CONTRATO N.º 031/2026.

Contrato que entre si celebram a DAE S.A. - ÁGUA E ESGOTO e a empresa INTERQUATTRI INFORMÁTICA E TELECOMUNICAÇÕES LTDA., para aquisição de um Firewall de Próxima Geração (NGFW) de alto desempenho, capaz de proteger redes corporativas de grande escala contra ameaças cibernéticas avançadas, com serviço de instalação, treinamento, suporte técnico e manutenção.

Processo n.º 319/26

Pregão Eletrônico n.º 006/26

De um lado, a DAE S.A. - ÁGUA E ESGOTO sociedade de economia mista, com sede na Avenida Alexandre Ludke n.º 1.500 na Vila Bandeirantes no município de Jundiaí/SP., inscrita no CNPJ sob o n.º 03.582.243/0001-73, neste ato representada na forma de seu Estatuto Social, por seus diretores:, Diretor Presidente Daniel Bocalão Júnior, portador do R.G. [redacted] e do CPF/MF n.º 052.198.048-80, e a Diretora Superintendente de Gestão Helen Cappelleti de Lima, portadora do R.G. n.º [redacted] e do CPF/MF n.º 259.583.418-55, doravante denominada simplesmente CONTRATANTE e, de outro lado, a empresa INTERQUATTRI INFORMÁTICA E TELECOMUNICAÇÕES LTDA., localizada na Rua Rafael Andrade Duarte n.º 441 - Bairro Nova Campinas no município de Campinas-SP., inscrita no CNPJ sob n.º 05.213.235/0001-85 e inscrição estadual n.º 244.915.024.110, doravante denominada simplesmente CONTRATADA, neste ato representada por seus diretores:, Diretor Comercial Afranio Silva Gomide, portador do R.G. n.º [redacted] -SSP/SP e do CPF/MF n.º 554.972.338-72, e o Diretor Financeiro Cláudio Cesar Grande, portador do R.G. [redacted] e do CPF/MF n.º 042.487.268-40, de acordo com os atos e documentos contidos no processo administrativo n.º 319-7/2026 têm entre si justo e acertado o presente contrato, nos termos do que determinam a Lei Federal n.º 13.303, de 30 de junho de 2016 e alterações posteriores, o Regulamento Interno de Licitações, Contratos e Convênios da DAE S.A. e demais normas aplicáveis a este objeto, mediante cláusulas e condições a seguir enunciadas:

CLÁUSULA PRIMEIRA - OBJETO

1.1. Constitui objeto do presente contrato a aquisição de um Firewall de Próxima Geração (NGFW) de alto desempenho, capaz de proteger redes corporativas de grande escala contra ameaças cibernéticas avançadas, com serviço de instalação, treinamento, suporte técnico e manutenção, conforme exigências e especificações técnicas descritas no respectivo Edital e seus anexos.

1.2. Para melhor caracterização da presente avença, bem como definir os procedimentos decorrentes das obrigações do contrato, o edital de 13 de fevereiro de 2026 - Pregão Eletrônico n.º 006/2026, bem como a proposta da CONTRATADA, insertos às fls. 51/82 e 152/153, respectivamente, do processo administrativo n.º 319-7/2026.

CLÁUSULA SEGUNDA - OBRIGAÇÕES DA CONTRATADA

2.1. São obrigações da CONTRATADA, além de outras fixadas neste contrato, no Termo de Referência e no respectivo Edital, as seguintes:

2.1.1. Todas as despesas de impostos, fretes, seguros, e outros custos que recaiam sobre o fornecimento ou serviços objeto do presente contrato.

2.1.2. Nomear um preposto responsável pelo contrato para atendimento e entendimentos junto a CONTRATANTE.

2.1.3. Não divulgar quaisquer informações a que tenha acesso em virtude dos serviços ou fornecimento a serem executados ou de que tenha tomado conhecimento em decorrência da execução do objeto, sem autorização, por escrito, da CONTRATANTE, sob pena de aplicação das sanções cabíveis.

2.1.4. Não transferir a terceiros, por qualquer meio ou forma, nem mesmo parcialmente, as obrigações assumidas neste instrumento, exceto se prévia e expressamente autorizada pela CONTRATANTE, no Termo de Referência ou Edital.

2.1.5. Assegurar o cumprimento dos prazos estabelecidos para todos os serviços ou fornecimentos decorrentes do presente contrato.

2.1.6. A CONTRATADA é obrigada a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados, e responderá por danos causados diretamente a terceiros ou à empresa pública ou sociedade de economia mista, independentemente da comprovação de sua culpa ou dolo na execução do contrato.

2.1.7. 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.

2.1.8. Ser interlocutor em caso de necessidade com o fabricante do produto fornecido.

2.1.9. Cumprir e fazer cumprir todas as normas e legislações aplicáveis ao objeto contratado.

2.2. A CONTRATADA responderá por todos os danos, inclusive materiais, lucros cessantes e danos a terceiros advindos da execução do presente instrumento, devendo ressarcir a CONTRATANTE.

2.3. Fornecer os equipamentos conforme especificações técnicas constantes da sua proposta comercial, nos prazos constantes no Termo de Referência e no local, prazos e quantidades discriminadas.

2.3.1. O serviço de instalação deverá seguir, obrigatoriamente, as normas regulamentares do fabricante.

2.4. A responsabilidade de transporte de qualquer natureza, materiais empregados, inclusive ferramentas, utensílios e equipamentos utilizados direta ou indiretamente na execução do contrato, correrão por conta da CONTRATADA. O transporte do objeto até o local de entrega especificado em contrato, incluindo operação de carga, deverá ser providenciado e pago pela CONTRATADA.

2.5. A DAE S.A. poderá rejeitar, no todo ou em parte, quaisquer bens que não tenham sido aprovados em qualquer das inspeções e/ou testes, ou não estejam em conformidade com as especificações. O contratado deverá retificar ou substituir os bens rejeitados ou suas partes rejeitadas, ou fazer as modificações necessárias para o cumprimento das especificações sem custos para a DAE S.A., bem como deverá, após dar a notificação, repetir as inspeções e/ou testes sem custos para a CONTRATANTE. O contratado concorda que nem a realização das inspeções e/ou testes no objeto ou em partes dele; nem a participação da DAE S.A.; liberará a CONTRATADA de quaisquer garantias ou outras obrigações acordadas no contrato.

2.6. Ciente dos termos, disposições e penalidades constantes do Código de Conduta e Integridade da DAE S.A. - Água e Esgoto, conforme declaração apresentada na fase habilitatória, é obrigação da CONTRATADA cumpri-lo integralmente, naquilo que lhe for aplicável, sob pena de aplicação das sanções nele previstas.

CLÁUSULA TERCEIRA - OBRIGAÇÕES DA CONTRATANTE

3.1. São obrigações da CONTRATANTE, além de outras fixadas neste contrato e no respectivo Edital, as seguintes:

3.1.1. Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com as cláusulas contratuais e os termos de sua proposta.

3.1.2. Exercer o acompanhamento e a fiscalização dos serviços, por funcionário(s) especialmente designado(s), e encaminhando os apontamentos à autoridade competente para as providências cabíveis.

3.1.3. Notificar por escrito, à CONTRATADA, quaisquer irregularidades encontradas na execução dos serviços.

3.1.4. Pagar à CONTRATADA o valor resultante da prestação do serviço/ fornecimento, no prazo e condições estabelecidas no Edital e seus anexos.

3.1.5. Efetuar as retenções tributárias devidas sobre o valor da Nota Fiscal/Fatura emitida pela CONTRATADA.

3.1.6. Designar, formalmente, Gestor(es) para acompanhar e fiscalizar a execução do contrato.

CLÁUSULA QUARTA - DOS PRAZOS E DA EXECUÇÃO

4.1. A entrega do material, quando solicitada, correrá por conta e risco da CONTRATADA, e será procedida de acordo com as necessidades do órgão requisitante e/ou condições estipuladas no Edital.

4.2. Os trabalhos serão realizados na sede da DAE S.A. no seguinte endereço: Avenida Alexandre Ludke n.º 1.500 na Vila Bandeirantes - Terceiro andar - Jundiaí - SP.

4.3. A **entrega deverá ser efetuada em até 90 (noventa) dias após a assinatura do contrato**. Nos casos em que não houver a elaboração de contrato, o prazo contará da emissão da Ordem de Compras pela DAE, nos mesmos termos do contrato.

4.3.1. A entrega deverá ser agendada com antecedência mínima de 24 horas, sob o risco de não ser autorizada.

4.3.2. Os serviços de instalação devem ser iniciados em, no máximo, 15 (quinze) dias corridos da entrega do equipamento e agendados com antecedência mínima de 3 dias, sob o risco de não ser autorizado; o prazo para finalização da instalação é 45 (quarenta e cinco) dias corridos;

4.3.3. Para itens de software, estes devem ser fornecidos com ou sem mídia de instalação. No caso de não fornecimento de mídia, deve ser indicado local para download da instalação;

4.3.4. Para itens de software, devem ser apresentados chave única tipo serial ou qualquer outra forma de validação da ferramenta, comprovando perante o fabricante que se trata de uma ferramenta devidamente licenciada.

4.4. Caso o objeto seja entregue / realizado em desacordo com os requisitos estabelecidos pela CONTRATANTE, a CONTRATADA obriga-se a reparar a falha e/ou, se houver necessidade, providenciar sua substituição em prazo convencionado entre as partes, sem quaisquer ônus para a CONTRATANTE, independentemente da aplicação das sanções cabíveis.

4.5. No caso de fornecimento, o objeto entregue pela CONTRATADA deverá estar acompanhado de Nota Fiscal - 02 (duas) vias ou DANFE no caso de Nota Fiscal Eletrônica.

CLÁUSULA QUINTA - ALTERAÇÃO CONTRATUAL

5.1. Qualquer alteração no presente contrato deverá observar o disposto no art. 72 e 81, da Lei Federal n.º 13.303/16 e procedimentos do Regulamento Interno de Licitações, Contratos e Convênios da DAE S.A.

5.1.1. Conforme parágrafo 8º do artigo 81 da Lei Federal n.º 13.303/2016, é vedada a celebração de aditivos decorrentes de eventos supervenientes alocados, na matriz de riscos, como de responsabilidade da CONTRATADA.

CLÁUSULA SEXTA - PREÇO E CONDIÇÕES DE PAGAMENTO

6.1. Dá-se à presente contratação o valor total de **R$ 668.053,00 (seiscentos e sessenta e oito mil, e cinquenta e três reais)**

6.2. No preço total referido na cláusula anterior, já estão inclusos todos os tributos incidentes.

6.3. O pagamento será efetuado em 14 (catorze) dias após a entrega, mediante a apresentação da Nota Fiscal/Fatura competente, devidamente assinada e vistada pelo órgão interessado, comprovando o recebimento dos produtos.

6.3.1. Em caso de atraso no pagamento efetuado pela CONTRATANTE, da fatura apresentada pela CONTRATADA, esta pode ter atualização do respectivo valor utilizando-se o INPC - Índice Nacional de Preços ao Consumidor.

6.4. Fica expressamente vedada qualquer pretensão de pagamento antecipado.

6.5. A CONTRATANTE efetuará os pagamentos, por meio de boleto bancário, que será enviado junto com a fatura, ou via depósito bancário em conta corrente de titularidade da CONTRATADA, informada na sua proposta de preço.

6.6. Na hipótese de o vencimento da fatura/boleto bancário recair em sábado, domingo ou feriado, o vencimento será prorrogado para o primeiro dia útil subsequente, sem a imposição de qualquer ônus à CONTRATANTE.

6.7. A Nota Fiscal da CONTRATADA deverá ser enviada à CONTRATANTE com a indicação do número do contrato, do processo e das parcelas de pagamento, destacando-se, caso haja, o Imposto de Renda Retido na Fonte, ISS, PIS, COFINS, CSLL e demais impostos inerentes ao objeto deste contrato com estrita observância das disposições legais vigentes, responsabilizando-se a CONTRATADA, assim, por eventuais sanções que possam ser impostas à CONTRATANTE caso deixe de descontar e destacar em sua fatura impostos e contribuições sociais que devessem ser retidos na fonte e recolhidos pela CONTRATANTE.

6.8. Em caso de emissão de Nota Fiscal eletrônica, a mesma deverá ser endereçada exclusivamente ao e-mail: **nfe@daejundiai.com.br**, bem como o respectivo arquivo XML.

6.9. A emissão das Notas Fiscais eletrônicas não desobriga a CONTRATADA de entregar ao gestor responsável da CONTRATANTE os demais documentos exigidos em contrato.

6.10. A Nota Fiscal/Fatura não aprovada será devolvida para as correções necessárias, com as informações que motivaram sua rejeição, contando-se o prazo estabelecido o item 6.4 a partir da data de sua reapresentação.

6.11. Do valor das faturas apresentadas para pagamento, poderão ser deduzidas, de pleno direito pela CONTRATANTE as seguintes verbas:

I- Multas previstas no presente ajuste;

II- As multas, indenizações ou despesas devidas por ato de autoridade competente, em decorrência do descumprimento, pela CONTRATADA, de leis ou regulamentos aplicáveis à espécie; e

III- Cobranças indevidas.

6.12. A CONTRATADA deverá abster-se de emitir títulos de quaisquer naturezas lastreados no presente contrato, ficando expressamente vedada a emissão e negociação destes títulos perante instituições financeiras ou afins, regulares ou não, devendo responder diretamente pelas eventuais perdas e danos decorrentes da inobservância desta cláusula.

CLÁUSULA SÉTIMA - CONDIÇÕES PARA A CONTRATAÇÃO

7.1. A CONTRATADA exibe neste ato as certidões expedidas pela Justiça do Trabalho - CNDT, Receita Federal/PGFN - Certidão de Débitos da União e Certificado de Regularidade com FGTS emitido pela Caixa Econômica Federal - CRF, com prazo de validade em vigor, que demonstrem sua regularidade no cumprimento dos encargos estabelecidos em lei, obrigando-se a atualizá-las sempre que se vencerem no prazo de execução deste contrato, demonstrando a manutenção das condições de habilitação e qualificação exigidas no certame que originou a presente avença.

CLÁUSULA OITAVA - ENCARGOS

8.1. Os encargos trabalhistas, previdenciários, fiscais, comerciais, de transportes e seguro, inclusive aqueles relativos a impostos e taxas, inclusive de administração, são de inteira responsabilidade da CONTRATADA, bem como despesas e obrigações financeiras de qualquer natureza, despesas operacionais com frete e entrega, o valor dos materiais, matérias-primas, mão-de-obra, inclusive horas extras e adicionais noturnos de profissionais, auxílio alimentação, auxílio transporte e

transporte local, sendo que sua inadimplência, com relação a tais encargos, não transfere a CONTRATANTE o ônus pelo seu pagamento, não podendo onerar a presente avença.

CLÁUSULA NONA - PENALIDADES

9.1. Pelo cometimento de quaisquer infrações previstas no Regulamento Interno de Licitações, Contratos e Convênios da DAE S.A. e a inexecução parcial ou total do contrato a CONTRATANTE, poderá, garantida a prévia defesa, aplicar à CONTRATADA as seguintes sanções:

I- Advertência por escrito;

II- Multa moratória, por atraso injustificado, no percentual de até 0,5% (cinco décimos por cento) sobre o valor da parcela descumprida, por dia corrido de atraso, até que se efetive o cumprimento do ajuste, limitado a 10% (dez por cento) do valor citado.

III- Multa compensatória, no percentual descrito abaixo:

a- até 10% (dez por cento) do valor global do contrato, pela inexecução parcial dos serviços ou sobre a parcela inadimplida, se o descumprimento for parcial;

b- até 20% (vinte por cento) do valor global do contrato, pela inexecução total, motivando a rescisão do ajuste.

IV- Suspensão do direito de participar de licitação e impedimento de contratar com a DAE S.A., por até 02 (dois) anos.

§ 1º. A inexecução total ou parcial do contrato poderá ensejar a sua rescisão, com as consequências cabíveis.

§ 2º. As sanções previstas nos incisos I e III deste dispositivo poderão ser aplicadas juntamente com a do inciso II.

§ 3º. São consideradas situações caracterizadoras de descumprimento total ou parcial das obrigações contratuais:

I- Não atendimento às especificações técnicas relativas aos bens, serviços ou obra prevista em contrato ou instrumento equivalente;

II- Retardamento imotivado de fornecimento de bens, da execução de obra, de serviço ou de suas parcelas;

III- Paralisação do serviço ou de fornecimento de bens, sem justa causa e prévia comunicação à DAE S.A.;

IV- Entrega de mercadoria falsificada, furtada, deteriorada, danificada ou inadequada para o uso, como se verdadeira ou perfeita fosse;

V- Alteração de substância, qualidade ou quantidade da mercadoria fornecida;

VI- Prestação de serviço de baixa qualidade.

§ 4º. A sanção de multa poderá ser aplicada cumulativamente às demais sanções previstas nesta cláusula.

§ 5º. A multa poderá ser descontada da garantia do contrato e/ou de pagamentos eventualmente devidos pela CONTRATADA.

CLÁUSULA DEZ - RESCISÃO CONTRATUAL

10.1. O presente contrato poderá ser rescindido de pleno direito pela CONTRATANTE, garantida a prévia defesa e o contraditório, na ocorrência de falhas reiteradas e não corrigidas, que demonstrem a falta de qualidade do produto ofertado ou de compromisso da CONTRATADA, na inexecução total do ajuste, na infração de qualquer cláusula do presente contrato, bem como na falta de manutenção das condições de habilitação e qualificação exigidas para a licitação, sem prejuízo da aplicação das sanções previstas neste contrato.

10.2 A rescisão do contrato, conforme artigo 173 do Regulamento Interno de Licitações Contratos e Convênios da DAE, poderá ser:

I- Por ato unilateral e escrito de qualquer das partes;
II- Amigável, por acordo entre as partes, reduzida a termo no processo de contratação, desde que haja conveniência para a DAE;
III- Judicial, nos termos da legislação.

§ 1°. A rescisão por ato unilateral a que se refere o inciso I deste item, deverá ser precedida de comunicação escrita e fundamentada da parte interessada e ser enviada à outra parte com antecedência mínima de 30 (trinta) dias.

§ 2°. Na hipótese de imprescindibilidade da execução contratual para a continuidade de serviços públicos essenciais, o prazo a que se refere o **§ 1°** será de 90 (noventa) dias.

§ 3°. Quando a rescisão ocorrer sem que haja culpa da outra parte CONTRATANTE, será esta ressarcida dos prejuízos que houver sofrido, regularmente comprovados, e no caso da CONTRATADA terá este ainda direito a:

I- Devolução da garantia;
II- Pagamentos devidos pela execução do contrato até a data da rescisão;

III- Pagamento do custo da desmobilização.

CLÁUSULA ONZE - REPARAÇÃO DOS DANOS

11.1. A CONTRATADA é obrigada a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados, e responderá por danos causados diretamente a terceiros ou à empresa pública ou sociedade de economia mista, independentemente da comprovação de sua culpa ou dolo na execução do contrato.

CLÁUSULA DOZE - VIGÊNCIA CONTRATUAL

12.1. O presente **contrato terá vigência de 120 (cento e vinte) dias**, tendo como termo inicial a data da assinatura.

CLÁUSULA TREZE - LEGISLAÇÃO APLICADA

13.1. A execução deste contrato será disciplinada, de forma específica, nos termos de suas cláusulas e conforme Lei Federal n.º 13.303/2016, e de formal geral e subsidiária, pela Lei n.º 10.406/2002 - Código Civil -, com alterações posteriores.

CLÁUSULA CATORZE - DISPOSIÇÕES GERAIS

14.1. As despesas decorrentes do presente contrato estarão sob as despesas, Conta Gerencial n.º: 8.4.1.03 - Orçamento PA-2024-0033 (PA-2024-DSG-007) - Origem do Recurso: Vinculada DAE (Recursos Próprios) - Gerência de Tecnologia da Informação.

14.2. A CONTRATADA não poderá subcontratar, ceder ou transferir, total ou parcialmente o fornecimento objeto deste Edital, bem como os direitos creditórios dele.

14.3. Quaisquer alterações ou modificações no presente contrato somente serão válidas e exequíveis perante as partes mediante aditamento contratual escrito e assinado pelas partes.

14.4. As Partes se obrigam a tomar todas as cautelas necessárias para a perfeita execução de todos os termos e condições aqui estabelecidos, responsabilizando-se a parte infratora por quaisquer perdas e danos, pessoais ou materiais que venha a causar, direta ou indiretamente à outra parte e a terceiros e que decorra de ato praticado por si própria, seus prepostos, empregados ou terceiros contratados.

14.5. A tolerância ou omissão de exigir o cumprimento de qualquer dos direitos oriundos do presente contrato não constituirá renúncia ao exercício de tal direito ou novação, podendo a exigência ser feita a qualquer tempo.

14.6. Na hipótese de qualquer cláusula deste contrato vir a ser julgada ilegal, inválida ou inexequível, as demais cláusulas permanecerão em vigor, devendo o presente ser interpretado como se referida cláusula nunca o tivesse integrado, desde que a intenção das partes contratantes não seja desvirtuada por referida ilegalidade, invalidade ou inexequibilidade.

14.7. A celebração do presente instrumento não acarreta nenhuma licença ou concessão de uso de marca de titularidade da CONTRATANTE, razão pela qual a CONTRATADA não poderá utilizar, exceto mediante prévia e expressa autorização por escrito da CONTRATANTE, qualquer marca, nome, logotipo ou símbolo de propriedade da CONTRATANTE, tampouco fazer qualquer declaração ou referência que indique a existência de vínculo, relação contratual ou negocial entre as partes que não seja a ora estabelecida, sob pena de responder pelas perdas e danos causados.

14.8. A CONTRATADA não poderá assumir qualquer obrigação em nome da CONTRATANTE ou, por qualquer forma ou condição, obrigar a CONTRATANTE perante terceiros, exceto se para tal obtiver prévia e expressa autorização ou mandato da outra parte.

14.9. Declaram as partes a total inexistência de vínculo trabalhista ou de responsabilidade da CONTRATANTE, seja com quaisquer sócios da CONTRATADA seja com relação ao pessoal que a CONTRATADA eventualmente utilizar, direta ou indiretamente, para a execução do objeto deste contrato.

CLÁUSULA QUINZE - PROTEÇÃO DE DADOS PESSOAIS

15.1. As Partes, sempre que aplicável, se comprometem a atuar no contrato em conformidade com a legislação aplicável sobre informações relacionadas a pessoas naturais identificadas ou identificáveis (“Dados Pessoais”), especialmente a Lei n.º 13.709/2018 (“Lei Geral de Proteção de Dados Pessoais” ou “LGPD”).

15.2. As Partes, incluindo seus funcionários, representantes e contratados, comprometem-se a tratar todos os Dados Pessoais a que eventualmente tiverem acesso por força do contrato como confidenciais, ainda que o contrato venha a ser resolvido e independentemente dos motivos que derem causa ao seu término ou resolução.

15.3. Cada Parte deverá monitorar, por meios adequados, sua própria conformidade, a de seus funcionários e de seus contratados com os controles de segurança da informação e com as respectivas obrigações de proteção dos Dados Pessoais que porventura sejam tratados no âmbito do contrato.

15.4. Na hipótese de uma Parte ser demandada judicial ou administrativamente em relação aos Dados Pessoais eventualmente tratados no âmbito do contrato, as Partes comprometem-se a auxiliar uma à outra no cumprimento de suas obrigações, de acordo com a Lei Geral de Proteção de Dados Pessoais e demais normas aplicáveis.

CLÁUSULA DEZESSEIS - FORO

16.1. Fica eleito o Foro da Comarca de Jundiaí/SP., por mais privilegiado que outro seja, para conhecer e dirimir quaisquer questões oriundas do presente contrato.

16.2. E por estarem justas e contratadas, as partes assinam o presente instrumento, em 01 (uma) via, para todos os efeitos de direito.

Jundiaí, 30 de março de 2026.

a) p/contratante:

DAE S.A. - ÁGUA E ESGOTO

DANIEL BOCALAO JUNIOR:05219804880

Assinado de forma digital por DANIEL BOCALAO JUNIOR:05219804880
Dados: 2026.03.30 17:59:24 -03'00'

DANIEL BOCALÃO JÚNIOR

DIRETOR PRESIDENTE

CPF/MF: 052.198.048-80

HELEN CAPPELLETTI DE LIMA:25958341855

Assinado de forma digital por HELEN CAPPELLETTI DE LIMA:25958341855
Dados: 2026.03.30 14:06:15 -03'00'

HELEN CAPPELLETTI DE LIMA

DIRETORA SUPERINTENDENTE DE GESTÃO

CPF/MF: 259.583.418-55

b) p/contratada:

INTERQUATTRI INFORMÁTICA E TELECOMUNICAÇÕES LTDA.

AFRANIO SILVA GOMIDE:55497233872
Assinado de forma digital por AFRANIO SILVA GOMIDE:55497233872
Dados: 2026.03.31 15:12:28 -03'00'

AFRANIO SILVA GOMIDE

DIRETOR COMERCIAL

CPF/MF: 554.972.338-72

CLAUDIO CESAR GRANDE:04248726840
Assinado de forma digital por CLAUDIO CESAR GRANDE:04248726840
Dados: 2026.03.31 15:33:35 -03'00'

CLAUDIO CESAR GRANDE

DIRETOR FINANCEIRO

CPF/MF: 042.487.268-40

TERMO DE CIÊNCIA E NOTIFICAÇÃO

CONTRATANTE: DAE S.A. - ÁGUA E ESGOTO.

CONTRATADA: INTERQUATTRI INFORMÁTICA E TELECOMUNICAÇÕES LTDA.

CONTRATO N.º: 031/2026.

OBJETO: Aquisição de um Firewall de Próxima Geração (NGFW) de alto desempenho, capaz de proteger redes corporativas de grande escala contra ameaças cibernéticas avançadas, com serviço de instalação, treinamento, suporte técnico e manutenção.

Pelo presente TERMO, nós, abaixo identificados:

1. Estamos CIENTES de que:

a- O ajuste acima referido, seus aditamentos, bem como o acompanhamento de sua execução contratual, estarão sujeitos a análise e julgamento pelo Tribunal de Contas do Estado de São Paulo, cujo trâmite processual ocorrerá pelo sistema eletrônico;

b- Poderemos ter acesso ao processo, tendo vista e extraindo cópias das manifestações de interesse, Despachos e Decisões, mediante regular cadastramento no Sistema de Processo Eletrônico, em consonância com o estabelecido na Resolução n.º 01/2011 do TCESP;

c- Além de disponíveis no processo eletrônico, todos os Despachos e Decisões que vierem a ser tomados, relativamente ao aludido processo, serão publicados no Diário Oficial Eletrônico do Tribunal de Contas do Estado de São Paulo (https://doe.tce.sp.gov.br/), em conformidade com o artigo 90 da Lei Complementar nº. 709, de 14 de janeiro de 1993, iniciando-se, a partir de então, a contagem dos prazos processuais, conforme regras do Código de Processo Civil;

d- As informações pessoais dos responsáveis pela contratante estão cadastradas no módulo eletrônico do "Cadastro Corporativo TCESP - CadTCESP", nos termos previstos no artigo 2º das Instruções n.º 01/2024, conforme "Declaração(ões) de Atualização Cadastral" anexa(s);

e- É de exclusiva responsabilidade do contratado manter seus dados sempre atualizados.

2. Damo-nos por NOTIFICADOS para:

a- O acompanhamento dos atos do processo até seu julgamento final e consequente publicação;

b- Se for o caso e de nosso interesse, nos prazos e nas formas legais e regimentais, exercer o direito de defesa, interpor recursos e o que mais couber.

Jundiaí, 30 de março de 2026.

- AUTORIDADE MÁXIMA DO ÓRGÃO / ENTIDADE

Nome: **Daniel Bocalão Júnior**

Cargo: Diretor Presidente

CPF/MF: 052.198.048-80

Assinatura: DANIEL BOCALAO JUNIOR:05219804880 Assinado de forma digital por DANIEL BOCALAO JUNIOR:05219804880 Dados: 2026.03.30 18:00:16 -03'00'

- RESPONSÁVEL PELA HOMOLOGAÇÃO DO CERTAME OU RATIFICAÇÃO DA DISPENSA / INEXIGIBILIDADE DE LICITAÇÃO

Nome: **Helen Cappelletti de Lima**

Cargo: Diretora Superintendente de Gestão

CPF/MF: 259.583.418-55

Assinatura: HELEN CAPPELLETTI DE LIMA:25958341855 Assinado de forma digital por HELEN CAPPELLETTI DE LIMA:25958341855 Dados: 2026.03.30 14:06:54 -03'00'

RESPONSÁVEIS QUE ASSINARAM O AJUSTE:

P/CONTRATANTE: DAE S.A. - ÁGUA E ESGOTO.

Nome: **Daniel Bocalão Júnior**

Cargo: Diretor Presidente

CPF/MF: 052.198.048-80

Assinatura: DANIEL BOCALAO JUNIOR:05219804880 Assinado de forma digital por DANIEL BOCALAO JUNIOR:05219804880 Dados: 2026.03.30 18:01:34 -03'00'

Nome: **Helen Cappelletti de Lima**

Cargo: Diretora Superintendente de Gestão

CPF/MF: 259.583.418-55

Assinatura: HELEN CAPPELLETTI DE LIMA:25958341855 Assinado de forma digital por HELEN CAPPELLETTI DE LIMA:25958341855 Dados: 2026.03.30 14:07:08 -03'00'

PELA CONTRATADA: INTERQUATTRI INFORMÁTICA E TELECOMUNICAÇÕES LTDA.

Nome: **Afranio Silva Gomide**

Cargo: Diretor Comercial

CPF/MF: 554.972.338-72

Assinatura: AFRANIO SILVA GOMIDE:55497233872 Assinado de forma digital por AFRANIO SILVA GOMIDE:55497233872 Dados: 2026.03.31 15:49:25 -03'00'

Nome: **Claudio Cesar Grande**

Cargo: Diretor Financeiro

CPF/MF: 042.487.268-40

Assinatura: CLAUDIO CESAR GRANDE:04248726840 Assinado de forma digital por CLAUDIO CESAR GRANDE:04248726840 Dados: 2026.03.31 14:28:10 -03'00'

ORDENADORA DE DESPESAS DA CONTRATANTE: DAE S.A. – ÁGUA E ESGOTO.

Nome: **Helen Cappelletti de Lima**

Cargo: Diretora Superintendente de Gestão

CPF/MF: 259.583.418-55

Assinatura: HELEN CAPPELLETTI DE LIMA:25958341855 Assinado de forma digital por HELEN CAPPELLETTI DE LIMA:25958341855 Dados: 2026.03.30 14:07:27 -03'00'

GESTORA DO CONTRATO: DAE S.A. – ÁGUA E ESGOTO

Nome: **Helen Cappelletti de Lima**

Cargo: Diretora Superintendente de Gestão

CPF/MF: 259.583.418-55

Assinatura: HELEN CAPPELLETTI DE LIMA:25958341855 Assinado de forma digital por HELEN CAPPELLETTI DE LIMA:25958341855 Dados: 2026.03.30 14:07:44 -03'00'

DEMAIS RESPONSÁVEIS:

- TIPO DE ATO SOB SUA RESPONSABILIDADE:

- PARECER JURÍDICO

Nome: **Gisela Vicenzi Fernandes**

Cargo: Advogada

CPF/MF: 270.036.318-30

Assinatura: GISELA VICENZI FERNANDES Assinado de forma digital por GISELA VICENZI FERNANDES Dados: 2026.03.30 09:20:36 -03'00'

- TIPO DE ATO SOB SUA RESPONSABILIDADE:

- PREGOEIRO

Nome: **Leonardo Cesar Franco Puttini**

Cargo: Assistente Administrativo

CPF/MF: 421.777.228-96

Assinatura: gov.br Documento assinado digitalmente LEONARDO CESAR FRANCO PUTTINI Data: 30/03/2026 09:31:42-0300 Verifique em https://validar.iti.gov.br

V - TERMO DE REFERÊNCIA

1. DESCRIÇÃO DO OBJETO

Aquisição de um Firewall de Próxima Geração (NGFW) de alto desempenho, capaz de proteger redes corporativas de grande escala contra ameaças cibernéticas avançadas. O equipamento deve fornecer segurança robusta, inspeção de tráfego em tempo real e recursos de gerenciamento centralizado.

Deve possuir licenciamento completo durante o período de 36 meses a partir da implantação.

2. JUSTIFICATIVA

O ambiente computacional da empresa depende de uma infraestrutura de segurança e conectividade robusta para garantir a continuidade dos serviços e a proteção dos ativos de informação. Atualmente, o firewall em uso já se encontra em fase de obsolescência, com ciclo de vida expirado pelo fabricante previsto para o primeiro semestre de 2026, o que implica no encerramento de atualizações de firmware, correções de segurança e suporte técnico. A permanência desse equipamento após esse período expõe a organização a riscos significativos de vulnerabilidades, incidentes de segurança e interrupções de operação, impactando diretamente a disponibilidade e a integridade dos sistemas corporativos.

Diante disso, faz-se necessária a aquisição de um novo firewall em arquitetura de alta disponibilidade, de forma a garantir que, em caso de falhas de hardware, necessidade de manutenção ou atualização, o tráfego seja automaticamente assumido por um equipamento redundante, sem interrupção dos serviços. Essa abordagem reduz riscos operacionais, assegura a continuidade dos serviços críticos e permite a execução de atualizações e ajustes sem impacto para os usuários, além de estar alinhada às melhores práticas de governança e segurança da informação.

Com essa aquisição, os colaboradores poderão acessar sistemas e dados corporativos de forma imediata e segura, o que viabiliza maior agilidade em processos internos, tomada de decisão mais rápida e um ambiente de trabalho moderno, alinhado às atuais necessidades de segurança.

Além disso, como a aquisição do atual equipamento ocorreu em 2018, portanto, há pelo menos sete anos, a capacidade de atendimento já não é a mesma, tendo algumas limitações, por exemplo, ao novo link de dados contratado e o aumento de demanda computacional, com novos usuários e serviços.

Portanto, a aquisição proposta não apenas responde a uma necessidade de substituição tecnológica por obsolescência, mas também representa um investimento estratégico em segurança, continuidade de negócio e modernização da infraestrutura de TI, garantindo que a empresa mantenha níveis elevados de disponibilidade, proteção da informação, mobilidade e eficiência operacional.

3. ITENS

ITEM	DESCRIÇÃO	UN. MED.	QTD.
1	Appliance NGFW (Next-Generation Firewall) com Alta Disponibilidade (High Availability) - solução de segurança integrada (Firewall+IPS) com funcionalidades de Filtro de Conteúdo, Controle de Pontos de Acesso Wireless, Filtro de Aplicações e Classificação de Sites, software de gerenciamento e de relatórios.	Unidade	2
2	Serviço de Instalação, Configuração e Migração das Regras do Antigo Firewall	Serviço	1
3	Treinamento / Capacitação para equipe de até 3 (três) pessoas	Serviço	1
4	Serviço de Suporte Técnico e garantia do produto por 36 (trinta e seis) meses	Meses	36

4. CRITÉRIO DE JULGAMENTO

4.1. O critério de julgamento sugerido na avaliação das propostas é o de menor preço global.

ESPECIFICAÇÕES TÉCNICAS DO OBJETO

5.1. ITEM 1: NGFW (Next-Generation Firewall)

5.1.1. CARACTERÍSTICAS MÍNIMAS DO EQUIPAMENTO:

5.1.1.1. Possuir desempenho em modo Threat Prevention (Proteção Anti-Malware, IPS e Controle de Aplicação habilitados) mínimo de 15 Gbps.

5.1.1.2. Possuir desempenho em modo de Inspeção (decriptografia e criptografia) de tráfego criptografado (SSL/TLS) mínimo de 7 Gbps.

5.1.1.3. Desempenho mínimo de 17 Gbps de IPS.

5.1.1.4. Desempenho mínimo de 28 Gbps de Firewall.

5.1.1.5. Suporte mínimo de 5.000.000 conexões simultâneas/concorrentes.

5.1.1.6. Suporte mínimo de 220.000 novas conexões por segundo.

5.1.1.7. Deve possuir armazenamento interno de no mínimo 128 GB.

5.1.1.8. Deve possuir fonte de alimentação redundante (Hot Swap) com chaveamento automático de 100-240 VAC

5.1.1.9. Deve possuir, no mínimo, 6 interfaces 10GbE SFP/SFP+;

5.1.1.10. Deve possuir, no mínimo, 2 interfaces 10/5/2.5/1 GbE RJ45;

5.1.1.11. Deve possuir, no mínimo, 1 interface dedicada ao gerenciamento do equipamento.

5.1.1.12. A VPN Client-to-Site IPsec deve ser licenciada para, no mínimo, 2.000 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 4000 usuários simultâneos.

5.1.1.13. A VPN SSL deve ser licenciada para, no mínimo, 2 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 1500 usuários simultâneos.

5.1.1.14. Deve suportar 6.000 túneis de VPN tipo Site-to-Site padrão IPSEC simultâneos.

5.1.1.15. Deve suportar, no mínimo, 14 Gbps de desempenho de VPN IPSEC.

5.1.1.16. Os desempenhos apontados devem ser comprovados por documento de domínio público do fabricante. A ausência de tais documentos comprobatórios reservará a DAE o direito de aferir a performance dos equipamentos em bancada, assim como o atendimento de todas as funcionalidades especificadas neste edital. Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, o fornecedor será considerado inabilitado. Todos os custos oriundos do teste de bancada serão custeados pelo fornecedor/vendedor do certame.

5.1.1.17. O fornecimento dos produtos e seus licenciamentos devem ser entregues através de empresa credenciada e autorizada pelo fabricante. Isto deve ser comprovado através de carta de reconhecimento assinada pelo representante legal do fabricante no Brasil para o licitante declarado vencedor.

5.1.1.18. O Equipamento deverá ser homologado pela ANATEL.

5.1.1.19. Não serão aceitas cartas ou declarações de fabricantes para atendimento aos valores de desempenho solicitados.

5.1.1.20. O licenciamento para todos os serviços do Firewall deverá ser de no mínimo 36 (trinta e seis) meses, a partir da implantação.

5.1.1.21. A **garantia do hardware deverá ser de 36 (trinta e seis) meses** no mínimo, acompanhando os serviços.

5.1.1.22. O equipamento deverá possuir, ao menos, dois ventiladores, para prover redundância.

5.1.1.23. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, prevenção de ataques zero-day, filtro de URL, identificação de usuários e controle granular de permissões.

5.1.1.24. Para proteção do ambiente contra ataques, o dispositivo de proteção deve possuir módulos de IPS, Antivírus e Anti-Spyware (para bloqueio de arquivos maliciosos), integrados ao próprio appliance de NGFW;

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

5.1.1.26. Define-se o termo “appliance” como sendo um equipamento dotado de processamento, memória e outros recursos tecnológicos exclusivos para um

determinado serviço. Um appliance é projetado para executar uma tarefa específica de forma eficiente e simplificada, com recursos e software otimizados para essa finalidade;

5.1.1.27. Não serão aceitas soluções baseadas em PC's (personal computers) de uso geral, assim como, soluções de "appliance" que utilizam hardware e software de fabricantes diferentes;

5.1.1.28. Deve ser capaz de atualizar de forma automática o Firmware, patches e atualizações de segurança;

5.1.1.29. A solução deve permitir o uso de armazenamento externo para System Logs, Threat Logs garantindo persistência de dados após reinicializações do firewall;

5.1.1.30. O painel deve exibir detalhes sobre o último contato do Firewall com o gerenciador de licenciamento, mostrando o status de atualização de licenças e atualizações de assinaturas;

5.1.1.31. Deve fornece APIs para que os fornecedores externos de NAC possam transmitir o contexto de segurança aos firewalls e que esta funcionalidade seja compatível com a utilização simultânea de fornecedores externos distintos;

5.1.1.32. A solução de segurança não pode aplicar nenhum tipo de exceção de inspeção de tráfego (bypass) oriunda de condições de limitação de capacidade de processamento de forma automática. Toda e qualquer exceção (bypass) de inspeção e tráfego deve ser possível apenas através de ação explícita e específica criada pelo administrador da plataforma através de configurações realizadas pela console gráfica do appliance, ou pela plataforma centralizada de gerenciamento da solução;

5.1.2. **CARACTERÍSTICAS DIVERSAS:**

5.1.2.1. Deve implementar controle do tráfego para os protocolos TCP, UDP, ICMP, e serviços como FTP, DNS, P2P entre outros, baseados nos endereços de origem e destino;

5.1.2.2. Implementar recurso de NAT (network address translation) tipo one-to-one, one-to-many, many-to-many, many-to-one, porta TCP de conexão (NAPT) e NAT Traversal em VPN IPSec (NAT-T) e NAT dentro do tunel IPSec;

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

5.1.2.4. Deve possuir proteção anti-spoofing;

5.1.2.5. Suportar protocolos de roteamento RIP, RIPng, OSPF, OSPFv3 e BGP;

5.1.2.6. Suportar Equal Cost Multi-Path (ECMP) no mínimo para roteamento estático e protocolo OSPF;

5.1.2.7. Suporte a Policy-Based Routing (PBR), com a capacidade de roteamento no mínimo, mas não limitado a endereço de origem, endereço de destino, serviço e aplicação;

5.1.2.8. A solução deverá possuir a tecnologia SD-WAN (Software Defined WAN), e que a mesma seja nativa da solução, sem a necessidade de qualquer tipo de licenciamento complementar, para evitar indisponibilidade no ambiente mesmo em caso de expiração do licenciamento vigente.

5.1.2.9. Capacidade de agregar no mínimo 4 (quatro) circuitos WAN distintos em um único canal lógico onde seja possível criar controles de caminho automático baseado em políticas, com habilidade de selecionar o melhor caminho, no mínimo, através dos seguintes parâmetros simultâneos: Latência, Jitter e Perda de pacotes;

5.1.2.10. O administrador da solução deverá ter a capacidade de configurar o canal lógico de SD-WAN para encaminhar tráfego simultaneamente por todos os links pertencentes a esse canal lógico;

5.1.2.11. A comutação do SD-WAN deve ocorrer de maneira dinâmica e automática baseada nas políticas previamente aplicadas;

5.1.2.12. A solução de SD-WAN deve permitir encaminhamento de tráfego com base em assinaturas de aplicações conhecidas (DPI), como Office 365, Facebook e Youtube, bem como aplicações associadas como Facebook Messenger e Office 365 Outlook;

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

5.1.2.14. Deve suportar modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;

5.1.2.15. Implementar proxy transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das máquinas clientes.

5.1.2.16. Possuir servidor de DHCP (Dynamic Host Configuration Protocol) interno com capacidade de alocação de endereçamento IP para as estações conectadas às interfaces do firewall e via VPN;

5.1.2.17. Deve suportar DHCP relay;

5.1.2.18. Possibilitar a aplicação de regras de firewall e IPS por IP e grupo de usuários, permitindo a definição de regras para determinado horário ou período (dia da semana e hora) com matriz de horários que possibilite o bloqueio de serviços em horários específicos, tendo o início e fim das conexões vinculadas a essa matriz de horários;

5.1.2.19. Deve permitir a utilização de regras de Anti-Vírus, Anti-Spyware, IPS e filtro de conteúdo web por segmentos de rede. Todos os serviços devem ser

suportados no mesmo segmento de rede, interface (física e virtual) ou zona de segurança;

5.1.2.20. Possuir capacidade de inspecionar e bloquear em tempo real aplicativos e transferências de arquivos de softwares p2p (peer-to-peer) incluindo, no mínimo, Napster e de comunicadores instantâneos (instant messengers) incluindo, no mínimo, WhatsApp, Google Talk e Skype para usuários da rede, individualmente ou em grupo;

5.1.2.21. Deve ter suporte à proteção e identificação de hosts possivelmente infectados com "botnets". A solução ofertada deve permitir ao administrador a possibilidade de apenas registrar e identificar as máquinas possivelmente contaminadas, além de ter a possibilidade de habilitar e analisar todas as conexões que passam por este dispositivo de segurança, bem como ativar tal funcionalidade especificando análise por regra de firewall, permitindo assim maior granularidade da gestão e do recurso.

5.1.2.22. Possuir assinaturas específicas, ou implementar mecanismo interno no appliance, para mitigação de ataques DoS (denial-of-service) e DDoS devidamente licenciados;

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

5.1.2.24. Detectar e bloquear a origem de portscans;

5.1.2.25. Deve permitir o bloqueio de ataques;

5.1.2.26. Deve permitir o bloqueio de exploits conhecidos;

5.1.2.27. O gateway Anti-Vírus deve suportar a análise de pelo menos os protocolos HTTP, FTP, IMAP, e SMTP;

5.1.2.28. Deve ter a capacidade de analisar tráfegos criptografados HTTPS/SSL, que deverá ser decriptografado de forma transparente à aplicação;

5.1.2.29. Implementar DSCP (Differentiated Services Code Points);

5.1.2.30. Possuir mecanismo de forma a possibilitar o funcionamento transparente dos protocolos FTP, SIP, RTP, RTSP e H323, mesmo quando acessados por máquinas através de conversão de endereços. Este suporte deve funcionar tanto para acessos de dentro para fora quanto de fora para dentro da rede.

5.1.2.31. Implementar controle e gerenciamento de banda para a tecnologia VoIP(Voice Over IP) sobre diferentes segmentos de rede com inspeção profunda de segurança sobre este serviço;

5.1.2.32. Implementar mecanismo de sincronismo de horário através do protocolo NTP;

5.1.2.33. Possuir suporte ao protocolo SNMP versões 2 e 3;

5.1.2.34. Possuir suporte a log via syslog;

5.1.2.35. Possuir suporte aos protocolos de roteamento RIP, OSPF e BGP. As configurações de RIP E OSPF devem ser configuradas através da interface gráfica;

5.1.2.36. Reconhecer aplicações como, no mínimo, peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos e e-mail;

5.1.2.37. Para tráfego criptografado SSL/TLS, deve de-criptografar pacotes possibilitando a leitura de payload dos pacotes para checagem de assinaturas de aplicações conhecidas pelo fabricante;

5.1.2.38. Controle, inspeção e de-criptografia de SSL/TLS por política para tráfego de entrada (Inbound) ou saída (Outbound) com suporte a no mínimo SSLv3, TLS 1.2 e TLS 1.3;

5.1.2.39. Deve permitir a funcionalidade de ARP bridging;

5.1.2.40. Deve permitir a configuração de limite na taxa de envio ARP para um mesmo IP, para evitar "ARP Storm";

5.1.2.41. A solução deve permitir a visualização gráfica das regras de segurança e acesso.

5.1.2.42. Os equipamentos deverão estar em linha de produção e com o suporte ativo durante pelo menos cinco anos da data da compra. Equipamentos descontinuados ou com o ciclo de vida já determinado não serão aceitos.

5.1.3. **CARACTERÍSTICAS DE VPN:**

5.1.3.1. Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo site-to-site, com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC;

5.1.3.2. Suportar algoritmos de criptografia 3DES, AES 128, AES 256 e AES GCM16-256;

5.1.3.3. Suportar algoritmos Hash no mínimo SHA-1, SHA-256 e SHA-384;

5.1.3.4. Diffie-Hellman: Grupo 2 (1024 bits), Grupo 5 (1536 bits) e Grupo 14 (2048 bits).

5.1.3.5. Suportar os protocolos ESP e AH;

5.1.3.6. Deverá suportar algoritmo Internet Key Exchange (IKE)v1 e v2;

5.1.3.7. Autenticação via de túneis IPSec via certificado digital para VPNs Site-to-Site e Client-to-Site;

5.1.3.8. A solução deve suportar VPNs L2TP, incluindo suporte para Apple iOS e Android;

5.1.3.9. Solução deve suportar VPNs baseadas em políticas, e VPNs baseadas em roteamento estático e/ou dinâmico;

5.1.3.10. Solução deve incluir a capacidade de estabelecer VPNs com outros firewalls que utilizam IP públicos dinâmicos;

5.1.3.11. Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do circuito primário;

5.1.3.12. Permitir criação de políticas de roteamento estático utilizando IPs de origem, destino, serviços e a própria VPN como parte encaminhadora deste tráfego, sendo este visto pela regra de roteamento como uma interface simples de rede para encaminhamento do tráfego;

5.1.3.13. Suportar a criação de túneis IP sobre IP (IPSEC Tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet;

5.1.3.14. Implementar os esquemas de troca de chaves manual, IKE e IKEv2 por PréShared Key, certificados digitais e XAUTH client authentication;

5.1.3.15. Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do primário;

5.1.3.16. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SONICWALL;

5.1.4. **ALTA DISPONIBILIDADE:**

5.1.4.1. Devem ser fornecidos 02 (dois) appliances de NGFW com gerenciamento unificado, novos e sem uso anterior, funcionando em alta disponibilidade. O modelo ofertado deverá estar em linha de produção, sem previsão de encerramento de fabricação, na data de entrega da proposta. O software deverá ser fornecido em sua versão mais atualizada.

5.1.4.2. A solução deve ser entregue operando em alta disponibilidade no modo Ativo/Passivo ou Ativo/Ativo, com as implementações de Failover;

5.1.4.3. Não serão permitidas soluções de cluster (HA) que façam com que os equipamentos se reiniciem após qualquer modificação de parâmetro/configuração realizada pelo administrador;

5.1.4.4. A solução deve ter capacidade de fazer monitoramento físico das interfaces dos membros do cluster;

5.1.4.5. A solução deve operar em alta disponibilidade implementando monitoramento lógico de um host na rede, e possibilitar failover;

5.1.4.6. A solução deve permitir o uso de endereço MAC virtual para evitar problemas de expiração de tabela ARP em caso de Failover;

5.1.4.7. A solução deve possibilitar a sincronização de todas as configurações realizadas na caixa principal do cluster incluído, mas não limitado a objetos, regras, rotas, VPNs e políticas de segurança;

5.1.4.8. A solução deve permitir visualizar no equipamento principal, o status da comunicação entre os parceiros do cluster, status de sincronização das configurações, status atual do equipamento redundante;

5.1.4.9. A solução de HA deve permitir que o dispositivo primário trate todo o tráfego, mantendo o dispositivo secundário atualizado em tempo real sobre as informações de conexão de rede, garantindo uma transição transparente para o dispositivo secundário em caso de failover, sem que haja perda das conexões de VPN, FTP, Oracle SQL*NET, RSTP, Real Audio, VPN Client, Dynamic Arp Objects, Informações de DHCP Server, Multicast , IGMP, Usuários ativos, RIP e OSPF.

5.1.5. **CONTROLE DE AMEAÇAS:**

5.1.5.1. Para as ameaças de ZeroDay(dia-zero), a solução deve ter a habilidade de prevenir o ataque antes de qualquer assinatura ser criada. Deve possuir módulo de Antivírus e Anti-Bot integrado ao próprio appliance de segurança;

5.1.5.2. A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliances através de assinaturas;

5.1.5.3. Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego;

5.1.5.4. Implementar funcionalidade de detecção e bloqueio de “call-backs”;

5.1.5.5. A solução deverá ser capaz de detectar e bloquear comportamento suspeito ou anormal da rede;

5.1.5.6. A solução Anti-bot deve possuir mecanismo de detecção que inclua reputação de endereço IP;

5.1.5.7. Implementar interface gráfica WEB segura, utilizando o protocolo HTTPS;

5.1.5.8. Implementar interface CLI segura através do protocolo SSH;

5.1.5.9. Possuir Anti-Vírus em tempo real, para ambiente de gateway internet integrado à plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, IMAP, POP3, FTP, CIFS e TCP Stream;

5.1.5.10. A solução deve permitir criar regras de exceção de acordo com a proteção;

5.1.5.11. Deve possuir visualização na própria interface de gerenciamento referente aos top incidentes através de hosts, ou incidentes referentes a vírus e Bots;

5.1.5.12. Permitir o bloqueio de malwares (vírus, worms, spyware e etc);

5.1.5.13. A solução deve ser capaz de proteger contra ataques a DNS;

5.1.5.14. A solução deverá ser gerenciada a partir de uma console centralizada com políticas granulares;

5.1.5.15. A solução deve ser capaz de prevenir acesso a websites maliciosos;

5.1.5.16. A solução deve ser capaz de realizar inspeção de tráfego SSL/TLS e SSH;

5.1.5.17. A solução deverá receber atualizações de um serviço baseado em cloud;

5.1.5.18. A solução deverá ser capaz de bloquear a entrada de arquivos maliciosos;

5.1.5.19. A solução Anti-Vírus deverá suportar análise de arquivos que trafegam dentro do protocolo CIFS;

5.1.5.20. A solução deve suportar funcionalidade de Geo-IP, ou seja, a capacidade de identificar, isolar e controlar tráfego baseado na localização (origem e/ou destino), incluindo a capacidade de configuração de listas customizadas para esta mesma finalidade;

5.1.5.21. A solução de segurança deverá ter mecanismos de proteção de ameaças em tempo real pela análise de instruções e do uso da memória, sendo eficientes frente ameaças exploradas por vulnerabilidades do tipo meltdown/spectre;

5.1.5.22. A solução de Gateway AntiVirus deverá ter a tecnologia complementar de Anti Virus-Cloud, para que os mecanismos existentes de verificação sejam ampliados;

5.1.5.23. A solução deve bloquear proativamente o acesso a domínios maliciosos conhecidos por meio de filtragem DNS, reduzindo assim o risco de infecções por malware e outros ataques cibernéticos;

5.1.5.24. A solução deve prover o bloqueio de URL baseado em reputação, identificando e bloqueando proativamente entidades suspeitas;

5.1.6. **PROTEÇÃO CONTRA-ATAQUES AVANÇADOS:**

5.1.6.1. A solução deverá prover as funcionalidades de inspeção de tráfego de entrada e saída de malwares não conhecidos ou do tipo APT, com filtro de ameaças avançadas e análise de execução em tempo real, e inspeção de tráfego de saída de “call-backs”;

5.1.6.2. Suportar os protocolos HTTP assim como inspeção de tráfego criptografado através de HTTPS;

5.1.6.3. A solução deve ser capaz de inspecionar o tráfego criptografado SSL/TLS e SSH;

5.1.6.4. Identificar e bloquear a existência de malware em comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle;

5.1.6.5. Implementar mecanismo de bloqueio de vazamento não intencional de dados oriundos de máquinas existentes no ambiente LAN em tempo real;

5.1.6.6. Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar arquivo PDF com até 10Mb;

5.1.6.7. Implementar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows e Android;

5.1.6.8. Conter ameaças de dia zero permitindo ao usuário final o recebimento dos arquivos livres de malware;

5.1.6.9. A tecnologia de máquina virtual deverá suportar diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas;

5.1.6.10. A solução deve possuir nuvem de inteligência proprietária do fabricante, onde este seja responsável por atualizar toda a base de segurança dos appliance através de assinaturas;

5.1.6.11. Implementar a visualização dos resultados das análises de malwares de dia zero nos diferentes sistemas operacionais dos ambientes controlados (sandbox) suportados;

5.1.6.12. Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e quaisquer outros mecanismos de redirecionamento de tráfego;

5.1.6.13. Conter ameaças avançadas de dia zero;

5.1.6.14. Toda análise deverá ser realizada de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador;

5.1.6.15. Implementar mecanismo do tipo múltiplas fases para verificação de malware e/ou códigos maliciosos;

5.1.6.16. Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real. Não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos;

5.1.6.17. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx) e Android APKs no ambiente controlado.

5.1.6.18. Implementar a análise de arquivos executáveis, DLLs e ZIP no ambiente controlado;

5.1.6.19. Possuir Anti-Vírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, POP3, FTP, IMAP e CIFS;

5.1.6.20. Minimizar ameaças de dia zero de forma transparente para o usuário final;

5.1.6.21. Minimizar ameaças de dia zero através de tecnologias de emulação e código de registro;

5.1.6.22. Implementar mecanismo de pesquisa por diferentes intervalos de tempo;

5.1.6.23. Minimizar ameaças de dia zero via tráfego de internet;

5.1.6.24. Permitir a contenção de ameaças de dia zero sem a alteração da infraestrutura de segurança.

5.1.6.25. Minimizar ameaças de dia zero que possam burlar o sistema operacional emulado;

5.1.6.26. A solução deve permitir a criação de listas brancas (whitelist) baseadas no MD5 do arquivo.

5.1.6.27. Minimizar ameaças de dia zero antes da execução e evasão de qualquer código malicioso;

5.1.6.28. Conter e mitigar exploits avançados;

5.1.6.29. A análise em nuvem 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 Anti-Vírus 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);

5.1.6.30. Suporte a submissão manual de arquivos para análise através do serviço de Sandbox;

5.1.6.31. As estratégias de análise, identificação e mitigação de ameaças devem também oferecer a capacidade de proteção contra ameaças que se alojam em memória, atuando permanentemente e em tempo real;

5.1.6.32. A Solução de segurança de FireWalls deverá ter um sistema de inspeção baseado em fluxo que execute análises simultâneas de tráfego de entrada e saída em alta velocidade, sem proxying or buffering;

5.1.6.33. A Solução deve unificar diversas funções de segurança em um único conjunto integrado, inspecionando os arquivos de usuários locais, remotos e móveis;

5.1.6.34. A Solução deve unificar diversas funções de segurança em um único conjunto integrado inspecionando os arquivos de usuários locais, remotos e móveis.

5.1.6.35. A Solução deve descriptografar e inspecionar o tráfego criptografado, como HTTPS, SMTPS, NNTPS, etc., sem afetar o desempenho;

5.1.6.36. A solução de segurança de Firewalls deverá fornecer tecnologias avançadas de proteção contra ameaças, com sandboxing usando multi-mecanismos baseado em nuvem, permitindo:

5.1.6.36.1. Inspeção profunda de memória em tempo real;

5.1.6.36.2. Descriptografia e inspeção TLS/SSL;

5.1.6.36.3. Inteligência e controle de aplicativos;

5.1.6.36.4. Recursos SD-WAN seguros;

5.1.7. **CARACTERÍSTICAS DE FILTRO DE CONTEÚDO WEB:**

5.1.7.1. Possuir filtro de conteúdo integrado ao NGFW para classificação de páginas web com, no mínimo, 89 (oitenta e nove) categorias distintas, com mecanismo de atualização e consulta automáticas;

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

5.1.7.3. Devem ser fornecidas licenças de filtro de conteúdo para cada equipamento e quantidade de usuários ilimitada, provendo atualização automática e em tempo real através da categorização contínua de novos sites da Internet, sem custo adicional, por todo o período de vigência da garantia e do contrato de manutenção e suporte técnico;

5.1.7.4. Permitir a customização de página de bloqueio;

5.1.7.5. Controle de conteúdo filtrado por categorias de sites com base de dados continuamente atualizada pelo fabricante;

5.1.7.6. Deve permitir submissão de novos sites para categorização;

5.1.7.7. Permitir a classificação dinâmica de sites web, URLs e domínios;

5.1.7.8. Permitir a associação de grupos de usuários a diferentes regras de filtragem de sites web, definindo quais categorias deverão ser bloqueadas ou permitidas para cada grupo de usuários, podendo ainda adicionar ou retirar acesso a domínios específicos da Internet;

5.1.7.9. Permitir a definição de quais zonas de segurança terão aplicadas as regras de filtragem de web;

5.1.7.10. Permitir aplicar a política de filtro de conteúdo baseada em horário do dia, bem como dia da semana;

5.1.8. **CARACTERÍSTICAS DE AUTENTICAÇÃO:**

5.1.8.1. Prover autenticação de usuários para os serviços Telnet, FTP, HTTP e HTTPS, utilizando as bases de dados de usuários e grupos de servidores Windows e Unix, de forma simultânea;

5.1.8.2. Permitir a autenticação dos usuários utilizando servidores LDAP, AD, RADIUS, Tacacs+, Single Sign On e API, incluindo múltiplos domínios;

5.1.8.3. Permitir o cadastro manual dos usuários e grupos diretamente no NGFW por meio da interface de gerência remota do equipamento;

5.1.8.4. Permitir a integração com qualquer autoridade certificadora emissora de certificados X.509 que siga o padrão de PKI descrito na RFC 2459, inclusive verificando os certificados expirados/revogados, emitidos periodicamente pelas autoridades certificadoras, os quais devem ser obtidos automaticamente pelo NGFW;

5.1.8.5. Permitir o controle de acesso por usuário, para plataformas Microsoft Windows de forma transparente, para todos os serviços suportados, de forma que ao efetuar o logon na rede, um determinado usuário tenha seu perfil de acesso automaticamente configurado sem a instalação de softwares adicionais nas estações de trabalho e sem configuração adicional no browser;

5.1.8.6. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no NGFW;

5.1.8.7. Permitir aos usuários o uso de seu perfil independentemente do endereço IP da máquina que o usuário esteja utilizando;

5.1.8.8. Permitir a atribuição de perfil por faixa de endereço IP nos casos em que a autenticação não seja requerida;

5.1.8.9. Suportar a criação de túneis seguros sobre IP (IPSEC tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet;

5.1.8.10. A solução deve possibilitar SSO via API;

5.1.9. **CARACTERÍSTICAS DE ADMINISTRAÇÃO:**

5.1.9.1. Permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o NGFW, cada um responsável por determinadas tarefas da administração;

5.1.9.2. Possuir mecanismo para aplicar remotamente, pela interface gráfica, correções e atualizações para o NGFW;

5.1.9.3. Possuir mecanismo para realizar remotamente, através de interface gráfica, cópias de segurança (backup) e restauração de configurações e sistema operacional;

5.1.9.4. Possuir mecanismo para agendamento realização das cópias de segurança(backups) de configuração;

5.1.9.5. Possuir mecanismo para exportar as configurações através de FTP, HTTPs ou SFTP;

5.1.9.6. A solução deve permitir ao administrador aplicar ajustes rápidos das melhores práticas de segurança no dispositivo, possibilitando implementar as melhores práticas recomendadas pelo fabricante;

5.1.9.7. Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do NGFW e a remoção de qualquer uma destas sessões ou conexões;

5.1.9.8. Permitir a visualização, em forma gráfica, do percentual do uso de CPU e quantidade de tráfego de rede em todas as interfaces do NGFW em tempo real;

5.1.9.9. Permitir a visualização, em tempo real, dos serviços com maior tráfego e os endereços IP mais acessados;

5.1.9.10. Deve suportar minimamente dois tipos de negação de tráfego nas políticas de firewall: Descarte sem notificação do bloqueio ao usuário (discard), descarte com notificação do bloqueio ao usuário (drop), descarte com opção de envio de "ICMP

5.1.9.11. Unreachable" para máquina de origem do tráfego, "TCP-Reset" para o cliente, "TCPReset" para o servidor ou para os dois lados da conexão;

5.1.9.12. Ser capaz de visualizar, de forma direta no appliance e em tempo real, as aplicações mais utilizadas, os usuários que mais estão utilizando estes recursos informando sua sessão, total de pacotes enviados, total de bytes enviados e média de utilização em Kbps, URLs acessadas e ameaças identificadas;

5.1.9.13. Ser capaz de visualizar, de forma direta no appliance e em tempo real estado do processamento do produto e volume/desempenho de dados utilizado pela rede de computadores conectada ao equipamento;

5.1.9.14. Possibilitar a geração de relatório de ameaças com avaliação e gerenciamento de riscos e informações detalhadas sobre o ambiente, ajudando a identificar explorações de vulnerabilidades, intrusões e outras ameaças. Deve permitir a emissão deste relatório em formato PDF;

5.1.9.15. Ser capaz de visualizar, de forma direta no appliance e em tempo real, a largura de banda utilizada por política, por protocolo TCP/UDP IPV4 e IPV6;

5.1.9.16. Ser capaz de visualizar, de forma direta no appliance e em tempo real, as conexões estabelecidas, com possibilidade de aplicar filtros na visualização;

5.1.9.17. Possibilitar a geração de pelo menos os seguintes tipos de relatório, mostrados em formato HTML e CSV: máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas, ou categorias Web mais acessadas (considerando a existência do filtro de conteúdo Web);

5.1.9.18. Permitir habilitar auditoria de configurações no equipamento, possibilitando o rastreio das configurações aplicadas no produto;

5.1.9.19. Ser capaz de implementar a funcionalidade de “Zero-Touch”, permitindo que o equipamento se provisione autônoma e automaticamente no sistema de gestão centralizada;

5.1.9.20. O aplicativo móvel deve possibilitar conexão ao dispositivo via protocolo HTTPS;

5.1.9.21. O gerenciamento via aplicativo móvel deve permitir visualização de status de consumo de banda, CPU, conexões ativas dos dispositivos e topologia do NGFW;

5.1.9.22. O aplicativo móvel deve permitir visualização de status das ameaças observadas e bloqueadas pelas funcionalidades de segurança de NGFW;

5.1.9.23. O aplicativo móvel deve permitir visualização dos últimos logs gerados no NGFW;

5.1.9.24. O aplicativo móvel deve permitir diagnósticos simples na solução, como testes ICMP e verificação DNS;O aplicativo móvel deve permitir configurar interfaces, objetos e políticas de acesso, além de exportar configurações;

5.1.9.25. A solução deve possibilitar ao administrador habilitar ou desabilitar as capacidades de auto-provisionamento da plataforma através de ponto central de gerenciamento;

5.1.9.26. Deve ser capaz de emitir relatório, mostrando a saúde do ambiente, agendado ou sob demanda, que liste informações de aplicações, risco, atividade WEB, análise de botnets, análise de malware, ameaças, países por tráfego, arquivos compartilhados por aplicações, sessões e recomendações;

5.1.9.27. A solução deve suportar API como alternativa à interface de linha de comando (CLI), para configurar funções diversas;

5.1.9.28. Deve permitir que os administradores criem/recuperem/excluam listas de URLs ou endereços IP a serem bloqueados por meio de chamadas de API RESTful;

5.1.10. **SOFTWARE DE GERENCIAMENTO DA SOLUÇÃO EM NUVEM:**

Deverá ser fornecido com software de gerenciamento com as seguintes características:

5.1.10.1. Deve possuir solução de gerenciamento centralizado em nuvem de toda solução de firewall.

5.1.10.2. Deve permitir o controle sobre todos os equipamentos da plataforma de segurança em uma única console, com administração de privilégios e funções

5.1.10.3. Deve dar suporte a organização os dispositivos administrados por grupos;

5.1.10.4. Deve ser possível aplicar configurações de forma granular, um firewall, em grupos, ou em todos os firewalls.

5.1.10.5. Deve mostrar os status dos firewalls (standalone ou em alta disponibilidade) a partir da plataforma de gerenciamento centralizado;

5.1.10.6. Centralizar a administração de regras e políticas usando uma única interface de gerenciamento;

5.1.10.7. O gerenciamento deve permitir/possuir:

5.1.10.8. Criação e administração de políticas de firewall e controle de aplicação.

5.1.10.9. Monitoração de logs;

5.1.10.10. Debugging

5.1.10.11. Deve permitir acesso concorrente de administradores

5.1.10.12. Deve permitir o provisionamento de configuração por "Zero-Touch"

5.1.10.13. A solução de gerenciamento deverá ser acessível através de navegador WEB padrão, com criptografia de tráfego SSL

5.1.10.14. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança, possibilitando geração de relatórios analíticos e de forma centralizada de todos os dispositivos gerenciados.

5.1.10.15. A solução deve possuir tela situacional com todo os inventários de firewalls gerenciados centralizadamente, informando no mínimo para o administrador, nome do Hostname do firewall, número de série, modelo, versão do firmware e status da conectividade do equipamento com a gerência em online ou off-line.

5.1.10.16. Deverá permitir atualizar o sistema operacional de múltiplos equipamentos gerenciados de uma única vez;

5.1.10.17. Deve centralizar a administração de regras e políticas, usando uma única interface de gerenciamento;

5.1.10.18. A solução deve possuir Dashboard com sumário de alertas e informação de status de licença

5.1.10.19. A solução deverá permitir seu gerenciamento por Web GUI utilizando protocolo HTTPS sem a necessidade de uso de cliente ou console do tipo aplicativo

5.1.10.20. Deve manter um canal de comunicação segura, com encriptação baseada HTTPS, entre todos os componentes que fazem parte da solução de firewall, gerência

5.1.10.21. A solução deverá permitir que a partir da console de gerência centralizada seja feito conexão na console de gerência local do firewall sem a necessidade do administrador utilizar endereço IP do dispositivo, URL ou FQDN

5.1.10.22. A solução deve permitir a criação de modelos de configuração ou “Templates” para aplicá-los em grupos de dispositivos. Os modelos de configurações devem permitir visualização e edição para sua aplicação nos firewalls

5.1.10.23. Os modelos de configuração ou “templates” devem suportar configurações de interfaces físicas ou virtuais

5.1.10.24. A solução deve permitir a criação de grupos lógicos, para o agrupamento de dispositivos, com isso permitindo a aplicação de modelos de configuração a diversos equipamentos de uma única vez.

5.1.10.25. Deverá permitir visualizar a diferença nas mudanças antes que as configurações sejam implantadas.

5.1.10.26. De forma centralizada deve permitir gerenciar, mas não limitado há, políticas de firewall, NAT, rotas, PBR (Policy Based Routing), configuração de endereçamento IP das interfaces dos equipamentos, criação e administração de políticas de IPS, configuração de políticas de antivírus e antimalware, configuração e criação de políticas de controle de URL, criação e configuração de políticas de controle de aplicações, criação e configuração de política de SANDBOX, criação e configuração de políticas de controle de banda, criação e configuração de objetos necessários para configuração das políticas especificadas acima, usando uma única interface de gerenciamento;

5.1.10.27. Deverá possibilitar a criação de políticas SD-WAN, baseando-se em parâmetros de latência, perda de pacote e jitter, para a tomada de decisão de encaminhamento de tráfego no firewall.

5.1.10.28. Para cada alteração de configuração a solução deverá confirmar a aplicação da política, possibilitando a adição de comentários nas políticas instaladas, para futuras consultas de auditoria.

5.1.10.29. Durante a alterações de políticas de segurança dos firewalls, deverá ser possível o agendamento para determinar o horário que as mudanças entrarão em vigor, proporcionando ao administrador aplicar políticas de segurança em horários com menor impacto para o ambiente.

5.1.10.30. Deverá permitir que configurações realizadas pelos administradores da solução sejam validadas e aprovadas (workflow), por um colaborador responsável por aprovação e aplicação de políticas, esse processo de aprovação deve ser encaminhado de forma automatizada para o responsável da aprovação via e-mail ou console da solução, possibilitando mitigar erros de configuração e impactos negativos ao ambiente

5.1.10.31. A funcionalidade de Workflow deve permitir configurar, em dias, a validade dos pedidos de aprovação, caso o pedido de aprovação não seja aprovado no período configurado, essa mudança deve ser expirada e não efetivada.

5.1.10.32. A solução deve possuir um dashboard com informações como geolocalização dos Firewalls, status (online/offline), distribuição de tráfego, Top Users, ameaças observadas, aplicações mais usadas, e situação do licenciamento.

5.1.10.33. Deverá armazenar, pelo menos dos últimos 7 dias, informações como:

5.1.10.33.1. Top Aplicações por quantidade de conexões

5.1.10.33.2. Top Usuários por quantidade de dados transferidos

5.1.10.33.3. Top Usuários por quantidade de conexões

5.1.10.33.4. Top Virus

5.1.10.33.5. Top Web Categorias

5.1.10.33.6. Top Endereços por dados transferidos

5.1.10.33.7. Top Endereços por quantidade de conexões

5.1.10.33.8. Top Localizações por dados transferidos

5.1.10.33.9. Top Localizações por quantidade de conexões

5.1.10.34. Deverá permitir o agendamento de relatório periódico que contenha informações como:

5.1.10.34.1. Sumário Executivo

5.1.10.34.2. Recomendações

5.1.10.34.3. Gráfico de risco do ambiente

5.1.10.34.4. Informações de risco por aplicações

5.1.10.34.5. Informações de Compartilhamento de arquivos

5.1.10.34.6. Informações de Malwares e Vírus

5.1.10.34.7. Mapa com estatísticas de geolocalização

5.1.10.35. Estatísticas de utilização:

5.1.10.35.1. De sessões por IP

5.1.10.35.2. De Uso de tráfego por IP

5.1.10.35.3. De Usuário por sessão

5.1.10.35.4. De usuário por tráfego

5.1.11. **RELATÓRIOS:**

5.1.11.1. A solução poderá ser entregue como appliance físico ou appliance virtual, sendo todos do mesmo fabricante dos firewalls, não sendo aceita solução de software livre;

5.1.11.2. Caso seja entregue em appliance virtual, deve ser compatível com KVM ou VMware ESXi

5.1.11.3. A solução deverá permitir visualizar sumário com as informações referentes às principais ameaças protegidas pelos firewalls

5.1.11.4. Deverá suportar logs do tipo Netflow, IPFIX ou Syslog, para gerar relatórios

5.1.11.5. O operador da solução de relatórios poderá ter acesso a informações com buscas por um período predefinido pela solução (última hora, ontem, última semana e último mês) ou customizados para um período específico definido pelo operador.

5.1.11.6. A solução deverá prover relatórios referente as atividades dos usuários

5.1.11.7. A solução deverá prover relatórios referente ao uso de aplicações web, com no mínimo as seguintes informações: nome da aplicação, nível de ameaça, quantidade de conexões e quantidade de bytes trafegados

5.1.11.8. A solução deverá possuir as informações de "Uptime" dos equipamentos (de si próprio).

5.1.11.9. A solução deverá prover relatórios referente ao consumo de rede por endereço IP, com no mínimo as seguintes informações: endereço IP, quantidade de conexões, Usuário, quantidade de bytes trafegados e MAC Address de origem.

5.1.11.10. A solução deverá prover relatórios referente aos acessos web com no mínimo informações referentes às categorias acessadas, quantitativo de acessos e bytes transferidos.

5.1.11.11. A solução deverá permitir o agendamento para envio de relatórios periódicos, em formato PDF

5.1.11.12. A solução deverá mostrar dados de uso de VPN, informando no mínimo dados como: IP de origem, usuário, conexões e quantidade de bytes trafegados

5.1.11.13. A solução deve permitir visualização de eventos correlacionados que possam ser investigados por:

5.1.11.13.1. Lista de eventos correlacionados com opção de navegação "drilldown"; ou Modo gráfico; ou Lista de logs

5.1.11.14. A solução deve possibilitar a criação de relatórios de uso de VPN.

5.1.12. **INTEGRAÇÃO COM SOLUÇÃO DE ACCESS POINT EXISTENTE**

5.1.12.1. Visando a compatibilidade e, consequentemente, a economicidade, a solução de firewall deve possibilitar a integração e gerenciamento centralizado local com a atual solução de Access Points no ambiente da CONTRATANTE, sendo estes dos seguintes modelos:

5.1.12.1.1. Sonicwall Sonicpoint ACi - 08 unidades;

5.1.12.1.2. Sonicwall Sonicwave 432i – 02 Unidades.

5.1.12.2. A integração deve possibilitar a qualquer configuração, gerenciamento e atualização dos Access Points listados, como, mas não somente:

5.1.12.2.1. Criação de SSID;

5.1.12.2.2. Alteração de nome dos Access Point;

5.1.12.2.3. Atualização de Firmwares;

5.1.12.2.4. Reboots;

5.1.12.2.5. Visualização dos usuários conectados em cada AP e todos rede WLAN;

5.1.12.2.6. Configuração de potência dos rádios.

5.1.12.2.7. Ativar e desativar individualmente os rádios 5GHz e 2,4GHz;

5.1.12.2.8. Análise e monitoramento do espectro de RF no ambiente;

5.1.12.2.9. Definir quais SSIDs serão propagados para cada Access Poin0t;

5.1.12.2.10. Configuração dos canais utilizados para cada Access Point: Configuração de VLAN para cada Access Point;

5.1.12.2.11. Criação de Grupos de Access Point.

5.1.13. **INTEGRAÇÃO COM FIREWALL DE NÍVEL DE ENTRADA DE REDE**

5.1.13.1. Visando a compatibilidade e, consequentemente, a economicidade, a solução de firewall deve possibilitar a integração e gerenciamento centralizado local com a atual solução de Firewall de Nível de Entrada de Rede no ambiente da CONTRATANTE, sendo estes dos seguintes modelos:

5.1.13.1.1. Sonicwall TZ300 - 10 unidades;

5.1.13.1.2. Sonicwall TZ270 - 01 unidade;

5.1.13.2. A integração deve possibilitar a conectividade via VPN site2site utilizando qualquer configuração IPSEC descrita em 5.1.3.

5.2. **ITEM 2: SERVIÇO DE INSTALAÇÃO, CONFIGURAÇÃO E MIGRAÇÃO DAS REGRAS E CONFIGURAÇÕES DO ANTIGO FIREWALL**

5.2.1. **INSTALAÇÃO FÍSICA E CONECTIVIDADE**

A proposta deverá compreender todos os requisitos abaixo citados:

5.2.1.1. Prever a Instalação física e configuração de cada produto suportado de acordo com as necessidades do ambiente específico da DAE, para assegurar que o dispositivo esteja pronto para a implementação no ambiente de rede IP e acesso a todos os recursos existentes;

5.2.1.2. Criação da arquitetura de cibersegurança do ambiente contendo:

5.2.1.2.1. Arquitetura lógica;

5.2.1.2.2. Mapa IP;

5.2.1.2.3. Topologia do ambiente;

5.2.1.2.4. Detalhamento IPv4;

5.2.1.2.5. Checklist de implementação.

5.2.1.3. Deverão ser realizadas todas as atualizações de firmwares, drivers, e demais softwares necessários para funcionamento da solução para versão(ões) recomendada(s) pelo fornecedor;

5.2.1.4. Prover assistência para definir os requisitos do caso de uso da DAE;

5.2.1.5. Configuração dos recursos e funcionalidades do produto para atender ao caso de uso da DAE;

5.2.1.6. Validação da funcionalidade de cada Produto suportado;

5.2.1.7. Na conclusão deste Serviço, a empresa vencedora deverá conduzir uma breve sessão de orientação sobre o Produto suportado e fornecerá a documentação completa da implementação;

5.2.1.8. O Firewall deverá ser instalado fisicamente em rack 19 polegadas fornecido pela contratante;

5.2.1.9. A CONTRATADA deverá fornecer cabos, transceivers e acessórios necessários para a conexão do firewall aos dispositivos de rede definidos pela contratante;

5.2.1.10. A instalação deve ser executada por profissionais certificados pelo fabricante, com a utilização das melhores práticas.

5.2.1.11. É recomendável que a CONTRATADA elabore um projeto de implantação realizando os levantamentos de todas as regras, objetos e serviços e dos insumos a serem utilizados na conectividade com os dispositivos de rede da DAE e demais itens que julgar necessários à boa execução do contrato, incluindo:

5.2.1.11.1. Cronograma com as etapas e fases, incluindo previsão da entrega dos equipamentos;

5.2.1.11.2. Reuniões de alinhamento com a Equipe de Operações da Diretoria de Sustentação e Operações;

5.2.1.11.3. A Implementação tem prazo máximo para iniciar em 15 dias úteis a partir do aceite do projeto, salvo exceções quando a DAE solicitar maior prazo para início dos trabalhos.

5.2.1.11.4. Processos: ITIL / NIST 800-181 / NIST 800-61.

5.2.2. **DOCUMENTAÇÃO**

5.2.2.1. Entregar documentação de todas as configurações do firewall, incluindo diagramas de rede e políticas de segurança aplicadas;

5.2.2.2. Entregar documentação referente a gestão dos recursos, emissão de relatórios e exemplos de criação de objetos e regras;

5.2.2.3. Entregar documentação referente aos dados e instruções para emissão de evidências para a correta abertura de chamados junto ao fabricante;

5.3. **ITEM 3: TREINAMENTO / CAPACITAÇÃO DE EQUIPE**

5.3.1. A CONTRATADA deverá transferir todo o conhecimento e know-how desenvolvido e aplicado na instalação e prestação dos serviços para 3 (três) técnicos, no prazo de 3 (três) dias contados a partir da data de recebimento definitivo da solução.

5.3.2. Essa transferência deverá capacitar os técnicos para conseguir interpretar os manuais técnicos, compreender a estrutura e a interoperabilidade de toda a solução, realizar manutenções preventivas e corretivas, instalar/ reinstalar / reconfigurar, operar o equipamento, de forma a realizar testes e configurações em todos os elementos envolvidos, gerar relatórios sobre os

dados armazenados no sistema, configurar os requisitos funcionais e operacionais do sistema de gerência, bem como utilizar corretamente as potencialidades de todos os aplicativos.

5.3.3. Treinar a equipe (formato Hands-On) da GTI para gerenciar e monitorar o novo firewall.

5.3.4. Fornecer treinamento sobre as políticas de segurança e os procedimentos de resposta a incidentes.

5.3.5. Treinar a equipe de TI para efetuar backups e restores de logs e configurações.

5.3.6. A CONTRATADA deverá apresentar o programa de capacitação e o cronograma com antecedência mínima de 05 (cinco) dias úteis antes de começar a capacitação.

5.4. **ITEM 4: SERVIÇOS DE SUPORTE E GARANTIA**

5.4.1. A licitante CONTRATADA deverá apresentar garantia ao(s) produto(s) de 36 (trinta e seis) meses contados do recebimento e aceite do(s) produto(s) pela DAE, com cobertura total para peças e serviços, incluindo deslocamentos de técnicos, quando necessários, para a execução dos serviços necessários à garantia.

5.4.2. Entende-se por "Suporte" ou "Manutenção", doravante denominada unicamente como Suporte", toda atividade do tipo "corretiva" não periódica que variavelmente poderá ocorrer, durante todo o período de garantia. A mesma possui suas causas em falhas e erros no Software/Hardware e trata da correção dos problemas atuais e não iminentes de fabricação dos mesmos. Este "Suporte" inclui os procedimentos destinados a recolocar em perfeito estado de operação os serviços e produtos ofertados, tais como:

5.4.2.1. Do hardware: apoio no processo de desinstalação, reconfiguração ou reinstalação decorrente de falhas de fabricação no hardware, fornecimento de peças de reposição, substituição de hardware defeituoso por defeito de fabricação, atualização da versão de drivers e firmwares, correção de defeitos de fabricação, ajustes e reparos necessários, de acordo com os manuais e as normas técnicas específicas para os recursos utilizados

5.4.2.2. Do software: atualização da versão de software (firmware e qualquer outro componente necessário para o funcionamento da solução), correção de defeitos de desenvolvimento do software, de acordo com os manuais e as formas técnicas específicas do fabricante para os recursos utilizados;

5.4.2.2.1. Quanto às atualizações pertinentes aos softwares: Entende-se como "atualização" o provimento de toda e qualquer evolução de software, incluindo correções, "patches", "fixes", "updates", "service packs", novas "releases", "versions", "builds", "upgrades", englobando inclusive versões não sucessivas, nos casos em que a solicitação de atualização de tais versões ocorra durante o período de garantia do contrato.

5.4.3. A CONTRATADA deverá fornecer Suporte técnico 24x7 com tempos de resposta definidos.

5.4.4. Abertura de chamados deverá ser diretamente no FABRICANTE via telefone (0800) ou Internet (Portal, Chat ou Sistema de Tickets) com envio de confirmação do número do chamado e demais andamentos via e-mail.

5.4.5. Os serviços de "Suporte" incluem:

5.4.5.1. Solução de problemas relativos à indisponibilidade da solução decorrentes de problemas e fabricação e desenvolvimento;

5.4.5.2. Solução de falhas ou defeitos no funcionamento, incluindo a instalação de arquivos para correção dos erros;

5.4.5.3. Substituição de hardware por outro de igual ou superior sem perdas de desempenho e/ou comprometimento dos serviços configurados (ex: RMA).

5.4.5.4. Atualizações de software e firmware.

5.4.5.5. Serviços de inteligência de ameaças e segurança.

5.4.5.6. Opções de serviços gerenciados e consultoria especializada.

5.4.6. Firewall de Alta Disponibilidade

5.4.6.1. Os prazos para a prestação dos serviços devem garantir a observância ao atendimento do seguinte Acordo de Níveis de Serviços (ANS) e sua SEVERIDADE:

Grau de Severidade	Quantidade equipamentos envolvidos	Prazo máx. para início do atendimento remoto	Prazo máx. para solução de contingência	Abertura RMA
Crítica	2	1 h	24 h	24 h
Importante	1	2 h		
Alta	1	2 h		
Média	1	8 h		
Baixa	1	48 h		

5.4.6.2. SEVERIDADE CRÍTICA - Solução totalmente inoperante (Interrupção total do serviço, falha completa do firewall). Isso em caso da parada dos 2 equipamentos simultaneamente (sendo problemas de hardware e/ou software): Prazo máximo de início de atendimento remoto de até 1 hora contados a partir do horário de abertura do chamado; Em caso de não solução do problema em até 4 horas, o fornecedor deverá fornecer uma solução de contingência com equipamento similar e/ou superior totalmente configurado e operacional em até 24 (vinte e quatro) horas contadas a partir da abertura do chamado.

5.4.6.3. SEVERIDADE IMPORTANTE - Solução parcialmente inoperante (1 dos hardwares param de funcionar) - Prazo máximo de início de atendimento remoto de até 02

horas úteis contadas a partir do horário de abertura do chamado. Em caso de identificação de problemas com hardware, deverá ser aberto a RMA em um prazo de até 72 horas do início da abertura do chamado.

5.4.6.4. SEVERIDADE ALTA - Degradação severa do desempenho, funções principais afetadas. Prazo máximo de início de atendimento remoto de até 02 horas contadas a partir do horário de abertura do chamado. Em caso de identificação de problemas com hardware, deverá ser aberto a RMA em um prazo de até 72 horas do início da abertura do chamado.

5.4.6.5. SEVERIDADE MÉDIA - Problemas menores, sem impacto direto na operação. Prazo máximo de início de atendimento de até 08 horas contadas a partir do horário de abertura do chamado.

5.4.6.6. SEVERIDADE BAIXA - Dúvidas, informações sobre procedimentos, Base de conhecimento sobre configuração ou atualização. Prazo máximo de início de atendimento de até 48 horas contadas a partir do horário de abertura do chamado.

5.4.6.7. SEVERIDADE EXTERNO - Solução inoperante, de forma parcial ou total, fruto de falha de elemento de hardware e/ou software não fornecido pela CONTRATADA. Neste caso, ficam suspensos todos os prazos de atendimento até que a CONTRATANTE resolva os problemas externos que provocam a inoperância da solução. Após a CONTRATANTE disponibilizar o ambiente de forma estável para a reativação da solução, a CONTRATADA Realizará avaliação da extensão do dano a solução e as partes definirão em comum acordo o prazo para a reativação da solução.

5.4.6.8. RMA CRÍTICA (Em caso de Severidade CRÍTICA). - O fornecedor deverá no prazo de no máximo 24 horas, habilitar uma solução de contingência para restabelecer o ambiente/serviços e no prazo máximo de 30 (trinta) dias corridos, substituir pela solução temporária pela solução definitiva.

5.4.6.9. RMA padrão (Em caso de Severidade IMPORTANTE, ALTA, MÉDIA E BAIXA) - O prazo máximo para substituição do equipamento não poderá exceder 30 (trinta) dias corridos da abertura do chamado.

5.4.6.10. Um chamado técnico somente poderá ser fechado após a confirmação do responsável da CONTRATANTE e o término de atendimento dar-se-á com a disponibilidade do recurso para uso em perfeitas condições de funcionamento no local onde o mesmo está instalado, ou se não houver resposta da CONTRATANTE pelo período de 72 horas úteis, poderá ocorrer o auto encerramento.

5.4.6.11. Na abertura de chamados técnicos, serão fornecidas informações, como Número de série (quando aplicável), anormalidade observada, nome do responsável pela solicitação do serviço e versão do software utilizada e severidade do chamado.

5.4.6.12. 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;

5.4.6.13. A CONTRATADA poderá solicitar a prorrogação de qualquer dos prazos para conclusão de atendimentos de chamados, desde que o faça antes do seu vencimento e devidamente justificado.

5.4.7. Um chamado técnico somente poderá ser fechado após a confirmação do responsável da CONTRATANTE e o término de atendimento dar-se-á com a disponibilidade do recurso para uso em perfeitas condições de funcionamento no local onde o mesmo está instalado, ou se não houver resposta da CONTRATANTE pelo período de 72 horas úteis, poderá ocorrer o auto encerramento.

5.4.8. Na abertura de chamados técnicos, serão fornecidas informações, como Número de série (quando aplicável), anormalidade observada, nome do responsável pela solicitação do serviço e versão do software utilizada e severidade do chamado.

5.4.9. 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;

5.4.10. A CONTRATADA poderá solicitar a prorrogação de qualquer dos prazos para conclusão de atendimentos de chamados, desde que o faça antes do seu vencimento e devidamente justificado.

5.4.11. A CONTRATADA deve prover, após a solução implementada, um pacote de, no mínimo, 40 horas válido por 12 meses, para suporte remoto especializado, com atendimento por especialistas bilíngues (português / inglês), baseados no Brasil.

5.4.12. Este suporte visa dirimir dúvidas, fazer um primeiro atendimento de nível 1 ou 2 e 3, em caso de ocorrências e fazer a interface com os especialistas do fabricante quando necessário.

5.5. CATÁLOGOS

5.5.1. A licitante declarada vencedora provisória do certame deverá apresentar, juntamente com a proposta final, catálogos dos produtos, equipamentos e materiais técnicos, manuais de uso e garantia, fornecidos para avaliação e validação do atendimento aos Requisitos deste Termo de Referência.

5.5.2. Caso seja constatado o não atendimento dos requisitos previstos neste Termo de Referência, a licitante será desclassificada.

5.5.3. Havendo no catálogo, mais de um modelo do objeto licitado, caberá a licitante indicar àquele que corresponde ao ofertado em sua proposta. A indicação do endereço eletrônico do catálogo do fabricante, em documento anexo à proposta, será aceita como alternativa, para fins de averiguação das especificações técnicas.

5.5.4. A exigência de catálogo e amostra, para a presente aquisição, se dá em razão da necessidade de verificar a compatibilidade do produto ofertado na proposta comercial das licitantes com o produto que será efetivamente entregue, bem como a necessidade de verificar a qualidade e preenchimento dos requisitos técnicos mínimos desse produto, com base em teste simples de conformidade de suas funcionalidades e desempenho, segundo as características mínimas descritas neste Termo de Referência, mediante aferição objetiva da equipe técnica da DAE. A amostra e catálogos deverão ser exigidos apenas da licitante que ofertar a melhor proposta, para efeitos de julgamento da licitação.

5.6. **CONSIDERAÇÕES FINAIS**

5.6.1. O equipamento selecionado deve ser capaz de se integrar à infraestrutura de rede existente e fornecer uma solução de segurança escalável e flexível para atender às necessidades futuras da organização.

5.6.2. A proposta deve incluir detalhes sobre licenciamento, garantia, serviços de implementação e treinamento.

5.6.3. A solução não se deve limitar à inspeção SSL, filtro web e de conteúdo, controle de aplicações, filtro DNS, proteção avançada contra malware, IPS, antivírus, proteção contra botnet e sandbox para ataques do dia zero.

5.6.4. A solução também deve possuir um gerenciamento centralizado, permitir relatórios e logs.

6. PRAZO DE ENTREGA

6.1. O prazo de entrega do (s) equipamento (s), objeto desta licitação, em conformidade com as amostras ou catálogos/folders apresentados e adjudicados, será de no máximo 90 (noventa) dias corridos, após a assinatura do contrato. Nos casos em que não houver a elaboração de contrato, o prazo contará da emissão da Ordem de Compras pela DAE, nos mesmos termos do contrato.

6.2. A entrega deve ser agendada com antecedência mínima de 24 horas, sob o risco de não ser autorizada;

6.3. Os SERVIÇOS DE INSTALAÇÃO devem ser iniciados em, no máximo, 15(quinze) dias corridos da entrega do equipamento e agendados com antecedência mínima de 3 dias, sob o risco de não ser autorizado; o prazo para finalização da instalação é 45(quarenta e cinco) dias corridos;

6.4. Para itens de software, estes devem ser fornecidos com ou sem mídia de instalação. No caso de não fornecimento de mídia, deve ser indicado local para download da instalação;

6.5. Para itens de software, devem ser apresentados chave única tipo serial ou qualquer outra forma de validação da ferramenta, comprovando perante o fabricante que se trata de uma ferramenta devidamente licenciada.

7. MODELO DE GESTÃO DO CONTRATO

7.1. A Fiscalização da execução de serviços caberá à GTI (Gerência de Tecnologia da Informação) da CONTRATANTE, ou a quem dela proposto seja, a quem incumbirá à prática de todos e quaisquer atos próprios ao exercício desse mister.

7.2. A LICITANTE VENCEDORA tem a obrigação de atender a todas as exigências informadas no Termo de Referência emitido e sendo parte integrante do edital.

7.3. O não cumprimento do prazo sem a devida justificativa ou dos pré-requisitos de contratação, em qualquer hipótese, poderá acarretar a rescisão contratual e sanções impostas pela CONTRATANTE.

8. CRITÉRIO DE PAGAMENTO

8.1. O pagamento referente aos itens previstos neste Termo de Referência será realizado de acordo com a entrega de cada item, após a emissão, por parte da CONTRATANTE, do TERMO DE ACEITE (conforme Anexo VI).

9. LOCAL DA PRESTAÇÃO DO SERVIÇO

9.1. Os trabalhos serão realizados na sede da DAE, localizada na Avenida Alexandre Ludke n.º 1500 na Vila Bandeirantes em Jundiaí - SP.

10. OBRIGAÇÕES DA LICITANTE VENCEDORA

Além das disposições contidas no Edital, constituirão ainda obrigações da licitante vencedora:

10.1. Fornecer os equipamentos conforme especificações técnicas constantes da sua proposta comercial, nos prazos constantes neste documento e no local, prazos e quantidades discriminadas;

10.2. O serviço de instalação deverá seguir, obrigatoriamente, as normas regulamentares do fabricante;

10.3. Fornecer e instalar materiais novos (sem uso, reforma ou recondicionamento) e que não estarão fora de linha de fabricação, pelo menos, nos próximos 90 (noventa) dias, de maneira a não prejudicar a execução dos objetos ora contratados;

10.4. Cumprir a garantia de funcionamento e prestar assistência técnica on-site aos equipamentos, na forma e prazos do presente Termo de Referência;

10.5. Nomear um preposto responsável pela contratação, para atendimento e entendimentos junto A DAE S.A.:

10.5.1. O preposto deverá ter competência para resolver imediatamente todo e qualquer assunto relacionado aos serviços contratados;

10.5.2. O preposto, não poderá executar efetivamente nenhuma das atividades contempladas nos itens do contrato, cabendo somente atuação nas atividades de gestão da equipe e relacionamento com a CONTRATADA;

10.5.3. O preposto deverá prestar apoio aos componentes da equipe da CONTRATADA;

10.5.4. O preposto deverá estar permanentemente à disposição para contato da DAE S.A., ou equipe técnica, nos dias úteis, no horário comercial para orientar em dúvidas relacionadas a garantia/suporte.

10.5.5. Atender prontamente quaisquer orientações e exigências do Fiscal do Contrato, inerentes à execução do objeto contratual;

10.6. Reparar quaisquer danos diretamente causados à CONTRATANTE ou a terceiros, por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da presente relação contratual, não excluindo ou reduzindo essa responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela CONTRATANTE. Apurado o dano e caracterizada sua autoria por qualquer empregado da Licitante Vencedora, esta pagará à CONTRATANTE o valor correspondente de acordo com instruções a serem fornecidas;

10.7. Responder por quaisquer acidentes de que possam ser vítimas seus empregados, quando em serviço nas dependências da CONTRATANTE;

10.8. Propiciar todos os meios e facilidades necessárias à fiscalização dos serviços pela CONTRATANTE, cujo representante terá poderes para sustar o serviço, total ou parcialmente, em qualquer tempo, sempre que considerar a medida necessária e recusar os materiais e equipamentos empregados que julgar inadequado;

10.9. Manter, durante toda a execução do contrato, as mesmas condições da habilitação;

10.10. Aprovar a conexão ou instalação, nos equipamentos, de produtos de hardware, externos ou internos, e/ou de software de outros fornecedores ou fabricantes, desde que tal iniciativa não implique em danos físicos ao equipamento e não constitua perda da vigência da Garantia;

10.11. Manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para prestação dos serviços;

10.12. Manter sigilo e não divulgar informações, dados pessoais e/ou pessoais sensíveis a que vier (em) ter acesso em decorrência de sua contratação;

10.13. Garantir o cumprimento dos prazos previstos neste Termo de Referência;

10.14. Se responsabilizar por todas as despesas de impostos, fretes, seguros, e outros custos que recaiam sobre os serviços objeto do presente Termo;

10.15. A CONTRATADA deverá recrutar em seu nome e sob sua inteira responsabilidade os profissionais conforme objeto da contratação, necessários à perfeita execução dos serviços, que tenham as qualificações técnicas constantes neste Termo, cabendo-lhes efetuar os pagamentos de salários e arcar com as demais obrigações trabalhistas, previdenciárias, fiscais e comerciais, inclusive responsabilidades decorrentes de acidentes, indenizações, substituições, seguros, assistência médica e quaisquer outros, em decorrência da sua condição de empregadora, sem qualquer solidariedade por parte do DAE S.A.

10.16. A CONTRATADA responsabiliza-se, em caráter irretratável e irrevogável, por quaisquer reclamações trabalhistas ou qualquer ato de natureza administrativa ou judicial, inclusive decorrentes de acidente de trabalho, que venham a ser intentadas por seus empregados, prepostos, colaboradores ou subcontratados, contra a DAE S.A., destacados pela CONTRATADA para a execução do objeto deste contrato, a qualquer tempo, seja a que título for, respondendo integralmente pelo pagamento de eventuais condenações, indenizações, multas, honorários advocatícios, custas processuais e demais encargos que houver, podendo ser denunciada em qualquer ação que for proposta para indenizar seus autores, aplicando-se ao presente contrato o disposto no artigo 125, inciso II, do Código de Processo Civil Brasileiro de 2015.

10.17. Efetuar o pagamento dos seguros, tributos, impostos e de toda e qualquer despesa referente aos serviços contratados e dos documentos a eles relativos, se necessários.

10.18. Substituir o profissional que seja considerado inapto para os serviços a serem prestados em até 05 (cinco) dias úteis, seja por incapacidade técnica, atitude inconveniente ou falta de urbanidade ou que venha a transgredir as normas disciplinares ou ao código de ética da DAE S.A.;

10.19. Aceitar que a DAE S.A. possa rejeitar, no todo ou em parte, os serviços executados em desacordo com as normas estabelecidas neste Termo de Referência e/ou nos instrumentos que o integram.

10.20. Responsabilizar-se pelo comportamento dos seus empregados e por quaisquer danos que estes ou seus prepostos venham porventura a ocasionar a DAE S.A., seus clientes, ou a terceiros, durante a execução dos serviços.

10.21. Solicitar autorização prévia da DAE S.A. antes de utilizar recursos de softwares que necessitem de aquisição de licença de uso;

10.22. Reportar à DAE S.A. quaisquer anormalidades, erros e irregularidades observados no desenvolvimento dos serviços contratados, causados por ações dos profissionais contratados, de servidores públicos ou de terceiros.

11. DAS OBRIGAÇÕES E RESPONSABILIDADES DA DAE S.A.

Serão obrigações e responsabilidade da DAE S.A., além de outras previstas neste Termo e futuro contrato:

11.1. Exigir o cumprimento de todas as obrigações assumidas pela LICITANTE VENCEDORA;

11.2. Exercer o acompanhamento e a fiscalização do contrato a ser celebrado com a LICITANTE VENCEDORA, por funcionário especialmente designado como gestor e encaminhando os apontamentos à autoridade competente para eventuais providências cabíveis;

11.3. Notificar, por escrito, à LICITANTE VENCEDORA sobre quaisquer irregularidades encontradas no cumprimento da contratação;

11.4. Pagar a LICITANTE VENCEDORA os valores devidos à execução dos serviços, no prazo e condições estabelecidas neste Termo e futuro contrato;

11.5. Efetuar as retenções tributárias devidas sobre o valor da Nota Fiscal/Fatura emitida pela LICITANTE VENCEDORA; e

11.6. Designar, formalmente, gestor (es) para acompanhar e fiscalizar a execução do contrato a ser firmado com a LICITANTE VENCEDORA.

11.7. Acompanhar e fiscalizar a qualidade dos serviços realizados;

11.8. Quando o serviço for realizado nas dependências da DAE S.A., disponibilizar o acesso, espaço físico e infraestrutura técnica para que o serviço possa ser realizado pela LICITANTE VENCEDORA, resguardadas as normas de sigilo e segurança impostas pela DAE S.A.;

11.9. Acompanhar, fiscalizar e validar, todas as etapas da prestação dos serviços correlatos à sua respectiva área de atuação através dos gestores definidos pela Diretoria Técnica;

11.10. Fiscalizar e cobrar o cumprimento dos prazos estabelecidos em todas as atividades nas quais os recursos da LICITANTE VENCEDORA estiverem envolvidos;

11.11. Fornecer as especificações técnicas dos sistemas e serviços a serem executados pela LICITANTE VENCEDORA.

12. CONDIÇÕES DE ACEITE

12.1. Os equipamentos deverão ser novos e sem uso. Não serão aceitos equipamentos usados, remanufaturados ou de demonstração. Os equipamentos deverão ser entregues nas caixas lacradas pelo fabricante, não sendo aceitos equipamentos com caixas violadas. A DAE S.A. poderá efetuar consulta do número de série do equipamento, junto ao fabricante, informando data de compra e empresa adquirente, confirmando a procedência legal dos equipamentos;

12.2. Após a instalação física e lógica, os equipamentos deverão prontos para uso;

12.3. O TERMO DE ACEITE (Anexo VI) somente será dado após comprovação da entrega e o efetivo cumprimento de todas as exigências e serviços da presente especificação técnica.

12.4. Declaração que ateste a inexistência da prática de "registro de oportunidade" (conforme Anexo I deste Edital). Essa declaração tem por objetivo garantir o princípio constitucional da isonomia e a seleção da proposta mais vantajosa para a Administração Pública.

13. SIGILO

Condições de Manutenção de Sigilo.

13.1. Quaisquer informações obtidas durante a execução das atividades devem ficar restritas ao conhecimento das pessoas que estejam diretamente envolvidas nas atividades relacionadas à execução do objeto do Termo de Referência.

13.2. Em caso de dúvida acerca da confidencialidade de determinada informação, ela deve ser tratada sob sigilo até que a DAE S.A. autorize, formalmente, a tratá-la de forma diferente.

13.3. A DAE S.A. e a LICITANTE VENCEDORA devem formalizar compromisso para não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução

dos serviços objeto do Termo de Referência, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas informações, que se restringem estritamente ao cumprimento do objeto contratual.

13.4. É vedado efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio da DAE S.A.

13.5. A LICITANTE VENCEDORA deve comprometer-se a estar ciente e em conformidade com as normas de segurança da informação da DAE S.A., bem como à legislação pertinente.

13.6. Devem ser tomadas todas as medidas necessárias à proteção da informação sigilosa da DAE S.A., evitando e prevenindo a revelação a terceiros, sem a devida e prévia autorização formal da DAE S.A.

13.7. Tanto no âmbito administrativo, quanto técnico, a LICITANTE VENCEDORA deve formalmente informar as medidas aplicadas para a manutenção da confidencialidade das informações obtidas durante a execução do objeto.

13.8. Estas medidas passarão por uma avaliação da área responsável pela informática da DAE S.A. que determinará a eficácia das mesmas, e poderá solicitar alterações ou complementações.

13.9. Quando requeridas, as informações deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

13.10. A DAE S.A. deverá ser comunicada, de imediato e de forma expressa, e antes de qualquer divulgação, os casos em que houver obrigação de revelar qualquer uma das informações, por determinação judicial ou ordem de órgão competente.

13.11. As pessoas que, em nome da LICITANTE VENCEDORA, terão acesso às informações sigilosas deverão ser previamente nominadas.

13.12. Quando do encerramento definitivo do CONTRATO, deverá ser entregue à DAE S.A. todo e qualquer material de propriedade deste, inclusive notas pessoais envolvendo matérias sigilosas relacionadas com a DAE S.A., registros de documentos de qualquer natureza que tenham sido usados, criados ou estado sob controle da LICITANTE VENCEDORA.

MATRIZ DE RISCOS

Os principais riscos envolvidos na contratação estão indicados nas planilhas abaixo e devem ser considerados e avaliados pela CONTRATADA para um perfeito desenvolvimento das atividades.

É vedada a celebração de aditivos decorrentes de eventos supervenientes alocados, na matriz de riscos, como de responsabilidade da CONTRATADA.

EVENTO DE RISCO	IMPACTO	RESPONSÁVEL
Indisponibilidade financeira	Alto	CONTRATANTE
Especificação insuficiente para contratação do serviço	Alto	CONTRATANTE
Recursos administrativos procedentes	Baixo	CONTRATANTE
Recebimento de propostas com valores imprecisos	Médio	CONTRATANTE
Falência do contrato	Médio	CONTRATANTE
Não haver participantes no Processo Licitatório	Alto	CONTRATANTE
Haver somente um participante no Processo Licitatório	Médio	CONTRATANTE
O não fornecimento dos produtos contratados	Alto	CONTRATADA
Entrega dos produtos com as características divergentes ao processo licitado	Médio	CONTRATADA
Emissão de Nota Fiscal com dados incorretos ou divergentes	Baixo	CONTRATADA

.X.X.X.