meses), contados a partir da data do recebimento definitivo do objeto;

5.1.4. A garantia deve obrigatoriamente prover, ao longo de sua duração e sem ônus adicionais para o contratante:

5.1.5. Acesso para downloads de patches, drivers, e quaisquer outras atualizações de software necessárias, que devem estar disponíveis no website do fabricante da solução, sem custos adicionais ao Contratante, durante todo o período de garantia.

5.1.6. Disponibilizar as revisões dos manuais técnicos e/ou documentação dos equipamentos adquiridos.

5.2. **ASSISTÊNCIA TÉCNICA – SUPORTE TÉCNICO**

5.2.1. A contratada deverá disponibilizar por meio da Internet uma aplicação WEB para registro dos chamados de suporte técnico através de login e senha fornecida para os usuários autorizados da contratante, em regime de 24x7x365 (vinte e quatro horas por dia durante todos os dias do ano, inclusive sábados, domingos e feriados);

5.2.2. A contratante poderá efetuar um número ilimitado de chamados para suporte técnico, durante a vigência da garantia, para suprir suas necessidades com relação a solução adquirida;

5.2.3. Considera-se "suporte técnico" a facilidade de comunicação colocada à disposição do CONTRATANTE para a prestação de informações, esclarecimentos ou orientações sobre a utilização, funcionalidades (dicas e atalhos), configuração de softwares/hardwares básicos, aplicativos, sistemas da informação em geral envolvidos na solução objeto da contratação, bem como a intervenção direta nos equipamentos para configurações, instalações e remoções de aplicativos, atualizações de softwares e reparos diversos necessários ao bom funcionamento da solução;

5.2.4. O suporte técnico será acionado sempre que a solução apresentar falha que impeça o seu funcionamento regular e requeira uma intervenção técnica especializada e mesmo a substituição de seus componentes;

5.2.5. Durante o atendimento, a contratada poderá analisar a solução, sua atual condição de funcionamento, seus logs de sistema e sugerir mudanças para uma melhor prática de utilização da ferramenta. A equipe técnica do contratante decidirá sobre a aplicação ou não das recomendações;

5.2.6. Cada pessoa cadastrada no sistema como usuário deverá receber identificação e senha que permitam acesso seguro tanto ao sistema, como ao recurso de abertura de chamadas de suporte técnico, de maneira a evitar que pessoas não autorizadas possam acionar o suporte;

5.2.7. O fabricante deverá efetuar a troca de peças ou do equipamento, em que sejam constatadas quaisquer falhas ou defeitos de fabricação. Eventuais substituições de hardware deverão ser realizadas em até 1 (um) dia útil, a partir da constatação da necessidade de substituição do componente de hardware;

5.2.8. Os prazos de atendimento do suporte técnico da solução devem ter como referência os níveis de severidade, todos informados na tabela abaixo, ficando a contratada sujeita às sanções previstas na lei em caso de descumprimento contratual:

5.2.9. **Tabela de Severidades dos Chamados e Prazos de Atendimento / Solução**

Severidade	Descrição	Tempo de 1º contato após abertura do chamado	Tempo
Urgente	Objeto totalmente inoperante	até 30 minutos	até
Importante	Solução parcialmente inoperante – Necessidade de suporte na solução com a necessidade de interrupção de funcionamento da solução	até 1 hora	até
Normal	Solução não inoperante, mas com problema de funcionamento – Necessidade de suporte na solução sem a necessidade de interrupção de funcionamento da solução	até 2 horas	até
Informação	Solicitações de informações diversas ou dúvidas sobre a solução	até 8 horas	até

5.2.9.1. A severidade do chamado poderá ser reavaliada quando verificado que a mesma foi erroneamente aplicada, passando a contar no momento da reavaliação os novos prazos de atendimento e solução;

5.2.9.2. A cada abertura de chamado CONTRATADA poderá solicitar a prorrogação de quaisquer dos prazos para conclusão de atendimentos de chamados, desde que o faça antes do seu vencimento e devidamente justificado. Caberá à CONTRATANTE aceitar ou não o pedido de prorrogação do prazo.

5.2.9.3. Todos os prazos para atendimento do suporte começarão a ser contados a partir da abertura do chamado independentemente de este ter sido feito via telefone, e-mail ou website do fornecedor.

5.2.9.4. cada abertura de chamado CONTRATADA poderá solicitar a prorrogação de quaisquer dos prazos para conclusão de atendimentos de chamados, desde que o faça antes do seu vencimento e devidamente justificado. Caberá à CONTRATANTE aceitar ou não o pedido de prorrogação do prazo.

5.2.9.5. Todos os prazos para atendimento do suporte começarão a ser contados a partir da abertura do chamado independentemente de este ter sido feito via telefone, e-mail ou website do fornecedor.

6. PAGAMENTO

6.1. A CONTRATANTE deverá pagar o preço ao CONTRATADO na conta corrente de titularidade do CONTRATADO a ser indicada, junto à instituição financeira contratada pelo Estado do Rio de Janeiro, da seguinte forma:

6.2. Para os itens de compra (nº 01, 02, 03 e 04 de todos os Lotes) o pagamento é à vista;

6.3. Para itens de serviço de treinamento (nº 05 de todos os Lotes) o pagamento é à vista, sob demanda.

6.4. No caso de o CONTRATADO estar estabelecido em localidade que não possua agência da instituição financeira contratada pelo Estado do Rio de Janeiro ou, caso verificada pela CONTRATANTE a impossibilidade de o CONTRATADO, em razão de negativa expressa da instituição financeira contratada pelo Estado do Rio de Janeiro, abrir ou manter conta corrente naquela instituição financeira, o pagamento poderá ser feito mediante crédito em conta corrente de outra instituição financeira. Nesse caso, eventuais ônus financeiros e/ou contratuais adicionais serão suportados exclusivamente pelo CONTRATADO.

6.5. OS Pagamentos dar-se-ão, 30 dias após o recebimento definitivo do objeto ou de cada parcela, mediante atestado pela comissão de fiscalização, com a emissão da Nota Fiscal.

6.6. Quando houver glosa parcial do objeto, a CONTRATANTE deverá comunicar ao CONTRATADO para que emita Nota Fiscal ou Fatura com o valor exato dimensionado.

6.7. O CONTRATADO deverá encaminhar a Nota Fiscal ou Fatura para pagamento à CONTRATANTE, para o endereço eletrônico a ser indicado.

6.8. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente.

6.9. Havendo erro na apresentação da Nota Fiscal ou Fatura, ou circunstância que impeça a liquidação da despesa, o pagamento ficará sobrestado até que o CONTRATADO providencie as medidas saneadoras. Nessa hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a CONTRATANTE.

6.9.1. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

6.9.2. Independentemente do percentual de tributo inserido na planilha, no pagamento serão retidos na fonte os percentuais estabelecidos na legislação vigente.

7. JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DA CONTRATAÇÃO

7.1.1. Tendo em vista o incentivo à competitividade no certame, optou-se por separar os três diferentes “tamanhos” de equipamentos de firewall e incluí-los em três diferentes grupos de itens (lotes), adicionando a cada um deles seus respectivos itens agregados e opcionais, de forma a resguardar que as soluções constituintes de cada lote sejam oriundas de um mesmo fabricante por lote. Não há necessidade de compatibilização tecnológica entre os três lotes, bastando apenas que os itens de cada lote sejam compatíveis com os outros itens dentro daquele mesmo lote. Assim, o parcelamento do presente objeto alinha-se com as previsões do Enunciado nº 45 da Douta Procuradoria-Geral do Estado do Rio de Janeiro - PGE/RJ.

7.2. O objeto foi concebido de modo a proporcionar aos órgãos participantes/aderentes a opção de contratação modular dos itens, não sendo necessária portanto, a contratação da totalidade dos mesmos, nem mesmo dentro de cada lote, e ao invés disso, a contratação daqueles itens e quantidades que atendam às necessidades específicas, na forma da Intenção no Registro de Preços (IRP) registrada pelos órgãos partícipes para o certame, consideradas as suas estruturas e especificidades de topografia e infraestrutura.

7.3. O objeto ora pretendido se configura em uma solução de TI composta por mais de um item e disposta em três lotes distintos. A aquisição dos itens da solução de firewall, bem como a execução dos treinamentos, tem por objetivo o melhor cumprimento dos requisitos técnicos e tecnológicos da solução, para a entrega das funcionalidades requisitadas pelo PRODERJ.

7.4. O agrupamento dos itens correspondentes à solução de firewall justifica-se por conta da diversidade em infraestruturas tecnológicas nos órgãos da Administração Pública Estadual. Por exemplo, os itens 1, que estão distribuídos respectivamente nos Lotes I e III, tratam sobre firewalls com as mesmas funcionalidades, mas foram concebidos em três diferentes lotes, uma vez que deveriam ser ofertados aos órgãos, equipamentos com diferentes capacidades, no que diz respeito aos tipos, quantidades e throughput de interfaces, número de conexões VPN simultâneas etc.

7.5. Optou-se por agrupar os dois “tamanhos” de firewall em lotes distintos, para que fosse possível aos órgãos participantes escolherem as especificações e capacidades de equipamentos de acordo com suas necessidades, e ao mesmo tempo, garantir a interoperabilidade entre as soluções presentes dentro de cada lote, pois a referida interoperabilidade será fundamental em várias topologias de rede (clusterização e alta disponibilidade, por exemplo), e ainda facilitará o gerenciamento, replicação de regras e atualização dos equipamentos. Além disso, tal escolha deve proporcionar maior competitividade por conta da separação do objeto em lotes distintos, possibilitando que diversos fabricantes participem do certame.

7.6. O modelo de contratação ora pretendido permite a preservação do funcionamento integrado (dentro de cada lote), não comprometendo a funcionalidade de toda a solução, tendo em vista que o fornecimento, a instalação, a configuração, suporte técnico e o treinamento das soluções serão executados pelos fornecedores representantes dos fabricantes em cada um dos lotes. Desta forma, há uma redução do risco de perda, interrupção ou queda do funcionamento da solução e consequente indisponibilidade do serviço de TI, por conta de uma possível divisão de responsabilidades entre diferentes fornecedores. Tais entendimentos buscam o suporte do §3º do Art.40 da Lei nº 14.133/21 que autoriza a não adoção de parcelamento quando o objeto a ser contratado configurar sistema único e integrado e houver a possibilidade de risco ao conjunto do objeto pretendido.

7.7. Assim, entende-se que é fundamental para a pretensa contratação, e necessário para o alcance dos objetivos técnicos e estratégicos para os quais este projeto foi desenvolvido, que todos os itens ora propostos sejam adquiridos/contratados de forma agrupada, por exemplo, se o órgão participante escolher a solução de firewall do Lote I, ele poderá adicionar outros itens opcionais daquele mesmo lote, porém seria inviável a composição com itens de lotes diferentes.

7.8. Justifica-se, portanto, o agrupamento dos itens da contratação com vista ao melhor aproveitamento das práticas de mercado adotadas pelos fabricantes das soluções e melhor gerenciamento do contrato.

7.9. Em suma, a opção pelo fornecimento por grupos de itens leva em conta a modalidade de contratação pretendida e os benefícios associados. Tal agrupamento não compromete a competitividade do certame, uma vez que várias empresas do segmento têm condições de apresentar as suas propostas nos moldes aqui alinhados.

8. EXECUÇÃO DO SERVIÇO E IMPLANTAÇÃO DA SOLUÇÃO

8.1. Os equipamentos objetos deste termo deverão ser entregues, em até 90 dias após a Ordem de Início expedida pela CEDAE;

8.2. A instalação física dos equipamentos e todas as configurações deverão estar operacionais em até 90 dias após a Ordem de Início expedido pela CEDAE;

8.3. Instalação Física e Configuração Lógica

8.3.1. A solução deverá ser instalada em cluster de alta disponibilidade (ativo/passivo), em localidades definidas pela CEDAE;

8.3.2. A implantação dos equipamentos deverá ser planejada previamente em conjunto com a CEDAE, onde deveram ser definidos todos os passos necessários para a instalação, incluindo o cronograma de implantação, planos de testes e homologação da solução;

8.3.3. Antes da instalação devem ser identificados todos os ativos de rede, servidores, switches, links e qualquer outro equipamento da CEDAE que tenha comunicação com a solução ofertada;

8.3.4. A instalação dos equipamentos só poderá ser iniciada após a conclusão do planejamento e levantamento de todos os requisitos para implantação, testes e homologação da solução;

8.3.5. A instalação física dos equipamentos em rack de 19 polegadas e a parte elétrica deverá ser realizada de acordo com as recomendações do fabricante;

8.3.6. Deverão ser fornecidos todos os cabos, suportes (se necessários, "gavetas", "braços" e "trilhos") para a instalação do equipamento no rack;

8.3.7. Antes da configuração deverá ser feito a atualização da versão do software ou sistema operacional do Appliance para última versão recomendada pelo fabricante;

8.3.8. A CONTRATADA vencedora deverá migrar todas as regras, objetos, VPN e quaisquer outras configurações da solução atual para a nova solução ofertada;

8.3.9. Para as soluções ofertadas, a contratada deverá cotar um valor total para a instalação e customização inicial dos dispositivos adquiridos;

8.3.10. Este serviço deverá ser utilizado para a operacionalização inicial dos produtos adquiridos, customização, funcionalidades e políticas;

8.3.11. A instalação deve ser feita por técnicos treinados e certificados, comprovados através de atestado emitido pelo fabricante;

8.3.12. Toda a despesa de deslocamento e hospedagem deve ser de responsabilidade da CONTRATADA;

8.3.13. O projeto de planejamento e execução das atividades de instalação e configuração deverão ser assinadas por um profissional com certificação em gerenciamento de projetos – PMP (Project Management Professional);

9. CRITÉRIO DE JULGAMENTO DAS PROPOSTAS DE PREÇO

9.1. As propostas deverão ser apresentadas conforme Modelo de Proposta de Preços constante em anexo específico integrante do edital de licitação;

9.2. Será considerado vencedor o licitante que apresentar o menor valor global para o objeto deste Termo de Referência.

10. TIPO DE CONTRATAÇÃO E REGIME/FORMA DE EXECUÇÃO/FORNECIMENTO

10.1. (_X_) AQUISIÇÃO:

10.1.1. (_X_) Forma de fornecimento integral (__) Forma de fornecimento parcelado;

10.1.2. (___) Forma de fornecimento contínuo;

11. LOCAL DE EXECUÇÃO DOS SERVIÇOS

11.1. Prédio Sede da CEDAE – Av Presidente Vargas, 2655, no horário das 08:00 às 19:00 h;

12. CONDIÇÕES DE RECEBIMENTO

12.1. Conforme a Ordem de Serviço “E” nº 14.693 de 23 de maio de 2017;

13. RESPONSABILIDADES E OBRIGAÇÕES

13.1. **CONTRATADA**

13.1.1. Manter durante toda a execução do contrato, em compatibilidade com as obrigações por ela assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

13.1.2. Assumir a responsabilidade pelos encargos fiscais e comerciais resultantes da execução dos serviços, objeto desta contratação;

13.1.3. Responsabilizar-se por todos os ônus referentes aos serviços;

13.1.4. Responsabilizar-se por todas as providências e obrigações estabelecidas na legislação específica de acidentes de trabalho, quando, em ocorrência da espécie, forem vítimas os seus empregados no desempenho dos serviços ou em conexão com eles, ainda que acontecido nas dependências da CEDAE;

13.1.5. Responsabilizar-se por qualquer prejuízo caudado à CEDAE, a seus prepostos ou a terceiros, provocados por ação ou omissão da CONTRATADA, em decorrência de falhas ou imperfeições na execução dos serviços;

13.1.6. Responsabilizar-se pelos eventuais danos ou desvios causados aos bens que lhe forem confiados, devendo efetuar o ressarcimento correspondente, imediatamente após o recebimento da notificação expressa da Administração, sob pena de glosa de qualquer importância que tenha direito a receber;

13.1.7. Garantir absoluto sigilo sobre todos os processos, informações e quaisquer outros dados disponibilizados pela CEDAE, em função das peculiaridades dos serviços a serem prestados;

13.1.8. Abster-se, qualquer que seja a hipótese, de veicular publicidade ou qualquer outra informação acerca das atividades, objeto deste projeto básico, sem prévia autorização da CEDAE;

13.1.9. Esclarecer em tempo hábil eventuais dúvidas e indagações da CEDAE;

13.1.10. Comunicar ao gestor do contrato, designado formalmente pela CEDAE, qualquer fato extraordinário ou anormal que ocorra durante a vigência do contrato;

13.1.11. Exigir dos seus empregados, quando em serviço nas dependências da CEDAE, o uso obrigatório de uniformes e crachás de identificação;

13.1.12. Realizar a manutenção dos equipamentos de forma a garantir o atendimento às exigências deste documento;

13.1.13. Responsabilizar-se por todos os procedimentos de aquisição, recebimento, estocagem, transporte, distribuição e substituição de peças e equipamentos, estabelecendo um estoque suficiente para garantir a disponibilidade dos serviços, nos níveis exigidos neste documento;

13.1.14. Apresentar as informações detalhadas dos serviços disponibilizados e as restrições porventura existentes;

13.1.15. Remover, após a instalação destes equipamentos, qualquer resíduo oriundo desta atividade;

13.1.16. Entregar os equipamentos novos, sem utilização anterior, embalados adequadamente, de forma que os proteja contra avarias e garanta a completa segurança durante o transporte;

13.1.17. Refazer os serviços que foram executados de maneira incorreta ou insatisfatória, sem ônus para a CEDAE;

13.1.18. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, os equipamentos em que se verificarem vícios, defeitos ou incorreções resultantes da fabricação, da execução do serviço de assistência técnica ou de materiais empregados;

13.1.19. Em observância ao princípio de desenvolvimento sustentável, a CONTRATADA deve adotar práticas de sustentabilidade para evitar o desperdício de água tratada, reduzir o consumo de energia elétrica, de produção de resíduos sólidos, assim como realizar a separação dos resíduos recicláveis descartados, nos termos dos Arts. 6º de Decreto Estadual do Rio de Janeiro nº 43.629, de 5 de junho de 2012.

13.2. **CEDAE**

13.2.1. Cumprir com os compromissos financeiros assumidos com a empresa a ser CONTRATADA, de acordo com o contrato, mediante as notas fiscais/faturas devidamente atestadas comprovando a correta prestação do serviço;

13.2.2. Fornecer e colocar à disposição da CONTRATADA, todos os elementos e informações que se fizerem necessários à prestação do serviço, conforme especificado neste equipamento;

13.2.3. Notificar, formal e tempestivamente, a CONTRATADA sobre quaisquer irregularidades observadas na prestação dos serviços;

13.2.4. Notificar a CONTRATADA, por escrito e com antecedência mínima de 72 horas sobre multas, penalidades e quaisquer débitos de sua

responsabilidade;

13.2.5. Exigir o cumprimento de todos os compromissos assumidos pela CONTRATADA, de acordo com os termos de sua proposta comercial, do contrato e do edital de licitação;

13.2.6. Permitir o livre acesso dos empregados da CONTRATADA às dependências da CEDAE para execução dos serviços;

13.2.7. Prestar as informações e os esclarecimentos relativos ao objeto do contrato, que venham a ser solicitados pela CONTRATADA;

13.2.8. Promover, caso necessário, auditoria técnica e operacional do ambiente e recursos utilizados pela CONTRATADA, por meio de pessoal próprio ou equipe de terceiros;

13.2.9. Conferir toda a documentação técnica gerada e apresentada durante a execução dos serviços, efetuando o seu atesto quando estiverem em conformidade com os padrões de informação e qualidade exigidos no contrato;

13.2.10. Fornecer toda a infraestrutura necessária (local físico, mobiliário, tomadas elétricas e pontos de acesso à rede) para a instalação e funcionamento dos equipamentos.

14. HOMOLOGAÇÃO DOS EQUIPAMENTOS

14.1. A homologação dos equipamentos ficará condicionada à entrega dos catálogos/manuais oficiais dos produtos ofertados, em até 5 (cinco) dias úteis contados a partir da Convocação do Pregoeiro durante o certame;

14.1.1. A convocação se dará por escrito ou por meio eletrônico, através dos endereços fornecidos pelo licitante, sendo de única e exclusiva responsabilidade do licitante o fornecimento correto dos dados de contato;

14.1.2. No momento da homologação serão efetuadas a verificação dos catálogos/manuais oficiais dos produtos ofertados. As características dos equipamentos oferecidos deverão estar em conformidade com a especificação técnica;

14.1.3. A homologação dos equipamentos será realizada nas dependências da CEDAE e sem qualquer ônus para ela;

14.1.4. A CEDAE poderá rejeitar a homologação de um equipamento caso sua equipe técnica considere que os componentes do equipamento fornecido são de baixa qualidade;

14.1.5. Em caso de rejeição do equipamento apresentado, a Licitante terá um prazo de 5 (cinco) dias úteis para a apresentação de um novo modelo para homologação;

14.1.6. A apresentação de novo modelo para homologação será aceita apenas 1 (uma) única vez, sob pena de desclassificação do certame em caso de nova rejeição;

14.1.7. Em caso de alteração no fabricante e/ou modelo do equipamento, deverá ser realizada nova homologação do equipamento, respeitando os procedimentos descritos neste item.

15. VISITA TÉCNICA

15.1. Não se aplica.

16. FORMALIZAÇÃO DO CONTRATO

16.1. Haverá a formalização do Contrato.

17. ASSINATURA

Rio de Janeiro, 12 abril de 2025

Documento assinado eletronicamente por **Ricardo Batista Moreira**, **Chefe de Departamento**, em 14/04/2025, às 15:04, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **98143181** e o código CRC **0CAF8144**.

ANEXO IX – ACORDO DE NÍVEL DE SERVIÇO

1. Metodologia de avaliação da qualidade e aceite do objeto executado:

1.1. Acordo de Nível de Serviço

I - Finalidade: Garantir a qualidade dos Serviços de Treinamentos (item 05 de cada lote).

II - Periodicidade: eventual, ao final do treinamento contratado, para fins de ateste de Nota Fiscal e emissão do Termo de Recebimento Definitivo

III - Início da medição: Imediatamente após a entrega do Relatório de Cumprimento do serviço de treinamento pela Contratada.

IV - Mecanismo de cálculo: Os servidores participantes farão avaliação do curso com atribuição de grau, conforme os percentuais indicados abaixo:

a) I (insatisfatório) – 0 a 25%;

b) R (regular) – 25 a 50%;

c) B (bom) – 50 a 75%;

d) MB (muito bom) – 75 a 100%.

V - Sanções

a) A Comissão de Fiscalização de Contrato atestará a Nota Fiscal do treinamento realizado, sem aplicação de glosa, se no mínimo 60% das avaliações indicarem os graus B (bom) e/ou MB (muito bom).

b) A Comissão de Fiscalização de Contrato poderá aplicar alternativamente glosa de 2% sobre o valor da Nota Fiscal se 50% das avaliações indicarem o grau R (regular).

c) A Comissão de Fiscalização de Contrato poderá aplicar alternativamente glosa de 5% sobre o valor da Nota Fiscal se 50% das avaliações indicarem o grau I (insatisfatório).

d) Qualquer descumprimento do Acordo de Nível de Serviço poderá implicar as sanções previstas na da Lei de Licitações e Contratos.

e) Ficam resguardadas todas as sanções administrativas previstas na Lei de Licitações e Contratos.

TERMO DE REFERÊNCIA

SOLUÇÃO NEXT GENERATION FIREWALL (NGFW)

1. OBJETIVO

1.1. Justificativa da contratação

1.1.1. A contratação justifica-se pela necessidade de utilização de solução de Next Generation Firewall - NGFW nas atividades operacionais desenvolvidas pela Administração, atuando como camada protetiva para o tráfego de dados e informações críticas, a ocorrer nas condições e quantitativos propostos pela Diretoria de Segurança da Informação por meio dos estudos técnicos preliminares realizados.

1.1.2. A utilização da referida solução, enquanto mecanismo de inspeção, detecção e bloqueio de ameaças de forma automatizada e segura, é fundamental como forma de prevenção contra possíveis incidentes e promoção de aprimoramento dos níveis de segurança dos serviços prestados pela Administração Pública, protegendo informações sigilosas que transitam na Rede Governo.

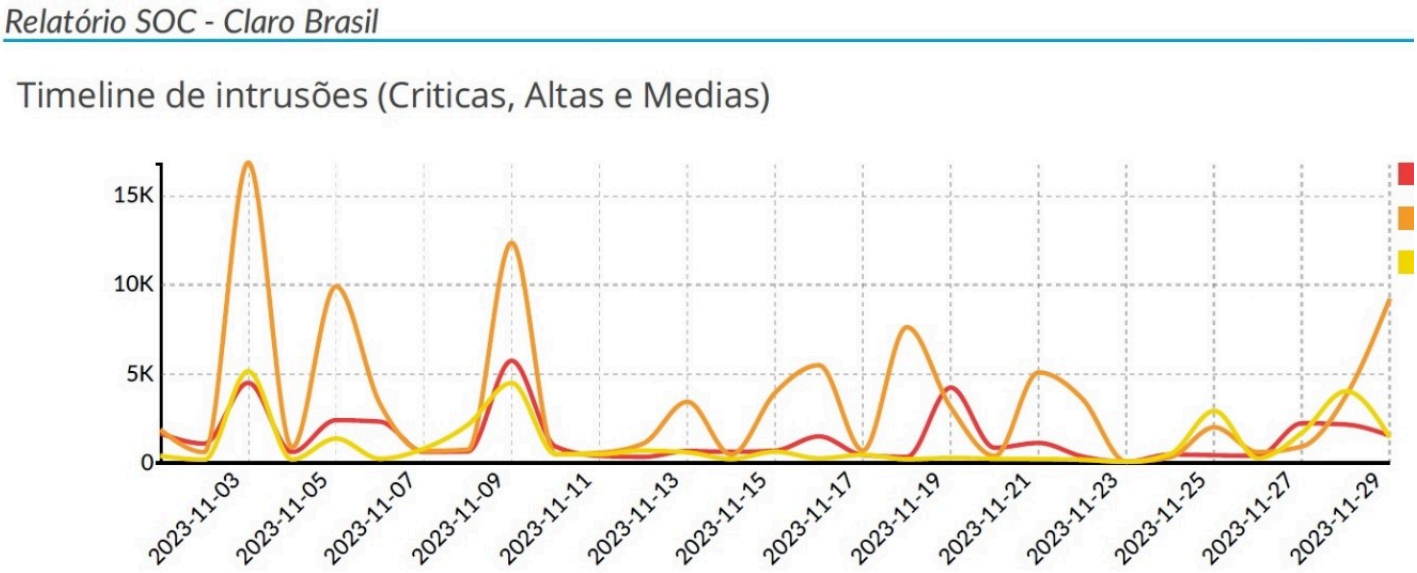
1.1.3. Saliente-se que o Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro - PRODERJ, Autarquia vinculada à Secretaria de Estado de Transformação Digital, atua como Órgão Gestor da Tecnologia da Informação e Comunicação, no âmbito do Governo do Estado do Rio de Janeiro, na forma do art. 3º, do Decreto Estadual nº 48.997/2024, que reestrutura o Sistema Estadual de Tecnologia da Informação e Comunicação - SETIC.

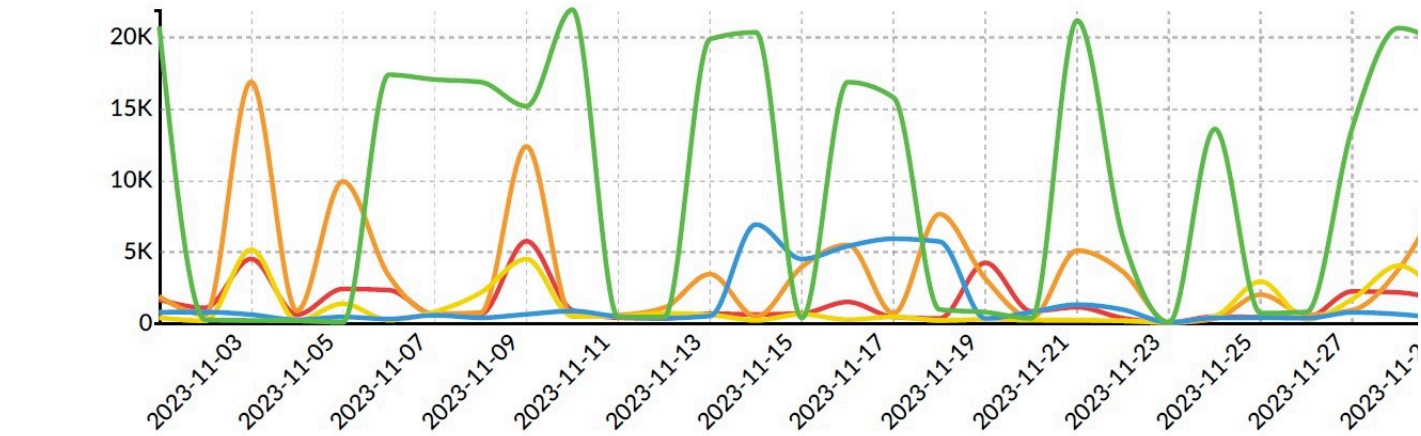
1.1.4. É responsável por sediar, manter e operar a TIC do Estado, ou seja, os sistemas de informações, o desenvolvimento de sistemas, as bases de dados de vários Órgãos estaduais e os diversos equipamentos hospedados no Data Center do Estado. É responsável também por prover serviços de Internet aos Órgãos da administração estadual, tais como correio eletrônico, consultoria, desenvolvimento e hospedagem de páginas, portais, intranets e extranets.

1.1.5. Também tem por competência o Registro de Preços em contratações de bens e serviços relativos à Tecnologia da Informação e Comunicação, para o atendimento das demandas dos demais órgãos da administração direta e indireta da Administração Pública Estadual, conforme o art. 3º, XIII, do Decreto Estadual nº 48.997/2024.

1.1.6. A tarefa de manter a área de TIC sempre alinhada às estratégias do PRODERJ constitui-se desafio permanente. Busca-se garantir em todas as questões relacionadas à infraestrutura de TIC, que o foco se mantenha na estratégia e nas necessidades finalísticas da Autarquia. Além desta, existe também a tarefa e obrigação de manter o ambiente tecnológico em alta disponibilidade e de preservar a qualidade dos serviços por ele providos sempre alinhados às suas funções institucionais.

1.1.7. Ante o crescente número de eventos de ataques de agentes malignos vive-se num cenário crítico de segurança cibernética onde os dados institucionais/corporativos estão cada vez mais vulneráveis. Abaixo, relatórios do Centro Integrado de Comando e Controle - CICC, da Polícia Militar do Estado do Rio de Janeiro / PMERJ, referentes ao mês novembro/2023 com estatísticas de ataques de rede ocorridos no período:





1.1.8. Para contribuir na manutenção dos níveis de serviços oferecidos pelo PRODERJ aos demais órgãos e entidades da Administração, bem como se preparar para oferecer novos serviços na vanguarda da tecnologia da informação, é necessário realizar uma reestruturação no fornecimento de ativos de segurança (neste caso, dos firewalls de perímetro).

1.1.9. Ademais, a presente demanda contribuirá para o atendimento da Lei 13.709/2018, Lei Geral de Proteção a Dados (LGPD) que intensifica a obrigatoriedade de proteção e privacidade dos dados dos titulares, no nosso caso, os cidadãos, reforçando a necessidade do PRODERJ, Órgão de Tecnologia do Estado, contratar e fornecer aos demais Órgãos da Administração Pública Estadual, uma solução que possa proteger os ativos de TIC contra os diversos tipos de ameaças existentes no mundo cibernético, conforme se observa no Art. 46 da LGPD, onde consta:

> "Art. 46.Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito."

1.1.10. **Resultados pretendidos**

A presente demanda visa a mitigação de diversas ameaças de segurança cibernética que afetam a rede governo, bem como obter os seguintes benefícios:

a) Aumentar o nível de proteção das informações trafegadas na rede governo;

b) Proteger contra acesso remoto não autorizado;

c) Permitir uso da internet com maior proteção;

d) Controlar o uso da internet pelos servidores;

e) Bloquear conteúdo ilegal, imoral e improdutivo;

f) Proteger a rede corporativa contra malwares e outros tipos de ameaças cibernéticas

g) Inibir e impedir a invasão de hackers;

h) Permitir que funcionários remotos acessem a rede VPN de forma segura;

i) Elevar o nível de confiabilidade dos sistemas;

j) Promover compartilhamento seguro dos dados.

1.2. **Instrumentos de planejamento**

1.2.1. Demonstração da previsão da contratação no Plano de Contratações Anual - PCA do órgão ou entidade:

a) ID PCA no PNCP (Portal Nacional de Contratações Públicas): 42498600000171-0-000053/2024;

b) Data de publicação no PNCP: 02/01/2024;

c) ID do item no PCA: vide tabelas dos subtópicos 2.2.5 e 2.2.6 deste documento.

1.2.2. Previsão no PEDTIC (67546441, p 34 e 35) do órgão ou entidade:

a) **Objetivo Estratégico 1 - Prover, manter e atualizar a infraestrutura e as Soluções e Serviços de Tecnologia da Informação e Comunicação**: Prover continuamente a inovação tecnológica para compor e atualizar a infraestrutura, as Soluções e os Serviços de Tecnologia da Informação e Comunicação, atendendo às crescentes demandas da Autarquia e dos Órgãos do Poder Executivo Estadual, visando o desenvolvimento, manutenção, integração e a padronização da TIC do estado (Alinhamento ao PPA 2024-2027 - Programa: 0493 / Ações: 1293 e 1294);

b) **Objetivo Estratégico 2 - Ampliar a capacitação técnica e profissional dos servidores em TIC**: Promover a qualificação exponencial dos servidores por meio da capacitação e participação em eventos que desenvolvam e aprimorem suas competências e a gestão do conhecimento em TIC (Alinhamento ao PPA 2024-2027 - Programa 0493 / Ação 1293);

c) **Objetivo Estratégico 3 - Aprimorar os Processos de TIC**: Promover a melhoria contínua dos processos, métodos e técnicas gerando uma maior efetividade na gestão e no uso dos recursos que fornecem as soluções de TIC (Alinhamento ao PPA 2024-2027 - Programa 0493 / Ação 1294);

d) **Objetivo Estratégico 6 - Garantir os padrões de qualidade dos serviços e soluções de TIC**: Assegurar que os serviços de TIC prestados pelo PRODERJ atendam seus requisitos mínimos, suprindo as expectativas dos órgãos da Administração Pública Direta e Indireta, de modo que contribuam para a agregação de seus valores institucionais e o cumprimento de seus objetivos estratégicos, potencializando sua capacidade de entrega, reforçando a aptidão em produzir, entregar novas soluções e aprimorar as existentes, assim como, o fornecimento de uma infraestrutura inovadora que garantam que os recursos tecnológicos investidos sejam capazes de preservar e promover a segurança, a privacidade, a disponibilidade e a continuidade dos serviços públicos, reduzindo os riscos inerentes aos serviços de TIC (Alinhamento ao PPA 2024-2027 - Programa 0493 / Ações 1293 e 1294).

1.3. **Disponibilidade orçamentária e financeira**

Na licitação para registro de preços não é necessário indicar a dotação orçamentária, que somente será exigida para a formalização do contrato.

1.4. **Sistema de Registro de Preços**

1.4.1. A contratação pelo sistema de registro de preços deverá ser adotada, preferencialmente, nas seguintes hipóteses no art. 3º do Decreto Estadual nº 48.843/2023:

a) Quando a contratação se voltar ao atendimento de necessidade permanente, prolongada ou frequente do bem ou do serviço a ser contratado;

b) Quando for mais conveniente a aquisição de bens com previsão de entregas parceladas ou contratação de serviços remunerados por unidade de medida, por quantidade de horas de serviço ou postos de trabalho, ou em regime de tarefa;

c) Quando for conveniente para atendimento a mais de um órgão ou entidade, bem como aos programas de governo; ou

d) Quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela Administração.

1.4.2. A presente demanda se enquadra na alínea "c" ante as competências institucionais do PRODERJ, na forma do art. 3º, XIII do Decreto Estadual nº 48.997/2024, para a disponibilização de atas de registro de preços aos órgãos da Administração, para o suprimento de soluções de Tecnologia da Informação e Comunicação.

1.4.3. Também se enquadra na hipótese constante da alínea "d" acima descrita uma vez que ante o crescente aumento de sistemas e bancos de dados absorvidos pela plataforma de dados do PRODERJ, como a exemplo da recente migração de toda a plataforma do Sistema Eletrônico de Informações - SEI/RJ, fazem-se necessárias eventuais ampliações da infraestrutura, notadamente acerca da segurança cibernética, de forma a resguardar a confidencialidade, integridade e disponibilidade dos ativos de dados desta Autarquia ou sob sua guarda.

1.4.4. O Governo do Estado, como toda grande organização, tem gastos volumosos com produtos e serviços de Tecnologia da Informação e Comunicação (TIC) entre os órgãos que o compõe. Os crescentes desafios colocados para o governo acabam induzindo o aumento da máquina administrativa e, consequentemente, dos gastos com seus serviços.

1.4.5. Parte significativa desses dispêndios pode ser reduzida com processos de contratações eficientes, planejados previamente em conjunto por grupos de Órgãos. Além de melhorar a qualidade técnica dos artefatos de contratação, um planejamento integrado de contratação reduz a duplicidade de esforços entre os órgãos e otimiza o trabalho dos técnicos das áreas de licitações e contratos, ensejando ainda economia processual.

1.4.6. O grande benefício, entretanto, advém da utilização do poder de compra do governo. Na medida em que aproveita as oportunidades de economia de escala, a Administração Pública pode obter melhores preços junto ao mercado, reduzindo seus custos em benefício do atendimento às demandas sociais.

1.4.7. Esta é uma inteligência trazida pelo Sistema de Registro de Preços - SRP, utilizado sempre que conveniente à contratação de serviços para atendimento a vários Órgãos, que trabalham de forma integrada as suas estimativas de consumo e os aspectos técnicos da contratação.

1.4.8. Saliente-se que a adoção do Sistema de Registro de Preços viabilizará:

- Melhoria da qualidade técnica dos documentos preliminares ao certame, tais como: especificações técnicas, alinhamento estratégico com o planejamento dos órgãos e condições jurídicas para a contratação;
- Redução do esforço administrativo para a realização de diversos processos licitatórios sendo que a execução conjunta culmina em um único certame;
- Redução de custos de manutenção e melhor eficiência pelo uso racional dos recursos, uma vez que estes foram definidos de forma a atender precisamente as necessidades do usuário;
- Ganho de economia de escala, pois, ao prospectar grandes volumes licitados, a Administração Pública amplia seu poder de compra junto aos fornecedores e consegue reduções consideráveis de preços, fato que certamente não ocorreria quando do fracionamento de certames.

1.4.9. Portanto, a utilização do Sistema de Registro de Preços se faz razoável e oportuna neste certame, uma vez que atenderá as demandas do PRODERJ e demais órgãos da Administração Pública, podendo o quantitativo ora definido sofrer alterações.

1.5. **Ata de Registro de Preços**

1.5.1. O Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro - PRODERJ será a entidade gerenciadora da Ata de Registro de Preços - ARP.

1.5.2. Os demais órgãos e entidades participantes da futura ARP estão listados na tabela do subtópico 2.2.7 deste documento.

1.5.3. O prazo de assinatura da ARP, a contar da publicação no Portal Nacional de Compras Públicas da homologação do resultado do certame, é de 5 (cinco) dias úteis, sob pena de decair o direito, sem prejuízo das sanções previstas na Lei n 14.133/21 e no Decreto Estadual nº 48.483/23, sendo certo que:

a) O prazo acima estipulado poderá ser prorrogado uma vez, por igual período, mediante solicitação justificada da parte interessada e desde que aceito pelo PRODERJ;

b) É facultado ao PRODERJ, quando o convocado não assinar a ARP no prazo e condições estabelecidas, convocar os proponentes do cadastro de reserva, na ordem de classificação, para fazê-lo em igual prazo e nas mesmas condições propostas pelo primeiro classificado.

1.5.4. A Ata de Registro de Preços terá duração de 1 (um) ano a contar de sua publicação no Portal Nacional de Contratações Públicas, prorrogável por igual período desde que comprovado o preço vantajoso.

1.5.5. A prorrogação referida no item anterior se aplicará tão somente ao saldo remanescente da ARP, vedada a ampliação nos quantitativos originalmente previstos para os itens registrados.

1.5.6. A Ata de Registro de Preços poderá ser aderida por quaisquer órgãos ou entidades do Estado que não tenham participado do certame licitatório, ora denominados não-participantes.

1.5.7. Podem também ser considerados não-participantes os órgãos ou entidades municipais, distritais, de outros Estados e federais, resguardadas as disposições de cada ente, desde que atendidas as condições do Edital e da Ata de Registro de Preços.

1.5.8. As eventuais adesões ocorrerão mediante os seguintes requisitos:

I - Apresentação de justificativa da vantagem da adesão, inclusive em situações de provável desabastecimento ou descontinuidade de serviço público;

II - Apresentação de estudo que demonstre eficiência, viabilidade e economicidade para a Administração contratante

III - Demonstração de que os valores registrados estão compatíveis com os valores praticados pelo mercado na forma do art. 23 da Lei Federal nº 14.133/2021;

IV - Prévias consulta e aceitação do PRODERJ e do fornecedor.

1.5.9. Não se vislumbra obrigações específicas do PRODERJ enquanto entidade gestora da ARP, relativas ao objeto pretendido.

1.5.10. Não se vislumbra obrigações específicas aos órgãos PARTICIPANTES enquanto entidade beneficiária da ARP, relativas ao objeto pretendido.

1.5.11. São obrigações do fornecedor beneficiário da ARP:

a) Entregar o bem e/ou fornecer o serviço, na quantidade, qualidade, local e prazos especificados, de acordo com as condições estabelecidas no Edital de Pregão; Termo de Referência – Anexo I do Edital; Formulário de Proposta de Preços – Anexo V do Edital e Anexo I – Consolidação das Informações desta Ata de Registro de Preços;

b) Entregar o objeto do contrato sem qualquer ônus para o **CONTRATANTE**, estando incluído no valor do pagamento todas e quaisquer despesas, tais como tributos, frete, seguro e descarregamento das mercadorias;

c) Manter em estoque um mínimo de bens necessários à execução do objeto do contrato;

d) Comunicar ao Fiscal do contrato, por escrito e tão logo constatado problema ou a impossibilidade de execução de qualquer obrigação contratual, para a adoção das providências cabíveis;

e) Reparar, corrigir, remover, reconstruir ou substituir, no todo ou em parte e às suas expensas, bens objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes de execução irregular ou do fornecimento de materiais inadequados ou desconformes com as especificações;

f) Indenizar todo e qualquer dano e prejuízo pessoal ou material que possa advir, direta ou indiretamente, do exercício de suas atividades ou serem causados por seus prepostos à **CONTRATANTE** ou terceiros e o constante no subitem 3.9.2 do Termo de Referência – Responsabilidades da Contratada – Anexo I do Edital.

1.5.12. Não será admitida justificativa de atraso no fornecimento dos produtos adquiridos que tenha como fundamento o não cumprimento da sua entrega pelos fornecedores do fornecedor beneficiário da ARP.

1.5.13. As quantidades estimadas e limites para adesão à ARP por órgãos não participantes constam no subtópico 2.2.8 deste documento.

2. DESCRIÇÃO DO OBJETO

2.1. **Definição do objeto**

Contratação de empresa do ramo de Tecnologia da Informação para o fornecimento de solução de firewall, com garantia de 60 meses, contemplando hardware e software, com instalação e configuração, nas dependências do contratante e curso de treinamento oficial da solução, conforme as especificações e quantidades estabelecidas neste Termo de Referência e nos requisitos da contratação descritos nos Estudos Técnicos Preliminares realizados com a finalidade de atender a demanda identificada pela Diretoria de Segurança da Informação.

2.2. **Identificação dos itens, quantidades e unidades**

2.2.1. As tabelas abaixo apresentam as quantidades estimadas da solução conforme as demandas do PRODERJ.

2.2.2. A estimativa das quantidades foi realizada pela Diretoria responsável pela Infraestrutura Tecnológica do PRODERJ, mesma área que, inclusive, será responsável pela operação técnica da solução a ser contratada.

2.2.3. A quantidade estimada dos appliances e consoles leva em conta a topologia de rede dos dois data centers do PRODERJ, além da necessária duplicidade de equipamentos, já que a redundância deles garantirá a resiliência da solução em caso de falhas. Por exemplo, caso seja necessário implementar firewall em um data center, deverão ser fornecidas ao menos duas unidades (por motivos de Alta Disponibilidade ou ainda Clusterização).

2.2.4. A quantidade estimada para os treinamentos considerou a capacitação, para os lotes 1 e 2, de um grupo de até 6 (seis) técnicos de cada uma das três áreas técnicas (infraestrutura, sistemas e segurança da informação) e para o lote 3 de um grupo de até 2 (dois) técnicos por área. Tais quantitativos consideraram o grau de relevância, na infraestrutura, das soluções tecnológicas às quais os treinamentos estão relacionados. Considerou ainda eventuais desligamentos de servidores treinados, de forma a viabilizar o treinamento de um outro servidor.

2.2.5. Não há expectativa de compra pelo PRODERJ para o Lote 3 (Firewall Tipo 3). Não obstante, o item foi concebido para oferta como opção técnica aos outros órgãos partícipes/aderentes do futuro Sistema de Registro de Preços, observadas as suas topologias e infraestruturas tecnológicas.

LOTE 1 - FIREWALL TIPO 1					
Item	**ID SIGA**	**ID PCA**	**Descrição**	**Métrica**	**Quantidade**
1	168256	86	AQUISIÇÃO DE APPLIANCE FIREWALL TIPO 1 - INCLUSOS: HARDWARE, LICENCIAMENTO, INSTALAÇÃO, CONFIGURAÇÃO E GARANTIA POR 60 MESES	UN	2
2	172443	87	AQUISIÇÃO DE CONSOLE DE GERENCIAMENTO CENTRALIZADO PARA O FIREWALL TIPO 1 COM GARANTIA DE 60 MESES	UN	2
3	172442	88	AQUISIÇÃO DE CONSOLE DE GERENCIAMENTO DE LOGS PARA O FIREWALL TIPO 1 COM GARANTIA DE 60 MESES	UN	1
4	172444	89	AQUISIÇÃO DE CONSOLE DE RELATORIA CENTRALIZADA PARA O FIREWALL TIPO 1 COM GARANTIA DE 60 MESES	UN	1
5	180944	90	SERVIÇO DE TREINAMENTO OPERACIONAL PARA A SOLUÇÃO DO LOTE 1	Aluno	6

LOTE 2 - FIREWALL TIPO 2					
Item	**ID SIGA**	**ID PCA**	**Descrição**	**Métrica**	**Quantidade**
1	168257	07	AQUISIÇÃO DE APPLIANCE FIREWALL TIPO 2 - INCLUSOS: HARDWARE, LICENCIAMENTO, INSTALAÇÃO, CONFIGURAÇÃO E GARANTIA POR 60 MESES	UN	2
2	180938	08	AQUISIÇÃO DE CONSOLE DE GERENCIAMENTO CENTRALIZADO PARA O FIREWALL TIPO 2 COM GARANTIA DE 60 MESES	UN	1
3	180940	09	AQUISIÇÃO DE CONSOLE DE GERENCIAMENTO DE LOGS PARA O FIREWALL TIPO 2 COM GARANTIA DE 60 MESES	UN	1
4	180942	10	AQUISIÇÃO DE CONSOLE DE RELATORIA CENTRALIZADA PARA O FIREWALL TIPO 2 COM GARANTIA DE 60 MESES	UN	1
5	180945	11	SERVIÇO DE TREINAMENTO OPERACIONAL PARA A SOLUÇÃO DO LOTE 2	Aluno	6

LOTE 3 - FIREWALL TIPO 3					
Item	**ID SIGA**	**ID PCA**	**Descrição**	**Métrica**	**Quantidade**
1	168258	01	AQUISIÇÃO DE APPLIANCE FIREWALL TIPO 3 - INCLUSOS: HARDWARE, LICENCIAMENTO, INSTALAÇÃO, CONFIGURAÇÃO E GARANTIA POR 60 MESES	UN	0
2	180939	02	AQUISIÇÃO DE CONSOLE DE GERENCIAMENTO CENTRALIZADO PARA O FIREWALL TIPO 3 COM GARANTIA DE 60 MESES	UN	0
3	180941	03	AQUISIÇÃO DE CONSOLE DE GERENCIAMENTO DE LOGS PARA O FIREWALL TIPO 3 COM GARANTIA DE 60 MESES	UN	0
4	180943	04	AQUISIÇÃO DE CONSOLE DE RELATORIA CENTRALIZADA PARA O FIREWALL TIPO 3 COM GARANTIA DE 60 MESES	UN	0
5	180946	05	SERVIÇO DE TREINAMENTO OPERACIONAL PARA A SOLUÇÃO DO LOTE 3	Aluno	0

2.2.6. Após a realização da Intenção de Registro de Preços - IRP nº 0689/2024, o quantitativo estimado para a contratação, considerado o Sistema de Registro de Preços, passou a ser o seguinte (conforme Art. 16, inciso V do Decreto Estadual nº 48.843/2023):

LOTE 1 - FIREWALL TIPO 1					
Item	**ID SIGA**	**ID PCA**	**Descrição**	**Métrica**	**Quantidade**
1	168256	86	AQUISIÇÃO DE APPLIANCE FIREWALL TIPO 1 - INCLUSOS: HARDWARE, LICENCIAMENTO, INSTALAÇÃO, CONFIGURAÇÃO E GARANTIA POR 60 MESES	UN	8
2	172443	87	AQUISIÇÃO DE CONSOLE DE GERENCIAMENTO CENTRALIZADO PARA O FIREWALL TIPO 1 COM GARANTIA DE 60 MESES	UN	5
3	172442	88	AQUISIÇÃO DE CONSOLE DE GERENCIAMENTO DE LOGS PARA O FIREWALL TIPO 1 COM GARANTIA DE 60 MESES	UN	4
4	172444	89	AQUISIÇÃO DE CONSOLE DE RELATORIA CENTRALIZADA PARA O FIREWALL TIPO 1 COM GARANTIA DE 60 MESES	UN	4
5	180944	90	SERVIÇO DE TREINAMENTO OPERACIONAL PARA A SOLUÇÃO DO LOTE 1	Aluno	26

LOTE 2 - FIREWALL TIPO 2					
Item	**ID SIGA**	**ID PCA**	**Descrição**	**Métrica**	**Quantidade**
1	168257	07	AQUISIÇÃO DE APPLIANCE FIREWALL TIPO 2 - INCLUSOS: HARDWARE, LICENCIAMENTO, INSTALAÇÃO, CONFIGURAÇÃO E GARANTIA POR 60 MESES	UN	33
2	180938	08	AQUISIÇÃO DE CONSOLE DE GERENCIAMENTO CENTRALIZADO PARA O FIREWALL TIPO 2 COM GARANTIA DE 60 MESES	UN	18
3	180940	09	AQUISIÇÃO DE CONSOLE DE GERENCIAMENTO DE LOGS PARA O FIREWALL TIPO 2 COM GARANTIA DE 60 MESES	UN	17
4	180942	10	AQUISIÇÃO DE CONSOLE DE RELATORIA CENTRALIZADA PARA O FIREWALL TIPO 2 COM GARANTIA DE 60 MESES	UN	17
5	180945	11	SERVIÇO DE TREINAMENTO OPERACIONAL PARA A SOLUÇÃO DO LOTE 2	Aluno	77

LOTE 3 - FIREWALL TIPO 3					
Item	**ID SIGA**	**ID PCA**	**Descrição**	**Métrica**	**Quantidade**
1	168258	01	AQUISIÇÃO DE APPLIANCE FIREWALL TIPO 3 - INCLUSOS: HARDWARE, LICENCIAMENTO, INSTALAÇÃO, CONFIGURAÇÃO E GARANTIA POR 60 MESES	UN	48
2	180939	02	AQUISIÇÃO DE CONSOLE DE GERENCIAMENTO CENTRALIZADO PARA O FIREWALL TIPO 3 COM GARANTIA DE 60 MESES	UN	11
3	180941	03	AQUISIÇÃO DE CONSOLE DE GERENCIAMENTO DE LOGS PARA O FIREWALL TIPO 3 COM GARANTIA DE 60 MESES	UN	11
4	180943	04	AQUISIÇÃO DE CONSOLE DE RELATORIA CENTRALIZADA PARA O FIREWALL TIPO 3 COM GARANTIA DE 60 MESES	UN	11
5	180946	05	SERVIÇO DE TREINAMENTO OPERACIONAL PARA A SOLUÇÃO DO LOTE 3	Aluno	52

2.2.7. Quantidades estimadas por órgão participante (conforme Art. 16, inciso V do Decreto Estadual nº 48.843/2023):

Órgão participante	**LOTE 1**					**LOTE 2**					**LOTE 3**				
	item 01 ID 168256	**item 02 ID 172443**	**item 03 ID 172442**	**item 04 ID 172444**	**item 05 ID 180944**	**item 01 ID 168257**	**item 02 ID 180938**	**item 03 ID 180940**	**item 04 ID 180942**	**item 05 ID 180945**	**item 01 ID 168258**	**item 02 ID 180939**	**item 03 ID 180941**	**item 04 ID 180943**	**item 05 ID 180946**
SEPM - Secretaria de Estado de Polícia Militar	2	1	1	1	8	2	1	1	1	8	30	2	2	2	8
RIO SEGURANÇA	0	0	0	0	0	1	1	0	0	2	0	0	0	0	0
PRODERJ - Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro (Órgão Gestor deste SRP)	2	2	1	1	6	2	1	1	1	6	0	0	0	0	0
DER RJ - Departamento de Estradas e Rodagens do Estado do Rio de Janeiro	0	0	0	0	0	2	1	1	1	4	2	1	1	1	4

INEA - Instituto Estadual do Ambiente	0	0	0	0	0	2	1	1	1	4	0	0	0	0	0
AGETRANSP - Agência Reguladora de Serviços Públicos Concedidos de Transportes Aquaviários, Ferroviários, Metroviários e de Rodovias do Estado do Rio de Janeiro	0	0	0	0	0	2	1	1	1	3	0	0	0	0	0
SEPOL - Secretaria Estadual de Polícia Civil	2	1	1	1	6	0	0	0	0	0	0	0	0	0	0
CECIERJ - Centro de Ciências e Educação Superior a Distância do Estado do Rio de Janeiro	0	0	0	0	0	2	1	1	1	5	2	1	1	1	5
FAF - Fundo de Administração Fazendária	2	1	1	1	6	2	1	1	1	6	2	1	1	1	6
FAPERJ - Fundação Carlos Chagas Filho de Amparo à Pesquisa do Estado do Rio de Janeiro	0	0	0	0	0	2	1	1	1	4	2	1	1	1	4
FSERJ - Fundação Estadual de Saúde do Estado do Rio de Janeiro	0	0	0	0	0	0	0	0	0	0	2	1	1	1	5
PROCON RJ	0	0	0	0	0	2	1	1	1	2	0	0	0	0	0
CEPERJ - Fundação Centro Estadual de Estatísticas, Pesquisas e Formação de Servidores Públicos do Rio de Janeiro	0	0	0	0	0	2	1	1	1	5	2	1	1	1	5
SMGSI	0	0	0	0	0	2	1	1	1	5	2	1	1	1	5
SEAPPA - Secretaria de Estado de Agricultura, Pecuária, Pesca e Abastecimento	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
AGENERSA - Agência Reguladora de Energia e Saneamento Básico do Estado do Rio de Janeiro	0	0	0	0	0	2	1	1	1	2	0	0	0	0	0
RIO PREVIDÊNCIA - Fundo Único de Previdência Social do Estado do Rio de Janeiro	0	0	0	0	0	1	1	1	1	6	0	0	0	0	0
EMATER RIO - Empresa de Assistência Técnica e Extensão Rural do Estado do Rio de Janeiro	0	0	0	0	0	1	1	1	1	3	0	0	0	0	0
FIA - Fundação para a Infância e Adolescência	0	0	0	0	0	1	1	1	1	2	0	0	0	0	0
GSI - Gabinete de Segurança Institucional	0	0	0	0	0	2	1	1	1	5	2	1	1	1	5
FUNESBOM - Fundo Especial do Corpo de Bombeiros	0	0	0	0	0	2	1	1	1	5	0	0	1	0	0
SEENEMAR - Secretaria de Energia e Economia do Mar	0	0	0	0	0	0	0	0	0	0	2	1	1	1	5
TOTAL	**8**	**5**	**4**	**4**	**26**	**33**	**18**	**17**	**17**	**77**	**48**	**11**	**11**	**11**	**52**

2.2.8. Quantidades estimadas para adesão por órgãos não participantes (conforme Art. 16, inciso VI do Decreto Estadual nº 48.843/2023):

PARÂMETRO	LOTE 1					LOTE 2					LOTE 3				
	item 01 ID 168256	item 02 ID 172443	item 03 ID 172442	item 04 ID 172444	item 05 ID 180944	item 01 ID 168257	item 02 ID 180938	item 03 ID 180940	item 04 ID 180942	item 05 ID 180945	item 01 ID 168258	item 02 ID 180939	item 03 ID 180941	item 04 ID 180943	item 05 ID 180946
Quantidade máxima de contratação por meio de adesão (dobro da estimativa por item)	16	10	8	8	52	66	36	34	34	154	96	22	22	22	104
Quantidade máxima de contratação por órgão aderente (metade da estimativa por item)	4	2	2	2	13	16	9	8	8	38	24	5	5	5	26

2.3. **Definição da natureza do objeto**

2.3.1. Os itens que integram o objeto possuem características comuns e usuais encontradas atualmente no mercado de TIC, cujos padrões de desempenho e de qualidade podem ser objetivamente definidos. Portanto, se enquadram como BENS e SERVIÇOS COMUNS ou usuais de mercado, na forma do parágrafo único, do art. 6º, XIII, da Lei nº 14.133/2021

2.3.2. O Objeto constitui solução em TIC, parcelado em três lotes que agregam o fornecimento de itens diversos para as soluções de firewall (Lote 1, Lote 2 e Lote 3), observados os seguintes aspectos:

a) Os itens nº 1, 2, 3, 4 de todos os lotes são medidos em unidades, e correspondem a aquisição de bens (compra);

b) Os itens nº 5 de todos os lotes são medidos por aluno/vaga, e correspondem a serviços de treinamento a ocorrerem sob demanda.

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO / MODELO DE EXECUÇÃO DO OBJETO

3.1. **Justificativa para o parcelamento ou não da contratação**

3.1.1. Tendo em vista o incentivo à competitividade no certame, optou-se por separar os três diferentes "tamanhos" de equipamentos de firewall e incluí-los em três diferentes grupos de itens (lotes), adicionando a cada um deles seus respectivos itens agregados e opcionais, de forma a resguardar que as soluções constituintes de cada lote sejam oriundas de um mesmo fabricante por lote. Não há necessidade de compatibilização tecnológica entre os três lotes, bastando apenas que os itens de cada lote sejam compatíveis com os outros itens dentro daquele mesmo lote. Assim, o parcelamento do presente objeto alinha-se com as previsões do Enunciado nº 45 da Douta Procuradoria-Geral do Estado do Rio de Janeiro - PGE/RJ.

3.1.2. O objeto foi concebido de modo a proporcionar aos órgãos participantes/aderentes a opção de contratação modular dos itens, não sendo necessária portanto, a contratação da totalidade dos mesmos, nem mesmo dentro de cada lote, e ao invés disso, a contratação daqueles itens e quantidades que atendam às necessidades específicas, na forma da Intenção no Registro de Preços (IRP) registrada pelos órgãos partícipes para o certame, consideradas as suas estruturas e especificidades de topografia e infraestrutura.

3.1.3. O objeto ora pretendido se configura em uma solução de TI composta por mais de um item e disposta em três lotes distintos. A aquisição dos itens da solução de firewall, bem como a execução dos treinamentos, têm por objetivo o melhor cumprimento dos requisitos técnicos e tecnológicos da solução, para a entrega das funcionalidades requisitadas pelo PRODERJ.

3.1.4. O agrupamento dos itens correspondentes à solução de firewall justifica-se por conta da diversidade em infraestruturas tecnológicas nos órgãos da Administração Pública Estadual. Por exemplo, os itens 1, que estão distribuídos respectivamente nos Lotes I, II e III, tratam sobre firewalls com as mesmas funcionalidades, mas foram concebidos em três diferentes lotes, uma vez que deveriam ser ofertados aos órgãos, equipamentos com diferentes capacidades, no que diz respeito aos tipos, quantidades e throughput de interfaces, número de conexões VPN simultâneas, etc.

3.1.5. Optou-se por agrupar os três "tamanhos" de firewall em lotes distintos, para que fosse possível aos órgãos participantes escolherem as especificações e capacidades de equipamentos de acordo com suas necessidades, e ao mesmo tempo, garantir a interoperabilidade entre as soluções presentes dentro de cada lote, pois a referida interoperabilidade será fundamental em várias topologias de rede (clusterização e alta disponibilidade, por exemplo), e ainda facilitará o gerenciamento, replicação de regras e atualização dos equipamentos. Além disso, tal escolha deve proporcionar maior competitividade por conta da separação do objeto em lotes distintos, possibilitando que diversos fabricantes participem do certame.

3.1.6. O modelo de contratação ora pretendido permite a preservação do funcionamento integrado (dentro de cada lote), não comprometendo a funcionalidade de toda a solução, tendo em vista que o fornecimento, a instalação, a configuração, suporte técnico e o treinamento das soluções serão executados pelos fornecedores representantes dos fabricantes em cada um dos lotes. Desta forma, há uma redução do risco de perda, interrupção ou queda do funcionamento da solução e consequente indisponibilidade do serviço de TI, por conta de uma possível divisão de responsabilidades entre diferentes fornecedores. Tais entendimentos buscam o suporte do §3º do Art.40 da Lei nº 14.133/21 que autoriza a não adoção de parcelamento quando o objeto a ser contratado configurar sistema único e integrado e houver a possibilidade de risco ao conjunto do objeto pretendido.

3.1.7. Assim, entende-se que é fundamental para a pretensa contratação, e necessário para o alcance dos objetivos técnicos e estratégicos para os quais este projeto foi desenvolvido, que todos os itens ora propostos sejam adquiridos/contratados de forma agrupada, por exemplo, se o órgão participante escolher a solução de firewall do Lote I, ele poderá adicionar outros itens opcionais daquele mesmo lote, porém seria inviável a composição com itens de lotes diferentes.

3.1.8. Justifica-se, portanto, o agrupamento dos itens da contratação com vista ao melhor aproveitamento das práticas de mercado adotadas pelos fabricantes das soluções e melhor gerenciamento do contrato.

3.1.9. Em suma, a opção pelo fornecimento por grupos de itens leva em conta a modalidade de contratação pretendida e os benefícios associados. Tal agrupamento não compromete a competitividade do certame, uma vez que várias empresas do segmento têm condições de apresentar as suas propostas nos moldes aqui alinhados.

3.2. **Requisitos de Negócios**

A solução a ser adotada deverá ser capaz de entregar:

I - Equipamentos do tipo firewall de próxima geração (NGFW), a serem disponibilizados em três diferentes capacidades, bem como os sistemas complementares da solução (gerenciamento, logs e relatórios);

II - Treinamentos operacionais nas soluções contratadas, voltados para os técnicos da Contratante.

III - Garantia de 60 meses para todos os componentes da solução, observados os seguintes aspectos:

a) A garantia para os itens de aquisição em modalidade perpétua, por período de 60 meses, costuma ser praxe em licitações para contratações de soluções de TIC, tanto pelo governo federal como pelos demais entes, em que pese significar um aspecto diferencial do produto que, por fugir da condição básica ofertada pelo fornecedor, decerto que interfere em sua precificação e poderá repercutir numa majoração do lance do licitante no momento do pregão.

b) O referido lapso temporal, contudo, se apresenta razoável uma vez que corresponde ao prazo médio de vida útil de uma solução tecnológica, em que os fabricantes amiúde, permanecem ofertando peças de reposição ou mesmo o suporte técnico, por exemplo.

c) Esta garantia visa resguardar o bom funcionamento do inventário de TIC, com soluções de software e hardware em boas condições de forma a preservar o desempenho e a produtividade dos órgãos que venham a contratar o objeto (bens e serviços) ora proposto.

d) Enfim, dentro da mesma lógica do legislador, ao autorizar o poder público para contratações iniciais por prazos de até 5 (cinco) anos, naturalmente com o fim de resguardar a continuidade dos serviços públicos, que aliás, é um princípio da Administração Pública, é que se propõe a garantia de 60 meses para as soluções de TIC a serem adquiridas neste certame.

3.3. **Requisitos de Capacitação**

3.3.1. A capacitação compreende os serviços de treinamento oficial dos itens nº 05 de todos os lotes.

3.3.2. O treinamento deverá abranger a operação da solução ofertada. Assim, os treinamentos dos itens nº 05, correspondem respectivamente à operacionalização dos itens nº 1 até nº 4 de todos os lotes.

3.3.3. O treinamento será direcionado aos técnicos da CONTRATANTE, deverá ser focado na solução adotada, de forma que haja transferência do conhecimento dos recursos, configurações existentes e sua utilização.

3.3.4. Deverá ser entregue para a contratante a proposta com o conteúdo do treinamento.

3.3.5. A Contratante reserva-se o direito de não aceitar o módulo ministrado, podendo, a seu critério, solicitar a troca de instrutor ou até mesmo repetição do mesmo, caso não seja satisfatório.

3.3.6. Deverá ser ministrado por instrutor capacitado na ferramenta, devendo ser comprovado por meio de certificados ou declaração emitida pelo fabricante.

3.3.7. Deverá ser fornecido pela contratada certificado de capacitação para os participantes do treinamento.

3.3.8. Demais aspectos da capacitação:

I - **Objetivo da capacitação**

a) Capacitação do contratante para a operacionalização da ferramenta tecnológica.

b) Formação de facilitadores que possam vir a replicar futuramente o conhecimento no âmbito do órgão contratante.

II - **Métrica da capacitação**

a) O treinamento será contratado por aluno (vaga).

III - **Carga horária da capacitação**

a) Deverá ter carga horária mínima de 40 (quarenta) horas.

b) Deverá iniciar no prazo máximo de até 20 dias úteis contados da emissão da Ordem de Serviço, quando o contratante não especificar prazos no documento.

c) Os treinamentos deverão ser realizados em dias úteis e não poderão exceder o horário comercial.

IV - **Forma de realização da capacitação**

a) O treinamento será em português, ministrado na modalidade remota, em plataforma virtual disponibilizada pela contratada.

V - **Materiais didáticos e acessórios da capacitação**

a) É de responsabilidade da contratada todo material audiovisual, didático e eletrônico para a realização dos treinamentos, e quaisquer outras despesas diretas ou indiretas.

b) O material didático será fornecido em português, pela contratada, abordando todos os tópicos do curso.

VI - **Conteúdo programático da capacitação**

a) O treinamento deverá englobar a realização de laboratórios práticos, fornecidos pela CONTRATADA, para configuração e execução de exercícios práticos na mesma versão dos produtos ofertados.

b) O evento abordará no mínimo: o uso da ferramenta, instalação, configuração, operação da ferramenta, gerenciamento, resolução de problemas, e poderá ser gravado para fins de documentação, caso seja de interesse da CONTRATANTE.

c) Deverá contemplar todos os recursos e configurações existentes na solução ofertada.

3.4. **Requisitos Legais**

3.4.1. **Gerais:**

a) **Lei Federal nº 14.133/2021**, que trata das normas gerais sobre licitações e contratos administrativos;

b) **Lei Complementar nº 123/2006**, que estabelece normas gerais relativas ao tratamento diferenciado e favorecido a ser dispensado às microempresas e empresas de pequeno porte atualizada;

c) **Decreto Estadual 43.629/2012**, que dispõe s*obre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços e obras pela Administração Pública Estadual Direta e Indireta e dá outras providências;*

d) **Decreto Estadual nº 48.322/2023**, que dispõe sobre o enquadramento dos bens de consumo, adquiridos para suprir as demandas das estruturas da administração pública estadual, nas categorias de qualidade comum e de luxo;

e) **Decreto Estadual nº 48.760/2023**, que implementa o Plano de Contratações Anual - PCA e institui o Sistema PCA RJ, no âmbito da administração pública estadual direta, autárquica e fundacional;

f) **Decreto Estadual nº 48.778/2023**, que regulamenta as licitações pelos critérios de julgamento por menor preço ou por maior desconto, no âmbito da administração pública estadual direta, autárquica e fundacional;

g) **Decreto Estadual 48.816/2023**, que regulamenta a fase preparatória das contratações, de que trata a Lei nº 14.133, de 1º de abril de 2021, no âmbito da administração pública estadual direta, autárquica e fundacional;

h) **Decreto Estadual nº 48.817/2023**, que regulamenta a gestão e a fiscalização das contratações no âmbito da administração pública estadual direta, autárquica e fundacional e dá outras providências;

i) **Decreto Estadual nº 48.843/2023**, que regulamenta o sistema de registro de preços - SRP, no âmbito da administração pública estadual direta, autárquica e fundacional e dá outras providências;

j) **Decreto Estadual nº 48.865/2023**, que regulamenta as licitações pelo critério de julgamento por técnica e preço, no âmbito da administração pública estadual direta, autárquica e fundacional;

k) **Decreto Estadual 48.997/2024**, que dispõe sobre a reestruturação do Sistema Estadual de Tecnologia da Informação e Comunicação - SETIC e estabelece as competências do PRODERJ enquanto órgão de Direção Geral do SETIC/RJ;

l) **Instrução Normativa SLTI/MP nº 94/2022** (a título de boas práticas), que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC;

m)**Nota técnica SGE TCE-RJ nº 06/2023**, que orienta os jurisdicionados do TCE-RJ acerca da realização do planejamento para aquisição de bens e serviços de Tecnologia da Informação (TI) visando a atender ao princípio da economicidade.

3.4.2. **Aplicáveis ao objeto**

a) **Lei de Proteção de Dados Pessoais (LGPD):** Estabelece diretrizes para o tratamento de dados pessoais e impõe a implementação de medidas de segurança para proteger esses dados.

3.5. **Requisitos de Manutenção**

3.5.1. Todas as rotinas para fins de manutenção com vistas ao pleno e adequado funcionamento da solução ao longo da vigência da garantia do produto estarão a cargo da CONTRATADA na forma do Suporte Técnico previsto no subtópico 6.1.2 deste documento.

3.5.2. O fornecedor deve disponibilizar ambiente web, número de telefone ou e-mail para abertura de chamados e acompanhamento das soluções e esclarecimentos de dúvidas.

3.6. **Requisitos Temporais**

Resguardado o cronograma previsto no subtópico 5.3.13 deste documento, não há outros requisitos temporais a serem considerados.

3.7. **Requisitos de Segurança da Informação e Privacidade**

3.7.1. Caso se faça necessário, para um eventual suporte nas dependências da CONTRATANTE, a CONTRATADA deverá exigir dos seus empregados, o uso obrigatório de uniformes e crachás de identificação.

3.7.2. Caso se faça necessário, para um eventual suporte nas dependências da CONTRATANTE, a CONTRATADA não poderá se utilizar da presente situação para obter qualquer acesso não autorizado às informações de propriedade da CONTRATANTE.

3.7.3. A CONTRATADA não pode obter, capturar, copiar ou transferir qualquer tipo informação de propriedade do CONTRATANTE, sem autorização.

3.7.4. **Proteção de Dados Pessoais**

3.7.4.1. As partes (CONTRATANTE e CONTRATADA), no âmbito do quaisquer atividades oriundas da execução deste Termo de Referência, observarão o regime legal concernente à proteção de dados pessoais, especialmente as diretrizes veiculadas pela Lei nº 13.709 de 14 de agosto de 2018 (LGPD) na realização de qualquer operação que se amolde ao preceito de tratamento de dados pessoais durante a execução do objeto.

3.7.4.2. Para atender aos ditames da Lei n° 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), a justificativa da necessidade compatível com as finalidades institucionais, assim como a apresentação de um relatório de impacto à proteção de dados pessoais (art. 5º, XVII, da LGPD) que aborde como serão usadas as tecnologias, deverá ser apresentada:

a) no momento da manifestação de interesse de participação da Intenção de Registro de Preços (IRP) pelos órgãos participantes; e

b) no momento da contratação realizada pelos órgãos não participantes.

3.7.4.3. A CONTRATANTE e a CONTRATADA deverão adotar, em relação aos dados pessoais, medidas de segurança, técnicas e administrativas, aptas a proteger os dados e informações de acessos, não autorizados, e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

3.7.4.4. A CONTRATADA deve notificar imediatamente, à CONTRATANTE, a ocorrência de incidente de segurança, relacionado a dados pessoais, por ela tratados, fornecendo informações suficientes para que a CONTRATANTE cumpra quaisquer obrigações de comunicação da ocorrência, à autoridade nacional, e aos titulares dos dados.

3.7.4.5. As partes deverão, nomeadamente:

a) Tratar os dados pessoais nos moldes expressamente definidos e em estrita consonância com a finalidade específica delineada pelo CONTROLADOR;

b) Armazenar os dados pessoais apenas durante o período definido pelo CONTROLADOR;

c) Não desviar o tratamento dos dados pessoais da finalidade específica e da hipótese legal legitimadora;

d) Informar imediatamente a outra parte contratante acerca da ocorrência de qualquer incidente que envolva os dados pessoais tratados, assim como prestar toda colaboração necessária para instruir o respectivo Relatório;

e) Assegurar os direitos dos titulares, abrangendo a disponibilidade de canal acessível ao Encarregado Setorial pelo tratamento de dados pessoais;

f) Garantir que os respectivos colaboradores ou prestadores de serviços que tenham acesso aos dados pessoais no contexto deste Termo de Referência cumpram as diretrizes protetivas dos dados pessoais, vinculando-os a um Termo de Confidencialidade.

3.7.4.6. O CONTROLADOR e OPERADOR deverão manter o registro das operações de tratamento de dados pessoais que realizarem, assim como estabelecer regras de boas práticas, considerando a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.

3.7.4.7. O CONTROLADOR e OPERADOR, no âmbito de suas competências, deverão estabelecer regras de boas práticas e de governança que estabeleçam os aspectos procedimentais adequados para o cumprimento das diretrizes normativas, como:

a) as condições de organização;

b) o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares;

c) as normas de segurança;

d) os padrões técnicos;

e) as obrigações específicas para os diversos envolvidos no tratamento; e

f) as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos.

3.7.4.8. É vedada a transferência de dados pessoais, pela CONTRATADA, para fora do território do Brasil sem o prévio consentimento, por escrito, do CONTRATANTE, e demonstração da observância, pela CONTRATADA, da adequada proteção desses dados, cabendo à CONTRATADA o cumprimento de toda a legislação de proteção de dados ou de privacidade de outro (s) país (es) que for aplicável.

3.7.4.9. A responsabilidade pelo cumprimento das diretrizes contempladas na Lei nº 13.709/18, especialmente no tocante ao tratamento de dados pessoais adequados e legítimos, será de responsabilidade do órgão contratante que, ao figurar como agente de tratamento, assumirá as obrigações imputadas na legislação.

3.7.4.10. A CONTRATADA poderá responder por quaisquer danos, perdas ou prejuízos causados a CONTRATANTE, ou a terceiros, decorrentes do descumprimento da Lei Federal nº13.709/2018, não excluindo ou reduzindo dessa responsabilidade a fiscalização do CONTRATANTE em seu acompanhamento.

3.7.4.11. A CONTRATADA deve atender à Política de Segurança da Informação instituída pela Instrução Normativa PRODERJ PRE nº 02, de 28 de abril de 2022, e demais normativos correlatos publicados pelo CONTRATANTE.

3.8. **Sigilo e Inviolabilidade**

A Contratada deverá garantir o sigilo e a inviolabilidade das informações a que eventualmente possa ter acesso, durante os procedimentos de fornecimento dos produtos objeto deste Termo de Referência.

3.9. **Requisitos Tecnológicos:**

3.9.1. **De arquitetura tecnológica**

3.9.1.1. Os requisitos tecnológicos de arquitetura da solução, relacionados aos itens de compra do objeto, encontram-se no Anexo I - Especificações Técnicas do Objeto.

3.9.1.2. Os requisitos tecnológicos relacionados aos itens de serviço (treinamento) do objeto, encontram-se no subtópico 3.3 (requisitos de capacitação) deste documento.

3.9.2. **De projeto e de implementação**

3.9.2.1. A CONTRATADA deve realizar, nas dependências da CONTRATANTE, antes do início da implantação da solução, uma reunião inicial de projeto (kick-off) em conjunto com as áreas de Segurança da Informação e infraestrutura da Contratada para definir o Plano de Trabalho de instalação e configuração da solução.

3.9.2.2. Após a reunião de kick-off a CONTRATADA deverá produzir e entregar ao CONTRATANTE o Projeto Executivo elaborado com base no quanto acertado ao longo da reunião, contemplando o planejamento, escopo, cronograma, discriminação dos produtos entregáveis, dimensionamento da infraestrutura tecnológica necessária, discriminação da equipe do projeto com perfis e quantitativos mínimos, relatório de controle e tratamento de riscos do projeto e demais artefatos que se façam necessários no entendimento da Contratada.

3.9.2.3. Compreende-se nesta etapa a instalação de equipamentos, sistemas, softwares e aplicativos da CONTRATANTE nos PRODUTOS fornecidos, bem como a migração das configurações existentes na CONTRATANTE para os produtos fornecidos pela CONTRATADA, caso haja viabilidade;

3.9.2.4. A etapa de instalação e configuração deve acontecer de forma gradual e transparente, de acordo com a conveniência da CONTRATANTE.

3.9.2.5. Durante esta etapa, a equipe da CONTRATADA deverá estar presente nos horários de testes, implantação e migração, definidos pela CONTRATANTE.

3.9.2.6. As atividades de instalação e configuração, de acordo com a necessidade, poderão ser executadas em horário comercial, período noturno ou final de semana.

3.9.2.7. Durante a etapa de instalação e configuração, os produtos fornecidos pela CONTRATADA serão colocados em plena operação, em condições reais de produção.

3.9.2.8. A CONTRATADA deverá, com a supervisão e aprovação da CONTRATANTE, planejar e realizar a instalação e configuração dos softwares com total interoperabilidade no ambiente atual da CONTRATANTE, sem impacto no ambiente de produção.

3.9.2.9. Durante a implantação e integração, caso seja necessário, a CONTRATADA deverá realizar, entre outras atividades: instalação de softwares, acompanhamento de migrações de regras e políticas, elaboração e execução de scripts, análise de performance, tunning, resolução de problemas e implementação de segurança.

3.9.2.10. Para instalação e configuração devem ser consideradas as seguintes premissas:

a) Caberá à CONTRATADA a disponibilização de todos os recursos necessários, tais como hardwares, softwares e recursos humanos necessários à instalação das soluções;

b) Caberá à CONTRATADA disponibilização de ferramentas / scripts de retorno imediato ao estado original da estrutura da CONTRATANTE caso a instalação dos produtos / softwares da CONTRATADA apresente falha.

c) A CONTRATADA deverá fornecer todas as licenças necessárias dos PRODUTOS ofertados e dos elementos adicionais que se fizerem necessários à instalação e ao pleno funcionamento do ambiente de produção.

3.9.2.11. O fornecedor deverá submeter previamente, por escrito, à Contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações acordadas.

3.9.2.12. O encaminhamento formal das demandas, considerados cada um dos itens do objeto, ocorrerá sempre por meio de emissão da Ordem de Fornecimento ou Ordem de Serviço.

3.10. **Requisitos Materiais e Humanos**

3.10.1. Materiais, insumos e acessórios necessários ao perfeito funcionamento da solução deverão ser arcados pela CONTRATADA, sem custos adicionais para a CONTRATANTE.

3.10.2. Em observação ao entendimento do Enunciado nº 14, item 5 da Procuradoria-Geral do Estado do Rio de Janeiro - PGE/RJ, saliente-se que o objeto da presente contratação, que contempla serviços de treinamento, não prevê o uso de mão de obra residente/dedicada nas dependências do órgão contratante. Adicionalmente registre-se que o objeto também não caracteriza, forma alguma, terceirização de atividade-fim, tendo em vista que se trata de contratação, em regime de compra de equipamentos de tecnologia e respectivos cursos de treinamento, bem como suporte técnico específico do fabricante/fornecedor representante, no âmbito da garantia comum de mercado, que estão diretamente relacionado à atuação de profissionais e especialistas nas soluções contratadas.

3.11. **Providências a serem adotadas pela administração previamente à celebração do contrato**

Capacitação de servidores ou de empregados para fiscalização e gestão contratual, não havendo outras providências a serem adotadas que sejam antecedentes e necessárias à celebração do contrato.

3.12. **Especificação de marca /padronização**

Não se aplica.

3.13. **Forma de Execução**

3.13.1. Para os itens 05 de todos os Lotes, o regime de execução do é o de EMPREITADA POR PREÇO UNITÁRIO.

3.13.2. Para os itens 01, 02, 03 e 04 de todos os Lotes, enquanto bens de aquisição, a forma de fornecimento é a de entrega imediata e integral.

3.14. **Duração do contrato**

3.14.1. O prazo de vigência do contrato será de:

a) 180 (cento e oitenta) dias para os itens de compra (nº 01, 02, 03 e 04 dos lotes), contados da data da divulgação no Portal Nacional de Contratações Públicas, vedada a prorrogação.

b) 12 (doze) meses para os itens de serviço de treinamento (nº 05 dos Lotes), contados da data da divulgação no Portal Nacional de Contratações Públicas, vedada a prorrogação, salvo quando obrigatória nos termos da Lei nº 14.133/2021.

3.15. **Reajuste de Preços**

3.15.1. Os preços contratados serão reajustados após o interregno de 1 (um) ano, mediante solicitação do CONTRATADO.

3.15.2. O interregno mínimo de 1 (um) para o primeiro reajuste será contado da data do orçamento estimado.

3.15.3. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir do fato gerador que deu ensejo ao último reajuste.

3.15.4. Os preços iniciais serão reajustados, mediante a aplicação, pela CONTRATANTE, do Índice de Custos de Tecnologia da Informação – ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada - IPEA.

3.15.5. No caso de atraso ou não divulgação do(s) índice(s) de reajustamento, a CONTRATANTE pagará ao CONTRATADO a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

3.15.6. Fica o CONTRATADO obrigado a apresentar memória de cálculo referente ao reajustamento de preços do valor remanescente, sempre que este ocorrer, sendo adotado na aferição final o índice definitivo.

3.15.7. Caso o índice estabelecido para o reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

3.15.8. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

3.15.9. O pedido de reajuste deverá ser formulado durante a vigência do contrato e antes de eventual prorrogação contratual, sob pena de preclusão.

3.15.10. Os efeitos financeiros do pedido de reajuste serão contados:

a) da data-base prevista no contrato, desde que requerido o reajuste no prazo de 60 (sessenta) dias da data de publicação do índice ajustado contratualmente;

c) a partir da data do requerimento do CONTRATADO, caso o pedido seja formulado após o prazo fixado na alínea a, acima, o que não acarretará a alteração do marco para cômputo da anualidade do reajustamento, já adotado no edital e no contrato.

3.15.11. Caso, na data de eventual prorrogação contratual, ainda não tenha sido divulgado o índice de reajuste, deverá, a requerimento do CONTRATADO, ser inserida cláusula no termo aditivo de prorrogação para resguardar o direito futuro do CONTRATADO, a ser exercido tão logo se disponha dos valores reajustados, sob pena de preclusão.

3.15.12. A extinção do contrato não configurará óbice para o deferimento do reajuste solicitado tempestivamente, hipótese em que será concedido por meio de termo indenizatório.

3.15.13. O reajuste será realizado por apostilamento, se esta for a única alteração contratual a ser realizada.

3.15.14. O reajuste de preços não interfere no direito das partes de solicitar, a qualquer momento, a manutenção do equilíbrio econômico dos contratos com base no disposto no art. 124, inciso II, alínea “d”, da Lei n.º 14.133/2021.

3.17. **Garantias contratuais**

3.17.1. O Contrato conta com garantia de execução, nos moldes do artigo 96 da Lei nº 14.133/2021, correspondente a 5% (cinco por cento) de seu valor anual.

3.17.2. O referido percentual, resguardada a discricionariedade prevista no citado art. 96, caput e o teto estabelecido no caput do art. 98 do mesmo diploma legal, considera a natureza do objeto (bens e serviços), enquanto ferramenta estratégica de caráter tecnológico de relevância para as atividades do órgão contratante em razão das exigências trazidas pela nova legislação quanto ao tratamento de dados pessoais.

3.17.3. O CONTRATADO poderá optar pelas seguintes modalidades de garantia:

a) caução em dinheiro ou em títulos da dívida pública;

b) seguro-garantia;

c) fiança bancária; e

d) título de capitalização custeado por pagamento único, com resgate pelo valor total.

3.17.4. Qualquer que seja a modalidade escolhida pelo CONTRATADO, a garantia assegurará o pagamento de:

a) prejuízos advindos do não cumprimento do objeto do Contrato e do não adimplemento das demais obrigações nele previstas;

b) multas moratórias, compensatórias e administrativas aplicadas pela Administração ao CONTRATADO; e

c) obrigações trabalhistas e previdenciárias de qualquer natureza, assim como as obrigações de regularidade perante o FGTS, não adimplidas pelo CONTRATADO, quando couber.

3.17.5. A garantia, qualquer que seja a modalidade escolhida, terá validade durante a vigência do Contrato e por mais 90 (noventa) dias após o término deste prazo de vigência.

3.17.6. Na hipótese de suspensão do contrato por ordem ou inadimplemento da Administração, o CONTRATADO ficará desobrigado de renovar a garantia ou de endossar a apólice de seguro até a ordem de reinício da execução ou o adimplemento pela Administração.

3.17.7. Ressalvada a hipótese de seguro-garantia, em que deverá ser observado o prazo do item 3.17.8, o CONTRATADO apresentará, no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério da CONTRATANTE, contado da assinatura do Contrato, o comprovante de prestação de garantia, na forma do item 3.17.3.

3.17.8. Caso oferecida a modalidade de seguro-garantia, sua apresentação deve ocorrer em 1 (um) mês, contado da data de homologação da licitação e anterior à assinatura do contrato, e observar-se-ão as seguintes condições:

a) a apólice permanecerá em vigor mesmo que o CONTRATADO não pague o prêmio nas datas convencionadas;

b) a apólice deverá acompanhar as modificações referentes à vigência do Contrato principal, mediante a emissão do respectivo endosso pela seguradora;

c) será permitida a substituição da apólice na data de renovação ou de aniversário, desde que mantidas as condições e coberturas da apólice vigente e nenhum período fique descoberto, ressalvado o disposto no item 3.17.6 deste documento; e

d) a apólice somente será aceita se contemplar todos os eventos indicados no item 3.17.4, observada a legislação que rege a matéria.

3.17.9. Em caso de oferecimento de títulos da dívida pública, estes devem ser emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Fazenda.

3.17.10. Caso a opção seja por fiança bancária, esta deverá ser emitida por banco ou instituição financeira devidamente autorizada a operar no País pelo Banco Central do Brasil, e deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

3.17.11. Caso a opção seja por garantia em dinheiro, deverá ser efetuada em favor da CONTRATANTE, na conta-corrente da instituição financeira contratada pelo Estado, cujo valor será corrigido monetariamente e restituído ao CONTRATADO, na forma do item 3.17.19.

3.17.12. O CONTRATADO obriga-se a fazer a reposição, a suplementação ou a renovação da garantia, no prazo máximo de 10 (dez) dias úteis, contados da data em que for notificado, no caso desta ser executada, total ou parcialmente, ou o Contrato for prorrogado ou tiver o seu valor alterado, assim como em qualquer outra situação que exija a manutenção da condição disposta no item 3.17.1 neste documento.

3.17.13. A inobservância do prazo fixado para apresentação, reposição, suplementação ou renovação da garantia acarretará a aplicação de multa e/ou outras penalidades, na forma disposta no contrato.

3.17.14. O atraso superior a 25 (vinte e cinco) dias autoriza a CONTRATANTE a promover a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas, com a aplicação das sanções cabíveis.

3.17.15. A CONTRATANTE executará a garantia na forma prevista na legislação que rege a matéria.

3.17.16. O emitente da garantia ofertada pelo CONTRATADO deverá ser notificado pela CONTRATANTE quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.

3.17.17. O garantidor não é parte para figurar em processo administrativo instaurado pela CONTRATANTE com o objetivo de apurar prejuízos e/ou aplicar sanções ao CONTRATADO.

3.17.18. Caso se trate da modalidade seguro-garantia, ocorrido o sinistro durante a vigência da apólice, sua caracterização e comunicação poderão ocorrer fora desta vigência, não caracterizando fato que justifique a negativa do sinistro, desde que respeitados os prazos prescricionais aplicados ao contrato de seguro, nos termos do art. 20 da Circular Susep n° 662, de 11 de abril de 2022.

3.17.19. Extinguir-se-á a garantia com a restituição da apólice, carta fiança, título da dívida pública ou autorização para a liberação da caução em dinheiro, atualizada monetariamente, acompanhada de declaração da CONTRATANTE, mediante termo circunstanciado, de que o CONTRATADO cumpriu todas as cláusulas do contrato.

3.17.20. A garantia somente será liberada ou restituída, após a fiel execução do Contrato ou pela sua extinção, por culpa exclusiva da Administração, ou quando assim convencionado, em se tratando de extinção consensual da contratação.

3.17.21. O CONTRATADO autoriza a CONTRATANTE a reter, a qualquer tempo, a garantia, na forma prevista no edital e no Contrato.

3.18. **Possíveis impactos ambientais**

3.18.1. A contratada deverá promover a correta destinação dos resíduos resultantes da prestação do serviço, tais peças substituídas, embalagens, entre outros, observando a legislação e princípios de responsabilidade socioambiental (Lei nº 12.305/2010).

3.18.2. Deverá ainda obedecer aos critérios previstos no capítulo I do Decreto 43.629/2012, por meio dos artigos 1º e 2º, in verbis:

> Art. 1º - As especificações para a aquisição de bens, contratação de serviços e obras por parte dos órgãos e entidades da Administração Pública Estadual Direta e Indireta, a fixação de critérios de julgamento e a execução e fiscalização dos respectivos contratos, observarão critérios de sustentabilidade ambiental, na forma deste Decreto.
>
> Art. 2º - Consideram-se critérios de sustentabilidade ambiental, dentre outros:
>
> I - economia no consumo de água e energia;
>
> II - minimização da geração de resíduos e destinação final ambientalmente adequada dos que forem gerados;
>
> III - racionalização do uso de matérias-primas;
>
> IV - redução da emissão de poluentes;
>
> V - adoção de tecnologias menos agressivas ao meio ambiente;
>
> VI - implementação de medidas que reduzam as emissões de gases de efeito estufa e aumentem os sumidouros;
>
> VII - utilização de produtos de baixa toxicidade;
>
> VIII- utilização de produtos com a origem ambiental sustentável comprovada, quando existir certificação para o produto.

3.19. **Possibilidade de subcontratação**

3.19.1. Não será admitida a subcontratação do objeto contratual, no todo ou em parte, em razão da composição do objeto, distribuído em lotes compostos por itens de aquisição perpétua, de natureza indivisível.

3.19.2. Saliente-se que, em caso do item de treinamento ser ministrado pelo mesmo fabricante da solução ofertada pela contratada ou com uso de sua plataforma, isso não configura subcontratação, sub-rogação, cessão ou transferência, uma vez que compõe a mesma solução a mesma.

3.20. **Possibilidade de participação de consórcio**

3.20.1. É vedada a participação de pessoas jurídicas reunidas em consórcio.

3.20.2. A vedação se dá em razão das características específicas da solução a ser contratada, que não pressupõe multiplicidade ou heterogeneidade de atividades empresariais distintas, nem envolve questões de alta complexidade ou de relevante vulto, em que empresas, isoladamente, não teriam condições de suprir os requisitos de habilitação do edital.

3.20.3. Entende-se que os itens a serem contratados não exigem empresas de diferentes segmentos e/ou capacidades reunidas para atuarem na execução do objeto proposto.

3.20.4. Ademais, a gestão compartilhada poderá gerar vícios ou lacunas no fluxo dos processos de atendimento. A cadeia de responsabilidades entre as empresas será maior que se o objeto estiver sob responsabilidade de uma única empresa, ainda que operacionalizado por meio de atuação conjunta com outras empresas.

3.20.5. Mesmo a garantia produzida como consequência da aquisição é resultado de equipes, técnicas e procedimento complementar, não havendo benefício ou necessidade de segmentação para a realização do objeto proposto, além de repercutir em vários canais de atendimento de eventuais chamados técnicos, gerando uma morosidade no atendimento e ocasionando o não cumprimento dos itens expostos no edital.

3.20.6. A ausência de consórcio não trará prejuízos à competitividade do certame, visto que, em regra, a formação de consórcios é admitida quando o objeto a ser licitado envolve questões de alta complexidade ou de relevante vulto, em que empresas, isoladamente, não teriam condições de suprir os requisitos de habilitação do edital. Nestes casos, a Administração, com vistas a aumentar o número de participantes, admite a formação de consórcio.

3.20.7. Tendo em vista que é prerrogativa do Poder Público, na condição de CONTRATANTE, a escolha da participação ou não de empresas constituídas sob a forma de consórcio, com as devidas justificativas, conforme a literalidade do texto da Lei nº o 14.133, art 15 e seus incisos e parágrafos, pelos motivos já expostos, conclui-se que a vedação de constituição de empresas em consórcio, para o caso concreto, é o que melhor atende o interesse público, por prestigiar os princípios da competitividade, economicidade e moralidade.

3.20.8. Por fim, a vedação da participação de empresas reunidas em regime de consórcio visa exatamente afastar a restrição à competição, na medida em que a reunião de empresas que, individualmente, poderiam fornecer os equipamentos, reduziria o número de licitantes e poderia, eventualmente, proporcionar a formação de conluios/cartéis para manipular os preços nas licitações.

3.21. **Possibilidade de participação de cooperativa**

Não será admitida a participação de cooperativa de trabalho, qualquer que seja a sua forma de constituição, já que o objeto principal trata de compra de bens de aquisição perpétua e, no caso dos itens secundários de treinamento, há vínculo de subordinação direta entre o empregado e a empresa contratada para a prestação dos serviços.

3.22. **Incidência do Programa de Integridade**

3.22.1. Será exigida da empresa contratada a efetivação do Programa de Integridade, nos termos da Lei nº 7.753/2017, uma vez que o objeto se enquadra no art. 1º do referido diploma.

3.22.2. A implantação do Programa de Integridade no âmbito da empresa contratada dar-se-á no prazo de 180 (cento e oitenta) dias corridos, contados da data da divulgação no Portal Nacional de Contratações Públicas.

3.22.3. A empresa que possuir o Programa de Integridade implantado deverá apresentar no momento da contratação declaração informando a sua existência.

3.23. **Obrigações das Partes**

3.23.1. **Obrigações da CONTRATANTE**

São obrigações da CONTRATANTE:

a) Fornecer à Contratada documentos, informações e demais elementos que possuir pertinentes à execução dos serviços.

3.23.2. **Obrigações da CONTRATADA**

A CONTRATADA deverá cumprir todas as obrigações constantes deste documento e em seus Anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas:

a) Indicar formalmente preposto apto a representá-lo junto à CONTRATANTE, que deverá responder pela fiel execução do contrato;

b) Assinar o Termo de Sigilo e Confidencialidade, conforme o modelo apresentado no Anexo VI deste documento.

3.23.3. As disposições nos subtópicos 3.23.1 e 3.23.2 correspondem às obrigações específicas relativas ao objeto deste certame, ficando resguardadas todas as demais obrigações constantes da minuta do contrato que compõe anexo do Edital deste certame.

3.23.4. Observada a Lei Geral de Proteção de Dados Pessoais LGPD, deverá ser incluído na Minuta de Contrato cláusula de responsabilidade da CONTRATADA nos termos abaixo transcritos:

> **"CLÁUSULA (incluir número): DO SIGILO E DA PROTEÇÃO A DADOS PESSOAIS, COM BASE NA LGPD**
>
> **PARÁGRAFO PRIMEIRO:** A CONTRATADA deverá manter sigilo sobre toda e qualquer informação confidencial, reservada ou exclusiva, incluindo informações técnicas, de negócio ou financeira, comunicada pela Contratante, ou obtida em função da execução do objeto contratado, exceto as informações que:
> a- Sejam de domínio público à época da comunicação;
> b- Seja conhecida pela parte receptora antes da comunicação ou caia no domínio público sem culpa da parte receptora;
> c- Seja desenvolvida, de modo independente, pela parte receptora, sem uso de informação confidencial.
>
> **PARÁGRAFO SEGUNDO:** Na forma do disposto no Termo de Referência – Anexo I ao instrumento convocatório, a CONTRATANTE, e a CONTRATADA, devem cumprir a Lei Federal nº 13.709/2018, no âmbito da fiscalização, da guarda dos dados e da execução do objeto deste Contrato.
>
> **PARÁGRAFO TERCEIRO:** A CONTRATADA deve assegurar que o acesso a dados pessoais seja limitado aos empregados, prepostos ou colaboradores que necessitem conhecer/acessar os dados de guarda e responsabilidade da CONTRATANTE, na medida em que sejam estritamente necessários para as finalidades deste Contrato, e cumprir a legislação aplicável, assegurando que todos esses indivíduos estejam sujeitos a compromissos de confidencialidade ou
> obrigações profissionais de confidencialidade.
>
> **PARÁGRAFO QUARTO:** Considerando a natureza dos dados tratados, pertinentes ao objeto desta contratação, a CONTRATANTE e a CONTRATADA deverão adotar, em relação aos dados pessoais, medidas de segurança, técnicas e administrativas, aptas a proteger os dados e informações de acessos, não autorizados, e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de

tratamento inadequado ou ilícito.

PARÁGRAFO QUINTO: A CONTRATADA deve notificar imediatamente, à CONTRATANTE, a ocorrência de incidente de segurança, relacionado a dados pessoais, por ela tratados, fornecendo informações suficientes para que a CONTRATANTE cumpra quaisquer obrigações de comunicação da ocorrência, à autoridade nacional, e aos titulares dos dados.

PARÁGRAFO SEXTO: A CONTRATANTE e a CONTRATADA devem adotar as medidas cabíveis para auxiliar na investigação, mitigação e reparação de cada um dos incidentes de segurança, quando identificada a responsabilização exclusiva, de uma parte e/ou outra.

PARÁGRAFO SÉTIMO: Por ocasião do encerramento deste Contrato, a CONTRATADA deve, imediatamente, ou, mediante justificativa, em até 10 (dez) dias úteis da data de seu encerramento, fornecer, a CONTRATANTE, a base de dados do atendimento, inclusive eventuais cópias de dados pessoais tratados no âmbito do Contrato, certificando por escrito, ao CONTRATANTE, o cumprimento desta obrigação.

PARÁGRAFO OITAVO: A CONTRATADA deve colocar à disposição do CONTRATANTE, conforme solicitado, toda informação necessária para demonstrar o cumprimento do disposto nesta CLÁUSULA, e deve permitir auditorias e contribuir com elas, incluindo inspeções, pelo CONTRATANTE, ou auditor por ele indicado, em relação ao tratamento de dados pessoais do cidadão, que acessar na base de dados da CONTRATANTE.

PARÁGRAFO NONO: Todas as notificações e comunicações, realizadas nos termos desta cláusula, devem se dar por escrito e serem entregues pessoalmente, encaminhadas pelo correio ou por e-mail para os endereços físicos ou eletrônicos informados em documento escrito emitido por ambas as partes por ocasião da assinatura deste Instrumento Contratual, ou outro endereço informado em notificação posterior.

PARÁGRAFO DÉCIMO: A CONTRATADA poderá responder por quaisquer danos, perdas ou prejuízos causados a CONTRATANTE, ou a terceiros, decorrentes do descumprimento da Lei Federal nº 13.709/2018, não excluindo ou reduzindo essa responsabilidade a fiscalização do CONTRATANTE em seu acompanhamento.

PARÁGRAFO DÉCIMO PRIMEIRO: É vedada a transferência de dados pessoais, pela CONTRATADA, para fora do território do Brasil sem o prévio consentimento, por escrito, do CONTRATANTE, e demonstração da observância, pela CONTRATADA, da adequada proteção desses dados, cabendo à CONTRATADA o cumprimento de toda a legislação de proteção de dados ou de privacidade de outro (s) país (es) que for aplicável.

PARÁGRAFO DÉCIMO SEGUNDO: A CONTRATADA não poderá realizar subcontratação.

4. REQUISITOS MÍNIMOS PARA EXECUÇÃO

4.1. Habilitação jurídica

4.1.1. Para fins de comprovação da habilitação jurídica, deverão ser apresentados, conforme o caso, os seguintes documentos:

I - Pessoa física: cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional.

II - Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede.

III - Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio www.portaldoempreendedor.gov.br.

IV - Sociedade Limitada Unipessoal - SLU: ato constitutivo, estatuto ou contrato social em vigor inscrito no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhado de documento comprobatório do administrador, sendo assim enquadrada a sociedade identificada como Empresas Individual de Responsabilidade Limitada – EIRELI, na forma do art. 41, da Lei nº 14.195, de 26 de agosto de 2021.

V - Sociedade Empresária Estrangeira em funcionamento no País: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020 ou norma posterior que regule a matéria.

VI - Sociedade Simples: inscrição do ato constitutivo no Registro Civil das Pessoas Jurídicas do local de sua sede, acompanhada de prova da indicação dos seus administradores.

VII - Filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz.

4.1.2. Quando cabível, os documentos apresentados devem estar acompanhados de todas as alterações ou da consolidação respectiva.

4.2. Regularidades Fiscal e Trabalhista

4.2.1. Para fins de comprovação da regularidade fiscal e trabalhista, deverão ser apresentados, conforme o caso, os seguintes documentos:

I - Inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso.

II - Regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social.

III - Regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS).

IV - Declaração de que não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7°, XXXIII, da Constituição.

V - Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943.

VI - Prova de inscrição no cadastro de contribuintes estadual/distrital e municipal, relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual.

VII - O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar nº 123/2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal, eis que a apresentação do Certificado de Condição de Microempreendedor Individual – CCMEI supre tais requisitos.

VIII - Prova de regularidade com a Fazenda do Estado do Rio de Janeiro, mediante a apresentação de:

a) Certidão Negativa de Débitos, ou Certidão Positiva com efeito de Negativa, expedida pela Secretaria de Estado de Fazenda; e

b) Certidão Negativa de Débitos em Dívida Ativa, ou Certidão Positiva com efeito de Negativa, para fins de participação em licitação, expedida pela Procuradoria-Geral do Estado.

IX - Regularidade com a Fazenda Estadual e Municipal do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre, com a apresentação, conforme o caso, de:

X - Certidão Negativa de Débitos, ou Certidão Positiva com efeito de Negativa, perante o Fisco estadual, pertinente ao Imposto sobre Operações relativas à Circulação de Mercadorias e sobre Prestações de Serviços de Transporte Interestadual, Intermunicipal e de Comunicação – ICMS, bem como de Certidão perante a Dívida Ativa estadual, podendo ser apresentada Certidão Conjunta em que constem ambas as informações;

XI - Certidão Negativa de Débitos, ou Certidão Positiva com efeito de Negativa do Imposto sobre Serviços de Qualquer Natureza – ISS.

4.2.2. Excepcionalmente, havendo contratação que envolva tributação tanto de ICMS como de ISS, deverá ser exigida tanto inscrição nos cadastros quanto prova de regularidade com as Fazendas estadual e municipal.

4.2.3. Caso o fornecedor seja considerado isento dos tributos estaduais e municipais relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

4.2.4. Na hipótese de cuidar-se de microempresa ou de empresa de pequeno porte, na forma do art. 42 da Lei Complementar nº 123/2016, a documentação somente será exigida para efeito de assinatura do contrato, caso se sagre vencedora no certame.

4.2.5. Em sendo declarada vencedora do certame microempresa ou empresa de pequeno porte com débitos fiscais e trabalhistas, ficará assegurado, a partir de então, o prazo de 5 (cinco) dias úteis para a regularização da documentação, pagamento ou parcelamento do débito, e emissão de eventuais certidões negativas ou positivas com efeito de negativas, na forma do art. 42, § 1º, da Lei Complementar nº 123/2016.

4.2.6. O prazo acima poderá ser prorrogado por igual período, a critério exclusivo da Administração Pública.

4.2.7. A não regularização da documentação no prazo estipulado implicará a decadência do direito à contratação, na forma do § 2º, do art. 42, da Lei Complementar nº 123/2016, sem prejuízo da aplicação das sanções previstas neste Aviso.

4.3. Habilitação Econômico-Financeira

4.3.1. Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor, caso se trate de pessoa jurídica, ou certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do fornecedor, caso se trate de pessoa física ou de sociedade simples.

4.3.1.1. Não será causa de inabilitação do licitante a anotação de distribuição de processo de recuperação judicial ou de pedido de homologação de recuperação extrajudicial.

4.3.2. Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, vedada a sua substituição por balancetes ou balanços provisórios.

4.3.2.1. Os documentos referidos acima limitar-se-ão ao último exercício social no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos.

4.3.2.2. Os fornecedores criados no exercício financeiro da contratação deverão atender a todas as exigências da habilitação e ficam autorizados a substituir os demonstrativos contábeis pelo balanço de abertura;

- Poderá ser apresentado o balanço intermediário, caso autorizado por lei ou pelo contrato/estatuto social.

4.3.2.3. Para fins de habilitação econômico-financeira de sociedade empresária em recuperação judicial deverão ser considerados os valores constantes no Plano de Recuperação Judicial, homologado pelo Juízo competente, para fins de apuração dos índices contábeis previstos no edital.

4.3.3. Comprovação da boa situação financeira da empresa mediante obtenção de índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), iguais ou superiores a 1 (um), obtidos pela aplicação das seguintes fórmulas:

LG = Ativo Circulante + Realizável a Longo Prazo
Passivo Circulante + Passivo Não Circulante

SG = Ativo Total
Passivo Circulante + Passivo Não Circulante

LC = Ativo Circulante
Passivo Circulante

4.3.3.1. Caso seja apresentado resultado inferior ou igual a 1(um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), deverá ser comprovado capital ou patrimônio líquido mínimo de 5% (cinco por cento) do valor total estimado da contratação ou do item pertinente.

4.3.3.2. O atendimento dos índices econômicos previstos neste item deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo fornecedor.

4.4. **Qualificação técnica**

4.4.1. Para fins de comprovação de qualificação técnica deverão ser apresentados Atestado(s) fornecido(s) por pessoas jurídicas de direito público ou privado, que comprovem a experiência e aptidão de desempenho de atividade pertinente e compatível com o objeto da licitação, na forma do artigo 67, § 2º, da Lei Federal nº 14.133/2021 que indiquem nome, função, endereço de contato do(s) atestador(es), ou qualquer outro meio para eventual contato pelo órgão licitante.

4.4.2. Um único atestado é suficiente para a demonstração da experiência anterior do licitante em relação a execução do objeto licitado, sendo possível o somatório de atestados de períodos concomitantes para comprovar a sua capacidade técnica.

4.4.3. O(s) atestado(s) deverão demonstrar o cumprimento de um quantitativo mínimo de 30% (trinta por cento) do volume estimado para os itens: 1 dos lotes, os quais correspondem às respectivas parcelas de maior relevância ou de valor significativo para o objeto deste certame.

4.4.4. A motivação para os itens necessários à comprovação de aptidão técnica, bem como o percentual acima referido, se dá em virtude realização do certame via Sistema de Registro de Preços com demanda em larga escala, para atendimento de inúmeros órgãos da Administração. Portanto, se faz razoável a verificação de que o futuro prestador do serviço tem capacidade de atendimento compatível com a criticidade do projeto, mitigando riscos à disponibilidade dos serviços do Governo, bem como diante da importância do objeto a ser contratado, que tem relação direta com a segurança institucional dos órgãos e secretarias do estado.

4.5. **Entrega, avaliação da qualidade e aceite do objeto**

4.5.1. **Objetivo da Prova de Conceito**

Será exigido do LICITANTE classificado em primeiro lugar Prova de Conceito para a demonstração de que a solução ofertada é compatível com as exigências técnicas necessárias e prescritas para este objeto (itens de compra), conforme os roteiro apresentados nos Anexos II, III e IV deste documento, respectivamente correspondentes aos lotes 1, 2 e 3.

4.5.2. **Prazos e condições da Prova de Conceito**

4.5.2.1. O referido LICITANTE será convocado no prazo máximo de até 10 (dez) dias úteis, a contar da aprovação da sua documentação de habilitação, para uma reunião (que poderá ocorrer em plataforma virtual), onde serão definidas as providências preparatórias do ambiente de teste. Nessa reunião o LICITANTE deverá informar os requisitos necessários para a instalação do ambiente de teste a serem disponibilizados pelo PRODERJ conforme entendimento durante a reunião. Entende-se por "requisitos necessários":

a) Disponibilização de máquinas virtuais e/ou estações de trabalho, projetor e link de internet;

b) Criação de VLAN's e/ou disponibilização de endereços IP;

c) Criação de usuários no AD e/ou modificações de regras de firewall, IPS, etc;

d) Disponibilização de periféricos, tais como: cabos, switches e outros componentes semelhantes não mencionados.

4.5.2.2. Nesta reunião o LICITANTE deverá, sob pena de desclassificação, entregar os documentos da(s) solução(ões) que permitam comprovar o atendimento aos requisitos técnicos constantes do Anexo I deste documento, apresentando no mínimo:

a) ID do requisito;

b) Descrição do requisito;

c) Nome do produto ofertado (modelo, marca e fabricante);

d) Nome do documento de referência onde é possível verificar evidência do atendimento do requisito;

e) Página do documento referência onde é possível verificar evidência do atendimento do requisito;

f) Outras informações necessárias.

4.5.2.3. Até o prazo de 5 dias úteis após a realização da reunião preparatória, será divulgada a equipe técnica que avaliará a solução durante a sessão da prova.

4.5.2.4. O teste será realizado no ambiente do PRODERJ, em um dos endereços abaixo mencionados a ser definido na reunião acima preparatória acima referida:

a) Data Center – Universidade do Estado do Rio de Janeiro (UERJ). End.: R. São Francisco Xavier 524, 2º andar, bloco “F”, Maracanã, Rio de Janeiro – RJ, CEP: 20550-013;

b) Data Center – Centro Integrado de Comando e Controle (CICC). End.: Rua Carmo Neto s/nº, Cidade Nova, Rio de Janeiro – RJ - CEP 20210-051; ou

c) Sede – Centro de Tecnologia de Informação e Comunicação do Governo do Estado do Rio de Janeiro (PRODERJ). End.: R. da Conceição 69, 24º e 25º andar, Centro, Rio de Janeiro – RJ CEP 20051-011

4.5.2.5. Admite-se, alternativamente, o uso de ambiente virtual do próprio LICITANTE ou do fabricante, para a comprovação das funcionalidades da solução ofertada, caso seja acordado na reunião preparatória. Nesta hipótese, o LICITANTE deverá disponibilizar o link de acesso ao acompanhamento da sessão virtual de demonstração até 3 (três) dias úteis antes da realização da sessão, para que o mesmo possa ser repassado em tempo hábil a todos os que acompanharão a sessão.

4.5.2.6. Em caso de não comparecimento à reunião (por problema único e exclusivo do LICITANTE) a prova acontecerá no ambiente padrão de teste do PRODERJ, em um dos endereços acima citados, sendo vedado ao LICITANTE reivindicar qualquer adaptação na infraestrutura oferecida.

4.5.2.7. O PRODERJ, por meio da Comissão Permanente de Licitação (Pregoeiro), dará publicidade, através do chat de mensagens do SIGA-RJ, da data de realização do teste que deverá ocorrer no prazo de 10 (dez) dias úteis após a realização da reunião preparatória. O referido prazo poderá ser prorrogado por igual período, mediante requisição fundamentada do LICITANTE.

4.5.2.8. Se o teste for realizado em ambiente do PRODERJ, o LICITANTE terá até as 17h do último dia útil anterior ao da realização do mesmo para providenciar a instalação do ambiente nas condições definidas na reunião.

4.5.2.9. A prova será realizada entre 10:00 e 18:00 horas (horário de Brasília), com intervalo de 1 hora para almoço, e poderá durar de 1 a 5 dias úteis.

4.5.3. ***Possibilidade e forma de participação dos interessados***

Os outros licitantes que tenham participado da etapa competitiva e demais interessados que desejem acompanhar a sessão, poderão indicar um representante para acompanhamento, devendo para tanto enviar para o e-mail da Comissão Permanente de Licitação (cdl@proderj.rj.gov.br) até as 16hs do último dia útil que antecede a sessão de teste. No e-mail deverão constar: dados da empresa interessada (nome e contato), de seu representante (nome e contato) para o devido credenciamento.

4.5.4. ***Roteiro e critérios de avaliação***

4.5.4.1. No dia de realização do teste, o LICITANTE, bem como os demais interessados em acompanhar, deverão chegar ao local indicado com antecedência mínima de 30 minutos.

4.5.4.2. A equipe técnica do PRODERJ considerará apto o sistema que atender aos requisitos conforme descritos no respectivo Roteiro para Prova de Conceito (Anexos II, III e IV) do Termo de Referência, onde cada item deverá ser preenchido, observados os critérios "atende" ou "não atende".

4.5.4.3. Durante a prova poderá ser feito questionamento, exclusivamente pelos representantes do PRODERJ à proponente, permitindo a verificação dos requisitos estabelecidos.

4.5.4.4. Após a prova será emitido, via Sistema Eletrônico de Informações, relatório descrevendo os testes realizados e a conclusão sobre a aprovação da proposta ou desclassificação bem como eventuais ocorrências ou manifestações de quaisquer dos presentes na sessão.

4.5.4.5. Para a solução ser considerada apta para ser contratada pela Administração, todos os requisitos de software que constam no presente documento e seu anexo de especificações técnicas, deverão ser considerados ATENDIDOS.

4.5.4.6. Será desclassificada a licitante que for convocada para a prova de conceito e não demonstrar a compatibilidade de seu produto conforme as especificações técnicas exigidas ou não comparecer no dia marcado sob qualquer pretexto.

4.5.4.7. Em caso de desclassificação na prova de conceito deverá ser convocada o próximo licitante na ordem de classificação, resguardadas todas as condições e prazos previstos neste tópico.

4.5.5. ***Responsabilidades***

4.5.5.1. Os custos para a demonstração da solução são de responsabilidade do LICITANTE e em hipótese alguma caberá qualquer tipo de indenização.

4.5.5.2. O LICITANTE deverá disponibilizar ao menos 01 (um) técnico que se responsabilizará pela instalação do software da solução, caso o teste seja realizado utilizando a infraestrutura do PRODERJ.

4.5.5.3. A disponibilização de equipamentos, sistemas, demais materiais e/ou acessórios necessários ao ambiente de demonstração durante a prova não informados pelo LICITANTE na reunião preparatória citada no subtópico 4.5.2.1 são de inteira responsabilidade do LICITANTE.

4.5.5.4. Ficará sob responsabilidade do PRODERJ o resguardo dos itens eventualmente entregues pelo licitante para a avaliação na prova de conceito, devendo restituí-los ao final nas condições recebidas, resguardados eventuais consumos decorrentes da realização da prova.

4.6. **Autorizações e Licenças necessárias para a Execução do Objeto**

Não se aplica.

4.7. **Exigência de exame de conformidade, ensaio ou certificação**

Não se aplica.

4.8. **Da exigência de carta de solidariedade**

Não se aplica.

4.9. **Catálogos de operação**

Não se aplica.

4.10. **Cessão de Direitos à Contratante**

Não se aplica.

5. GESTÃO E FISCALIZAÇÃO DO CONTRATO

5.1. **Modelo de gestão do contrato, com a definição de como a execução do objeto será acompanhada e fiscalizada pelo órgão ou entidade**

5.1.1. O contrato deverá ser executado, fielmente, de acordo com as cláusulas avençadas, respondendo o inadimplente pelas consequências da inexecução total ou parcial;

5.1.2. A gestão e a fiscalização da execução de cada contratação poderá ser realizada por uma Comissão de Gestão e Fiscalização, composta por, no mínimo, 3 (três) membros, integrada por gestor, fiscais e complementada conforme a necessidade pelos agentes definidos nos incisos I a III do art. 5º deste Decreto, considerando a especificidade e complexidade do objeto ou da solução, de acordo com a necessidade e a critério da administração.

5.1.3. A Comissão de Gestão e Fiscalização anotará, em registro próprio, todas as ocorrências relacionadas com a execução do contrato, determinando o que for necessário à regularização das faltas ou defeitos observados.

5.1.4. A execução dos contratos deverá ser acompanhada e fiscalizada por meio de instrumentos de controle que compreendam a mensuração dos seguintes aspectos, quando for o caso:

I - os resultados alcançados em relação ao contratado, com a verificação dos prazos de execução e da qualidade demandada;

II - os recursos humanos empregados em função da quantidade e da formação profissional exigidas;

III - a qualidade e quantidade dos recursos materiais utilizados;

IV - a adequação dos serviços prestados à rotina de execução estabelecida;

V - o cumprimento das demais obrigações decorrentes do contrato;

VI - a satisfação do público usuário, quando possível.

5.1.5. Deve ser estabelecido, desde o início da execução contratual, mecanismo de controle da utilização dos materiais empregados nos contratos, para efeito de acompanhamento da execução do objeto bem como para subsidiar a estimativa para as futuras contratações.

5.1.6. É vedada a atribuição à contratada da avaliação de desempenho e qualidade da prestação dos serviços por ela realizada.

5.1.7. Na hipótese de comportamento contínuo de desconformidade da prestação do serviço em relação à qualidade exigida, bem como quando esta não atingir os níveis mínimos toleráveis previstos nos indicadores, além dos fatores redutores, deve ser instaurado processo administrativo punitivo para apuração das infrações e, se for o caso, aplicação de sanções, conforme regulamento específico.

5.1.8. Havendo indícios de irregularidade, caberá ao gestor do contrato intimar o licitante ou o contratado para, no prazo de 15 (quinze) dias úteis, estabelecido na Lei nº 14.133, de 2021, contado da data de intimação, apresentar defesa escrita e especificar provas que pretenda produzir.

5.1.9. Encerrada a instrução, o gestor do contrato elaborará relatório com a finalidade de subsidiar a tomada de decisão pela autoridade competente, o qual conterá breve exposição dos fatos documentados, referência às provas colhidas e opinião conclusiva sobre existência, ou não, de culpa da licitante ou da contratada.

5.1.10. A CONTRATADA declara, antecipadamente, aceitar todas as condições, métodos e processos de inspeção, verificação e controle adotados pela fiscalização, obrigando-se a fornecer todos os dados, elementos, explicações, esclarecimentos e comunicações de que esta necessitar e que forem julgados necessários ao desempenho de suas atividades.

5.1.11. A instituição e a atuação da fiscalização não exclui ou atenua a responsabilidade da CONTRATADA, nem a exime de manter fiscalização própria.

5.1.12. No caso de inexecução total ou parcial do objeto, que acarrete a rescisão do Contrato, será automaticamente devida multa compensatória no valor de 5% (cinco por cento) do valor do Contrato.

5.2. **Mecanismos de comunicação a serem estabelecidos**

5.2.1. São instrumentos formais de comunicação entre a CONTRATANTE e a CONTRATADA:

a) Ordem de Serviço/Fornecimento;

b) Plano de Inserção;

c) Termos de Recebimento;

d) Ordem de Serviço;

e) Chamado registrado na Central de Atendimento;

f) Ofícios;

g) Relatórios e Atas de Reunião;

h) E-mail;

i) Demais Termos previstos no instrumento convocatório.

5.2.2. A comunicação entre a CONTRATANTE e a CONTRATADA, para fins de encaminhamento de Ordem de Fornecimento ou Ordem de Serviço, ocorrerá sempre por intermédio do preposto, ou seu substituto, designado pela CONTRATADA;

5.2.3. A comunicação dos usuários com a Central de Atendimento/Suporte da CONTRATADA poderá ser realizada por meio de abertura de chamado via telefone com registro de protocolo ou utilização de sistema informatizado que permita o registro da demanda.

5.3. **Recebimento provisório e definitivo do objeto**

5.3.1. O objeto do contrato, nos três Lotes, será recebido na seguinte forma:

I - Para os itens nº 5 de todos os lotes (SERVIÇO):

a) provisoriamente, pelos fiscais do contrato, mediante termo, no prazo de 02 (dois) dias úteis, quando verificado o cumprimento das exigências de caráter técnico;

b) definitivamente, pelos fiscais ou comissão de fiscalização, após decorrido o prazo de 20 (vinte) dias úteis do recebimento provisório, mediante termo detalhado que comprove o atendimento das exigências contratuais.

II - Para os itens nº 1, 2, 3, 4 de todos os lotes (AQUISIÇÃO):

a) provisoriamente, de forma sumária, pelo gestor de bens ou pelos fiscais do contrato, com verificação posterior da conformidade do material com as exigências contratuais;

b) definitivamente, mediante parecer circunstanciado da comissão de fiscalização, após decorrido o prazo 20 (vinte) dias úteis do recebimento provisório, para observação e vistoria, que comprove o exato cumprimento das obrigações contratuais.

5.3.2. A CONTRATADA deverá elaborar um Relatório de Cumprimento do Objeto (modelo no Anexo V deste documento) a ser entregue à Comissão de Fiscalização de Contrato quando da entrega do bem ou serviço, para a análise antes da emissão do Termo de Recebimento Provisório. No caso dos itens de compra (itens 1, 2, 3 e 4 de todos os lotes) o relatório deverá ser entregue no momento do recebimento sumário correspondente ao momento da efetiva entrega dos bens. O relatório deve contemplar todas as etapas e procedimentos realizados, eventuais problemas verificados e qualquer fato relevante sobre a execução do objeto contratual (bens e serviços). O relatório deverá estar acompanhado, conforme item ou etapa entregue, das seguintes informações e/ou documentos:

a) Para os itens 1 de todos os lotes: dados para acionamento dos serviços de suporte ou garantia, documentos oficiais do fabricante e documentação do produto (manuais, prospectos etc..);

b) Para os itens 2, 3 e 4 de todos os lotes: documentação que comprove o licenciamento das soluções contratadas, tais como número de séries, chaves, dados para acionamento dos serviços de suporte, documentos oficiais do fabricante e documentação do produto e disponibilização das soluções;

c) Para os itens 5 de todos os lotes: certificados dos alunos treinados.

5.3.3. Após a emissão do Termo de Recebimento Provisório, a CONTRATANTE, por meio de sua Comissão de Fiscalização de Contrato, analisará a documentação entregue e poderá fazer inspeções ou promover diligências internas quanto às etapas executadas para a entrega do objeto (bens e serviços), com a finalidade de verificar a adequação no cumprimento do objeto (bens e serviços) pela contratada, bem como verificar a necessidade de arremates, retoques e revisões finais que eventualmente se fizerem necessários.

5.3.4. A CONTRATADA fica obrigada a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas o objeto (bens e serviços) em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não proceder ao Termo de Recebimento Definitivo até que sejam sanadas todas as eventuais pendências que possam vir a ser

apontadas na fase do recebimento provisório.

5.3.5. Com o recebimento definitivo, que concretiza o ateste do cumprimento do objeto (bens e serviços) contratado, a CONTRATANTE comunicará à CONTRATADA para que, em até 5 dias, emita a Nota Fiscal ou Fatura.

5.3.6. A Comissão de Fiscalização de Contrato, sob pena de responsabilidade administrativa, anotará em registro próprio as ocorrências relativas à execução do contrato, determinando o que for necessário à regularização das faltas ou defeitos observados. No que exceder à sua competência, comunicará o fato à autoridade superior, em 10 (dez) dias, para ratificação.

5.3.7. A CONTRATADA declarará, antecipadamente, aceitar todas as condições, métodos e processos de inspeção, verificação e controle adotados pela fiscalização, obrigando-se a lhes fornecer todos os dados, elementos, explicações, esclarecimentos e comunicações de que este necessitar e que forem julgados necessários ao desempenho de suas atividades.

5.3.8. A instituição e a atuação da fiscalização do objeto (bens e serviços) do contrato não exclui ou atenua a responsabilidade da CONTRATADA, nem a exime de manter fiscalização própria.

5.3.9. O objeto do contrato poderá ser rejeitado, no todo ou em parte, quando estiver em desacordo com o contrato ou termo de referência, podendo ser fixado pelo fiscal do contrato um prazo para a substituição do bem, ou o refazimento do serviço, às custas do contratado, sem prejuízo da aplicação das penalidades, sendo sempre necessário a motivação da recusa.

5.3.10. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança da obra ou serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato, nos limites estabelecidos por este Decreto e pelo contrato.

5.3.11. Salvo disposição em contrário constante do edital, os ensaios, os testes e as demais provas para aferição da boa execução do objeto do contrato exigidos por normas técnicas oficiais correrão por conta do contratado.

5.3.12. A entrega do objeto, considerados todos os itens de compra componentes dos lotes, bem como eventuais atendimentos presenciais de suporte técnico, será realizada no endereço indicado pela Contratante.

5.3.13. O cronograma para entrega do objeto, contado em dias úteis, será conforme a tabela abaixo:

Prazo	Marco para contagem do prazo	Atividades	Responsável
1	Publicação do extrato do contrato no Portal Nacional de Compras Públicas - PNCP	Emissão da "Ordem de Fornecimento"	Contratante
15	Publicação do extrato do contrato no PNCP	Realização da Reunião Kick-Off	Contratante e Contratada
10	Emissão da "Ordem de Fornecimento"	Entrega dos itens de compra (hardware + software + licença padrão)	Contratada
35	Reunião kick-off	Instalação completa da solução de firewall (incluindo configurações, regras, políticas, etc.)	Contratada
20	Emissão da Ordem de Serviço (sob demanda)	Início do treinamento da solução	Contratada
2	Entrega do Relatório de Cumprimento do Objeto	Emissão do Termo de Recebimento Provisório	Contratante
20	Emissão do Termo de Recebimento Provisório ou Sumário	Emissão do Termo de Recebimento Definitivo / autorização para emissão de Nota Fiscal ou fatura, resguardadas as disposições deste documento.	Contratante

5.3.14. O objeto em sua totalidade é composto por equipamentos e seus respectivos treinamentos. A entrega dos itens nº 1, 2, 3, 4 de todos os lotes, será através da disponibilização dos equipamentos no ambiente da contratada devidamente instalados e configurados. Já a execução dos itens nº 5 de todos os lotes (cursos de treinamento) acontecerá através do portal de treinamentos da contratada ou que esta venha a viabilizar.

5.4. **Metodologia de avaliação da qualidade e aceite do objeto executado**

5.4.1. **Acordo de Nível de Serviço**

I - **Finalidade:** Garantir a qualidade dos Serviços de Treinamentos (item 05 de cada lote).

II - **Periodicidade**: eventual, ao final do treinamento contratado, para fins de ateste de Nota Fiscal e emissão do Termo de Recebimento Definitivo

III - **Início da medição**: Imediatamente após a entrega do Relatório de Cumprimento do serviço de treinamento pela Contratada.

IV - **Mecanismo de cálculo**: Os servidores participantes farão avaliação do curso com atribuição de grau, conforme os percentuais indicados abaixo:

a) I (insatisfatório) – 0 a 25%;

b) R (regular) – 25 a 50%;

c) B (bom) – 50 a 75%;

d) MB (muito bom) – 75 a 100%.

V - **Sanções**

a) A Comissão de Fiscalização de Contrato atestará a Nota Fiscal do treinamento realizado, sem aplicação de glosa, se no mínimo 60% das avaliações indicarem os graus B (bom) e/ou MB (muito bom).

b) A Comissão de Fiscalização de Contrato poderá aplicar alternativamente glosa de 2% sobre o valor da Nota Fiscal se 50% das avaliações indicarem o grau R (regular).

c) A Comissão de Fiscalização de Contrato poderá aplicar alternativamente glosa de 5% sobre o valor da Nota Fiscal se 50% das avaliações indicarem o grau I (insatisfatório).

d) Qualquer descumprimento do Acordo de Nível de Serviço poderá implicar as sanções previstas na da Lei de Licitações e Contratos.

e) Ficam resguardadas todas as sanções administrativas previstas na Lei de Licitações e Contratos.

5.5. **Pagamento (Critérios de medição e de pagamento e condições de aquisição e pagamento semelhantes às do setor privado, através de cronograma físico-financeiro, quando cabível)**

5.5.1. A CONTRATANTE deverá pagar o preço ao CONTRATADO na conta corrente de titularidade do CONTRATADO a ser indicada, junto à instituição financeira contratada pelo Estado do Rio de Janeiro, da seguinte forma:

a) Para os itens de compra (nº 01, 02, 03 e 04 de todos os Lotes) o pagamento é à vista;

b) Para itens de serviço de treinamento (nº 05 de todos os Lotes) o pagamento é à vista, sob demanda.

5.5.2. No caso de o CONTRATADO estar estabelecido em localidade que não possua agência da instituição financeira contratada pelo Estado do Rio de Janeiro ou, caso verificada pela CONTRATANTE a impossibilidade de o CONTRATADO, em razão de negativa expressa da instituição financeira contratada pelo Estado do Rio de Janeiro, abrir ou manter conta corrente naquela instituição financeira, o pagamento poderá ser feito mediante crédito em conta corrente de outra instituição financeira. Nesse caso, eventuais ônus financeiros e/ou contratuais adicionais serão suportados exclusivamente pelo CONTRATADO.

5.5.3. A emissão da Nota Fiscal ou Fatura será precedida do recebimento definitivo do objeto ou de cada parcela, mediante atestação, que não poderá ser realizada pelo ordenador de despesas, conforme disposto neste instrumento e/ou neste Termo de Referência, bem ainda no artigo 140, II, alínea "b", da Lei nº 14.133/2021 e arts. 20 e 22, XXIII, do Decreto nº 48817/2023.

5.5.4. Quando houver glosa parcial do objeto, a CONTRATANTE deverá comunicar ao CONTRATADO para que emita Nota Fiscal ou Fatura com o valor exato dimensionado.

5.5.5. O CONTRATADO deverá encaminhar a Nota Fiscal ou Fatura para pagamento à CONTRATANTE, para o endereço eletrônico a ser indicado.

5.5.6. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do Contrato, caso o CONTRATADO não regularize sua situação, ressalvado o disposto no art. 121, § 3º, da Lei nº 14.133, de 2021, no art. 29 do Decreto nº 48.817, de 2023, e no Termo de Referência.

5.5.7. O pagamento será efetuado no prazo máximo de até 30 (trinta) dias, contados do recebimento da Nota Fiscal ou Fatura.

5.5.8. Havendo erro na apresentação da Nota Fiscal ou Fatura, ou circunstância que impeça a liquidação da despesa, o pagamento ficará sobrestado até que o CONTRATADO providencie as medidas saneadoras. Nessa hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a CONTRATANTE.

5.5.9. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

5.5.10. Independentemente do percentual de tributo inserido na planilha, no pagamento serão retidos na fonte os percentuais estabelecidos na legislação vigente.

5.5.11. O CONTRATADO regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123/2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele Regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar nº 123/2006.

5.5.12. Os pagamentos eventualmente realizados com atraso, desde que não decorram de ato ou fato atribuível ao CONTRATADO, sofrerão a incidência de atualização monetária e juros de mora pelo IPCA-E, calculado pro rata die, e aqueles pagos em prazo inferior ao estabelecido no instrumento convocatório serão feitos mediante desconto de 0,5% (um meio por cento) ao mês, calculado pro rata

die.

5.5.13. O CONTRATADO deverá emitir a Nota Fiscal Eletrônica – NF-e, consoante o Protocolo ICMS nº 42/2009, com a redação conferida pelo Protocolo ICMS nº 85/2010, e caso seu estabelecimento esteja localizado no Estado do Rio de Janeiro, deverá observar a forma prescrita nas alíneas a, b, c, d e e, do §1º, do art. 2º da Resolução SEFAZ nº 971/2016.

5.5.14. Caso o CONTRATADO não esteja aplicando o regime de cotas na forma da Lei estadual nº 7.258, de 12 de abril de 2016, deste edital e do contrato, suspender-se-á o pagamento devido, até que seja sanada a irregularidade apontada pelo órgão de fiscalização do Contrato.

5.5.15. O Edital poderá conter outras disposições acerca de Pagamento.

6. OBRIGAÇÕES FUTURAS

6.1. **Garantia técnica do produto fornecido**

6.1.1. A Garantia dos itens 1, 2, 3, 4 de todos os lotes, obedecerá às seguintes regras:

I - Considera-se "garantia" a obrigação da CONTRATADA em reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, o objeto do contrato (e quaisquer de seus componentes) em que se verificarem vícios de produto, defeitos ou incorreções, durante o prazo de garantia especificado neste documento;

II - A garantia terá duração de 60 (sessenta meses), contados a partir da data do recebimento definitivo do objeto;

III - A garantia deve obrigatoriamente prover, ao longo de sua duração e sem ônus adicionais para o contratante:

- Acesso para downloads de patches, drivers, e quaisquer outras atualizações de software necessárias, que devem estar disponíveis no website do fabricante da solução, sem custos adicionais ao Contratante, durante todo o período de garantia.
- Disponibilizar as revisões dos manuais técnicos e/ou documentação dos equipamentos adquiridos.

6.1.2. **Assistência técnica / Suporte Técnico**

I - A contratada deverá disponibilizar por meio da Internet uma aplicação WEB para registro dos chamados de suporte técnico através de login e senha fornecida para os usuários autorizados da contratante, em regime de 24x7x365 (vinte e quatro horas por dia durante todos os dias do ano, inclusive sábados, domingos e feriados);

II - A contratante poderá efetuar um número ilimitado de chamados para suporte técnico, durante a vigência da garantia, para suprir suas necessidades com relação a solução adquirida;

III - Considera-se "suporte técnico" a facilidade de comunicação colocada à disposição do CONTRATANTE para a prestação de informações, esclarecimentos ou orientações sobre a utilização, funcionalidades (dicas e atalhos), configuração de softwares/hardwares básicos, aplicativos, sistemas da informação em geral envolvidos na solução objeto da contratação, bem como a intervenção direta nos equipamentos para configurações, instalações e remoções de aplicativos, atualizações de softwares e reparos diversos necessários ao bom funcionamento da solução;

IV - O suporte técnico será acionado sempre que a solução apresentar falha que impeça o seu funcionamento regular e requeira uma intervenção técnica especializada e mesmo a substituição de seus componentes;

V - Durante o atendimento, a contratada poderá analisar a solução, sua atual condição de funcionamento, seus logs de sistema e sugerir mudanças para uma melhor prática de utilização da ferramenta. A equipe técnica do contratante decidirá sobre a aplicação ou não das recomendações;

VI - Cada pessoa cadastrada no sistema como usuário deverá receber identificação e senha que permitam acesso seguro tanto ao sistema, como ao recurso de abertura de chamadas de suporte técnico, de maneira a evitar que pessoas não autorizadas possam acionar o suporte;

VII - O fabricante deverá efetuar a troca de peças ou do equipamento, em que sejam constatadas quaisquer falhas ou defeitos de fabricação. Eventuais substituições de hardware deverão ser realizadas em até 1 (um) dia útil, a partir da constatação da necessidade de substituição do componente de hardware;

VIII - Os prazos de atendimento do suporte técnico da solução devem ter como referência os níveis de severidade, todos informados na tabela abaixo, ficando a contratada sujeita às sanções previstas na lei em caso de descumprimento contratual:

Tabela de Severidades dos Chamados e Prazos de Atendimento / Solução			
Severidade	**Descrição**	**Tempo de 1º contato após abertura do chamado**	**Tempo de Solução**
Urgente	Objeto totalmente inoperante	até 30 minutos	até 2 horas
Importante	Solução parcialmente inoperante – Necessidade de suporte na solução com a necessidade de interrupção de funcionamento da solução	até 1 hora	até 4 horas
Normal	Solução não inoperante, mas com problema de funcionamento – Necessidade de suporte na solução sem a necessidade de interrupção de funcionamento da solução	até 2 horas	até 24 horas
Informação	Solicitações de informações diversas ou dúvidas sobre a solução	até 8 horas	até 48 horas

IX - A severidade do chamado poderá ser reavaliada quando verificado que a mesma foi erroneamente aplicada, passando a contar no momento da reavaliação os novos prazos de atendimento e solução;

X - A cada abertura de chamado CONTRATADA poderá solicitar a prorrogação de quaisquer dos prazos para conclusão de atendimentos de chamados, desde que o faça antes do seu vencimento e devidamente justificado. Caberá à CONTRATANTE aceitar ou não o pedido de prorrogação do prazo.

XI - Todos os prazos para atendimento do suporte começarão a ser contados a partir da abertura do chamado independentemente de este ter sido feito via telefone, e-mail ou website do fornecedor.

7. FORMA DE SELEÇÃO, CRITÉRIOS DE PREÇOS E JULGAMENTO DE PROPOSTAS

7.1. **Critério de julgamento**

7.1.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, em SISTEMA DE REGISTRO DE PREÇOS, com adoção do critério de julgamento pelo **MENOR PREÇO** por lote, em observação do Art. 33, inciso I, da Lei nº 14.133/2021.

7.1.2. Para se obter o menor preço por lote, consideradas as justificativas de não parcelamento, constantes deste Termo de Referência, deverão ser negociados os valores individualizados de cada item que o compõe, buscando também o menor preço unitário, tendo em vista que os itens se encontram agrupados, meramente em razão da compatibilidade técnica/operacional intrínseca dentro de cada um dos lotes previstos.

7.2. **Modo de disputa**

7.3. O envio de lances no pregão eletrônico se dará pelo modo aberto de disputa, na forma do Art. 56, inciso I da Lei nº 14.133/21, hipótese em que os licitantes apresentarão suas propostas por meio de lances públicos e sucessivos, crescentes ou decrescentes.

7.4. A combinação da modalidade de licitação prevista, bem como dos parâmetros de julgamento das propostas e também o modo de disputa, consideram a natureza comum dos bens e serviços componentes do objeto licitado, e também a composição em lotes e as justificativas acerca do parcelamento ou não do objeto, na forma do disposto no subtópico 3.1 deste documento.

7.4.1. Em consonância ao inciso I do Art. 56 da Lei nº 14.133, de 2021 e atendimento ao art. 17, VI, "a" do Decreto 48.816/23, no modo de disputa aberto, os licitantes apresentarão suas propostas por meio de lances públicos e sucessivos, crescentes ou decrescentes, visto que se trata de um pregão cujo o critério de julgamento é menor preço por lote.

7.4.3. Os preços em disputa aberta ficam claros para melhor competição entre os participantes. Então, evitar riscos na contratação contribui para ter uma licitação que alcance mais prontamente os resultados pretendidos.

7.4.5. Outrossim, não foi possível identificar que optar por modo disputa diferente do "modo aberto" venha a trazer vantagem para a Administração e nem mesmo aponta simplificação do processo ou celeridade no resultado da licitação.

7.5. **Estabelecimento de reserva de cota ou da exclusividade da licitação**

Não se aplica, tendo em vista que o objeto desta licitação é indivisível, ou seja, não pode ser adquirido separadamente, sem prejuízo do resultado ou da qualidade do serviço.

7.6. **Prazo de validade da proposta**

O prazo de validade da proposta não será inferior a 60 (sessenta) dias corridos, a contar da data de sua apresentação, podendo ser prorrogado, por igual período, salvo se houver justificativa para prazo diverso aceita pela Administração.

7.7. **Condições da proposta**

7.7.1. Os prazos mínimos para a apresentação das propostas e lances, contados a partir do 1º dia útil da data de divulgação do edital de licitação no PNCP, será de 10 (dez) dias úteis, no caso de serviços comuns. (Art. 55, II, a, da Lei nº 14.133/2021).

7.7.2. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos:

I - Valor unitário e total do item;

II - Marca;

III - Fabricante;

IV - Descrição do objeto, contendo as informações similares à especificação deste Termo de Referência;

V - Quantidade cotada, que não poderá ser inferior ao quantitativo máximo de cada item que poderá ser adquirido.

7.7.3. Todas as especificações do objeto contidas na proposta vinculam o licitante.

7.7.4. O licitante não poderá oferecer proposta em quantitativo inferior ao máximo previsto para contratação.

7.7.5. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na execução do objeto.

7.7.6. Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.

7.7.7. Se o regime tributário da empresa implicar o recolhimento de tributos em percentuais variáveis, a cotação adequada será a que corresponde à média dos efetivos recolhimentos da empresa nos últimos doze meses.

7.7.8. Independentemente do percentual de tributo inserido na planilha, no pagamento serão retidos na fonte os percentuais estabelecidos na legislação vigente.

7.7.9. Na presente licitação, a Microempresa e a Empresa de Pequeno Porte poderão se beneficiar do regime de tributação pelo Simples Nacional, desde que atendidas as disposições do subtópico 5.5.11. deste Termo de Referência.

7.7.10. O licitante cujo estabelecimento esteja localizado no Estado do Rio de Janeiro deverá apresentar proposta isenta de ICMS, quando cabível, de acordo com o Convênio CONFAZ nº 26/2003 e a Resolução SEFAZ nº 971/2016, sendo este valor considerado para efeito de competição na licitação.

7.7.11. A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o que dispõe o Termo de Referência, assumindo o proponente o compromisso de executar o objeto licitado nos seus termos, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.

7.8. **Critérios de desempate com base no desenvolvimento pelo licitante de ações de equidade entre homens e mulheres no ambiente de trabalho, conforme regulamento**

7.8.1. O art. 5ºdo Decreto Federal 11.430/2023, dispõe que desenvolvimento, pelo licitante, de ações de equidade entre mulheres e homens no ambiente de trabalho será critério de desempate em processos licitatórios, nos termos do disposto no inciso III do caput do art. 60 da Lei nº 14.133, de 2021.

§ 1º Para fins do disposto no caput, serão consideradas ações de equidade, respeitada a seguinte ordem:

I - medidas de inserção, de participação e de ascensão profissional igualitária entre mulheres e homens, incluída a proporção de mulheres em cargos de direção do licitante;

II - ações de promoção da igualdade de oportunidades e de tratamento entre mulheres e Termo de Referência de Material/Serviço 70439738 SEI SEI-430002/000048/2024 / pg. 41 homens em matéria de emprego e ocupação;

III - igualdade de remuneração e paridade salarial entre mulheres e homens;

IV - práticas de prevenção e de enfrentamento do assédio moral e sexual;

V - programas destinados à equidade de gênero e de raça; e

VI - ações em saúde e segurança do trabalho que considerem as diferenças entre os gêneros.

7.9. **Critérios de desempate na forma no Art. 60 da Lei nº 14.133, de 2021**

7.9.1. Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 60 da Lei nº 14.133/2021, nesta ordem:

a) disputa final, hipótese em que os licitantes empatados poderão apresentar nova proposta em ato contínuo à classificação;

b) avaliação do desempenho contratual prévio dos licitantes, para a qual deverão preferencialmente ser utilizados registros cadastrais para efeito de atesto de cumprimento de obrigações previstos na Lei;

c) desenvolvimento pelo licitante de ações de equidade entre homens e mulheres no ambiente de trabalho, conforme regulamento;

d) desenvolvimento pelo licitante de programa de integridade, conforme orientações dos órgãos de controle.

7.9.2. Persistindo o empate, será assegurada preferência, sucessivamente, aos bens e serviços produzidos ou prestados por:

a) empresas estabelecidas no território do Estado ou do Distrito Federal do órgão ou entidade da Administração Pública estadual ou distrital licitante ou, no caso de licitação realizada por órgão ou entidade de Município, no território do Estado em que este se localize;

b) empresas brasileiras;

c) empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

d) empresas que comprovem a prática de mitigação, nos termos da Lei nº 12.187, de 29 de dezembro de 2009.

8. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

Conforme autorizam, o inciso VIII, artigo 17 do Decreto 48.816/2023 e o item 6.2.2 da Nota Técnica nº 6/2023 do TCE/RJ, o valor estimado para esta contratação será apresentado em documento apartado.

9. MATRIZ DE RISCOS (ART. 17, X)

Observadas as condições de Suporte Técnico, Garantia de Produto e Acordo de Nível de Serviço, constantes deste Termo de Referência, bem como considerado o Mapa de Riscos realizado durante os estudos técnicos preliminares, os quais apresentam as correspondentes ações de prevenção e contingência, não se vislumbra riscos inerentes ao futuro contrato, os quais possam impactar e seu equilíbrio financeiro. Ademais, o presente objeto, observado o valor estimado em sede de cotação de preços, não se enquadra acima do teto previsto no Art. 6º, inciso XXII da Lei nº 14.133/2023, cujo parâmetro é condicionante no Art. 17, inciso X, alínea "c" do Decreto Estadual nº 48.816/23 para a apresentação da matriz de riscos.

10. DISPOSIÇÕES FINAIS

10.1. O presente termo de referência foi concebido com base nas normas legais aplicadas à matéria e nas premissas recomendadas pelo Tribunal de Contas do Estado do Rio de Janeiro – TCE-RJ e a Procuradoria-Geral do Estado - PGE/RJ. Este documento constituirá parte integrante do edital da licitação a ser instaurado para viabilizar a contratação de empresa devidamente qualificada e que apresente o melhor preço para fornecimento do bem objeto desta demanda.

10.2. As empresas interessadas em participar da licitação serão integralmente responsáveis pela avaliação e levantamento dos custos relativos à execução do objeto, sendo inteiramente responsáveis por eventuais prejuízos decorrentes de avaliação equivocada ou da sua ausência.

10.3. Observadas as disposições da Lei Federal nº 12.527/2011 e do Decreto Estadual nº 46.475/2018, que tratam do direito e das restrições de acesso às informações sob guarda do poder público, fica registrado que o presente documento, assim como os seus anexos, são de acesso PÚBLICO.

11. ANEXOS

Abaixo, estão listados os documentos anexos cujas disposições estão em plena concordância com este Termo de Referência, do qual correspondem a parte integrante e indissociável:

I - Especificações Técnicas do Objeto (83089505);

II - Roteiro para Prova de Conceito - Firewall Tipo 1 (83090165);

III - Roteiro para Prova de Conceito - Firewall Tipo 2 (83090167);

IV - Roteiro para Prova de Conceito - Firewall Tipo 3 (83090170);

V - Modelo de Relatório de Cumprimento do Objeto (83089840;

VI - Modelo de Termo de Sigilo e Confidencialidade (83089841);

VII - Modelo da Ordem de Fornecimento / Ordem de Serviço (83090176);

VIII - Modelo de Planilha de Composição de Preços (83089514);

IX - Modelo de Termo de Recebimento Definitivo (83090192);

X - Modelo de Termo de Recebimento Provisório (83089515);

XI - Modelo de Declaração de Sustentabilidade Ambiental (83089517);

12. RESPONSÁVEIS PELA ELABORAÇÃO DO TERMO DE REFERÊNCIA

Monique Gonçalves Paz Diretora de Segurança da Informação ID 4349648-2	Manuelito de Sousa Reis Júnior Responsável pela demanda Gerente de Riscos e Ameaças ID nº 4406953-7	Isabela Rebouças Costa Analista de Sistemas ID nº 4349659-8	Rosana Alves de Andrade Analista de Sistemas Gerente de Proteção de Dados e Sistemas ID nº 4347470-5	_____ Fabio Ivo Analista de Rede / Telecom ID nº 5143032-0	Marco Antônio de Andrade Assessor-chefe na Vice-Presidência de Administração ID nº 4284601-3	I

Rio de Janeiro, 09 de julho de 2024

Documento assinado eletronicamente por **Charles Monteiro Guimarães**, **Diretor**, em 12/09/2024, às 14:42, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Manuelito de Sousa Reis Junior**, **Gerente**, em 12/09/2024, às 14:43, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Fabio Ivo**, **Assistente**, em 12/09/2024, às 15:01, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Marco Antonio de Andrade**, **Assessor Chefe**, em 12/09/2024, às 15:04, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Isabela Reboucas Costa**, **Analista de Sistemas**, em 12/09/2024, às 15:14, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Monique Goncalves Paz**, **Diretora**, em 12/09/2024, às 15:15, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Rosana Alves de Andrade**, **Analista de Sistemas**, em 12/09/2024, às 15:40, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **83090161** e o código CRC **3BAE7500**.

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone:

ANEXO I DO TERMO DE REFERÊNCIA

ESPECIFICAÇÕES TÉCNICAS DO OBJETO

1. OBJETO

I - Os lotes com os itens componentes do objeto se encontram descritos na tabela do subtópico 2.2.6. do Termo de Referência.

II - Este anexo deve ser interpretado conforme as disposições do Termo de Referência do qual é parte integrante e indissociável.

1.1. Características Gerais das Soluções de Firewall dos Lotes 1, 2 e 3

1.1.1. Arquitetura

1.1.1.1. As soluções de Firewall presentes nos Lotes 1, 2 e 3 do objeto são compostas por equipamentos do tipo appliance, o software complementar para gerenciamento, logs e relatórios, bem como os treinamentos operacionais para as distintas soluções presentes nos Lotes 1, 2 e 3.

1.1.1.2. O firewall gerenciado, especificado no Lote 1, deve ser capaz de encaminhar pacotes para serem analisados por um sistema e/ou equipamento concentrador.

1.1.1.3. O firewall gerenciado, especificado no Lote 2, deve ser capaz de encaminhar pacotes para serem analisados por um sistema e/ou equipamento concentrador.

1.1.1.4. O firewall gerenciado, especificado no Lote 3, deve ser capaz de encaminhar pacotes para serem analisados por um sistema e/ou equipamento concentrador.

1.1.2. Licenciamento

1.1.2.1. Licença Padrão

I - Entende-se por Licença Padrão a licença de uso do fabricante em caráter permanente e perpétuo para todas as funcionalidades e quantidades mencionadas neste documento, com exceção aos itens relacionados à Atualização de Assinaturas de Proteção.

II - Entende-se por Atualização de Assinaturas de Proteção todas as funcionalidades, manuais ou automatizadas, necessárias para manter a solução em seu nível de identificação e proteção mais atualizado, tais como: atualização de assinaturas de prevenção de intrusão, assinaturas de identificação de vírus, assinaturas de identificação de aplicações, listas de classificação de URLs, listas de geolocalização, listas de endereços IPs utilizados por botnets, listas de endereços IPs de reputação duvidosa etc.

III - Todos os equipamentos firewall devem possuir esta licença ativada.

1.1.2.2. Licença de Atualização de Segurança

I - Entende-se por Licença de Atualização de Segurança a licença de uso do fabricante que permita a utilização das funcionalidades e quantidades mencionadas neste documento para os itens relacionados à Atualização de Assinaturas de Proteção (subtópico 1.1.2.1.).

II - A licença deve permitir que todas as assinaturas, listas e demais métodos de detecção e prevenção de ameaças e de filtros de conteúdo e aplicação empregados pela solução sejam atualizados até suas últimas versões disponíveis.

III - As Licenças de Atualização de Segurança devem ter prazo de vigência de 60 (sessenta) meses, contados a partir da aplicação destas nos produtos.

1.1.3. Hardware

1.1.3.1. Deve ser fornecido em formato appliance físico.

1.1.3.2. Deve ser novo, sem uso, entregue em perfeito estado de funcionamento, sem marcas, amassados, arranhões ou outros problemas físicos, acondicionados em suas embalagens originais.

1.1.3.3. Nenhum dos equipamentos fornecidos pode estar em modo End of Life, End of Sale e End of Support no dia do Pregão Eletrônico.

1.1.3.4. Deve ser apropriado para o uso em ambiente tropical com umidade relativa na faixa de 10 a 90% (sem condensação) e temperatura ambiente na faixa de 0 a 40°C.

1.1.3.5. Deve possuir fonte com alimentação nominal de 100~120VAC e 210~230VAC e frequência de 50 ou 60 Hz ou auto-ranging. Deve vir acompanhado de cabo de alimentação com, no mínimo, 1,80m (6 pés), com plug tripolar 2P+T no padrão ABNT NBR 14136.

1.1.3.6. Deve possuir, no mínimo, 1 (uma) interface Ethernet dedicada para gerenciamento.

1.1.3.7. O plano de gerenciamento da solução deve ser apartado do plano de dados, com recursos de CPU, memória e interface de rede dedicados para esta função;

1.1.3.8. Deve ser fornecido em sua capacidade máxima de processamento, memória e armazenamento interno.

1.1.3.9. Deve ser fornecido com todas as suas portas de comunicação, interfaces e afins habilitadas, operacionais e prontas para operação, inclusive com seus respectivos transceivers instalados, sem custos adicionais.

1.1.4. **Funcionalidades Básicas**

1.1.4.1. Deve possuir MIB própria contemplando, no mínimo, indicadores de estado do hardware e de performance do equipamento.

1.1.4.2. Deve suportar o envio de notificações via e-mail, SNMP traps e mensagens de log.

1.1.4.3. Deve permitir o acesso ao equipamento via SSH e interface web HTTPS.

1.1.4.4. A comunicação entre a estação de trabalho do administrador e o firewall deve ser autenticada e criptografada.

1.1.4.5. Deve informar a utilização dos recursos de CPU, memória e atividade de rede.

1.1.4.6. Deve possuir visualização mínima sumarizada de aplicações, ameaças, URLs, endereços de origem, endereços de destino, levando-se em conta o quantitativo de sessões, de consumo de banda e categorização.

1.1.4.7. Deve possuir a funcionalidade de exportação automática dos logs para servidor syslog e para a solução de gerenciamento de logs.

1.1.4.8. Desejável possuir plano de gerenciamento segregado do plano de dados, inclusive com CPU e interfaces dedicadas.

1.1.4.9. Deve permitir a importação, criação e edição de regras SNORT.

1.1.4.10. Os Firewalls de segurança físico ou virtualizados, devem possuir processamento dedicado no equipamento de segurança para funções e ações de Gerenciamento, mesmo que o equipamento esteja com alto processamento de CPU. Assim evitando a falta de acesso do administrador para qualquer mitigação de problema e aplicação de política para solução de problemas. Entre as funções, deve suportar no mínimo: acesso SSH, acesso WEB, alterações de política, comunicação SNMP; 1.6. Console de Gerenciamento centralizado.

1.1.4.11. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7.

1.1.5. **Rede**

1.1.5.1. Deve suportar os protocolos IPv4 e IPv6.

1.1.5.2. Deve suportar VLAN no padrão 802.1q.

1.1.5.3. Deve suportar Jumbo Frames.

1.1.5.4. Deve suportar sub interfaces Ethernet lógicas.

1.1.5.5. Deve suportar o protocolo NTP.

1.1.5.6. Deve implementar mecanismo de conversão de endereços NAT (Network Address Translation), de forma a possibilitar a realização de NAT estático (1-1), dinâmico (N-1), NAT pool (N-N) e NAT condicional (possibilitando que um endereço tenha mais de um NAT dependendo da origem, destino ou porta).

1.1.5.7. Deve permitir o registro de eventos de NAT com as informações de endereço interno, endereço público, data e hora do evento, portas de origem e destino.

1.1.5.8. Deve suportar tradução de porta (PAT).

1.1.5.9. Deve suportar as funcionalidades de roteamento estático e dinâmico em IPv4 e IPv6.

1.1.5.10. Deve suportar os protocolos RIP, OSPF v2, OSPF v3 e BGP v4.

1.1.5.11. Deve suportar os protocolos IGMP v2, IGMP v3, PIM-SM.

1.1.5.12. Deve suportar Virtual Routing Redundancy Protocol (VRRP) ou equivalente.

1.1.5.13. Deve suportar os protocolos SNMP v2 e SNMP v3.

1.1.5.14. Deve permitir monitorar, via SNMP, falhas de hardware, uso de recursos por número elevado de sessões, número de túneis estabelecidos na VPN, CPU, memória, status do cluster de Alta Disponibilidade e estatísticas de uso das interfaces de rede.

1.1.5.15. Deve suportar Policy Based Routing (PBR), possibilitando políticas de roteamento condicionado ao endereço IP de origem, endereço IP de destino e porta de comunicação.

1.1.5.16. Deve suportar no mínimo as seguintes funcionalidades em IPv6: SLAAC (address auto configuration), NAT64, Identificação de usuários a partir do LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Regras de proteção contra DoS (Denial of Service), De-criptografia SSL e SSH, PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, IPSEc, Ativo/Ativo, Ativo/Passivo, SNMP, NTP, SYSLOG, DNS, Neighbor Discovery (ND), Recursive DNS Server (RDNSS).

1.1.6. **Autenticação e Identificação de Usuários**

1.1.6.1. Deve promover a integração com serviços de diretório LDAP e Active Directory, baseados em caracteres da língua portuguesa, para a identificação, autenticação, autorização e registro de eventos de acessos ou ameaças.

1.1.6.2. Deve identificar de forma transparente os usuários autenticados por meio de serviço de diretório LDAP ou Active Directory.

1.1.6.3. Não será permitida a utilização de agentes instalados nos servidores LDAP, Active Directory, proxies internos e equipamentos dos usuários, nem configuração adicional no navegador.

1.1.6.4. Não será permitida a interceptação ou espelhamento do tráfego destinado aos servidores LDAP, Active Directory e proxies internos.

1.1.6.5. Deve possuir portal de autenticação (captive portal) para a identificação e autenticação de usuários não registrados ou não reconhecidos.

1.1.6.6. O portal de autenticação deve ser capaz de identificar e autenticar usuários cadastrados em serviço de diretório LDAP e Active Directory.

1.1.6.7. Deve permitir a criação de políticas de segurança baseadas em usuários e grupos de usuários pertencentes a um diretório LDAP ou ao Active Directory.

1.1.6.8. Deve registrar a identificação do usuário em todos os logs de eventos de acesso ou de ameaças gerados pelo equipamento.

1.1.6.9. Deve registrar os eventos dos usuários em tempo real, sem a utilização de processos em lote (batches) ou processos de correlação após a ocorrência do evento em questão.

1.1.6.10. Deve possuir a capacidade de definir administradores com diferentes perfis de acesso. Os perfis de acesso devem ser, no mínimo, de leitura/escrita e somente leitura.

1.1.6.11. Desejável possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente, mesmo que não sejam servidores Windows.

1.1.6.12. Desejável identificar usuários através de leitura do campo x-fowarded-for, populando nos logs do firewall o endereço IP, bem como o usuário de rede responsável pelo acesso.

1.1.7. **Geolocalização**

1.1.7.1. Deve identificar os países de origem e destino de todas as conexões estabelecidas através do equipamento.

1.1.7.2. Deve identificar, no mínimo, 180 países.

1.1.7.3. Deve armazenar as listas de geolocalização no próprio equipamento.

1.1.7.4. Deve permitir a criação de políticas de segurança baseadas em geolocalização, permitindo o bloqueio de tráfego com origem ou destino a determinado país ou grupo de países.

1.1.7.5. Deve possibilitar a visualização dos países de origem e destino nos logs de eventos de acessos e ameaças.

1.1.8. **VPN**

1.1.8.1. Deve suportar VPN site-to-site em topologia Full Meshed (todos os gateways possuem links específicos para todos os demais gateways) e Estrela (gateways satélites se comunicam somente com um único gateway central).

1.1.8.2. Deve suportar criptografia 3DES, AES-128, AES-256.

1.1.8.3. Deve suportar integridade de dados com MD5, SHA-1 e SHA-256.

1.1.8.4. Deve suportar o protocolo IKE, fases I e II.

1.1.8.5. Deve suportar os algoritmos RSA e Dif ie-He lman groups 1, 2, 5 e 14.

1.1.8.6. Deve suportar Certificado Digital X.509.

1.1.8.7. Deve suportar NAT-T (NAT Transversal).

1.1.8.8. Deve permitir a criação de túneis VPN SSL/TLS e IPSec.

1.1.8.9. Deve suportar VPN IPSec client-to-site (acesso remoto).

1.1.8.10. Deve possuir cliente próprio para instalação nos dispositivos móveis dos usuários, sem custo adicional.

1.1.8.11. Deve permitir que o usuário realize a conexão VPN por meio de cliente instalado nos sistemas operacionais: Windows, Mac OS ou Linux do seu equipamento ou então por meio de interface web do tipo portal.

1.1.8.12. Caso o acesso seja feito por meio da interface Web, deverá ser compatível com, no mínimo, as versões atualizadas dos seguintes navegadores: Microsoft Edge, Mozilla Firefox e Google Chrome.

1.1.8.13. Deve suportar atribuição de endereço IP nos clientes remotos de VPN.

1.1.8.14. Deve suportar atribuição de DNS nos clientes remotos de VPN.

1.1.8.15. Deve suportar, no mínimo, os protocolos de roteamento estático e dinâmico OSPF e BGP.

1.1.8.16. O túnel IPSec VPN do cliente ao gateway (client-to-site) deve fornecer uma solução de autenticação única (single-sign-on) aos usuários, integrando-se com as ferramentas de Windows login.

1.1.8.17. O túnel IPSec VPN client-to-site deve também possuir autenticação em fator duplo (2FA) aos usuários.

1.1.8.18. Deve permitir criar políticas por usuário e grupos para tráfego de VPN client-to-site.

1.1.8.19. Deve suportar autoridade certificadora integrada ao gateway VPN ou à solução de gerenciamento centralizado.

1.1.8.20. Deve promover a integração com diretórios LDAP e Active Directory para a autenticação de usuários de VPN e regras de acesso.

1.1.8.21. Deve suportar os métodos de autenticação de VPN: usuário e senha de base interna do próprio equipamento, usuário e senha de diretório LDAP, usuário e senha do Active Directory, certificação digital por meio de certificados emitidos por autoridade certificadora integrada ao equipamento ou à solução de gerenciamento centralizado, certificação digital por meio de certificados emitidos por autoridade certificadora integrada ao Active Directory, certificação digital por meio de certificados emitidos por autoridade certificadora no padrão ICP-Brasil.

1.1.8.22. Deve suportar a integração com autoridades certificadoras de terceiros que possam gerar certificados no formato PKCS#12.

1.1.8.23. Deve suportar a solicitação de emissão de certificados a uma autoridade certificadora de confiança (enro lment) via SCEP (Simple Certificate Enro lment Protocol) ou CSR (Certificate Signing Requests).

1.1.8.24. Deve suportar a leitura e verificação de CRLs (Certification Revogation Lists).

1.1.8.25. Deve permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis de SSL.

1.1.8.26. Deve possuir mecanismos de checagem de conformidade do dispositivo remoto.

1.1.8.27. A checagem de conformidade deve permitir verificar, no mínimo, as seguintes informações no cliente remoto: sistema operacional e patches instalados, antivírus e versão instalada, firewall no host.

1.1.9. **Qualidade de Serviço (QoS)**

1.1.9.1. Deve permitir o controle de políticas de uso com base nas aplicações: permitir, negar, agendar, inspecionar e controlar o uso da largura de banda que utilizam cada aplicação ou usuário.

1.1.9.2. Deve suportar a criação de políticas de controle de uso de largura de bandas baseadas em: porta ou protocolo, endereço IP de origem ou destino, usuário ou grupo de usuários, aplicações (por exemplo, Youtube e WhatsApp).

1.1.9.3. Deve suportar a priorização em tempo real de protocolos de voz (VoIP) como H.323, SIP.

1.1.9.4. Deve suportar a marcação de pacotes Dif Serv.

1.1.9.5. Deve permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.

1.1.10. **Balanceamento de Links**

1.1.10.1. Deve implementar balanceamento de links utilizando as seguintes métricas e critérios para a escolha do caminho: aplicações, jitter, latência e perda de pacotes, permitindo que administradores configurem os valores de tais parâmetros para definir por qual interface certo tipo de tráfego será enviado.

1.1.10.2. Caso o item acima não seja atendido em sua totalidade, será aceita composição com outro equipamento, do tipo appliance físico, desde que a configuração seja realizada através da interface de gerenciamento do firewall e da Solução de Gerenciamento Centralizada, sem nenhum ônus para a Contratante, garantindo o pleno atendimento das métricas e critérios para a escolha do caminho, segundo o item acima.

1.1.10.3. O appliance físico do item anterior deve possuir throughput igual ou superior à discriminada no throughput das “funcionalidades de Filtro de Pacotes, IPS, Filtro de Conteúdo e Proteção contra Malwares habilitadas simultaneamente” do respectivo firewall.

1.1.10.4. O appliance físico do item anterior deve possuir os mesmos requisitos de fontes de alimentação e de afixação em rack, quando exigidos, do respectivo firewall.

1.1.10.5. Os valores dos parâmetros jitter e latência devem poder ser configurados em unidade mínima de milissegundos (ms).

1.1.10.6. A interface virtual de balanceamento deve suportar agregar no mínimo 4 (quatro) interfaces, podendo ser do tipo: física, sub interface e VPN.

1.1.10.7. Deve suportar balanceamento de link por hash do IP de origem e destino.

1.1.10.8. Deve suportar balanceamento de link por peso. Nesta opção deve ser possível definir o peso de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, 4 (quatro) links WAN.

1.1.10.9. Deve permitir a configuração da funcionalidade de balanceamento em qualquer interface WAN, seja ela MPLS, Internet, 4G/LTE etc.

1.1.10.10. Deve possuir roteamento baseado em políticas e múltiplas saídas (e tipos de saídas) WANs.

1.1.10.11. Deve permitir a configuração de failover entre links principais e secundários, caso os links utilizados ultrapassem os limites previamente definidos de jitter, latência e perda de pacotes. Estes limites podem ser configurados para forçar o failover caso

apenas um ou todos os limites sejam atingidos simultaneamente.

1.1.10.12. Deve suportar a configuração de regras que permita o failback imediato.

1.1.10.13. Deve ser compatível com a solução de VPN, permitindo que suas características e análises sejam realizadas nas VPNs, assim como em links WAN.

1.1.10.14. Deve ser compatível com VPNs montadas em interfaces virtuais com roteamento dinâmico.

1.1.10.15. Deve realizar o gerenciamento de tráfego por tipo de aplicação.

1.1.10.16. Deve selecionar o melhor caminho baseado em tipo de tráfego e do host de origem.

1.1.10.17. Deve suportar o monitoramento de link com ping e TCP echo.

1.1.10.18. Deve suportar o monitoramento de links VPN (interfaces virtuais).

1.1.10.19. Deve permitir a exportação de informações via netflow.

1.1.11. **Recursos de Segurança**

1.1.11.1. Deve possuir, no mínimo, funcionalidades Anti-Vírus, Anti-Bot, Anti-Malware, AntiSpyware, Sistema de Prevenção de Intrusão (IPS), Filtro de Conteúdo Web, Controle de Aplicação, Prevenção de Perdas de Dados (DLP). E sistemas de prevenção de ameaças de ZeroDay;

1.1.11.2. Deve suportar o funcionamento nos modos snif er (para inspeção de tráfego gerado por uma porta de rede espelhada), layer-2, layer-3, de forma simultânea em uma única instância de firewall;

1.1.11.3. Deve aplicar novas políticas de segurança sem provocar indisponibilidade de serviço ou descontinuidade das conexões ativas;

1.1.11.4. Deve possuir capacidade de melhoria e análise das regras atuais, baseadas em camada 3 e 4 (porta/protocolo), indicando como a referida regra deverá ser configurada em camada 7 (aplicação);

1.1.11.5. O fluxo de análise de regras legadas deve permitir a visualização de quais aplicações estão em uso. Caso não possua essa funcionalidade, será permitida a integração com ferramentas que executam esta função;

1.1.11.6. Deve suportar as atualizações automáticas das bases de assinaturas utilizadas na identificação de vírus, intrusões (IPS) e aplicações sem a necessidade de intervenção manual pelo administrador, sem perda das conexões ativas e sem reinicialização do equipamento.

1.1.11.7. Deve suportar as atualizações automáticas das listas de geolocalização e das listas e categorias de URLs sem a necessidade de intervenção manual pelo administrador, sem perda das conexões ativas e sem reinicialização do equipamento;

1.1.11.8. Deve possuir proteção contra ataques, no mínimo, dos tipos: IP Spoofing, Negação de Serviço (DoS e DDoS), SYN Flood Attack, ICMP Flood Attack e UDP Flood Attack, Buffer Overflow, Port Scanning, Man-in-the-Middle;

1.1.11.9. Deve identificar, decriptografar e analisar o tráfego SSL tanto em conexões de entrada (inbound) quanto de saída (outbound), com suporte a HTTP/2 e TLS 1.2 e 1.3;

1.1.11.10. Deve permitir a decriptografia da área útil do pacote de dados (payload) para fins de controle de acesso à Internet e proteção contra ameaças;

1.1.11.11. Deve permitir a diferenciação de conexões pessoais (bancos, shopping etc) e conexões não pessoais por meio de classificação automática;

1.1.11.12. Deve possuir funcionalidade de backup e restore da configuração e das políticas de segurança através do carregamento de arquivo de configuração previamente salvo;

1.1.11.13. Deve armazenar os backups localmente, ou na solução de gerenciamento centralizado, e permitir que sejam transferidos para equipamentos externos por meio dos protocolos FTP ou SCP;

1.1.11.14. Deve possuir a capacidade de identificar ataques de Advanced Persistent Threat (APT) ou Zero-Day;

1.1.11.15. Deve possuir a capacidade de emular um ambiente operacional isolado e seguro (Sandbox), na nuvem do fabricante, para execução e observação de código malicioso, sem a utilização de assinaturas, com base na atividade, como, por exemplo, operações de arquivo, alterações de registro e sistema etc;

1.1.11.16. O equipamento do Lote 1 deve suportar a análise em, pelo menos, dois dos seguintes sistemas operacionais: Windows, Linux, MacOS e Android. Os equipamentos dos Lotes 2 e 3 devem suportar a análise em, pelo menos, um dos sistemas citados;

1.1.11.17. Deve suportar a análise dos tipos de arquivos: documentos Microsoft Office, dll, exe, pdf, gzip, tar, zip;

1.1.11.18. Deve suportar a análise dos protocolos HTTP/HTTPS, FTP e SMTP;

1.1.11.19. Desejável que a análise de links em sandbox seja capaz de classificar sites falsos na categoria de phishing e atualizar a base de filtro de URL da solução;

1.1.11.20. Para ameaças trafegadas em protocolo SMTP e POP3, é desejável que a solução seja capaz de mostrar nos relatórios o remetente, destinatário e assunto dos e-mails, permitindo identificação ágil do usuário vítima do ataque;

1.1.11.21. Deve permitir visualizar os resultados das análises de malwares de dia zero nos diferentes sistemas operacionais suportados;

1.1.11.22. Deve permitir informar ao fabricante quanto a suspeita de ocorrências de falso-positivo e falso- negativo na análise de malwares de dia zero;

1.1.11.23. Deve atualizar a base com assinaturas para bloqueio dos malwares identificados em sandbox de maneira automática, com frequência de pelo menos 30 minutos;

1.1.11.24. Desejável permitir o envio para análise em sandbox de malwares bloqueados pelo antivírus;

1.1.11.25. Para ameaças trafegadas em protocolo SMTP e POP3, a solução deve ter a capacidade de mostrar nos relatórios o remetente, destinatário e assunto dos e-mails permitindo identificação ágil do usuário vítima do ataque;

1.1.11.26. O sistema de análise "In Cloud" ou local deve prover informações sobre as ações do Malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo Malware, gerar assinaturas de Antivírus e Anti-spyware automaticamente, definir URLs não confiáveis utilizadas pelo novo Malware e prover informações sobre o usuário infectado (seu endereço IP e seu login de rede);

1.1.11.27. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e class), Android APKs MacOS (mach-O, DMG e PKG), Linux (ELF), RAR e 7-ZIP no ambiente de sandbox;

1.1.11.28. A solução deve analisar os arquivos do tipo malware em ambiente sandbox para baremetal, a fim de evitar técnicas de evasão;

1.1.11.29. A solução deve possuir a capacidade de analisar em sand-box os links (http e https) presentes no corpo de e-mails trafegados em SMTP e POP3.

1.1.12. **Filtro de Pacotes**

1.1.12.1. Não deve possuir restrições ao número de máquinas ou usuários protegidos.

1.1.12.2. Deve informar o número de sessões simultâneas.

1.1.12.3. Deve suportar a implementação tanto em modo transparente (layer-2) quanto em modo gateway (layer-3).

1.1.12.4. Deve suportar Statefull Packet Inspection de tráfego IPv4 e IPv6.

1.1.12.5. Deve suportar controle de acesso para serviços e protocolos pré-definidos, bem como possibilitar a adição de novos serviços e protocolos.

1.1.12.6. Deve suportar os protocolos H.323, SIP.

1.1.12.7. Deve implementar mecanismo de proteção contra ataques de falsificação de endereços IP (anti-spoofing).

1.1.12.8. Deve implementar mecanismo de captura de pacotes, de forma manual ou automática, quando uma ameaça for detectada.

1.1.12.9. Deve identificar os usuários para qualquer protocolo ou aplicação baseada em TCP, UDP e ICMP.

1.1.12.10. Deve suportar a utilização simultânea de políticas de segurança em IPv4 e IPv6.

1.1.12.11. Deve suportar a implementação de políticas de segurança baseadas em: portas, protocolos, usuários, grupos de usuários, endereços IP, redes CIDR/VLSM, horário ou período de tempo, e suas combinações.

1.1.12.12. Deve suportar a consulta a fontes externas de endereços IP, domínios e URL's podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego.

1.1.12.13. Desejável possuir mecanismos de otimização de regras. De forma que com base na análise de tráfego o sistema automaticamente faça sugestões e melhorias nas regras existentes.

1.1.12.14. 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.

1.1.13. **Filtro de Conteúdo**

1.1.13.1. Deve prover o controle e proteção de acesso à Internet por meio do reconhecimento de aplicações, independente de porta e protocolo, e da classificação de URLs.

1.1.13.2. Deve ser capaz de identificar aplicações, independentemente das portas e protocolos, bem como das técnicas de evasão utilizadas.

1.1.13.3. Deve ser capaz de identificar se as aplicações estão utilizando sua porta padrão.

1.1.13.4. Deve ser capaz de identificar aplicações encapsuladas dentro de protocolos, como HTTP e HTTPS.

1.1.13.5. Deve ser capaz de identificar aplicações criptografadas usando SSL.

1.1.13.6. Deve ser capaz de identificar um mínimo de 1.400 (mil e quatrocentas) aplicações, incluindo, mas não se limitando a: peer-to-peer, streaming e download de áudio, streaming e download de vídeo, update de software, instant messaging, redes sociais, proxies, anonymizers, acesso e controle remoto, VOIP e email.

1.1.13.7. Deve ser capaz de identificar, no mínimo, as seguintes aplicações: Bittorrent, Youtube, Livestream, Skype, Viber, WhatsApp, Snapchat, Facebook, Facebook Messenger, Instagram, Twitter, Linkedin, Dropbox, Google Drive, One Drive, Logmein, Teamviewer, MS-RDP, VNC, Ultrasurf, TOR, Webex.

1.1.13.8. Deve armazenar a base de assinaturas no próprio equipamento.

1.1.13.9. Deve classificar as aplicações em categorias.

1.1.13.10. Deve permitir o agrupamento de aplicações em grupos personalizados.

1.1.13.11. Deve identificar os usuários que estão utilizando as aplicações.

1.1.13.12. Deve permitir o bloqueio de aplicações que não estejam utilizando suas portas padrão.

1.1.13.13. Deve suportar a implementação de políticas de segurança baseadas em: aplicações, categorias de aplicações, endereço IP de origem ou destino, rede CIDR/VLSM de origem ou destino, usuário ou grupo de usuários, horário ou período de tempo, e suas

combinações.

1.1.13.14. Deve proteger contra o roubo de credenciais, usuários e senhas identificadas através da integração com Active Directory submetidos em sites não corporativos. Deve ainda permitir criação de regra onde usuários do Active Directory só possam enviar informações de login para sites autorizados na solução;

1.1.13.15. Deve permitir bloquear o acesso do usuário caso o mesmo tente fazer o envio de suas credenciais em sites classificados como phishing pelo filtro de URL da solução;

1.1.13.16. Deve permitir a utilização ou bloqueio individualizado das aplicações, como BitTorrent e Skype, para determinados usuários ou grupos de usuários.

1.1.13.17. Deve permitir o registro de todos os fluxos autorizados/bloqueados das aplicações, incluindo o usuário identificado.

1.1.13.18. Deve permitir o controle de uso de banda de download ou upload utilizada pelas aplicações (traffic shaping) baseado em: endereço IP ou rede CIDR/VLSM de origem ou destino, usuário ou grupo de usuários, horário ou período de tempo, e suas combinações.

1.1.13.19. Deve ser capaz de efetuar a classificação de conteúdo de páginas web em HTTP e HTTPS, baseado em listas de categoria.

1.1.13.20. Deve possuir funcionalidades de tratamento de conteúdo web, devendo sua base de dados conter, no mínimo, 10 (dez) milhões de sites internet web já registrados e classificados, distribuídos em, no mínimo, 60 (sessenta) categorias ou subcategorias pré-definidas ou suas semelhantes: conteúdo adulto, chat, drogas ilegais, jogos de azar, jogos, pirataria, proxy remoto, redes sociais, streaming media, violência, pornografia, racismo, malware.

1.1.13.21. Deve permitir a inclusão de URLs customizadas por política (whitelist).

1.1.13.22. Deve armazenar as listas de categoria no próprio equipamento.

1.1.13.23. Deve identificar os usuários que estão acessando as páginas web.

1.1.13.24. Deve suportar a implementação de políticas de segurança baseadas em: URLs, categorias de URLs, endereço IP de origem ou destino, rede CIDR/VLSM de origem ou destino, usuário ou grupo de usuários, horário ou período de tempo, e suas combinações.

1.1.13.25. Deve alertar o usuário quando uma URL for bloqueada, por meio de página de bloqueio que possa ser customizada, e que informe, no mínimo, o motivo do bloqueio e a categoria na qual a URL foi classificada.

1.1.13.26. Deve 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 possibilitar o usuário continuar acessando o site).

1.1.13.27. Deve permitir registrar todos os acessos autorizados ou bloqueados às páginas web, incluindo sua classificação e o usuário identificado.

1.1.13.28. Desejável permitir habilitar aplicações SaaS apenas no modo corporativo e bloqueá-las quando usadas no modo pessoal.

1.1.13.29. Desejável identificar o uso de táticas evasivas, ou seja, ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas.

1.1.13.30. Deve permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora).

1.1.13.31. Deve permitir bloquear o acesso a sites de busca (Google, Bing, Yahoo), caso a opção Safe Search esteja desabilitada.

1.1.13.32. Deve suportar base ou cache de URL's local no appliance, evitando delay de comunicação/validação das URL's.

1.1.13.33. Desejável que a categorização de URL's analise a URL ao menos até o nível de diretório.

1.1.13.34. Desejável que a solução proteja contra o roubo de credenciais, usuários e senhas identificadas através da integração com Active Directory submetidos em sites não corporativos. Desejável ainda que permita a criação de regras onde usuários do Active Directory só possam enviar informações de login para sites autorizados.

1.1.13.35. Deve prover análise em tempo real de páginas maliciosas e dessa forma permitir a proteção em tempo real antes mesmo da atualização das bases de dados de URLs. Caso o fabricante não possua esta funcionalidade em sua plataforma será permitida a composição da solução, sem ônus a este órgão.

1.1.14. **Prevenção de Intrusão (IPS)**

1.1.14.1. Deve possuir tecnologia de detecção e prevenção de ataques e intrusões baseada em assinatura.

1.1.14.2. Deve possuir, no mínimo, um conjunto de 10.000 (dez mil) assinaturas de detecção e prevenção de ataques.

1.1.14.3. Deve detectar protocolos independentemente da porta utilizada, identificando aplicações conhecidas em portas não-padrão.

1.1.14.4. Deve possuir, no mínimo, os seguintes mecanismos de detecção e prevenção: assinaturas de vulnerabilidades e exploits, assinaturas de ataques, validação de protocolos, detecção de anomalias, IP defragmentation, remontagem de pacotes TCP, nível de severidade do ataque.

1.1.14.5. Deve ser capaz de inspecionar tráfego criptografado usando SSL.

1.1.14.6. Deve ser capaz de inspecionar integralmente todos os pacotes de dados, independentemente de seus tamanhos.

1.1.14.7. Deve identificar os usuários relacionados aos eventos de intrusão.

1.1.14.8. Deve identificar os usuários relacionados aos eventos de bloqueio.

1.1.14.9. Deve permitir a criação de políticas de segurança que alertem, sem bloquear, sobre a ocorrência de um determinado ataque ou ameaça.

1.1.14.10. Deve permitir a criação de políticas de segurança que bloqueiem uma determinada ameaça.

1.1.14.11. Deve permitir a criação de políticas de segurança que bloqueiem um determinado ataque por meio de uma ação de DROP/RESET.

1.1.14.12. Deve permitir registrar todos os eventos de IPS, incluindo o usuário identificado.

1.1.14.13. Deve identificar e bloquear a comunicação com botnets.

1.1.14.14. Deve bloquear malwares e spywares.

1.1.14.15. Deve inspecionar e bloquear vírus nos seguintes tipos de tráfego, no mínimo: HTTP, HTTPS, SMTP, POP3, FTP e SMB.

1.1.14.16. Deve suportar proteção contra vírus em conteúdo HTML e javascrip, software espião (spyware) e worms.

1.1.14.17. Deve suportar a inspeção de vírus em arquivos comprimidos utilizando o algoritmo deflate (zip, gzip etc).

1.1.14.18. Deve suportar bloqueio de download de pelo menos 45 tipos de arquivos.

1.1.14.19. Deve armazenar as bases de assinaturas no próprio equipamento.

1.1.14.20. Deve possuir a capacidade de detectar e prevenir contra ameaças em tráfego HTTP/2.

1.1.15. **Instalação e Configuração da Solução (para os itens 1, 2, 3 e 4 dos Lotes 1, 2 e 3)**

As especificações de Instalação e Configuração das soluções de Firewall encontram-se no subtópico 3.9.2. do Termo de Referência.

1.1.16. **Garantia do Produto (Para os itens 1, 2, 3 e 4 dos Lotes 1, 2 e 3)**

As especificações de Garantia dos produtos adquiridos encontram-se no subtópico 6.1. do Termo de Referência.

1.2. **Características Gerais das Consoles dos Lotes 1, 2 e 3**

1.2.1. **Console de Gerenciamento Centralizado**

1.2.1.1. Deve ser fornecida em appliance virtual, compatível VMware vSphere ESXi 6.0 ou superior, ou baseado em software, compatível com Windows Server 2012 R2 ou superior, ou em appliance físico com suporte à fixação em bastidor (rack) padrãoEIA-310 com largura de 19’ (dezenove polegadas) e altura de até duas unidades de rack (2U), acompanhado de todos os acessórios necessários (cabos, suportes, gavetas, braços, trilhos etc).

1.2.1.2. Deve ser acessada via interface web ou através de um software cliente, com interface gráfica, instalado no Windows ou Linux.

1.2.1.3. Deve estar licenciada em caráter permanente/perpétuo para todas as funcionalidades e quantidades mencionadas.

1.2.1.4. Deve permitir o gerenciamento centralizado dos equipamentos de firewall sejam eles virtuais ou físicos em uma mesma console, permitindo os seguintes requisitos:

I - Coleta de logs;

II - Análise de logs;

III - Gerenciamento de firewalls;

IV - Correlação de logs.

1.2.1.5. Deve estar licenciada e permitir a gerência centralizada de, no mínimo, 15 equipamentos.

1.2.1.6. Deve estar licenciada para o limite máximo de usuários, objetos, regras de segurança, NAT e endereços IP suportados pela solução.

1.2.1.7. As comunicações entre a CGC e os firewalls e entre a CGC e as estações dos administradores do sistema devem ser criptografadas e autenticadas.

1.2.1.8. Deve ser capaz de realizar todas as configurações nos firewalls descritas nesta ata.

1.2.1.9. Deve possibilitar a aplicação simultânea de configurações em todos os firewalls gerenciados pela solução.

1.2.1.10. Deve permitir a criação e distribuição de políticas de segurança de forma centralizada, suportando organização hierárquica de regras.

1.2.1.11. Deve suportar, por meio da interface gráfica de gerenciamento, a criação e administração de políticas de filtro de pacotes, prevenção de intrusão, controle de aplicação, filtragem de URLs, monitoração de logs, debugging, troubleshooting e captura de pacotes.

1.2.1.12. Deve ser capaz de gerenciar os firewa ls em unidades remotas, fora da rede local.

1.2.1.13. Deve permitir a autenticação dos administradores através de contas locais e bases externas LDAP ou Active Directory.

1.2.1.14. Será permitido que a solução de gerenciamento centralizado possua um “appliance virtual” específico para atendimento às necessidades de identificação e autenticação de usuários.

1.2.1.15. Deve possuir a capacidade de definir administradores com diferentes perfis de acesso. Os perfis de acesso devem ser, no mínimo, de leitura/escrita e somente leitura,

1.2.1.16. Deve permitir a criação de perfis customizados.

1.2.1.17. Deve permitir, de forma granular, assinalar permissões para os administradores criarem outros usuários, alterarem e ler configurações etc.

1.2.1.18. Deve permitir múltiplos administradores acessando o equipamento simultaneamente, sem restrição para leitura e escrita.

1.2.1.19. Deve suportar o bloqueio de alterações, evitando o conflito de configurações entre diferentes administradores efetuando alterações simultaneamente.

1.2.1.20. Deve registrar, em log de auditoria, as ações dos usuários administradores com o horário da alteração.

1.2.1.21. Deve suportar a identificação e utilização de usuários nas políticas de segurança.

1.2.1.22. Deve suportar agrupamento lógico de objetos ("object grouping") para criação de regras.

1.2.1.23. Deve possibilitar o gerenciamento (incluindo a criação, alteração, monitoração e exclusão) de objetos de rede. Deve ainda permitir detectar se e onde, na base de regras, está sendo utilizado determinado objeto de rede. Os tipos de objetos deverão permitir especificar de forma distinta grupos e objetos de rede e serviços, diferenciando-os e agrupando-os conforme suas características ou descrição de maneira a permitir o reaproveitamento dos mesmos em diferentes políticas.

1.2.1.24. Deve possibilitar a especificação de política por tempo, ou seja, permitir a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora).

1.2.1.25. Deve garantir que quando houver novas versões de software dos equipamentos, seja realizada a distribuição e atualização remota, de maneira centralizada.

1.2.1.26. Deve ser capaz de testar a conectividade dos equipamentos gerenciados.

1.2.1.27. Deve suportar configuração das funcionalidades de alta disponibilidade dos dispositivos físicos.

1.2.1.28. Deve permitir localizar em quais regras um objeto está sendo utilizado.

1.2.1.29. Deve permitir a identificação e exclusão de regras e objetos que estão aplicadas nos dispositivos, mas não afetam o desempenho e a segurança da rede (regras e objetos em desuso sob o ponto de vista lógico).

1.2.1.30. Deve suportar a geração de alertas automáticos via SNMP e syslog.

1.2.1.31. Deve informar a utilização dos recursos de CPU, memória e atividade de rede dos equipamentos gerenciados.

1.2.1.32. Deve informar o número de conexões simultâneas dos equipamentos gerenciados.

1.2.1.33. O gerenciamento da solução deve suportar acesso via SSH, cliente, WEB (HTTPS) e API aberta.

1.2.1.34. As consoles de gerenciamento centralizado, gerenciamento de logs, relatoria centralizada, poderão ser entregues em um único appliance, desde que atenda a todas as exigências deste documento.

1.2.2. **Console de Gerenciamento de Logs**

1.2.2.1. Deve ser fornecida em appliance virtual, compatível VMware vSphere ESXi 6.0 ou superior, ou baseado em software, compatível com Windows Server 2012 R2 ou superior, ou em appliance físico com suporte à fixação em bastidor (rack) padrãoEIA-310 com largura de 19’ (dezenove polegadas) e altura de até duas unidades de rack (2U), acompanhado de todos os acessórios necessários (cabos, suportes, gavetas, braços, trilhos etc).

1.2.2.2. Deve possuir relatórios de utilização dos recursos por aplicação, URLs, ameaças e etc.

1.2.2.3. Deve possuir visualização sumarizada de todas as aplicações, ameaças e URLs que foram identificadas e controladas pela solução.

1.2.2.4. Deve permitir a criação de relatórios customizados.

1.2.2.5. Deve ser capaz de receber logs de todos os firewa ls especificados nesta ATA.

1.2.2.6. Deve possibilitar a filtragem dos logs do equipamento por, no mínimo: aplicação, endereço IP de origem e destino, país de origem e destino, usuário e horário.

1.2.2.7. Deve possibilitar o registro dos fluxos de dados relativos a cada sessão, armazenando: endereços IP de origem e destino dos pacotes, traduções NAT, portas e protocolos de origem e destino, usuário identificado, ação sobre o pacote (permitido ou negado).

1.2.2.8. Deve possuir relatórios com informações consolidadas sobre: as mais frequentes fontes de conexões bloqueadas com seus destinos e serviços; os mais frequentes ataques e ameaças de segurança detectados com suas origens e destinos; os serviços de rede mais utilizados, as aplicações maiores consumidoras de banda de Internet; os usuários maiores consumidores de banda de Internet; e os sítios na Internet mais visitados.

1.2.2.9. Deve possuir funcionalidade de exportação de relatórios e logs para o computador local ou via FTP, SFTP ou SCP.

1.2.2.10. Deve permitir a geração automática e agendada dos relatórios.

1.2.2.11. Deve estar licenciada em caráter permanente/perpétuo para todas as funcionalidades e quantidades mencionadas.

1.2.2.12. Deve estar licenciada e permitir a correlação de todos os eventos gerados por todos os equipamentos e contextos virtuais que compõem a solução.

1.2.2.13. O appliance virtual deve estar licenciado de maneira irrestrita quanto ao armazenamento, possibilitando cada órgão contratante armazenar o volume de logs que julgar necessário, utilizando recursos computacionais próprios;

1.2.2.14. Deve ser acessada via interface web ou através de um software cliente, com interface gráfica, instalado no Windows ou Linux.

1.2.2.15. Será permitida a entrega do “Console de Gerenciamento de Logs” como software agregado ao “Console de Gerenciamento Centralizado” ou ao “Console de Relatoria Centralizada”.

1.2.3. **Console de Relatoria Centralizada**

1.2.3.1. Deve ser fornecida em appliance virtual, compatível com VMware vSphere ESXi 6.5 ou superior, ou baseado em software, compatível com Windows Server 2012 R2 ou superior.

1.2.3.2. Deve ser acessada via interface web ou através de um software cliente, com interface gráfica, instalado no Windows ou no Linux.

1.2.3.3. Deve estar licenciada em caráter permanente/perpétuo para todas as funcionalidades e quantidades mencionadas.

1.2.3.4. Deve estar licenciada e permitir a gerência centralizada de relatórios, para no mínimo, 15 equipamentos.

1.2.3.5. As comunicações entre a Console de Relatoria e os firewalls e entre a Console de Relatoria e as estações dos administradores do sistema devem ser criptografadas e autenticadas.

1.2.3.6. Deve ser capaz de gerar relatórios de equipamentos em unidades remotas, fora da rede local.

1.2.3.7. Deve permitir a autenticação dos administradores através de contas locais e bases externas LDAP ou Active Directory.

1.2.3.8. A console deve suportar acesso via SSH, cliente e WEB (HTTPS).

1.2.3.9. Deve coletar logs dos Firewalls, do “Console de Gerenciamento Centralizado” e do “Console de Gerenciamento de Logs”.

1.2.3.10. Deve garantir a geração de relatórios com mapas geográficos, ou modo tabela, gerados em tempo real, para a visualização de origens e destinos do tráfego.

1.2.3.11. Deve permitir a extração de relatórios.

1.2.3.12. Deve possuir relatórios pré-definidos.

1.2.3.13. Deve permitir a geração de relatórios de logs de tráfego de dados.

1.2.3.14. Deve permitir a geração de relatórios de logs para auditoria das configurações de regras, objetos e acessos.

1.2.3.15. Deve possibilitar o envio de maneira automática de relatórios por e-mail.

1.2.3.16. Deve permitir o agendamento da geração de relatórios.

1.2.3.17. Deve ter a capacidade de definir filtros nos relatórios.

1.2.3.18. Deve gerar alertas automáticos via e-mail, snmp e syslog baseados em eventos de ocorrência como log, severidade de log, entre outros.

1.2.3.19. Deve permitir a criação de painéis (dashboards) customizados para visibilidades do tráfego de aplicativos, categorias de url, ameaças, serviços, países, origem e destino.

1.2.3.20. Deve possibilitar a visualização na interface gráfica de usuário (gui) da “console de relatoria centralizada as seguintes informações do sistema: logs diários recebidos, alertas gerados, entre outros.

1.2.3.21. Será permitida a entrega do “Console de Relatoria Centralizada” como software agregado ao “Console de Gerenciamento Centralizado” ou ao “Console de Gerenciamento de Logs”.

1.3. **Características Gerais dos Treinamentos Operacionais dos Lotes 1, 2 e 3**

As especificações dos cursos de treinamento, abrangendo os itens 5 dos Lotes 1, 2 e 3, encontram-se no subtópico 3.3 do Termo de Referência.

2. LOTE 1 - FIREWALL TIPO 1

2.1. **Características Específicas do Firewall Tipo 1**

2.1.1. Throughput de 40 Gbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito.

2.1.2. Em relação ao filtro de pacotes, deve possuir o Throughput de no mínimo 60 Gbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir.

2.1.3. Em relação ao túnel IPSec VPN, o throughput mínimo deverá ser de no mínimo 40 Gbps, com a inspeção e controle de aplicação e usuários ativada.

2.1.4. Deve permitir, no mínimo, 7.000.000 de conexões simultâneas.

2.1.5. Deve permitir, no mínimo, 380.000 novas conexões por segundo.

2.1.6. Deve permitir, no mínimo, 4000 VLANs.

2.1.7. Deve permitir, e estar licenciado para a utilização de 12.000 túneis VPN site-to-site simultâneos.

2.1.8. Deve permitir, e estar licenciado para a utilização de 25.000 túneis VPN client-to-site simultâneos.

2.1.9. Deve suportar afixação em bastidor (rack) padrão EIA-310 com largura de 19’ (dezenove polegadas) e altura de até quatro unidades de rack(4U), acompanhado de todos os acessórios necessários (cabos, suportes, gavetas, braços, trilhos etc).

2.1.10. Deve possuir 2 (duas) fontes de alimentação independentes, redundantes e hotswappable.

2.1.11. O appliance deve possuir, no mínimo, 8 (oito) portas 1G/2.5G/5G/10G BASE-T RJ45.

2.1.12. Deve possuir, no mínimo, 10 (dez) interfaces SFP/SFP+, com transceivers SFP+ 10GB-SR, para conexão ao meio via cabo de fibra ótica.

2.1.13. Deve possuir, no mínimo, 4 (quatro) interfaces 25 Gbps para utilização de transceivers padrão SFP28.

2.1.14. Deve possuir, no mínimo, 4 (quatro) interfaces 40/100 Gbps para utilização de transceivers padrão QSFP+/QSFP28.

2.1.15. Deve possuir, disco Solid State Drive (SSD) ou cartão eMMC de, no mínimo, 400 GB.

2.1.16. Deve possuir, no mínimo, 20 sistemas virtuais lógicos (Contextos) no firewall Físico.

2.2. **Alta Disponibilidade**

2.2.1. Deve possibilitar a operação em alta disponibilidade (HA) no equipamento, permitindo uma arquitetura ativo/ativo e ativo/passivo com no mínimo 2 (dois) membros, com sincronismo de estados integrado.

2.2.2. Deve suportar o balanceamento de carga na arquitetura ativo/ativo.

2.2.3. Deve sincronizar sessões TCP/IP, tabelas NAT, tabelas FIB, associações de segurança das VPNs e todas as configurações necessárias para a manutenção da continuidade dos serviços.

2.2.4. Deve monitorar a falha dos links de comunicação.

2.2.5. Deve ser capaz de identificar e iniciar automaticamente um procedimento de failover sempre que ocorrer: a falha de um dos membros do cluster, a falha de qualquer componente ou processo crítico de um dos membros do cluster, a falha de um dos links de comunicação monitorados.

2.2.6. Deve ser capaz de realizar os procedimentos de failover sem perda das conexões ativas e sessões estabelecidas de forma transparente para o usuário.

2.2.7. Deve suportar a operação em cluster com no mínimo 2 equipamentos.

2.2.8. Desejável possuir 2 fans independentes, redundantese hotswappable.

2.2.9. Deve possuir discos de sistema e de logs independentes e redundantes (RAID).

3. LOTE 2 - FIREWALL TIPO 2

3.1. **Características Específicas do Firewall Tipo 2**

3.1.1. Throughput de 09 Gbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito.

3.1.2. Em relação ao filtro de pacotes, deve possuir o throughput mínimo de 19 Gbps.

3.1.3. Em relação ao túnel IPSec VPN, deve possuir o throughput mínimo de 9 Gbps.

3.1.4. Deve permitir, no mínimo, 1.900.000 conexões simultâneas.

3.1.5. Deve permitir, no mínimo, 200.000 novas conexões por segundo.

3.1.6. Deve permitir, no mínimo, 4000 VLANs.

3.1.7. Deve permitir, e estar licenciado para a utilização de 2000 túneis VPN site-to-site simultâneos.

3.1.8. Deve permitir, e estar licenciado para a utilização de 1800 túneis VPN client-to-site simultâneos.

3.1.9. Deve suportar a fixação em bastidor (rack) padrão EIA-310 com largura de 19’ (dezenove polegadas) e altura de no máximo três unidades de rack (3U), acompanhado de todos os acessórios necessários (cabos, suportes, gavetas, braços, trilhos etc).

3.1.10. O appliance deve possuir, no mínimo, 10 (dez) portas 100/1000/10000 BASE-T ou SFP podendo ser uma composição entre os dois tipos, acompanhadas de seus respectivos transceivers.

3.1.11. Deve possuir, no mínimo, 4 (quatro) interfaces 10 (dez) Gigabit-Ethernet padrão SFP+, com transceivers SFP+ 10GB-SR, para conexão ao meio via cabo de fibra ótica.

3.1.12. Deve possuir, disco Solid State Drive (SSD) ou cartão eMMC de, no mínimo, 480GB cada disco.

3.1.13. Deve possuir, no mínimo, 5 (cinco) interfaces 1 (um) Gigabit-Ethernet padrão SFP, para conexão ao meio via cabo de fibra ótica.

4. LOTE 3 - FIREWALL TIPO 3

4.1. **Características Específicas do Firewall Tipo 3**

4.1.1. Throughput de 2 Gbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito.

4.1.2. Em relação ao filtro de pacotes, deve possuir o throughput mínimo de 4 Gbps.

4.1.3. Em relação ao túnel IPSec VPN, deve possuir o throughput mínimo de 3 Gbps.

4.1.4. Deve permitir, no mínimo, 350.000 conexões simultâneas.

4.1.5. Deve permitir, no mínimo, 65.000 novas conexões por segundo.

4.1.6. Deve permitir, no mínimo, 4000 VLANs.

4.1.7. Deve permitir, e estar licenciado para utilização de 2000 túneis VPN site-to-site simultâneos.

4.1.8. Deve permitir, e estar licenciado para utilização de 1500 túneis VPN client-to-site simultâneos.

4.1.9. Deve suportar a fixação em bastidor (rack) padrão EIA-310 com largura de 19’ (dezenove polegadas) e altura de no máximo uma unidade de rack (1U), acompanhado de todos os acessórios necessários (cabos, suportes, gavetas, braços, trilhos etc).

4.1.10. O appliance deve possuir, no mínimo, 08 (oito) portas de rede 1G RJ-45.

4.1.11. O appliance deve possuir uma porta 10/100/1000 para gerenciamento “out-of-band”.

4.1.12. Deve possuir, disco Solid State Drive (SSD) ou cartão eMMC de, no mínimo, 128GB.

Rio de Janeiro, 09 de julho de 2024

Documento assinado eletronicamente por **Charles Monteiro Guimarães**, **Diretor**, em 12/09/2024, às 14:42, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Manuelito de Sousa Reis Junior**, **Gerente**, em 12/09/2024, às 14:44, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Fabio Ivo**, **Assistente**, em 12/09/2024, às 15:01, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Marco Antonio de Andrade**, **Assessor Chefe**, em 12/09/2024, às 15:04, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Isabela Reboucas Costa**, **Analista de Sistemas**, em 12/09/2024, às 15:14, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Monique Goncalves Paz**, **Diretora**, em 12/09/2024, às 15:16, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Rosana Alves de Andrade**, **Analista de Sistemas**, em 12/09/2024, às 15:41, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **83089505** e o código CRC **2A59FD95**.

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone:

Governo do Estado do Rio de Janeiro

Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro

Vice Presidência de Tecnologia

ANEXO II DO TERMO DE REFERÊNCIA
Roteiro para Prova de Conceito - lote 01
firewall tipo 01

1. INTRODUÇÃO

1.1. Será realizada Prova de Conceito com o objetivo de verificar o atendimento dos requisitos funcionais considerados prioritários pelo PRODERJ, referente à proposta ofertada pela licitante classificada em primeiro lugar.

1.2. O roteiro da Prova de Conceito, nos termos que seguem abaixo, exigirá da referida licitante a comprovação de que sua solução atende as especificações de maior relevância aqui elencadas.

1.3. As especificações selecionadas neste anexo representam as características de maior impacto em relação à solução como um todo, e levam em consideração os aspectos técnicos que permitem comprovação em ambiente de teste, haja vista que determinados recursos/características/funcionalidades possuem restrições de comprovação quando a solução ainda não está completamente implementada.

1.4. Este anexo deve ser interpretado conforme as disposições do Termo de Referência do qual é parte integrante e indissociável.

2. CARACTERÍSTICAS E FUNCIONALIDADES A SEREM COMPROVADAS

LOTE I - FIREWALL (TIPO 1)					
APPLIANCE FIREWALL TIPO 1 - INCLUSOS: HARDWARE, LICENCIAMENTO, INSTALAÇÃO, CONFIGURAÇÃO E GARANTIA POR 60 MESES					
Nº	**REF. ANEXO I**	**DESCRIÇÃO DO ITEM PARA COMPROVAÇÃO**	**CONTEXTO DO REQUISITO**	**OBSERVAÇÃO**	**REQUISITO APROVADO? (SIM/NÃO)**
1	1.1.4.3.	Deve permitir o acesso ao equipamento via SSH e interface web HTTPS.	Funcionalidades Básicas		
2	1.1.4.6.	Deve possuir visualização mínima sumarizada de aplicações, ameaças, URLs, endereços de origem, endereços de destino, levando-se em conta o quantitativo de sessões, de consumo de banda e categorização.	Funcionalidades Básicas		
3	1.1.4.10.	Os Firewalls de segurança físico ou virtualizados, devem possuir mecanismo para dedicar processamento no equipamento de segurança para funções e ações de Gerenciamento, mesmo que o equipamento esteja com alto processamento de CPU.	Funcionalidades Básicas		
4	1.1.5.3.	Deve suportar os protocolos DHCP e DHCPv6 e suas funcionalidades como cliente, servidor e relay.	Rede		
5	1.1.5.4.	Deve suportar Jumbo Frames.	Rede		
6	1.1.5.5.	Deve suportar sub interfaces Ethernet lógicas.	Rede		
7	1.1.5.8.	Deve permitir o registro de eventos de NAT com as informações de endereço interno, endereço público, data e hora do evento, portas de origem e destino.	Rede		

8	1.1.5.10.	Deve suportar as funcionalidades de roteamento estático e dinâmico em IPv4 e IPv6.	Rede		
9	1.1.5.16.	Deve suportar Policy Based Routing (PBR), possibilitando políticas de roteamento condicionado ao endereço IP de origem, endereço IP de destino e porta de comunicação.	Rede		
10	1.1.6.1.	Deve promover a integração com serviços de diretório LDAP e Active Directory, baseados em caracteres da língua portuguesa, para a identificação, autenticação, autorização e registro de eventos de acessos ou ameaças.	Autentificação e Identificação		
11	1.1.6.7.	Deve permitir a criação de políticas de segurança baseadas em usuários e grupos de usuários pertencentes a um diretório LDAP ou ao Active Directory.	Autentificação e Identificação		
12	1.1.6.10.	Deve possuir a capacidade de definir administradores com diferentes perfis de acesso. Os perfis de acesso devem ser, no mínimo, de leitura/escrita e somente leitura.	Autentificação e Identificação		
13	1.1.7.1.	Deve identificar os países de origem e destino de todas as conexões estabelecidas através do equipamento.	Geolocalização		
14	1.1.7.4.	Deve permitir a criação de políticas de segurança baseadas em geolocalização, permitindo o bloqueio de tráfego com origem ou destino a determinado país ou grupo de países.	Geolocalização		
15	1.1.7.5.	Deve possibilitar a visualização dos países de origem e destino nos logs de eventos de acessos e ameaças.	Geolocalização		
16	1.1.8.6.	Deve suportar Certificado Digital X.509.	VPN	Não precisa implementar certificado, basta mostrar as opções na manager.	
17	1.1.8.9.	Deve suportar VPN IPSec client-to-site (acesso remoto).	VPN		
18	1.1.8.11.	Deve permitir que o usuário realize a conexão VPN por meio de cliente instalado nos sistemas operacionais Windows, Mac OS ou Linux do seu equipamento ou então por meio de interface web do tipo portal.	VPN	No teste, a licitante precisará demonstrar este tópico apenas no Windows.	
19	1.1.8.15.	Deve suportar, no mínimo, os protocolos de roteamento estático e dinâmico OSPF e BGP.	VPN		

20	1.1.8.20.	Deve promover a integração com diretórios LDAP e Active Directory para a autenticação de usuários de VPN e regras de acesso.	VPN		
21	1.1.8.25.	Deve permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis de SSL.	VPN		
22	1.1.9.2.	Deve suportar a criação de políticas de controle de uso de largura de banda baseadas em: porta ou protocolo, endereço IP de origem ou destino, usuário ou grupo de usuários, aplicações (por exemplo, Youtube e WhatsApp).	QoS		
23	1.1.9.5.	Deve permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.	QoS		
24	1.1.10.5.	Os valores dos parâmetros jitter e latência devem poder ser configurados em unidade mínima de milissegundos (ms).	Balanceamento de Links		
25	1.1.10.10.	Deve possuir roteamento baseado em políticas e múltiplas saídas (e tipos de saídas) WANs.	Balanceamento de Links		
26	1.1.10.12.	Deve suportar a configuração de regras que permita o failback imediato.	Balanceamento de Links	A licitante poderá demonstrar apenas as configurações na manager.	
27	1.1.11.3.	Deve aplicar novas políticas de segurança sem provocar indisponibilidade de serviço ou descontinuidade das conexões ativas.	Recursos de Segurança		
28	1.1.11.12.	Deve possuir funcionalidade de backup e restore da configuração e das políticas de segurança.	Recursos de Segurança		
29	1.1.10.15.	Deve possuir a capacidade de emular um ambiente operacional isolado e seguro (Sandbox), na nuvem do fabricante, para execução e observação de código malicioso, sem a utilização de assinaturas, com base na atividade, como, por exemplo, operações de arquivo, alterações de registro e sistema etc.	Recursos de Segurança		
30	1.1.12.5.	Deve suportar controle de acesso para, pelo menos, serviços e protocolos pré-definidos, bem como possibilitar a adição de novos serviços e protocolos.	Filtro de Pacotes		
31	1.1.12.9.	Deve identificar os usuários para qualquer protocolo ou aplicação baseada em TCP, UDP e ICMP.	Filtro de Pacotes		

32	1.1.12.11.	Deve suportar a implementação de políticas de segurança baseadas em: portas, protocolos, usuários, grupos de usuários, endereços IP, redes CIDR/VLSM, horário ou período de tempo, e suas combinações.	Filtro de Pacotes		
33	1.1.12.12.	Deve suportar a consulta a fontes externas de endereços IP, domínios e URL's podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego.	Filtro de Pacotes		
34	1.1.13.9.	Deve classificar as aplicações em categorias.	Filtro de Conteúdo		
35	1.1.13.11.	Deve identificar os usuários que estão utilizando as aplicações.	Filtro de Conteúdo		
36	1.1.13.21.	Deve permitir a inclusão de URLs customizadas por política (whitelist).	Filtro de Conteúdo		
37	1.1.13.24.	Deve suportar a implementação de políticas de segurança baseadas em: URLs, categorias de URLs, endereço IP de origem ou destino, rede CIDR/VLSM de origem ou destino, usuário ou grupo de usuários, horário ou período de tempo, e suas combinações.	Filtro de Conteúdo		
38	1.1.13.25.	Deve alertar o usuário quando uma URL for bloqueada, por meio de página de bloqueio que possa ser customizada, e que informe, no mínimo, o motivo do bloqueio e a categoria na qual a URL foi classificada.	Filtro de Conteúdo		
39	1.1.13.27.	Deve permitir registrar todos os acessos autorizados ou bloqueados às páginas web, incluindo sua classificação e o usuário identificado.	Filtro de Conteúdo		
40	1.1.14.5.	Deve ser capaz de inspecionar tráfego criptografado usando SSL.	Prevenção de Intrusão - IPS		
41	1.1.14.9.	Deve permitir a criação de políticas de segurança que alertem, sem bloquear, sobre a ocorrência de um determinado ataque ou ameaça.	Prevenção de Intrusão - IPS		
42	1.1.14.14.	Deve bloquear malwares e spywares.	Prevenção de Intrusão - IPS		

43	2.1.1.	Throughput de 40 Gbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito.	Características Específicas do Firewall Tipo 1		
44	2.1.2.	Em relação ao filtro de pacotes, deve possuir o Throughput de no mínimo 60 Gbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir.	Características Específicas do Firewall Tipo 1		
45	2.1.10.	Deve possuir 2 (duas) fontes de alimentação independentes, redundantes e hotswappable.	Características Específicas do Firewall Tipo 1		
46	2.1.11.	O appliance deve possuir, no mínimo, 8 (oito) portas 1G/2.5G/5G/10G BASE-T RJ45	Características Específicas do Firewall Tipo 1	Para a Prova de Conceito, comprovar somente a quantidade das referidas interfaces.	
47	2.1.12.	Deve possuir, no mínimo, 10 (dez) interfaces SFP/SFP+, com transceivers SFP+ 10GB-SR, para conexão ao meio via cabo de fibra ótica.	Características Específicas do Firewall Tipo 1	Para a Prova de Conceito, comprovar somente a quantidade das referidas interfaces.	
48	2.1.13.	Deve possuir, no mínimo, 4 (quatro) interfaces 25 Gbps para utilização de transceivers padrão SFP28.	Características Específicas do Firewall Tipo 1	Para a Prova de Conceito, comprovar somente a quantidade das referidas interfaces.	
49	2.1.14.	Deve possuir, no mínimo, 4 (quatro) interfaces 40/100 Gbps para utilização de transceivers padrão QSFP+/QSFP28.	Características Específicas do Firewall Tipo 1	Para a Prova de Conceito, comprovar somente a quantidade das referidas interfaces.	
50	2.2.1.	Deve possibilitar a operação em alta disponibilidade (HA) no equipamento, permitindo uma arquitetura ativo/ativo e ativo/passivo com no mínimo 2 (dois) membros, com sincronismo de estados integrado.	Características Específicas do Firewall Tipo 1 (HA)		
51	2.2.7.	Deve suportar a operação em cluster com no mínimo 2 equipamentos.	Características Específicas do Firewall Tipo 1 (HA)		
CONSOLE DE GERENCIAMENTO CENTRALIZADO PARA O FIREWALL TIPO 1 COM GARANTIA DE 60 MESES					
Nº	**REF. ANEXO I**	**DESCRIÇÃO DO ITEM PARA COMPROVAÇÃO**	**CONTEXTO DO REQUISITO**	**OBSERVAÇÃO**	**REQUISITO APROVADO? (SIM/NÃO)**
52	1.2.1.2.	Deve ser acessada via interface web ou através de um software cliente, com interface gráfica, instalado no Windows ou Linux;	Características Gerais das Consoles (Manager)		
53	1.2.1.9.	Deve permitir a criação e distribuição de políticas de segurança de forma centralizada, suportando organização hierárquica de regras.	Características Gerais das Consoles (Manager)		

54	1.2.1.11.	Deve ser capaz de gerenciar os firewalls em unidades remotas, fora da rede local.	Características Gerais das Consoles (Manager)		
55	1.2.1.12.	Deve permitir a autenticação dos administradores através de contas locais e bases externas LDAP ou Active Directory.	Características Gerais das Consoles (Manager)		
56	1.2.1.14.	Deve possuir a capacidade de definir administradores com diferentes perfis de acesso. Os perfis de acesso devem ser, no mínimo, de leitura/escrita e somente leitura.	Características Gerais das Consoles (Manager)		
57	1.2.1.19.	Deve registrar, em log de auditoria, as ações dos usuários administradores com o horário da alteração.	Características Gerais das Consoles (Manager)		
58	1.2.1.25.	Deve ser capaz de testar a conectividade dos equipamentos gerenciados.	Características Gerais das Consoles (Manager)		
59	1.2.1.26.	Deve suportar configuração das funcionalidades de alta disponibilidade dos dispositivos físicos.	Características Gerais das Consoles (Manager)		
60	1.2.1.27.	Deve permitir localizar em quais regras um objeto está sendo utilizado.	Características Gerais das Consoles (Manager)		
61	1.2.1.30.	Deve informar a utilização dos recursos de CPU, memória e atividade de rede dos equipamentos gerenciados.	Características Gerais das Consoles (Manager)		
CONSOLE DE GERENCIAMENTO DE LOGS PARA O FIREWALL TIPO 1 COM GARANTIA DE 60 MESES					
Nº	**REF. ANEXO I**	**DESCRIÇÃO DO ITEM PARA COMPROVAÇÃO**	**CONTEXTO DO REQUISITO**	**OBSERVAÇÃO**	**REQUISITO APROVADO? (SIM/NÃO)**
62	1.2.2.6.	Deve possibilitar a filtragem dos logs do equipamento por, no mínimo: aplicação, endereço IP de origem e destino, país de origem e destino, usuário e horário.	Características Gerais das Consoles (Logs)		
63	1.2.2.12.	Deve estar licenciada e permitir a correlação de todos os eventos gerados por todos os equipamentos e contextos virtuais que compõem a solução.	Características Gerais das Consoles (Logs)		
64	1.2.2.14.	Deve ser acessada via interface web ou através de um software cliente, com interface gráfica, instalado no Windows ou Linux	Características Gerais das Consoles (Logs)		
CONSOLE DE RELATORIA CENTRALIZADA PARA O FIREWALL TIPO 1 COM GARANTIA DE 60 MESES					
Nº	**REF. ANEXO I**	**DESCRIÇÃO DO ITEM PARA COMPROVAÇÃO**	**CONTEXTO DO REQUISITO**	**OBSERVAÇÃO**	**REQUISITO APROVADO? (SIM/NÃO)**
65	1.2.3.2.	Deve ser acessada via interface web ou através de um software cliente, com interface gráfica, instalado no Windows ou Linux.	Características Gerais das Consoles (Relatórios)		
66	1.2.3.6.	Deve ser capaz de gerar relatórios de equipamentos em unidades remotas, fora da rede local.	Características Gerais das Consoles (Relatórios)		
67	1.2.3.12.	Possuir relatórios pré-definidos.	Características Gerais das Consoles (Relatórios)		
68	1.2.3.13.	Permitir a geração de relatórios de logs de tráfego de dados.	Características Gerais das Consoles (Relatórios)		
69	1.2.3.14.	Permitir a geração de relatórios de logs para	Características Gerais das Consoles (Relatórios)		

		auditoria das configurações de regras, objetos e acessos.			
70	1.2.3.15.	Possibilitar o envio de maneira automática de relatórios por e-mail.	Características Gerais das Consoles (Relatórios)		
71	1.2.3.17.	Ter a capacidade de definir filtros nos relatórios.	Características Gerais das Consoles (Relatórios)		
72	1.2.3.20.	Possibilitar a visualização na interface gráfica de usuário (gui) da "console de relatoria centralizada as seguintes informações do sistema: logs diários recebidos, alertas gerados, entre outros.	Características Gerais das Consoles (Relatórios)		

Rio de Janeiro, 09 de julho de 2024

Documento assinado eletronicamente por **Charles Monteiro Guimarães**, **Diretor**, em 12/09/2024, às 14:42, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Manuelito de Sousa Reis Junior**, **Gerente**, em 12/09/2024, às 14:44, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Fabio Ivo**, **Assistente**, em 12/09/2024, às 15:02, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Marco Antonio de Andrade**, **Assessor Chefe**, em 12/09/2024, às 15:04, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Isabela Reboucas Costa**, **Analista de Sistemas**, em 12/09/2024, às 15:15, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Monique Goncalves Paz**, **Diretora**, em 12/09/2024, às 15:16, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Rosana Alves de Andrade**, **Analista de Sistemas**, em 12/09/2024, às 15:41, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **83090165** e o código CRC **1BA0DAE3**.

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone:

ANEXO III DO TERMO DE REFERÊNCIA
Roteiro para Prova de Conceito - lote 02
firewall tipo 02

1. INTRODUÇÃO

1.1. Será realizada Prova de Conceito com o objetivo de verificar o atendimento dos requisitos funcionais considerados prioritários pelo PRODERJ, referente à proposta ofertada pela licitante classificada em primeiro lugar.

1.2. O roteiro da Prova de Conceito, nos termos que seguem abaixo, exigirá da referida licitante a comprovação de que sua solução atende as especificações de maior relevância aqui elencadas.

1.3. As especificações selecionadas neste anexo representam as características de maior impacto em relação à solução como um todo, e levam em consideração os aspectos técnicos que permitem comprovação em ambiente de teste, haja vista que determinados recursos/características/funcionalidades possuem restrições de comprovação quando a solução ainda não está completamente implementada.

1.4. Este anexo deve ser interpretado conforme as disposições do Termo de Referência do qual é parte integrante e indissociável.

2. CARACTERÍSTICAS E FUNCIONALIDADES A SEREM COMPROVADAS

LOTE 2 - FIREWALL (TIPO 2)					
APPLIANCE FIREWALL TIPO 2 - INCLUSOS: HARDWARE, LICENCIAMENTO, INSTALAÇÃO, CONFIGURAÇÃO E GARANTIA POR 60 MESES					
Nº	**REF. ANEXO I**	**DESCRIÇÃO DO ITEM PARA COMPROVAÇÃO**	**CONTEXTO DO REQUISITO**	**OBSERVAÇÃO**	**REQUISITO APROVADO? (SIM/NÃO)**
1	1.1.4.3.	Deve permitir o acesso ao equipamento via SSH e interface web HTTPS.	Funcionalidades Básicas		
2	1.1.4.6.	Deve possuir visualização mínima sumarizada de aplicações, ameaças, URLs, endereços de origem, endereços de destino, levando-se em conta o quantitativo de sessões, de consumo de banda e categorização.	Funcionalidades Básicas		
3	1.1.4.10.	Os Firewalls de segurança físico ou virtualizados, devem possuir mecanismo para dedicar processamento no equipamento de segurança para funções e ações de Gerenciamento, mesmo que o equipamento esteja com alto processamento de CPU.	Funcionalidades Básicas		
4	1.1.5.3.	Deve suportar os protocolos DHCP e DHCPv6 e suas funcionalidades como cliente, servidor e relay.	Rede		
5	1.1.5.4.	Deve suportar Jumbo Frames.	Rede		
6	1.1.5.5.	Deve suportar sub interfaces Ethernet lógicas.	Rede		
7	1.1.5.8.	Deve permitir o registro de eventos de NAT com as informações de endereço interno, endereço público, data e hora do evento, portas de origem e destino.	Rede		

8	1.1.5.10.	Deve suportar as funcionalidades de roteamento estático e dinâmico em IPv4 e IPv6.	Rede		
9	1.1.5.16.	Deve suportar Policy Based Routing (PBR), possibilitando políticas de roteamento condicionado ao endereço IP de origem, endereço IP de destino e porta de comunicação.	Rede		
10	1.1.6.1.	Deve promover a integração com serviços de diretório LDAP e Active Directory, baseados em caracteres da língua portuguesa, para a identificação, autenticação, autorização e registro de eventos de acessos ou ameaças.	Autentificação e Identificação		
11	1.1.6.7.	Deve permitir a criação de políticas de segurança baseadas em usuários e grupos de usuários pertencentes a um diretório LDAP ou ao Active Directory.	Autentificação e Identificação		
12	1.1.6.10.	Deve possuir a capacidade de definir administradores com diferentes perfis de acesso. Os perfis de acesso devem ser, no mínimo, de leitura/escrita e somente leitura.	Autentificação e Identificação		
13	1.1.7.1.	Deve identificar os países de origem e destino de todas as conexões estabelecidas através do equipamento.	Geolocalização		
14	1.1.7.4.	Deve permitir a criação de políticas de segurança baseadas em geolocalização, permitindo o bloqueio de tráfego com origem ou destino a determinado país ou grupo de países.	Geolocalização		
15	1.1.7.5.	Deve possibilitar a visualização dos países de origem e destino nos logs de eventos de acessos e ameaças.	Geolocalização		
16	1.1.8.6.	Deve suportar Certificado Digital X.509.	VPN	Não precisa implementar certificado, basta mostrar as opções na manager.	
17	1.1.8.9.	Deve suportar VPN IPSec client-to-site (acesso remoto).	VPN		
18	1.1.8.11.	Deve permitir que o usuário realize a conexão VPN por meio de cliente instalado nos sistemas operacionais Windows, Mac OS ou Linux do seu equipamento ou então por meio de interface web do tipo portal.	VPN	No teste, a licitante precisará demonstrar este tópico apenas no Windows.	
19	1.1.8.15.	Deve suportar, no mínimo, os protocolos de roteamento estático e dinâmico OSPF e BGP.	VPN		

20	1.1.8.20.	Deve promover a integração com diretórios LDAP e Active Directory para a autenticação de usuários de VPN e regras de acesso.	VPN		
21	1.1.8.25.	Deve permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis de SSL.	VPN		
22	1.1.9.2.	Deve suportar a criação de políticas de controle de uso de largura de banda baseadas em: porta ou protocolo, endereço IP de origem ou destino, usuário ou grupo de usuários, aplicações (por exemplo, Youtube e WhatsApp).	QoS		
23	1.1.9.5.	Deve permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.	QoS		
24	1.1.10.5.	Os valores dos parâmetros jitter e latência devem poder ser configurados em unidade mínima de milissegundos (ms).	Balanceamento de Links		
25	1.1.10.10.	Deve possuir roteamento baseado em políticas e múltiplas saídas (e tipos de saídas) WANs.	Balanceamento de Links		
26	1.1.10.12.	Deve suportar a configuração de regras que permita o failback imediato.	Balanceamento de Links	A licitante poderá demonstrar apenas as configurações na manager.	
27	1.1.11.3.	Deve aplicar novas políticas de segurança sem provocar indisponibilidade de serviço ou descontinuidade das conexões ativas.	Recursos de Segurança		
28	1.1.11.12.	Deve possuir funcionalidade de backup e restore da configuração e das políticas de segurança.	Recursos de Segurança		
29	1.1.10.15.	Deve possuir a capacidade de emular um ambiente operacional isolado e seguro (Sandbox), na nuvem do fabricante, para execução e observação de código malicioso, sem a utilização de assinaturas, com base na atividade, como, por exemplo, operações de arquivo, alterações de registro e sistema etc.	Recursos de Segurança		
30	1.1.12.5.	Deve suportar controle de acesso para pelo menos serviços e protocolos pré-definidos, bem como possibilitar a adição de novos serviços e protocolos.	Filtro de Pacotes		
31	1.1.12.9.	Deve identificar os usuários para qualquer protocolo ou aplicação baseada em TCP, UDP e ICMP.	Filtro de Pacotes		

32	1.1.12.11.	Deve suportar a implementação de políticas de segurança baseadas em: portas, protocolos, usuários, grupos de usuários, endereços IP, redes CIDR/VLSM, horário ou período de tempo, e suas combinações.	Filtro de Pacotes		
33	1.1.12.12.	Deve suportar a consulta a fontes externas de endereços IP, domínios e URL's podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego.	Filtro de Pacotes		
34	1.1.13.9.	Deve classificar as aplicações em categorias.	Filtro de Conteúdo		
35	1.1.13.11.	Deve identificar os usuários que estão utilizando as aplicações.	Filtro de Conteúdo		
36	1.1.13.21.	Deve permitir a inclusão de URLs customizadas por política (whitelist).	Filtro de Conteúdo		
37	1.1.13.24.	Deve suportar a implementação de políticas de segurança baseadas em: URLs, categorias de URLs, endereço IP de origem ou destino, rede CIDR/VLSM de origem ou destino, usuário ou grupo de usuários, horário ou período de tempo, e suas combinações.	Filtro de Conteúdo		
38	1.1.13.25.	Deve alertar o usuário quando uma URL for bloqueada, por meio de página de bloqueio que possa ser customizada, e que informe, no mínimo, o motivo do bloqueio e a categoria na qual a URL foi classificada.	Filtro de Conteúdo		
39	1.1.13.27.	Deve permitir registrar todos os acessos autorizados ou bloqueados às páginas web, incluindo sua classificação e o usuário identificado.	Filtro de Conteúdo		
40	1.1.14.5.	Deve ser capaz de inspecionar tráfego criptografado usando SSL.	Prevenção de Intrusão - IPS		
41	1.1.14.9.	Deve permitir a criação de políticas de segurança que alertem, sem bloquear, sobre a ocorrência de um determinado ataque ou ameaça.	Prevenção de Intrusão - IPS		
42	1.1.14.14.	Deve bloquear malwares e spywares.	Prevenção de Intrusão - IPS		

43	3.1.1.	Throughput de 10 Gbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito.	Características Específicas do Firewall Tipo 2		
44	3.1.2.	Em relação ao filtro de pacotes, deve possuir o Throughput mínimo de 19 Gbps.	Características Específicas do Firewall Tipo 2		
45	3.1.10.	O appliance deve possuir, no mínimo, 10 (dez) portas 100/1000/10000 BASE-T ou SFP podendo ser uma composição entre os dois tipos, acompanhadas de seus respectivos transceivers.	Características Específicas do Firewall Tipo 2	Para a Prova de Conceito, comprovar somente a quantidade das referidas interfaces.	
46	3.1.11.	Deve possuir, no mínimo, 5 (cinco) interfaces 10 (dez) Gigabit-Ethernet padrão SFP+, com transceivers SFP+ 10GB-SR, para conexão ao meio via cabo de fibra ótica.	Características Específicas do Firewall Tipo 2	Para a Prova de Conceito, comprovar somente a quantidade das referidas interfaces.	
47	3.1.13.	Deve possuir, no mínimo, 5 (cinco) interfaces 1 (um) Gigabit-Ethernet padrão SFP, para conexão ao meio via cabo de fibra ótica.	Características Específicas do Firewall Tipo 2	Para a Prova de Conceito, comprovar somente a quantidade das referidas interfaces.	
48	3.1.14.	Deve possuir, no mínimo, 4 (quatro) interfaces 25 (vinte e cinco) Gigabit-Ethernet padrão SFP28.	Características Específicas do Firewall Tipo 2	Para a Prova de Conceito, comprovar somente a quantidade das referidas interfaces.	
CONSOLE DE GERENCIAMENTO CENTRALIZADO PARA O FIREWALL TIPO 2 COM GARANTIA DE 60 MESES					
Nº	**REF. ANEXO I**	**DESCRIÇÃO DO ITEM PARA COMPROVAÇÃO**	**CONTEXTO DO REQUISITO**	**OBSERVAÇÃO**	**REQUISITO APROVADO? (SIM/NÃO)**
49	1.2.1.2.	Deve ser acessada via interface web ou através de um software cliente, com interface gráfica, instalado no Windows ou Linux;	Características Gerais das Consoles (Manager)		
50	1.2.1.9.	Deve permitir a criação e distribuição de políticas de segurança de forma centralizada, suportando organização hierárquica de regras.	Características Gerais das Consoles (Manager)		
51	1.2.1.11.	Deve ser capaz de gerenciar os firewalls em unidades remotas, fora da rede local.	Características Gerais das Consoles (Manager)		
52	1.2.1.12.	Deve permitir a autenticação dos administradores através de contas locais e bases externas LDAP ou Active Directory.	Características Gerais das Consoles (Manager)		
53	1.2.1.14.	Deve possuir a capacidade de definir administradores com diferentes perfis de acesso. Os perfis de acesso devem ser, no mínimo, de leitura/escrita e somente leitura.	Características Gerais das Consoles (Manager)		
54	1.2.1.19.	Deve registrar, em log de auditoria, as ações dos usuários administradores com o horário da alteração.	Características Gerais das Consoles (Manager)		
55	1.2.1.25.	Deve ser capaz de testar a conectividade dos	Características Gerais das Consoles (Manager)		

		equipamentos gerenciados.			
56	1.2.1.26.	Deve suportar configuração das funcionalidades de alta disponibilidade dos dispositivos físicos.	Características Gerais das Consoles (Manager)		
57	1.2.1.27.	Deve permitir localizar em quais regras um objeto está sendo utilizado.	Características Gerais das Consoles (Manager)		
58	1.2.1.30.	Deve informar a utilização dos recursos de CPU, memória e atividade de rede dos equipamentos gerenciados.	Características Gerais das Consoles (Manager)		
CONSOLE DE GERENCIAMENTO DE LOGS PARA O FIREWALL TIPO 2 COM GARANTIA DE 60 MESES					
Nº	**REF. ANEXO I**	**DESCRIÇÃO DO ITEM PARA COMPROVAÇÃO**	**CONTEXTO DO REQUISITO**	**OBSERVAÇÃO**	**REQUISITO APROVADO? (SIM/NÃO)**
59	1.2.2.6.	Deve possibilitar a filtragem dos logs do equipamento por, no mínimo: aplicação, endereço IP de origem e destino, país de origem e destino, usuário e horário.	Características Gerais das Consoles (Logs)		
60	1.2.2.12.	Deve estar licenciada e permitir a correlação de todos os eventos gerados por todos os equipamentos e contextos virtuais que compõem a solução.	Características Gerais das Consoles (Logs)		
61	1.2.2.15.	Deve ser acessada via interface web ou através de um software cliente, com interface gráfica, instalado no Windows ou Linux	Características Gerais das Consoles (Logs)		
CONSOLE DE RELATORIA CENTRALIZADA PARA O FIREWALL TIPO 2 COM GARANTIA DE 60 MESES					
Nº	**REF. ANEXO I**	**DESCRIÇÃO DO ITEM PARA COMPROVAÇÃO**	**CONTEXTO DO REQUISITO**	**OBSERVAÇÃO**	**REQUISITO APROVADO? (SIM/NÃO)**
62	1.2.3.2.	Deve ser acessada via interface web ou através de um software cliente, com interface gráfica, instalado no Windows ou no Linux.	Características Gerais das Consoles (Relatórios)		
63	1.2.3.6.	Deve ser capaz de gerar relatórios de equipamentos em unidades remotas, fora da rede local.	Características Gerais das Consoles (Relatórios)		
64	1.2.3.12.	Possuir relatórios pré-definidos.	Características Gerais das Consoles (Relatórios)		
65	1.2.3.13.	Permitir a geração de relatórios de logs de tráfego de dados.	Características Gerais das Consoles (Relatórios)		
66	1.2.3.14.	Permitir a geração de relatórios de logs para auditoria das configurações de regras, objetos e acessos.	Características Gerais das Consoles (Relatórios)		
67	1.2.3.15.	Possibilitar o envio de maneira automática de relatórios por e-mail.	Características Gerais das Consoles (Relatórios)		
68	1.2.3.17.	Ter a capacidade de definir filtros nos relatórios.	Características Gerais das Consoles (Relatórios)		
69	1.2.3.20.	Possibilitar a visualização na interface gráfica de usuário (gui) da “console de relatoria centralizada as seguintes informações do sistema: logs diários recebidos, alertas gerados, entre outros.	Características Gerais das Consoles (Relatórios)		

Rio de Janeiro, 09 de julho de 2024

Documento assinado eletronicamente por **Charles Monteiro Guimarães**, **Diretor**, em 12/09/2024, às 14:42, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Manuelito de Sousa Reis Junior**, **Gerente**, em 12/09/2024, às 14:44, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Fabio Ivo**, **Assistente**, em 12/09/2024, às 15:02, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Marco Antonio de Andrade**, **Assessor Chefe**, em 12/09/2024, às 15:04, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Isabela Reboucas Costa**, **Analista de Sistemas**, em 12/09/2024, às 15:15, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Monique Goncalves Paz**, **Diretora**, em 12/09/2024, às 15:17, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Rosana Alves de Andrade**, **Analista de Sistemas**, em 12/09/2024, às 15:42, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **83090167** e o código CRC **A922D6A9**.

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone:

ANEXO IV DO TERMO DE REFERÊNCIA
Roteiro para Prova de Conceito - lote 03
firewall tipo 03

1. INTRODUÇÃO

1.1. Será realizado a Prova de Conceito com o objetivo de verificar o atendimento dos requisitos funcionais considerados prioritários pelo PRODERJ, referente à proposta ofertada pela licitante classificada em primeiro lugar.

1.2. O roteiro da Prova de Conceito, nos termos que seguem abaixo, exigirá da referida licitante a comprovação de que sua solução atende as especificações de maior relevância aqui elencadas.

1.3. As especificações selecionadas neste anexo representam as características de maior impacto em relação à solução como um todo, e levam em consideração os aspectos técnicos que permitem comprovação em ambiente de teste, haja vista que determinados recursos/características/funcionalidades possuem restrições de comprovação quando a solução ainda não está completamente implementada.

1.4. Este anexo deve ser interpretado conforme as disposições do Termo de Referência do qual é parte integrante e indissociável.

2. CARACTERÍSTICAS E FUNCIONALIDADES A SEREM COMPROVADAS

LOTE 3 - FIREWALL (TIPO 3)					
APPLIANCE FIREWALL TIPO 3 - INCLUSOS: HARDWARE, LICENCIAMENTO, INSTALAÇÃO, CONFIGURAÇÃO E GARANTIA POR 60 MESES					
Nº	**REF. ANEXO I**	**DESCRIÇÃO DO ITEM PARA COMPROVAÇÃO**	**CONTEXTO DO REQUISITO**	**OBSERVAÇÃO**	**REQUISITO APROVADO? (SIM/NÃO)**
1	1.1.4.3.	Deve permitir o acesso ao equipamento via SSH e interface web HTTPS.	Funcionalidades Básicas		
2	1.1.4.6.	Deve possuir visualização mínima sumarizada de aplicações, ameaças, URLs, endereços de origem, endereços de destino, levando-se em conta o quantitativo de sessões, de consumo de banda e categorização.	Funcionalidades Básicas		
3	1.1.4.10.	Os Firewalls de segurança físico ou virtualizados, devem possuir mecanismo para dedicar processamento no equipamento de segurança para funções e ações de Gerenciamento, mesmo que o equipamento esteja com alto processamento de CPU.	Funcionalidades Básicas		
4	1.1.5.3.	Deve suportar os protocolos DHCP e DHCPv6 e suas funcionalidades como cliente, servidor e relay.	Rede		
5	1.1.5.4.	Deve suportar Jumbo Frames.	Rede		
6	1.1.5.5.	Deve suportar sub interfaces Ethernet lógicas.	Rede		
7	1.1.5.8.	Deve permitir o registro de eventos de NAT com as informações de endereço interno, endereço público, data e hora do evento, portas de origem e destino.	Rede		

8	1.1.5.10.	Deve suportar as funcionalidades de roteamento estático e dinâmico em IPv4 e IPv6.	Rede		
9	1.1.5.16.	Deve suportar Policy Based Routing (PBR), possibilitando políticas de roteamento condicionado ao endereço IP de origem, endereço IP de destino e porta de comunicação.	Rede		
10	1.1.6.1.	Deve promover a integração com serviços de diretório LDAP e Active Directory, baseados em caracteres da língua portuguesa, para a identificação, autenticação, autorização e registro de eventos de acessos ou ameaças.	Autentificação e Identificação		
11	1.1.6.7.	Deve permitir a criação de políticas de segurança baseadas em usuários e grupos de usuários pertencentes a um diretório LDAP ou ao Active Directory.	Autentificação e Identificação		
12	1.1.6.10.	Deve possuir a capacidade de definir administradores com diferentes perfis de acesso. Os perfis de acesso devem ser, no mínimo, de leitura/escrita e somente leitura.	Autentificação e Identificação		
13	1.1.7.1.	Deve identificar os países de origem e destino de todas as conexões estabelecidas através do equipamento.	Geolocalização		
14	1.1.7.4.	Deve permitir a criação de políticas de segurança baseadas em geolocalização, permitindo o bloqueio de tráfego com origem ou destino a determinado país ou grupo de países.	Geolocalização		
15	1.1.7.5.	Deve possibilitar a visualização dos países de origem e destino nos logs de eventos de acessos e ameaças.	Geolocalização		
16	1.1.8.6.	Deve suportar Certificado Digital X.509.	VPN	Não precisa implementar certificado, basta mostrar as opções na manager.	
17	1.1.8.9.	Deve suportar VPN IPSec client-to-site (acesso remoto).	VPN		
18	1.1.8.11.	Deve permitir que o usuário realize a conexão VPN por meio de cliente instalado nos sistemas operacionais Windows, Mac OS ou Linux do seu equipamento ou então por meio de interface web do tipo portal.	VPN	No teste, a licitante precisará demonstrar este tópico apenas no Windows.	
19	1.1.8.15.	Deve suportar, no mínimo, os protocolos de roteamento estático e dinâmico OSPF e BGP.	VPN		

20	1.1.8.20.	Deve promover a integração com diretórios LDAP e Active Directory para a autenticação de usuários de VPN e regras de acesso.	VPN		
21	1.1.8.25.	Deve permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis de SSL.	VPN		
22	1.1.9.2.	Deve suportar a criação de políticas de controle de uso de largura de banda baseadas em: porta ou protocolo, endereço IP de origem ou destino, usuário ou grupo de usuários, aplicações (por exemplo, Youtube e WhatsApp).	QoS		
23	1.1.9.5.	Deve permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.	QoS		
24	1.1.10.5.	Os valores dos parâmetros jitter e latência devem poder ser configurados em unidade mínima de milissegundos (ms).	Balanceamento de Links		
25	1.1.10.10.	Deve possuir roteamento baseado em políticas e múltiplas saídas (e tipos de saídas) WANs.	Balanceamento de Links		
26	1.1.10.12.	Deve suportar a configuração de regras que permita o failback imediato.	Balanceamento de Links	A licitante poderá demonstrar apenas as configurações na manager.	
27	1.1.11.3.	Deve aplicar novas políticas de segurança sem provocar indisponibilidade de serviço ou descontinuidade das conexões ativas.	Recursos de Segurança		
28	1.1.11.12.	Deve possuir funcionalidade de backup e restore da configuração e das políticas de segurança.	Recursos de Segurança		
29	1.1.10.15.	Deve possuir a capacidade de emular um ambiente operacional isolado e seguro (Sandbox), na nuvem do fabricante, para execução e observação de código malicioso, sem a utilização de assinaturas, com base na atividade, como, por exemplo, operações de arquivo, alterações de registro e sistema etc.	Recursos de Segurança		
30	1.1.12.5.	Deve suportar controle de acesso para pelo menos serviços e protocolos pré-definidos, bem como possibilitar a adição de novos serviços e protocolos.	Filtro de Pacotes		
31	1.1.12.9.	Deve identificar os usuários para qualquer protocolo ou aplicação baseada em TCP, UDP e ICMP.	Filtro de Pacotes		

32	1.1.12.11.	Deve suportar a implementação de políticas de segurança baseadas em: portas, protocolos, usuários, grupos de usuários, endereços IP, redes CIDR/VLSM, horário ou período de tempo, e suas combinações.	Filtro de Pacotes		
33	1.1.12.12.	Deve suportar a consulta a fontes externas de endereços IP, domínios e URL's podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego.	Filtro de Pacotes		
34	1.1.13.9.	Deve classificar as aplicações em categorias.	Filtro de Conteúdo		
35	1.1.13.11.	Deve identificar os usuários que estão utilizando as aplicações.	Filtro de Conteúdo		
36	1.1.13.21.	Deve permitir a inclusão de URLs customizadas por política (whitelist).	Filtro de Conteúdo		
37	1.1.13.24.	Deve suportar a implementação de políticas de segurança baseadas em: URLs, categorias de URLs, endereço IP de origem ou destino, rede CIDR/VLSM de origem ou destino, usuário ou grupo de usuários, horário ou período de tempo, e suas combinações.	Filtro de Conteúdo		
38	1.1.13.25.	Deve alertar o usuário quando uma URL for bloqueada, por meio de página de bloqueio que possa ser customizada, e que informe, no mínimo, o motivo do bloqueio e a categoria na qual a URL foi classificada.	Filtro de Conteúdo		
39	1.1.13.27.	Deve permitir registrar todos os acessos autorizados ou bloqueados às páginas web, incluindo sua classificação e o usuário identificado.	Filtro de Conteúdo		
40	1.1.14.5.	Deve ser capaz de inspecionar tráfego criptografado usando SSL.	Prevenção de Intrusão - IPS		
41	1.1.14.9.	Deve permitir a criação de políticas de segurança que alertem, sem bloquear, sobre a ocorrência de um determinado ataque ou ameaça.	Prevenção de Intrusão - IPS		
42	1.1.14.14.	Deve bloquear malwares e spywares.	Prevenção de Intrusão - IPS		

43	4.1.1.	Throughput de 2 Gbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito.	Características Específicas do Firewall Tipo 3		
44	4.1.2.	Em relação ao filtro de pacotes, deve possuir o Throughput de no mínimo 4 Gbps.	Características Específicas do Firewall Tipo 3		
45	4.1.10.	O appliance deve possuir, no mínimo, 08 (oito) portas de rede 1G RJ-45.	Características Específicas do Firewall Tipo 3	Para a Prova de Conceito, comprovar somente a quantidade das referidas interfaces.	
46	4.1.11.	O appliance deve possuir uma porta 10/100/1000 para gerenciamento "out-of-band".	Características Específicas do Firewall Tipo 3	Para a Prova de Conceito, comprovar somente a quantidade das referidas interfaces.	
CONSOLE DE GERENCIAMENTO CENTRALIZADO PARA O FIREWALL TIPO 3 COM GARANTIA DE 60 MESES					
Nº	**REF. ANEXO I**	**DESCRIÇÃO DO ITEM PARA COMPROVAÇÃO**	**CONTEXTO DO REQUISITO**	**OBSERVAÇÃO**	**REQUISITO APROVADO? (SIM/NÃO)**
47	1.2.1.2.	Deve ser acessada via interface web ou através de um software cliente, com interface gráfica, instalado no Windows ou Linux;	Características Gerais das Consoles (Manager)		
48	1.2.1.9.	Deve permitir a criação e distribuição de políticas de segurança de forma centralizada, suportando organização hierárquica de regras.	Características Gerais das Consoles (Manager)		
49	1.2.1.11.	Deve ser capaz de gerenciar os firewalls em unidades remotas, fora da rede local.	Características Gerais das Consoles (Manager)		
50	1.2.1.12.	Deve permitir a autenticação dos administradores através de contas locais e bases externas LDAP ou Active Directory.	Características Gerais das Consoles (Manager)		
51	1.2.1.14.	Deve possuir a capacidade de definir administradores com diferentes perfis de acesso. Os perfis de acesso devem ser, no mínimo, de leitura/escrita e somente leitura.	Características Gerais das Consoles (Manager)		
52	1.2.1.19.	Deve registrar, em log de auditoria, as ações dos usuários administradores com o horário da alteração.	Características Gerais das Consoles (Manager)		
53	1.2.1.25.	Deve ser capaz de testar a conectividade dos equipamentos gerenciados.	Características Gerais das Consoles (Manager)		
54	1.2.1.26.	Deve suportar configuração das funcionalidades de alta disponibilidade dos dispositivos físicos.	Características Gerais das Consoles (Manager)		
55	1.2.1.27.	Deve permitir localizar em quais regras um objeto está sendo utilizado.	Características Gerais das Consoles (Manager)		
56	1.2.1.30.	Deve informar a utilização dos recursos de CPU,	Características Gerais das Consoles (Manager)		

		memória e atividade de rede dos equipamentos gerenciados.			
CONSOLE DE GERENCIAMENTO DE LOGS PARA O FIREWALL TIPO 3 COM GARANTIA DE 60 MESES					
Nº	**REF. ANEXO I**	**DESCRIÇÃO DO ITEM PARA COMPROVAÇÃO**	**CONTEXTO DO REQUISITO**	**OBSERVAÇÃO**	**REQUISITO APROVADO? (SIM/NÃO)**
57	1.2.2.6.	Deve possibilitar a filtragem dos logs do equipamento por, no mínimo: aplicação, endereço IP de origem e destino, país de origem e destino, usuário e horário.	Características Gerais das Consoles (Logs)		
58	1.2.2.12.	Deve estar licenciada e permitir a correlação de todos os eventos gerados por todos os equipamentos e contextos virtuais que compõem a solução.	Características Gerais das Consoles (Logs)		
59	1.2.2.15.	Deve ser acessada via interface web ou através de um software cliente, com interface gráfica, instalado no Windows ou Linux	Características Gerais das Consoles (Logs)		
CONSOLE DE RELATORIA CENTRALIZADA PARA O FIREWALL TIPO 3 COM GARANTIA DE 60 MESES					
Nº	**REF. ANEXO I**	**DESCRIÇÃO DO ITEM PARA COMPROVAÇÃO**	**CONTEXTO DO REQUISITO**	**OBSERVAÇÃO**	**REQUISITO APROVADO? (SIM/NÃO)**
60	1.2.3.2.	Deve ser acessada via interface web ou através de um software cliente, com interface gráfica, instalado no Windows ou no Linux.	Características Gerais das Consoles (Relatórios)		
61	1.2.3.6.	Deve ser capaz de gerar relatórios de equipamentos em unidades remotas, fora da rede local.	Características Gerais das Consoles (Relatórios)		
62	1.2.3.12.	Possuir relatórios pré-definidos.	Características Gerais das Consoles (Relatórios)		
63	1.2.3.13.	Permitir a geração de relatórios de logs de tráfego de dados.	Características Gerais das Consoles (Relatórios)		
64	1.2.3.14.	Permitir a geração de relatórios de logs para auditoria das configurações de regras, objetos e acessos.	Características Gerais das Consoles (Relatórios)		
65	1.2.3.15.	Possibilitar o envio de maneira automática de relatórios por e-mail.	Características Gerais das Consoles (Relatórios)		
66	1.2.3.17.	Ter a capacidade de definir filtros nos relatórios.	Características Gerais das Consoles (Relatórios)		
67	1.2.3.20.	Possibilitar a visualização na interface gráfica de usuário (gui) da “console de relatoria centralizada as seguintes informações do sistema: logs diários recebidos, alertas gerados, entre outros.	Características Gerais das Consoles (Relatórios)		

Rio de Janeiro, 09 de julho de 2024

Documento assinado eletronicamente por **Charles Monteiro Guimarães**, **Diretor**, em 12/09/2024, às 14:42, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Manuelito de Sousa Reis Junior**, **Gerente**, em 12/09/2024, às 14:45, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Fabio Ivo**, **Assistente**, em 12/09/2024, às 15:02, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Marco Antonio de Andrade**, **Assessor Chefe**, em 12/09/2024, às 15:04, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Isabela Reboucas Costa**, **Analista de Sistemas**, em 12/09/2024, às 15:16, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Monique Goncalves Paz**, **Diretora**, em 12/09/2024, às 15:17, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Rosana Alves de Andrade**, **Analista de Sistemas**, em 12/09/2024, às 15:42, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **83090170** e o código CRC **51164E34**.

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone:

Governo do Estado do Rio de Janeiro

Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro

Vice Presidência de Tecnologia

ANEXO V DO TERMO DE REFERÊNCIA
MODELO DE RELATÓRIO DE CUMPRIMENTO DO OBJETO
(para atendimento do subtópico 5.3.2 do TR)

obs: Este anexo deve ser interpretado conforme as disposições do Termo de Referência do qual é parte integrante e indissociável.

(logo da empresa)

1. IDENTIFICAÇÃO			
Contrato nº			
Contratada		**CNPJ**	
nº da OS/OF		**Período de Referência**	

2. ESPECIFICAÇÃO DOS BENS/SERVIÇOS E VOLUMES DE ENTREGA/EXECUÇÃO					
Descrição do Objeto Contratado					
Item	**Descrição do bem ou serviço**	**Métrica**	**Quantidade**	**Valor Unitário**	**Valor Total**
				Valor Total	

3. OBSERVAÇÕES

4. ENCAMINHAMENTO
Por este instrumento, encaminhamos as informações e documentos comprobatórios dos serviços correspondentes à OS/OF acima identificada, conforme definido no Modelo de Execução do contrato supracitado, para que seja verificado o devido cumprimento dos requisitos e demais condições contratuais

5. PREPOSTO
_____ Nome CPF Local e Data

Rio de Janeiro, 09 de julho de 2024

Documento assinado eletronicamente por **Charles Monteiro Guimarães**, **Diretor**, em 12/09/2024, às 14:42, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Manuelito de Sousa Reis Junior**, **Gerente**, em 12/09/2024, às 14:45, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Fabio Ivo**, **Assistente**, em 12/09/2024, às 15:03, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Marco Antonio de Andrade**, **Assessor Chefe**, em 12/09/2024, às 15:04, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Isabela Reboucas Costa**, **Analista de Sistemas**, em 12/09/2024, às 15:16, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Monique Goncalves Paz**, **Diretora**, em 12/09/2024, às 15:17, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Rosana Alves de Andrade**, **Analista de Sistemas**, em 12/09/2024, às 15:43, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **83089840** e o código CRC **FCC13469**.

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone:

Governo do Estado do Rio de Janeiro

Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro

Diretoria de Segurança da Informação

ANEXO VI DO TERMO DE REFERÊNCIA

MODELO DE TERMO DE CONFIDENCIALIDADE E SIGILO

este anexo deve ser interpretado conforme as disposições do Termo de Referência do qual é parte integrante e indissociável.

ANEXO XXX - DO CONTRATO

MODELO DE TERMO DE CONFIDENCIALIDADE E SIGILO

Eu, (nome completo), (ocupação institucional), (órgão público / entidade), (matrícula), (CPF), declaro a ciência das obrigações e responsabilidades decorrentes do tratamento de dados pessoais realizado durante a vigência contratual, observando o integral teor do presente Termo de Responsabilidade.

Considerando as obrigações a mim conferidas, no bojo deste Termo de Responsabilidade, comprometo-me a:

a) manusear as bases de dados com objetivo exclusivo de alcançar a finalidade específica atrelada ao tratamento dos dados pessoais envolvidos;
b) não compartilhar com terceiros os dados pessoais sujeitos a qualquer espécie de tratamento, salvo se por meio oficial e quando estritamente necessário à concretização das atribuições;
c) manter a absoluta cautela quando da exibição de dados pessoais em tela, por meio de impressões, ou, ainda, na gravação em meios eletrônicos, com escopo de inibir o acesso de terceiros não autorizados;
d) não me ausentar do terminal sem encerrar a sessão de uso das bases, inibindo a prática de ações virtuais por terceiros não autorizados;
e) não armazenar documentos de natureza particular em pastas institucionais;
f) manter o sigilo dos dados pessoais ou informações sigilosas obtidas por força de minhas atribuições, mediante abstenção de compartilhamento e/ou divulgação a terceiros, sob pena de incorrer em sanções administrativas, civis e/ou penais decorrentes de eventual violação; e
g) comunicar imediatamente ao Encarregado pelo tratamento de dados pessoais a ocorrência de qualquer ação ou omissão que contrarie o disposto neste termo, pelos meios formais disponibilizados pela instituição.

Rio de Janeiro, XX de XXXXXX de 20XX.

Rio de Janeiro, 09 de julho de 2024

Documento assinado eletronicamente por **Charles Monteiro Guimarães**, **Diretor**, em 12/09/2024, às 14:42, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Manuelito de Sousa Reis Junior**, **Gerente**, em 12/09/2024, às 14:45, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Marco Antonio de Andrade**, **Assessor Chefe**, em 12/09/2024, às 15:04, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Isabela Reboucas Costa**, **Analista de Sistemas**, em 12/09/2024, às 15:17, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Fabio Ivo**, **Assistente**, em 12/09/2024, às 15:18, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Monique Goncalves Paz**, **Diretora**, em 12/09/2024, às 15:18, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Rosana Alves de Andrade**, **Analista de Sistemas**, em 12/09/2024, às 15:44, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **83089841** e o código CRC **6C9B7A77**.

Referência: Processo nº SEI-430002/000045/2024 SEI nº 83089841

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone:

Governo do Estado do Rio de Janeiro

Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro

Diretoria de Segurança da Informação

ANEXO VII DO TERMO DE REFERÊNCIA

MODELO DE ORDEM DE SERVIÇO / FORNECIMENTO

Este anexo deve ser interpretado conforme as disposições do Termo de Referência do qual é parte integrante e indissociável.

1 - IDENTIFICAÇÃO DA AUTORIZAÇÃO DE FORNECIMENTO / ORDEM DE SERVIÇO			
N°da AF/OS:	Data de Emissao:	N° do Contrato:	Data do Contrato: Extrato DOERJ:

2 - IDENTIFICAÇÃO DA EMPRESA CONTRATADA		
Nome da Empresa:		
CNPJ:	Inscrição Estadual:	
Endereço:		
Cidade:	UF:	
CEP:	Telefone:	E-mail:
Preposto:		Celular: E-mail:

3 - ESPECIFICAÇÃO DOS PRODUTOS/SERVIÇOS E VOLUMES ESTIMADOS							
Item / Lote	**ID SIGA**	**Descrição do Produto ou Serviço**	**Métrica**	**Valor Unitário (R$)**	**Quantidade / Volume**	**Valor Total do item (R$)**	**Parcela R$** *(esta coluna pode ser descartada em caso de pgto a vista)*
						Valor Total (R$)	

4 – INSTRUÇÕES COMPLEMENTARES

5 – CIÊNCIA	
CONTRATANTE	
Gestor do Contrato	**Fiscal Requisitante do Contrato**
_____ nome ID nº	_____ nome ID nº
CONTRATADA	
PREPOSTO	
_____ nome CPF:	

Rio de Janeiro, 09 de julho de 2024

Documento assinado eletronicamente por **Charles Monteiro Guimarães**, **Diretor**, em 12/09/2024, às 14:42, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Manuelito de Sousa Reis Junior**, **Gerente**, em 12/09/2024, às 14:45, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Marco Antonio de Andrade**, **Assessor Chefe**, em 12/09/2024, às 15:04, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Isabela Reboucas Costa**, **Analista de Sistemas**, em 12/09/2024, às 15:17, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Fabio Ivo**, **Assistente**, em 12/09/2024, às 15:18, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Monique Goncalves Paz**, **Diretora**, em 12/09/2024, às 15:19, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Rosana Alves de Andrade**, **Analista de Sistemas**, em 12/09/2024, às 15:44, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **83090176** e o código CRC **E5DE049A**.

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone:

Governo do Estado do Rio de Janeiro

Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro

Diretoria de Segurança da Informação

ANEXO VIII DO TERMO DE REFERÊNCIA

MODELO DE PLANILHA DE COMPOSIÇÃO DE PREÇOS

Este anexo deve ser interpretado conforme as disposições do Termo de Referência do qual é parte integrante e indissociável.

Processo SEI Nº_____

Ata de Registro de Preços Nº ____/____

Fornecedor:

OBJETO: Sistema de Registro de Preços para Contratação de empresa do ramo de Tecnologia da Informação para o fornecimento de solução de firewall, com garantia de 60 meses, contemplando hardware e software, com instalação e configuração, nas dependências do contratante e curso de treinamento oficial da solução.

LOTE 1 - FIREWALL TIPO 1

Item	**ID SIGA**	**Descrição**	**Unidade de Fornecimento**	**Quantidade estimada**	**Valor Unitário (R$)**	**Valor Total (R$)**
1	168256	APPLIANCE FIREWALL TIPO 1 - INCLUSOS: HARDWARE, LICENCIAMENTO E GARANTIA POR 60 MESES	Unidade			
2	172443	CONSOLE DE GERENCIAMENTO CENTRALIZADO PARA O FIREWALL TIPO 1 COM GARANTIA DE 60 MESES	Unidade			
3	172442	CONSOLE DE GERENCIAMENTO DE LOGS PARA O FIREWALL TIPO 1 COM GARANTIA DE 60 MESES	Unidade			
4	172444	CONSOLE DE RELATORIA CENTRALIZADA PARA O FIREWALL TIPO 1 COM GARANTIA DE 60 MESES	Unidade			
5	180944	TREINAMENTO OPERACIONAL PARA A SOLUÇÃO DO LOTE 1	Aluno/vaga			
					Valor total do Lote 1	

LOTE 2 - FIREWALL TIPO 2

Item	ID SIGA	Descrição	Unidade de Fornecimento	Quantidade estimada	Valor Unitário (R$)	Valor Total (R$)
1	168257	APPLIANCE FIREWALL TIPO 2 - INCLUSOS: HARDWARE, LICENCIAMENTO E GARANTIA POR 60 MESES	Unidade			
2	180938	CONSOLE DE GERENCIAMENTO CENTRALIZADO PARA O FIREWALL TIPO 2 COM GARANTIA DE 60 MESES	Unidade			
3	180940	CONSOLE DE GERENCIAMENTO DE LOGS PARA O FIREWALL TIPO 2 COM GARANTIA DE 60 MESES	Unidade			

4	180942	CONSOLE DE RELATORIA CENTRALIZADA PARA O FIREWALL TIPO 2 COM GARANTIA DE 60 MESES	Unidade			
5	180945	TREINAMENTO OPERACIONAL PARA A SOLUÇÃO DO LOTE 2	Aluno/vaga			
					Valor total do Lote 2	
LOTE 3 - FIREWALL TIPO 3						
Item	ID SIGA	Descrição	Unidade de Fornecimento	Quantidade estimada	Valor Unitário (R$)	Valor Total (R$)
1	168258	APPLIANCE FIREWALL TIPO 3 - INCLUSOS: HARDWARE, LICENCIAMENTO E GARANTIA POR 60 MESES	Unidade			
2	180939	CONSOLE DE GERENCIAMENTO CENTRALIZADO PARA O FIREWALL TIPO 3 COM GARANTIA DE 60 MESES	Unidade			
3	180941	CONSOLE DE GERENCIAMENTO DE LOGS PARA O FIREWALL TIPO 3 COM GARANTIA DE 60 MESES	Unidade			
4	180943	CONSOLE DE RELATORIA CENTRALIZADA PARA O FIREWALL TIPO 3 COM GARANTIA DE 60 MESES	Unidade			
5	180946	TREINAMENTO OPERACIONAL PARA A SOLUÇÃO DO LOTE 3	Aluno/vaga			
					Valor total do Lote 3	

- Os preços deverão contemplar todos os custos de acordo com as condições estabelecidas no Termo de Referência.

Rio de Janeiro, 09 de julho de 2024

Documento assinado eletronicamente por **Charles Monteiro Guimarães**, **Diretor**, em 12/09/2024, às 14:42, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Manuelito de Sousa Reis Junior**, **Gerente**, em 12/09/2024, às 14:45, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Marco Antonio de Andrade**, **Assessor Chefe**, em 12/09/2024, às 15:04, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Isabela Reboucas Costa**, **Analista de Sistemas**, em 12/09/2024, às 15:17, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Fabio Ivo**, **Assistente**, em 12/09/2024, às 15:18, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Monique Goncalves Paz**, **Diretora**, em 12/09/2024, às 15:20, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Rosana Alves de Andrade**, **Analista de Sistemas**, em 12/09/2024, às 15:46, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **83089514** e o código CRC **FC58C9F9**.

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone:

ANEXO IX DO TERMO DE REFERÊNCIA

MODELO DE TERMO DE RECEBIMENTO DEFINITIVO

Este anexo deve ser interpretado conforme as disposições do Termo de Referência do qual é parte integrante e indissociável.

1 – IDENTIFICAÇÃO			
CONTRATO Nº			**Vigência:**
CONTRATADA		**CNPJ**	
Nº DA OS/OFB			

2 – ESPECIFICAÇÃO DOS PRODUTOS/BENS E VOLUMES DE EXECUÇÃO						
SOLUÇÃO DE TIC						
Objeto:						
ID SIGA	**Descrição do Produto ou Serviço**	**Métrica**	**Valor Unitário (R$)**	**Quantidade / Volume**	**Valor Total (R$)**	**Parcela 21/36 (R$)**
TOTAL						

3 – ATESTE DE RECEBIMENTO
Por este instrumento atestamos, que os serviços correspondentes à (link do documento) acima identificada foram prestados pela **CONTRATADA** e atendem às condições contratuais, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do Termo de Referência do Contrato acima indicado.

4 – DESCONTOS EFETUADOS E VALOR A LIQUIDAR

5 – AUTORIZAÇÃO PARA FATURAMENTO
GESTOR DO CONTRATO

AUTORIZA-SE a **CONTRATADA** a apresentar as notas fiscais dos bens entregues relativos à supracitada (link do documento), no valor discriminado no item 2, acima.

_____
Gestor do Contrato
Matrícula:

6 – CIÊNCIA

FISCAL TÉCNICO

_____
Fiscal
Matrícula:

FISCAL REQUISITANTE

_____
Fiscal
Matrícula:

PREPOSTO

_____
Nome do Preposto da Contratada
CPF:
Nome da Contratada

Rio de Janeiro, ___ de _____ de _____

Rio de Janeiro, 09 de julho de 2024

Documento assinado eletronicamente por **Charles Monteiro Guimarães**, **Diretor**, em 12/09/2024, às 14:42, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Manuelito de Sousa Reis Junior**, **Gerente**, em 12/09/2024, às 14:45, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Marco Antonio de Andrade**, **Assessor Chefe**, em 12/09/2024, às 15:04, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Isabela Reboucas Costa**, **Analista de Sistemas**, em 12/09/2024, às 15:18, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Fabio Ivo**, **Assistente**, em 12/09/2024, às 15:19, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Monique Goncalves Paz**, **Diretora**, em 12/09/2024, às 15:20, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Rosana Alves de Andrade**, **Analista de Sistemas**, em 12/09/2024, às 15:45, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone:

Governo do Estado do Rio de Janeiro

Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro

Vice Presidência de Tecnologia

ANEXO X DO TERMO DE REFERÊNCIA

MODELO DE TERMO DE RECEBIMENTO PROVISÓRIO

Este anexo deve ser interpretado conforme as disposições do Termo de Referência do qual é parte integrante e indissociável.

Identificação Contrato:	**Nº da OS**
Objeto:	
CONTRATANTE:	
Contratada:	

Por este instrumento, atestamos que os serviços integrantes da O.S. acima identificada, ou conforme definido no Modelo de Execução do contrato supracitado, foram recebidos nesta data e serão objetos de avaliação quanto à adequação da Solução de Tecnologia da Informação e à conformidade de qualidade, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do Contrato pela CONTRATANTE.

Ressaltamos que o recebimento definitivo destes serviços (ou bens) ocorrerá em até ___dias, desde que não ocorram problemas técnicos ou divergências quanto às especificações constantes do Termo de Referência do Contrato acima identificado.

De Acordo

CONTRATANTE	**CONTRATADA**
Membro da comissão fiscalizadora	**Preposto**
Nome: **Matrícula:**	***Nome:*** ***Qualificação:***

_____, _____ de _____ de 20___.

Rio de Janeiro, 09 de julho de 2024

Documento assinado eletronicamente por **Charles Monteiro Guimarães**, **Diretor**, em 12/09/2024, às 14:42, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Manuelito de Sousa Reis Junior**, **Gerente**, em 12/09/2024, às 14:45, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Marco Antonio de Andrade**, **Assessor Chefe**, em 12/09/2024, às 15:04, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Isabela Reboucas Costa**, **Analista de Sistemas**, em 12/09/2024, às 15:19, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Fabio Ivo**, **Assistente**, em 12/09/2024, às 15:19, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Monique Goncalves Paz**, **Diretora**, em 12/09/2024, às 15:21, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Rosana Alves de Andrade**, **Analista de Sistemas**, em 12/09/2024, às 15:45, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **83089515** e o código CRC **D85E63ED**.

Referência: Processo nº SEI-430002/000045/2024 SEI nº 83089515

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone:

ANEXO XI DO TERMO DE REFERÊNCIA

MODELO DE DECLARAÇÃO DE SUSTENTABILIDADE AMBIENTAL

(ESTE ANEXO DEVE SER INTERPRETADO CONFORME AS DISPOSIÇÕES DO TERMO DE REFERÊNCIA DO QUAL É PARTE INTEGRANTE E INDISSOCIÁVEL)

DECLARAÇÃO DE NÃO UTILIZAÇÃO DE PRODUTOS PERIGOSOS E ADERÊNCIA AOS REQUISITOS DE SUSTENTABILIDADE AMBIENTAL

Atestamos, para fins de comprovação junto à COMISSÃO DE LICITAÇÃO – [ÓRGÃO] relativamente ao Edital n°_/2024 a empresa [NOME DA EMPRESA], CNPJ_, não emprega substâncias perigosas em seus produtos e prestação de serviços, de acordo com as exigências do Edital.

[CIDADE],_de_de_.

Representante do Fornecedor:

Nome (*): RG:_CPF:

Representante da Empresa

/ Carimbo

(*) Apresentar ato constitutivo que subscreva a pessoa a representar o fabricante.

Rio de Janeiro, 09 de julho de 2024

Documento assinado eletronicamente por **Charles Monteiro Guimarães**, **Diretor**, em 12/09/2024, às 14:42, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Manuelito de Sousa Reis Junior**, **Gerente**, em 12/09/2024, às 14:46, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Marco Antonio de Andrade**, **Assessor Chefe**, em 12/09/2024, às 15:04, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Fabio Ivo**, **Assistente**, em 12/09/2024, às 15:19, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Isabela Reboucas Costa**, **Analista de Sistemas**, em 12/09/2024, às 15:19, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Monique Goncalves Paz**, **Diretora**, em 12/09/2024, às 15:21, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Rosana Alves de Andrade**, **Analista de Sistemas**, em 12/09/2024, às 15:44, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **83089517** e o código CRC **399A768E**.

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone:

CRONOGRAMA FINANCEIRO

Prazo Contratual	Quatidades	Junho	Julho	Agosto	Total Ano
Exercício 2025					
EQUIPAMENTOS					
APPLIANCE FIREWALL TIPO 1 - INCLUSOS: HARDWARE, LICENCIAMENTO E GARANTIA POR 60 MESES	4		R$ 24.360.000,00		
CONSOLE DE GERENCIAMENTO CENTRALIZADO PARA O FIREWALL TIPO 1 COM GARANTIA DE 60 MESES	2		R$ 148.000,00		
CONSOLE DE GERENCIAMENTO DE LOGS PARA O FIREWALL TIPO 1 COM GARANTIA DE 60 MESES	2		R$ 148.000,00		
CONSOLE DE RELATORIA CENTRALIZADA PARA O FIREWALL TIPO 1 COM GARANTIA DE 60 MESES	2		R$ 148.000,00		
APPLIANCE FIREWALL TIPO 3 - INCLUSOS: HARDWARE, LICENCIAMENTO E GARANTIA POR 60 MESES	12		R$ 2.452.125,00		
SERVIÇO					
SERVIÇO DE TREINAMENTO OPERACIONAL PARA A SOLUÇÃO	13 Alunos			R$ 71.500,00	
Total		R$ 0,00	R$ 27.256.125,00	R$ 71.500,00	R$ 27.327.625,00

CRONOGRAMA EXECUTIVO (ESTIMATIVA MÁXIMA)

	30	60	90
PERÍODO DE ENTREGA DOS EQUIPAMENTOS			
INSTALAÇÃO E CONFIGURAÇÃO DOS EQUIPAMENTOS			
MIGRAÇÃO E CRIAÇÃO DAS REGRAS DO FIREWALL			
SERVIÇO DE TREINAMENTO OPERACIONAL PARA A SOLUÇÃO			
PERÍODO DE TESTES			

Ricardo Batista de Moreira
Chefe do Departamento Suporte, Infraestrutura e Segurança da Informação
GTI-7 - CEDAE

Art. 2º - As designações dos candidatos para as vagas objetivam atender à necessidade da Procuradoria Geral do Estado. A não-apresentação dos documentos exigidos para a admissão, a recusa do candidato em aceitar a designação ou o não-comparecimento na data marcada pela Coordenadoria de Estágio tornará sem efeito a admissão, nos termos da Resolução PGE nº 1159/96.

Art. 3º - Esta Portaria entra em vigor na data de sua publicação, sendo as admissões consideradas realizadas na data da assinatura dos respectivos Termos de Compromisso, respeitada a validade neles indicada.

Rio de Janeiro, 23 de maio de 2025

RODRIGO DE ALMEIDA TÁVORA
Procurador-Assistente do Centro de Estudos Jurídicos
da Procuradoria Geral do Estado

Id: 2649635

PROCURADORIA GERAL DO ESTADO
CENTRO DE ESTUDOS JURÍDICOS

ATO DO PROCURADOR-ASSISTENTE

PORTARIA CEJUR/PGE Nº 843 DE 23 DE MAIO DE 2025

ADMITE ESTAGIÁRIOS DE DIREITO NA PROCURADORIA GERAL DO ESTADO.

O PROCURADOR-ASSISTENTE DO CENTRO DE ESTUDOS JURÍDICOS, no uso de suas atribuições legais e nos termos da delegação estabelecida pela Resolução PGE nº 3.723, de 02 de março de 2015,

RESOLVE:

Art. 1º - Admitir os candidatos abaixo relacionados, aprovados em Exame de Seleção a que se submeteram, para admissão no Estágio de Prática Forense e Organização Judiciária da Procuradoria Geral do Estado. As admissões em causa, com fundamento nos Decretos n°s 20.855, de 18.11.94; 22.304, de 27.06.96, e 25.999, de 28.01.2000 e nas Resoluções PGE n°s 1.159, de 06.05.96, 4.922, de 09.02.2023, 5.021, de 14.12.2023, 5.092, de 12.06.2024, e 5.165, de 09.01.2025, serão consideradas efetuadas na data da assinatura dos respectivos Termos de Compromisso, respeitada a validade neles indicada. Processo nº SEI-140001/018290/2020.

SEDE:
ANTONIO VITOR MIGUEZ DA TRINDADE
ARIADNE FERNANDA ALVES DA SILVA
ARTHUR RIBEIRO SENOS
BERNARDO MONTECHIARI TAVARES
BIANCA PEREIRA MARINATO
BRENDA GONZALEZ ALVAREZ
CLARA MOREIRA MARQUES
CRISTIANO REIS GONCALVES PEREIRA
DANIELA CHAVES AFONSO
DIOGO AMORIM VALENTE CARDOSO
DIOGO ARLIQUE DA SILVA COSTA
ELIDA PEREIRA CARDEAL
ESTHER OLIVEIRA DA SILVA
GABRIEL DO NASCIMENTO TEIXEIRA
GABRIEL MARCHIORI PIRES LOPES DA COSTA
GABRIELA LIMA CARNEIRO
JULIANA BASTOS DE OLIVEIRA
LAIS COSTA BARBOSA
LAYSE SANTOS DA SILVA
LEONARDO GOMES QUIRINO CAMARA
LETICIA PESSOA CARDOSO
LUIS BERNARDO BASTOS DOS SANTOS
MARIA DE MEDEIROS PALHARES
MARIA EDUARDA MEDEIROS MEDRADO
MAYARA LOPES DE MELO
NATALIA NUNES DOS SANTOS
PAULO ANDERSON DE AZEVEDO LIMA
PEDRO GIOIA PRADO UCHOA
RAFAEL FUCCINI NOBREGA DE ASSIS
REBECA SANT ANNA DOS SANTOS
RENAN CABRAL GUIMARAES
RODRIGO TEIXEIRA DE AS
SARA GRAZIELI CANDIDO DA SILVA
THIAGO ASSUMPCAO FALHEIRO
TIAGO PAULO ALVES DE OLIVEIRA

6ª PR - ANGRA DOS REIS:
VIVIANE RAMOS LEAO PONTES

Art. 2º - As designações dos candidatos para as vagas existentes objetivam atender às necessidades da Procuradoria Geral do Estado. A não-apresentação dos documentos exigidos para a admissão, a recusa do candidato em aceitar a designação ou o não-comparecimento na data marcada pela Coordenadoria de Estágio tornará sem efeito a admissão, nos termos do art. 9º da Resolução PGE n.º 1.159/96.

Art. 3º - O candidato convocado para a Procuradoria Regional assinará o Termo de Compromisso no local correspondente à sua designação.

Art. 4º - Esta Portaria entra em vigor na data de sua publicação, sendo as admissões consideradas realizadas na data da assinatura dos respectivos Termos de Compromisso, respeitada a validade neles indicada.

Rio de Janeiro, 23 de maio de 2025

RODRIGO DE ALMEIDA TÁVORA
Procurador-Assistente do Centro de Estudos Jurídicos
da Procuradoria Geral do Estado

Id: 2649636

AVISOS, EDITAIS E TERMOS DE CONTRATOS

Secretaria de Estado da Casa Civil

SECRETARIA DE ESTADO DA CASA CIVIL
COMISSÃO DE PREGÃO ELETRÔNICO

AVISO

A COMISSÃO DE PREGÃO ELETRÔNICO DA SECRETARIA DE ESTADO DA CASA CIVIL torna público que fará realizar a seguinte licitação:

PREGÃO ELETRÔNICO: PE 10/2025.
OBJETO: Aquisição com instalação de 02 (dois) transmissores e desinstalação dos equipamentos antigos da Rádio Roquette-Pinto, conforme detalhamento no Termo de Referência - ANEXO I.
DATA LIMITE DE ACOLHIMENTO DAS PROPOSTAS: 11/06/2025, às 10h50.
DATA/HORA DE INÍCIO DA DISPUTA DE PREÇOS: 11/06/2025, às 11h00.
PROCESSO ELETRÔNICO: SEI-150001/000755/2024.
ENDEREÇO ELETRÔNICO: https://www.compras.rj.gov.br.

O edital e seus anexos poderão ser obtidos, no endereço eletrônico www.compras.rj.gov.br, e no portal eletrônico da Secretaria de Estado da Casa Civil - https://www.rj.gov.br/casacivil/pregao.

Outras informações sobre a presente licitação através do telefone 2334.3341 ou pelo e-mail licitacao@casacivil.rj.gov.br.

Id: 2649788

ADMINISTRAÇÃO VINCULADA

SECRETARIA DE ESTADO DA CASA CIVIL
COMPANHIA ESTADUAL DE ÁGUAS E ESGOTOS

EXTRATO DE INSTRUMENTO CONTRATUAL

INSTRUMENTO: Contrato CEDAE nº 053/2025 (DPR).
PARTES: A COMPANHIA ESTADUAL DE ÁGUAS E ESGOTOS - CEDAE e a VIVA RIO.
OBJETO: ESPAÇO-ESCOLA VIVA DE SERVIÇOS SOCIOAMBIENTAIS PARA POPULAÇÃO EM SITUAÇÃO DE RUA: RESÍDUOS E AGROECOLOGIA.
PRAZO: 09 (nove) meses.
VALOR TOTAL: R$ 150.000,00 (cento e cinquenta mil reais).
DATA DE ASSINATURA: 22/05/2025.
FUNDAMENTO: Processo nº SEI-150017/002553/2024.

Id: 2649624

SECRETARIA DE ESTADO DA CASA CIVIL
COMPANHIA ESTADUAL DE ÁGUAS E ESGOTOS

EXTRATO DE INSTRUMENTO CONTRATUAL

INSTRUMENTO: Contrato CEDAE nº 054/2025 (DPR).
PARTES: A COMPANHIA ESTADUAL DE ÁGUAS E ESGOTOS - CEDAE e o INSTITUTO DE PROJETOS SOCIOAMBIENTAIS.
OBJETO: COLETIVO MULHERES DE GUAXINDIBA.
PRAZO: 08 (oito) meses.
VALOR TOTAL: R$ 150.000,00 (cento e cinquenta mil reais).
DATA DE ASSINATURA: 12/05/2025.
FUNDAMENTO: Processo nº SEI-150017/002553/2024.

Id: 2649625

SECRETARIA DE ESTADO DA CASA CIVIL
COMPANHIA ESTADUAL DE ÁGUAS E ESGOTOS

EXTRATO DE INSTRUMENTO CONTRATUAL

INSTRUMENTO: Contrato CEDAE nº 055/2025 (DPR).
PARTES: A COMPANHIA ESTADUAL DE ÁGUAS E ESGOTOS - CEDAE e o GRUPO ARTÍSTICO E CULTURAL ARTEIROS.
OBJETO: CDD VERDE - Socioambiental do Instituto Arteiros.
PRAZO: 12 (doze) meses.
VALOR TOTAL: R$ 150.000,00 (cento e cinquenta mil reais).
DATA DE ASSINATURA: 22/05/2025.
FUNDAMENTO: Processo nº SEI-150017/002553/2024.

Id: 2649626

SECRETARIA DE ESTADO DA CASA CIVIL
COMPANHIA ESTADUAL DE ÁGUAS E ESGOTOS

EXTRATO DE INSTRUMENTO CONTRATUAL

INSTRUMENTO: Contrato CEDAE nº 056/2025 (DPR).
PARTES: A COMPANHIA ESTADUAL DE ÁGUAS E ESGOTOS - CEDAE e o INSTITUTO ONDA AZUL.
OBJETO: SustentAção.
PRAZO: 12 (doze) meses.
VALOR TOTAL: R$ 150.000,00 (cento e cinquenta mil reais).
DATA DE ASSINATURA: 22/05/2025.
FUNDAMENTO: Processo nº SEI-150017/002553/2024.

Id: 2649627

SECRETARIA DE ESTADO DA CASA CIVIL
COMPANHIA ESTADUAL DE ÁGUAS E ESGOTOS

EXTRATO DE INSTRUMENTO CONTRATUAL

INSTRUMENTO: Contrato CEDAE nº 061/2025 (DPR).
PARTES: A COMPANHIA ESTADUAL DE ÁGUAS E ESGOTOS - CEDAE e a ASSOCIAÇÃO DO DESENVOLVIMENTO INTEGRAL E DA JUSTIÇA SOCIAL.
OBJETO: PROGRAMA DE INCLUSÃO PRODUTIVA.
PRAZO: 08 (oito) meses.
VALOR TOTAL: R$ 80.000,00 (oitenta mil reais).
DATA DE ASSINATURA: 22/05/2025.
FUNDAMENTO: Processo nº SEI-150017/002553/2024.

Id: 2649628

SECRETARIA DE ESTADO DA CASA CIVIL
COMPANHIA ESTADUAL DE ÁGUAS E ESGOTOS

EXTRATO DE INSTRUMENTO CONTRATUAL

INSTRUMENTO: Contrato CEDAE nº 079/2025 (DFI).
PARTES: A COMPANHIA ESTADUAL DE ÁGUAS E ESGOTOS - CEDAE e a 2R DATATEL TELEINFORMÁTICA LTDA.
OBJETO: Contratação de empresa do ramo de tecnologia da informação para o fornecimento de solução de firewall, com garantia de 60 meses, contemplando hardware e software, com instalação e configuração, nas dependências do contratante e curso de treinamento oficial da solução.
PRAZO: 90 (noventa) dias.
VALOR TOTAL: R$ 27.327.625,00 (vinte e sete milhões, trezentos e vinte e sete mil, seiscentos e vinte e cinco reais).
DATA DE ASSINATURA: 21/05/2025.
FUNDAMENTO: Processo nº SEI-150017/008939/2024 (ATA DE REGISTRO DE PREÇOS N. 007/2024 DO PRODERJ).

Id: 2649629

SECRETARIA DE ESTADO DA CASA CIVIL
COMPANHIA ESTADUAL DE ÁGUAS E ESGOTOS

EXTRATO DE INSTRUMENTO CONTRATUAL

INSTRUMENTO: Contrato CEDAE nº 057/2025 (DPR).
PARTES: A COMPANHIA ESTADUAL DE ÁGUAS E ESGOTOS - CEDAE e o CENTRO DE ASSESSORIA AO MOVIMENTO POPULAR-CAMPO.
OBJETO: Empoderando o Ciclo: Autonomia Menstrual e Sustentabilidade no Mineiro-Pau.
PRAZO: 12 (doze) meses.
VALOR TOTAL: R$ 148.125,00 (cento e quarenta e oito mil, cento e vinte e cinco reais).
DATA DE ASSINATURA: 22/05/2025.
FUNDAMENTO: Processo nº SEI-150017/002553/2024.

Id: 2649713

SECRETARIA DE ESTADO DA CASA CIVIL
COMPANHIA ESTADUAL DE ÁGUAS E ESGOTOS

EXTRATO DE INSTRUMENTO CONTRATUAL

INSTRUMENTO: Contrato CEDAE nº 059/2025 (DPR).
PARTES: A COMPANHIA ESTADUAL DE ÁGUAS E ESGOTOS - CEDAE e o INSTITUTO META EDUCAÇÃO.
OBJETO: TEATRO PARA ELAS 45+.
PRAZO: 12 (doze) meses.
VALOR TOTAL: R$ 79.110,00 (setenta e nove mil, cento e dez reais).
DATA DE ASSINATURA: 22/05/2025.
FUNDAMENTO: Processo nº SEI-150017/002553/2024.

Id: 2649714

SECRETARIA DE ESTADO DA CASA CIVIL
COMPANHIA ESTADUAL DE ÁGUAS E ESGOTOS

EXTRATO DE INSTRUMENTO CONTRATUAL

INSTRUMENTO: Contrato CEDAE nº 060/2025 (DPR).
PARTES: A COMPANHIA ESTADUAL DE ÁGUAS E ESGOTOS - CEDAE e a ASSOCIAÇÃO EXPERIMENTAL DE MÍDIA COMUNITÁRIA.
OBJETO: JOVENS COMUNICADORAS - A COMUNICAÇÃO PARA A IGUALDADE DE GÊNERO.
PRAZO: 08 (oito) meses.
VALOR TOTAL: R$ 79.750,00 (setenta e nove mil, setecentos e cinquenta reais).
DATA DE ASSINATURA: 22/05/2025.
FUNDAMENTO: Processo nº SEI-150017/002553/2024.

Id: 2649715

SECRETARIA DE ESTADO DA CASA CIVIL
COMPANHIA ESTADUAL DE ÁGUAS E ESGOTOS

EXTRATO DE INSTRUMENTO CONTRATUAL

INSTRUMENTO: Contrato CEDAE nº 067/2025 (DFI).
PARTES: A COMPANHIA ESTADUAL DE ÁGUAS E ESGOTOS - CEDAE e a CS BRASIL FROTAS S.A.
OBJETO: Prestação, por empresa especializada, do serviço de locação de veículos de serviço e de representação híbridos, sem fornecimento de condutores ou combustível, para atender às necessidades dos Órgãos do Estado do Rio de Janeiro.
PRAZO: 36 (trinta e seis) meses.
VALOR TOTAL: R$ 6.664.622,40 (seis milhões, seiscentos e sessenta e quatro mil, seiscentos e vinte e dois reais e quarenta centavos).
DATA DE ASSINATURA: 22/05/2025.
FUNDAMENTO: Processo nº SEI-150017/001628/2025 (ATA DE REGISTRO DE PREÇOS N. 04/2024 decorrente do PREGÃO ELETRÔNICO PARA REGISTRO DE PREÇOS N° PERP 01/2024, realizado pela SEPLAG).

Id: 2649716

SECRETARIA DE ESTADO DA CASA CIVIL
COMPANHIA ESTADUAL DE ÁGUAS E ESGOTOS

EXTRATO DE INSTRUMENTO CONTRATUAL

INSTRUMENTO: Contrato CEDAE nº 058/2025 (DPR).
PARTES: A COMPANHIA ESTADUAL DE ÁGUAS E ESGOTOS - CEDAE e o MOVIMENTO DE MULHERES EM SÃO GONÇALO.
OBJETO: João Pedro VIVE - JP VIVE.
PRAZO: 12 (doze) meses.
VALOR TOTAL: R$ 80.000,00 (oitenta mil reais).
DATA DE ASSINATURA: 22/05/2025.
FUNDAMENTO: Processo nº SEI-150017/002553/2024.

Id: 2649719

SECRETARIA DE ESTADO DA CASA CIVIL
COMPANHIA ESTADUAL DE ÁGUAS E ESGOTOS

EXTRATO DE TERMO

INSTRUMENTO: Termo CEDAE Nº 017/2025 de Distrato.
PARTES: A COMPANHIA ESTADUAL DE ÁGUAS E ESGOTOS - CEDAE e a FACTO TURISMO LTDA.
OBJETO: A Resilição do CONTRATO N. 097/2020 (DPR), celebrado para a "PRESTAÇÃO DOS SERVIÇOS DE AGENCIAMENTO DE VIAGENS, NA FORMA DO TERMO DE REFERÊNCIA (ANEXO I), PROPOSTA DA CONTRATADA, DA ATA DE REGISTRO DE PREÇOS E DO INSTRUMENTO CONVOCATÓRIO".
PRAZO: Sem prazo.
VALOR TOTAL: Sem valor.
DATA DE ASSINATURA: 23/05/2024.
FUNDAMENTO: Processo Nº SEI E-12/800.142/2019.

Id: 2649718

SECRETARIA DE ESTADO DA CASA CIVIL
COMPANHIA ESTADUAL DE ÁGUAS E ESGOTOS

EXTRATO DE TERMO ADITIVO
INSTRUMENTO: Aditivo nº 02 ao Contrato CEDAE nº 012/2023 (DTP).
PARTES: A COMPANHIA ESTADUAL DE ÁGUAS E ESGOTOS - CEDAE e a SCALLE CONSTRUÇÕES, REFORMAS E INSTALAÇÕES LTDA.
OBJETO: A renovação do prazo contratual e a alteração na razão social da CONTRATADA, de "NOLASCO CONSTRUÇÕES REFORMAS E INSTALAÇÕES LTDA." para "SCALLE CONSTRUÇÕES, REFORMAS E INSTALAÇÕES LTDA.
PRAZO: 12 (doze) meses.
VALOR TOTAL: R$ 27.310.658,19 (vinte e sete milhões, trezentos e dez mil, seiscentos e cinquenta e oito reais e dezenove centavos).
DATA DE ASSINATURA: 22/05/2025.
FUNDAMENTO: Processo nº SEI-150001/025453/2022 (Ata de Registro de Preços nº 011/2022).

Id: 2649717

DEPARTAMENTO DE TRÂNSITO DO ESTADO
DO RIO DE JANEIRO

EXTRATO DE INSTRUMENTO CONTRATUAL

INSTRUMENTO: Contrato de Prestação de Serviços nº 167/2025.
PARTES: DETRAN/RJ e Clima Air Reformas, Manutenção e Locação de Equipamentos Ltda.
OBJETO: Prestação de serviços de locação de aparelhos de ar condicionado e cortina de ar com instalação, desinstalação dos aparelhos existentes, que serão substituídos pelos do objeto, bem como a manutenção preventiva com elaboração de PMOC e manutenção corretiva, a serem executados nas condições estabelecidas no Termo de Referência e nos anexos do Contrato.
PRAZO: 12 (doze) meses, contados da divulgação no Portal Nacional de Contratações Públicas.
VALOR TOTAL ESTIMADO: R$ 6.059.286,90 (seis milhões, cinquenta e nove mil, duzentos e oitenta e seis reais e noventa centavos).
NOTA DE EMPENHO: 2025NE00946.
GESTORES: MARIANA ARAÚJO GOMES DE ALMEIDA, Diretora Geral de Engenharia, Id. Func. nº 4274291-9, será o Gestora do presente Contrato, Diretora Geral, Id. Func. nº 4274291-9, será a Gestora do contrato, ROZAN RODRIGUES PACHECO, Assistente III, Id. Func. nº 5161003-5, será o Gestor Substituto.
FISCAIS: VANESSA DA SILVA FLORES SOARES DE SOUZA, Chefe de Serviço, Id. Func. nº 4461240-0; PEDRO MONTENEGRO CARVALHO, Assistente III, Id. Func. nº 5132139-4; GABRIEL COUTINHO MACIEL MENDES, Assistente III, Id. Func. nº 5160903-7, como Fiscais e MARIA AMÉLIA MIRA VILELA, Chefe de Núcleo, Id. Func. nº 5160311-0, como substituta.
DATA DA ASSINATURA: 26/05/2025.
FUNDAMENTAÇÃO LEGAL: Lei Federal nº 14.133/21 e normativos estaduais aplicáveis, todos disponíveis no endereço eletrônico redelog.rj.gov.br/redelog/legislação-licitacoes.
PROCESSO ADMINISTRATIVO Nº SEI-150016/039723/2024

Id: 2649857

INSTITUTO DE PESOS E MEDIDAS DO ESTADO
DO RIO DE JANEIRO

EDITAL

O INSTITUTO DE PESOS E MEDIDAS DO ESTADO DO RIO DE JANEIRO - IPEM/RJ, ente delegado do INMETRO, no uso das suas atribuições legais, tendo em vista as infrutíferas tentativas, pelos usuais meios de comunicação (e-mail, fax e/ou correspondência postal), de agendamento para comparecimento e acompanhamento do procedimento pericial a ser realizado em seu laboratório, por meio do presente edital **NOTIFICA** os interessados abaixo relacionados para ciência da designação de data para realização do referido procedimento em estrita observância aos princípios do contraditório e da ampla defesa.
O procedimento pericial será realizado na data abaixo informada, na Regional do IPEM/RJ, localizada na Rua Professor Joaquim da Costa Ribeiro, 31, Centro, Niterói/RJ, e poderá ser acompanhado por representante legal da empresa, devidamente habilitado por procuração ou autorização nominal, ambas com finalidade específica ou, ainda, por contrato social e documento de identidade do sócio proprietário. Processo nº SEI-150014/000842/2025.