ATO CONVOCATÓRIO DE COLETA DE PREÇOS

PROCESSO Nº 133/25

CONTRATAÇÃO DE EMPRESA PARA FORNECIMENTO DE INFRAESTRUTURA DE FIREWALL COMO HAAS, INCLUINDO INSTALAÇÃO E CONFIGURAÇÃO, COM O OBJETIVO DE REFORÇAR A SEGURANÇA DA REDE E IMPLEMENTAR VPNS SITE-TO-SITE, INTEGRAÇÃO NA NUVEM E ASSEGURANDO COMUNICAÇÃO SEGURA, TRÁFEGO ENTRE AS UNIDADES DA SEDE ADMINISTRATIVA E SEDE ASSISTENCIAL DA FUNDAÇÃO DO ABC – CONTRATO DE GESTÃO DE SÃO MATEUS, PARA O PERÍODO DE 12 (DOZE) MESES.

1. PREÂMBULO

Acha-se aberta na FUNDAÇÃO DO ABC, localizada na Avenida Lauro Gomes, n° 2000 – Príncipe de Gales – Santo André/SP – CEP 09060-650, inscrita no CNPJ/MF sob o nº. 57.571.275/0001-00, **o ATO CONVOCATÓRIO visando a Contratação, "tipo menor preço GLOBAL", de empresa especializada em** FORNECIMENTO DE INFRAESTRUTURA DE FIREWALL COMO HAAS, INCLUINDO INSTALAÇÃO E CONFIGURAÇÃO, COM O OBJETIVO DE REFORÇAR A SEGURANÇA DA REDE E IMPLEMENTAR VPNS SITE-TO-SITE, INTEGRAÇÃO NA NUVEM E ASSEGURANDO COMUNICAÇÃO SEGURA, TRÁFEGO ENTRE AS UNIDADES DA SEDE ADMINISTRATIVA E SEDE ASSISTENCIAL DA FUNDAÇÃO DO ABC – CONTRATO DE GESTÃO DE SÃO MATEUS, PARA O PERÍODO DE 12 (DOZE) MESES, em conformidade com as especificações técnicas constantes do Termo de Referência – Anexo I, parte integrante deste Ato Convocatório.

1.1. O ATO CONVOCATÓRIO estará disponível para download no site da Fundação do ABC (www.fuabc.org.br), na aba "PUBLICAÇÕES OFICIAIS – EDITAIS".

1.2. Os envelopes (**Envelope 1 – Proposta e Envelope 2 – Documentação**) deverão ser entregues na Avenida Lauro Gomes, n° 2000 – Príncipe de Gales – Santo André/SP – CEP 09060-650, **até o dia 01 de agosto de 2025** às 16h00min, em conformidade com as disposições a seguir:

2. DO OBJETO

2.1. A presente coleta de preços tem por objeto a Contratação, "tipo menor preço GLOBAL", de empresa especializada em FORNECIMENTO DE INFRAESTRUTURA DE FIREWALL COMO HAAS, INCLUINDO INSTALAÇÃO E CONFIGURAÇÃO, COM O OBJETIVO DE REFORÇAR A SEGURANÇA DA REDE E IMPLEMENTAR VPNS SITE-TO-SITE, INTEGRAÇÃO NA NUVEM E ASSEGURANDO COMUNICAÇÃO SEGURA, TRÁFEGO ENTRE AS UNIDADES DA SEDE ADMINISTRATIVA E SEDE ASSISTENCIAL DA FUNDAÇÃO DO ABC – CONTRATO DE GESTÃO DE SÃO MATEUS, PARA O PERÍODO DE 12 (DOZE) MESES conforme condições estabelecidas no Termo de Referência e seus anexos, parte integrante deste instrumento.

3. DAS CONDIÇÕES DE PARTICIPAÇÃO E EXECUÇÃO DO CONTRATO

3.1. Cada proponente deverá apresentar **dois envelopes**, um contendo o **ENVELOPE 1 - PROPOSTAS COMERCIAIS GLOBAL**, outro com o **ENVELOPE 2 - DOCUMENTAÇÃO** - que deverão ser **entregues separadamente**, **única via**, **em envelopes fechados e lacrados**, **rubricados no fecho** e **identificados com o nome da empresa**, **o número do processo** e o **seu objeto**, **nome**, **telefone** **e** **e-mail** com o nome do proponente e contendo em suas partes externas e frontais, em caracteres destacados, os seguintes dizeres em:

ENVELOPE N° 01: PROPOSTA COMERCIAL
FUNDAÇÃO DO ABC - CONTRATO DE GESTÃO DE SÃO MATEUS – SEGURANÇA DA REDE E IMPLEMENTAR VPNS SITE-TO-SITE
COLETA DE PREÇOS Nº 133/25
RAZÃO SOCIAL DO PROPONENTE
CNPJ N° XXXX
NOME DO RESPONSAVEL:
EMAIL:
TELEFONE:

ENVELOPE N° 02: DOCUMENTAÇÃO
FUNDAÇÃO DO ABC - CONTRATO DE GESTÃO DE SÃO MATEUS – SEGURANÇA DA REDE E IMPLEMENTAR VPNS SITE-TO-SITE
COLETA DE PREÇOS Nº 133/25
RAZÃO SOCIAL DO PROPONENTE
CNPJ N° XXXX
NOME DO RESPONSAVEL:
EMAIL:
TELEFONE:

3.1.1. Os envelopes referentes as propostas (envelope 1) e documentação (envelope 2) deverão ser entregues até a data limite de recebimento, sob pena de, não o fazendo, ser considerada inabilitada para o certame;

3.2. A Razão ou Denominação Social da empresa constante dos envelopes ou de quaisquer outros documentos deverão ser a mesma constante do Cadastro Nacional de Pessoa jurídica, vedada a utilização de nome "fantasia" ou nome incompleto.

3.3. A proposta comercial deverá ser apresentada impressa sem emendas ou rasuras.

3.4. Não será admitida a participação de consórcios, bem como as participações de empresas impedidas por lei.

3.5. Não será admitida a subcontratação de serviços na execução do contrato decorrente desta Coleta de Preços, salvo se houver autorização da **CONTRATANTE**.

3.6. A administração da **CONTRATANTE** fica reservada o direito de efetuar diligências em qualquer fase da Coleta de Preços para verificar a autenticidade e veracidade dos

documentos e informações apresentadas nas Propostas, bem como esclarecer ou complementar a instrução do processo, vedada à inclusão, posterior de documento ou informação exigido neste ato convocatório.

3.7. O serviço do objeto deste certame terá validade de 12 (doze) meses, a contar da data de sua assinatura, nos termos do regulamento de compras da Fundação do ABC - Edição 2022, podendo ser acessado através do link (https://fuabc.org.br/comunicacao/regulamento-de-compras/).

4. DOCUMENTOS EXIGIDOS DA VENCEDORA DA PRESENTE COLETA DE PREÇOS (ENVELOPE 2)

4.1. A Documentação deverá estar contida no Envelope nº 02 – Documentação, devidamente lacrado, conforme item 3.1 acima.

4.1.1. O Envelope nº 2 (Documentação) deverá ser entregue juntamente com o Envelope nº 1 (Proposta Comercial), sob pena de, não o fazendo, ser considerada inabilitada para o certame.

4.1.2. Necessariamente a proposta comercial deverá ser entregue em envelope lacrado e identificado como envelope 1 e a documentação exigida pela cláusula 4 do presente Ato convocatório, deverá ser entregue em **envelope separado** e identificado como Envelope 2.

4.1.3. O Setor de Compras, procederá à abertura dos ENVELOPES 1 – PROPOSTA COMERCIAL apresentados e após julgamento da melhor oferta, será aberto o ENVELOPE 2 – DOCUMENTAÇÃO. **Somente a empresa melhor classificada** terá sua documentação submetida à avaliação. O Envelope nº 2 (Documentação) deverá conter:

4.2. Ato Constitutivo, Estatuto ou Contrato Social em vigor, devidamente registrados, tratando-se de sociedades comerciais e no caso de sociedades por ações, acompanhados de documentos de eleição de seus administradores. No ato constitutivo deverá estar contemplada, dentre os objetivos sociais, a atividade que autorize a prestação de serviços exigidos no objeto desta coleta de preços.

4.2.1. Registro comercial, no caso da empresa individual;

4.3. Cartão de Inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ), emitido em até 60 (sessenta) dias anteriores à data de publicação do Ato Convocatório, desde que não tenha ocorrido alterações contratuais societárias após sua emissão.

4.4. Prova de inscrição no Cadastro de Contribuintes estadual e/ou municipal, se houver, relativo à sede da empresa participante, pertinente ao seu ramo de atividade e compatível com o objeto contratado.

4.5. Prova de regularidade com as Fazendas Públicas:

4.5.1. Prova de quitação ou Certidão Conjunta Negativa ou Positiva com efeito de

Negativa dos Tributos Federais administrados pela Secretaria da Receita Federal do Brasil e quanto à Dívida Ativa da União de competência da Procuradoria Geral da Fazenda Nacional, expedida no local do domicílio ou sede da licitante, respectivamente, em conjunto, nos termos da IN/RFB nº 734/07 e do Decreto nº 6.106/2007).

4.5.2. Estadual (Débitos Tributários Não Inscritos na Divida Ativa do Estado de São Paulo e Certidão Negativa de Débito Inscritos da Dívida Ativa do Estado de São Paulo) conforme o domicílio ou sede da participante.

4.5.3. Municipal (certidão de tributos mobiliários e imobiliários), conforme o domicílio ou sede da participante.

4.5.3.1. Caso não a empresa não possua imóveis em seu CNPJ, para emissão da certidão de Rol Nominal;

4.5.4. Serão admitidas certidões positivas com efeito de negativas ou outras equivalentes na forma da lei.

4.6. Certidão Negativa, de pedido de falência, concordata, recuperação judicial ou extrajudicial expedida pelo distribuidor da sede da pessoa jurídica, emitida no período de até 30 (trinta) dias anteriores à data fixada para a entrega dos envelopes.

4.6.1 Nas hipóteses em que a certidão encaminhada for positiva, deve a licitante apresentar comprovante da homologação/deferimento pelo juízo competente do plano de recuperação judicial/extrajudicial em vigor, bem como deverá apresentar cópia do ato de nomeação do administrador judicial ou se o administrador for pessoa jurídica, o nome do profissional responsável pela condução do processo e, ainda, declaração, relatório ou documento equivalente do juízo ou do administrador, de que está cumprindo o plano de recuperação judicial;

4.7. Prova de inexistência de débitos trabalhistas, através do documento "Certidão Negativa de Débitos Trabalhistas – CNDT ou Certidão Positiva de Débitos Trabalhistas com os mesmos efeitos da CNDT", expedida pela Justiça do Trabalho conforme a Lei n° 12.440/2011.

4.8. Prova de Regularidade para com o Fundo de Garantia por Tempo de Serviço (FGTS).

4.9. Balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, vedada a substituição por balancete ou balanço provisório.

4.10. A empresa deverá apresentar com base no balanço e demonstrações contábeis referidos no subitem anterior, os cálculos dos índices contábeis abaixo relacionados, que deverão ser subscritos (atestados) por profissional devidamente registrado no CRC (Conselho Regional de Contabilidade), devendo constar o nome, assinatura e número do CRC do profissional.

4.11. A proponente deverá apresentar atestado(s) de capacidade técnica, expedido(s) por Pessoa Jurídica de Direito Público ou Privado, em nome da proponente, que comprove a execução, para quaisquer das entidades mencionadas neste item, de serviços similares ao objeto deste Memorial de Coleta de Preços, executados por no mínimo 12 (doze) meses.

4.11.1. O(s) Atestado(s) de Capacidade Técnica (Técnico Operacional), deverão ser elaborados(s) em papel timbrado e/ou conter carimbo oficial do CNPJ, contemplando as informações detalhadas do(s) fornecimento(s) ou serviço(s) prestado(s), sendo assinado(s) e com identificação do nome, cargo ou função do(s) emitente(s).

4.11.2. A comprovação de execução dos serviços mencionados poderá ser feita mediante apresentação de 01 (um) ou mais atestados referente a um único ou a diversos contratos e/ou Termos de Credenciamento.

4.12. Consulta de Idoneidade junto ao Tribunal de Contas do Município de São Paulo;

4.13. Consulta de Idoneidade junto ao Tribunal de Contas do Estado de São Paulo;

4.14. Consulta de Idoneidade junto ao Tribunal de Contas da União;

4.15. Consulta de Idoneidade junto ao Portal da Transparência da Controladoria Geral da União (CGU-PJ, CEIS, CNEP e CEPIM);

4.16. Consulta de Idoneidade junto ao Sistema de Cadastramento Unificado de Fornecedores – SICAF;

4.17. Consulta de Idoneidade junto ao Cadastro Integrado de Condenação por Ilícitos Administrativos - CADICON E CNIA;

4.18. Declaração de Cumprimento de Lei Anticorrupção e das políticas da Fundação do ABC, conforme modelo Anexo IV;

4.19. Declaração (com logotipo da empresa) "Quadro Societário", acerca da não incorrência da Proponente das vedações estabelecidas no artigo 6º do Regulamento Interno de Compras da Fundação do ABC, nos moldes do Anexo V;

4.20. Declaração de não impedimentos, conforme Anexo VI;

4.21. Declaração que, de acordo com as especificações fornecidas pela CONTRATANTE, há perfeitas condições para o serviço Anexo VII;

4.22. Declaração de aceitação do REGULAMENTO INTERNO DE COMPRAS E CONTRATAÇÕES DA FUNDAÇÃO DO ABC. Anexo VIII;

4.23. Questionario Due Diligence de Complience de Fornecedores Anexo IX;

4.24. Declaração de cumprimento ao código de conduta ética Anexo X;

4.25. Atestados de vistoria dos locais de execução dos serviços, onde será declarado que a Proponente tem pleno conhecimento dos locais em que se desenvolverão os serviços, dos acessos e de todas as demais condições e eventuais dificuldades para execução dos serviços do objeto, devendo a vistoria ser realizada pelo responsável técnico da empresa Anexo XI.

4.26. Caso a proponente opte pela não realização de visita técnica deverá apresentar declaração de declínio de sua realização, declarando ainda que tem pleno conhecimento das condições e peculiaridades inerentes à natureza do objeto da Coleta de Preço Anexo XII.

4.27. Declaração de que não empresa menor Anexo XIII;

4.28. Declaração da empresa, responsabilizando-se sob a pena da lei, no caso de seus funcionários ou prepostos vierem a mover futuras ações trabalhistas ou cíveis contra a mesma, ficando a Fundação do ABC excluída do polo passivo, ou seja, da responsabilidade solidária ou subsidiária Anexo XIV.

4.29. Certidão De Responsabilidade Técnica De Pessoa Jurídica;

4.30. Toda documentação específica, pertinente ao ramo de atividade;

4.31. Prova do Registro nos órgãos competentes, quando couber;

4.32. Certificação de órgão competente, quando cabível;

5. PROPOSTAS COMERCIAIS

5.1. As **propostas comerciais** estará contida no Envelope nº 01 – Proposta Comercial, **devidamente lacrado**, conforme item 3.1 acima, devendo ser apresentada da seguinte forma:

5.2. As propostas Comerciais em papel timbrado da empresa participante com o **valor por unidade, valor mensal e valor total**, em algarismo e por extenso, conforme modelo de proposta no Anexo II do Ato Convocatório.

5.3. Especificações dos materiais e/ou serviços oferecidos em consonância com o objeto do presente Ato convocatório.

5.4. Planilha de preços ofertados, contendo:
5.4.1. Preço por unidade;
5.4.2. Preço total mensal;
5.4.3. Preço global 12 (doze) meses;
5.4.4. Valor mensal e anual escrito por extenso.

5.5. Os preços apresentados deverão ser em reais, com até duas casas decimais, expressos em algarismos e por extenso, computados todos os custos básicos diretos, bem como tributos, encargos sociais e trabalhistas e quaisquer outros custos ou despesas que incidam ou venham a incidir direta ou indiretamente sobre o objeto do ato convocatório descritivo, relacionados à plena execução do objeto durante todos o período de contratação.

5.6. Prazo de validade da proposta: não inferior a 60 (sessenta) dias.

5.7. Deverão estar inclusos no preço global dos itens apresentados na proposta eventuais serviços de mão de obra, e todas as despesas necessárias à execução da entrega, incluindo-se transporte e montagem, livres de quaisquer ônus para a CONTRATANTE, sejam estes de natureza trabalhista, previdenciária, ou ainda, transportes, veículos, combustível, materiais, tributos, dentre outros.

5.8. O preço global deverá ser compatível com o de mercado, na data da apresentação da proposta, formulada em moeda corrente nacional.

5.8.1. O valor máximo global para os serviços será de **R$252.105,20 (duzentos e cinquenta e dois mil e cento e cinco reais e vinte centavos),** para 12 (doze) meses.

5.9. A apresentação da proposta significará expressa aceitação de todas as disposições deste instrumento.

5.10. Serão desclassificadas as propostas que não atenderem às exigências do presente ATO CONVOCATÓRIO e seus anexos, que sejam omissas ou apresentarem irregularidades ou defeitos capazes de dificultar o julgamento, e ainda, aquelas que contemplem preços acima do valor máximo para contratação ou inexequíveis.

6. DO PROCESSAMENTO E JULGAMENTO

6.3. As propostas comerciais serão analisadas pelo Setor de Compras que lavrará o competente Termo de Julgamento, cabendo submetê-lo à decisão do Diretor Geral da Fundação do ABC, nos termos regimentais.

6.4. A presente Coleta de Preços é do tipo "menor preço GLOBAL", que serão julgados de acordo com os seguintes critérios:

6.4.1. Adequação das propostas a especificação do produto a ser adquirido;
6.4.2. Qualidade;
6.4.3. Menor preço;
6.4.4. Prazo de fornecimento;
6.4.5. Condições de pagamento e maior retorno econômico;
6.4.6. Outros critérios previstos no Regulamento de Compras.

6.5. O Setor de Compras procederá a classificação das empresas, por preço, do menor para o maior;

6.6. Será considerada vencedora a empresa que atenda todas as exigências formais do presente ato convocatório, desde que os produtos e/ou serviços estejam de acordo com todas as exigências e especificações mencionadas nos Anexos;

6.7. Em caso de empate, entre duas ou mais propostas, serão utilizados os seguintes critérios de desempate, nesta ordem:

6.7.1. Disputa final, hipótese em que os participantes empatados poderão apresentar nova proposta em ato contínuo à classificação;
6.7.2. Caso o empate persista, será realizado sorteio.

6.8. As propostas comerciais serão avaliadas pelo Setor de Compras, devidamente assessorada por Comissão Técnica nomeada, caso julgue necessário.

6.9. Serão desclassificadas as propostas que não atendam às exigências deste Ato convocatório.
6.9.1. Serão desclassificadas as propostas que:
6.9.1.1. contiverem vícios insanáveis;
6.9.1.2. não obedecerem às especificações técnicas pormenorizadas no edital e seus anexos;
6.9.1.3. apresentarem preços inexequíveis ou permanecerem acima do orçamento estimado para a contratação;
6.9.1.4. não tiverem sua exequibilidade demonstrada, quando exigido pela Contratante;
6.9.1.5. apresentarem desconformidade com quaisquer outras exigências do edital, desde que insanável.

6.9.2. Consideram-se preços manifestamente inexequíveis aqueles que, comprovadamente, forem insuficientes para a cobertura dos custos decorrentes da contratação pretendida;

6.10. A inexequibilidade dos valores referentes a itens isolados da planilha de custos e formação de preços não caracteriza motivo suficiente para a desclassificação da proposta, desde que não contrariem exigências legais;

6.10.1. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderá ser efetuada diligência, para efeito de comprovação de sua exequibilidade, podendo ser adotado, dentre outros, os seguintes procedimentos:
6.10.1.1. questionamentos junto à proponente para a apresentação de justificativas e comprovações em relação aos custos com indícios de inexequibilidade;
6.10.1.2. verificação de Acordos, Convenções ou Dissídios Coletivos de Trabalho;
6.10.1.3. levantamento de informações junto ao Ministério do Trabalho;
6.10.1.4. consultas a entidades ou conselhos de classe, sindicatos ou similares;
6.10.1.5. pesquisas em órgãos públicos ou empresas privadas;
6.10.1.6. verificação de outros contratos que o proponente mantenha com a Administração ou com a iniciativa privada;
6.10.1.7. pesquisa de preço com fornecedores dos insumos utilizados, tais como: atacadistas, lojas de suprimentos, supermercados e fabricantes;
6.10.1.8. verificação de notas fiscais dos produtos adquiridos pelo proponente;
6.10.1.9. levantamento de indicadores salariais ou trabalhistas publicados por órgãos de pesquisa;
6.10.1.10. estudos setoriais;

6.10.1.11. consultas às Fazendas Federal, Distrital, Estadual ou Municipal; e
6.10.1.12. análise de soluções técnicas escolhidas e/ou condições excepcionalmente favoráveis que o proponente disponha para a prestação dos serviços.

6.11. Quando o proponente apresentar preço final inferior a 30% da média dos preços ofertados para o mesmo item, e a inexequibilidade da proposta não for flagrante e evidente pela análise da planilha de custos e formação de preços, não sendo possível a sua imediata desclassificação, será obrigatória a realização de diligências para aferir a legalidade e exequibilidade da proposta.

6.12. Na hipótese de todas as Propostas serem desclassificadas e a critério do Setor de Compras, poderá ser fixado o prazo de 05 (cinco) dias úteis para apresentação de nova proposta comercial.

6.13. O resultado final do presente certame será publicado no site da Fundação do ABC (www.fuabc.org.br).

6.14. Os interessados deverão acompanhar o resultado final através do sítio eletrônico da Fundação do ABC.

7. DOS QUESTIONAMENTOS E ESCLARECIMENTOS

7.1. Os questionamentos e/ou esclarecimentos do ATO CONVOCATÓRIO deverão ser formalizados em papel timbrado da empresa e protocolados no Departamento de Compras da FUNDAÇÃO DO ABC, em até 02 (dois) dias úteis anterior à data fixada para entrega de propostas;

7.2. Havendo questionamento por quaisquer dos interessados no certame, a FUNDAÇÃO DO ABC, poderá publicar a suspensão do ato convocatório, a fim de sanar as dúvidas eventualmente surgidas, se assim entender como necessária.

7.3. Os questionamentos e/ou esclarecimentos não suspendem o certame, salvo, em caso de análise técnica que demande tempo maior para análise, razão pela qual a suspensão será publicada no site da FUNDAÇÃO DO ABC (www.fuabc.org.br).

8. DAS IMPUGNAÇÕES DO ATO CONVOCATÓRIO

8.1. Qualquer pessoa é parte legitima para impugnar os termos dos Atos Convocatórios, desde que formalmente e protocoladas, junto ao Departamento de Compras da Fundação do ABC, em até 2 (dois) dias úteis anteriores a data final fixada para recebimento das propostas, das 09:00 às .16:00 horas de segunda a sexta-feira.

8.2. A impugnação oferecida dentro do prazo estabelecido no item anterior, será encaminhada imediatamente à autoridade máxima da Unidade, para que esta se manifeste

quanto à aplicação do efeito suspensivo ou não a essa.

8.3. Havendo acolhimento pelo Setor Jurídico da Fundação do ABC, das impugnações formuladas, o departamento responsável publicará no site da Fundação do ABC (www.fuabc.org.br).

8.4. Não serão reconhecidas as impugnações cuja petição tenha sido apresentada fora do prazo. Também não são reconhecidas as impugnações que tenham sido encaminhadas por Fax ou qualquer outra forma que não a descrita neste item.

8.5. Se procedente e acolhida a impugnação deste Edital, seus vícios serão sanados e nova data será designada para a realização do certame.

9. DAS VISTAS

9.1. Serão franqueadas vistas ao processo, a todos interessados, a partir da Publicação do resultado final, qual seja, expediente do Setor de Compras após análise da documentação da empresa classificada e convocada para referida entrega, ocasião em que será aberto prazo para Recursos e contrarrazões.

9.2. As vistas deverão ser realizadas formalmente e protocoladas, caso não seja a pessoa que compõe o quadro do contrato social, necessário apresentar de forma física a procuração dando a autorização, junto ao Departamento de Compras da Fundação da ABC, no período das 09:00 às 16:00 horas de segunda a sexta-feira.

10. DOS RECURSOS

10.1. Caberá recurso das decisões do Setor de Compras da Fundação do ABC, no prazo de 02 (dois) dias úteis da publicação do resultado final no site www.fuabc.org.br, desde que formalmente e protocolados, junto ao Departamento de Compras da Fundação do ABC, das 09:00 às 16:00 horas de segunda a sexta-feira.

10.2. Estarão legitimados, na apresentação de recurso, os representantes legais da empresa e/ou aqueles que por procuração específica.
10.3. A Fundação do ABC, havendo interposição de recurso por quaisquer das empresas, notificará as demais através de e-mail, para que, havendo interesse, apresentem suas impugnações e/ou contrarrazões, por escrito, em 02 (dois) dias úteis, impreterivelmente da notificação, das 09:00 às 16:00.

10.4. Os recursos deverão observar os seguintes requisitos:
10.4.1. serem dirigidos à autoridade competente para apreciá-los;
10.4.2. serem digitados e devidamente fundamentados;
10.4.3. serem rubricados e assinados por representante legal da recorrente, devidamente credenciado, ou por procurador devidamente habilitado.

10.5. Os recursos e contrarrazões deverão ser entregues na sede da Fundação do ABC - Santo André, endereçadas à autoridade que tiver editado o ato ou proferido a decisão recorrida, até às 16:00 horas da data de seu vencimento.

10.6. Não serão conhecidos os recursos apresentados fora do prazo legal e/ou subscritos por representante não habilitado legalmente ou não identificado no processo para responder pela proponente.

11. DO CONTRATO

11.1. A participante vencedora deverá comparecer à sede da CONTRATANTE, no prazo máximo de 01 (um) dia útil, contados da convocação feita pela Seção competente para esse fim, apta para assinatura do respectivo Contrato, sob pena de, não o fazendo, ficar a mesma impossibilitada de participar de futuras Coletas de Preços da CONTRATANTE.

11.2. O presente Ato convocatório, inclusive seus anexos, integrará o contrato que vier a ser firmado com a empresa vencedora da Coleta de Preços.

11.3. Fica desde já eleito o foro da Comarca de Santo André para dirimir quaisquer questões oriundas da presente coleta de preços e do contrato que em decorrência dela vier a ser firmado.

12. DA EXECUÇÃO DO CONTRATO

12.1. Os serviços deverão ser iniciados, pela CONTRATADA, somente após a assinatura do Contrato.

12.2. A CONTRATADA deverá realizar os serviços designado no contrato, emitindo a nota fiscal apenas após o relatório aprovado.

12.3. A CONTRATADA deverá estar em condições de executar os serviços a partir da data da assinatura do contrato e manter essa condição durante a vigência do contrato, atendendo a demanda encaminhada pelos setores e departamentos da CONTRATANTE, incluindo-se eventuais acréscimos ou supressões ao objeto e, consequentemente, ao valor do contrato, limitando a 25% (vinte e cinco por cento).

12.4. A CONTRATANTE fiscalizará obrigatoriamente a execução do contrato, a fim de verificar se para os serviços, foram observadas as especificações e demais requisitos nela previstas, reservando-se o direito de rejeitar os itens que, a seu critério, não forem considerados de acordo com a especificação.

12.5. A fiscalização, por parte da CONTRATANTE, não eximirá a CONTRATADA das responsabilidades previstas no Código Civil e dos danos que vier a causar à CONTRATANTE ou a terceiros, por culpa ou dolo de seus funcionários ou de seus prepostos na execução do Contrato.

13. DAS PENALIDADES

13.1. Pela inexecução total ou parcial do contrato, a **CONTRATANTE** poderá, garantida a defesa prévia, aplicar à **CONTRATADA**, as seguintes penalidades:

13.1.1. Multa de 3% (três por cento) sobre o valor do contrato, na recusa da empresa vencedora em assiná-lo dentro do prazo estabelecido.

13.1.2. Multa de 10% (dez por cento), sobre o valor do contrato, por inexecução parcial do contrato, podendo a CONTRATANTE autorizar a continuação do mesmo.

13.1.3. Multa de 20% (vinte por cento) sobre o valor do contrato, por inexecução total do mesmo.

13.1.4. Multa de 10% (dez por cento) sobre o valor do contrato, do mês em que ocorrer a infração, se a entrega tiver sido realizada em prazo superior ao previamente pactuado pela CONTRATANTE.

13.1.5. Multa de 1% (um por cento), sobre o valor do contrato, por dia de atraso no cumprimento dos prazos estipulados em contrato.

13.2. As multas são independentes entre si, podendo ser aplicadas cumulativamente. A aplicação de uma não exclui a das outras, bem como a das demais penalidades previstas em lei;

13.3. O valor relativo, às multas eventualmente aplicadas, será deduzido de pagamentos que a FUNDAÇÃO DO ABC efetuar, mediante a emissão de recibo;

13.4. As penalidades serão propostas pela fiscalização da CONTRATANTE e aplicadas, se for o caso, pela autoridade competente, garantindo o contraditório administrativo com defesa prévia.

14. DOS PAGAMENTOS

A CONTRATANTE compromete-se a pagar o preço constante da proposta da CONTRATADA, observando-se as seguintes condições:

14.1. A CONTRATADA deverá apresentar, mensalmente, a CONTRATANTE, documento contendo a relação dos serviços efetivamente realizados;

14.2. A CONTRATANTE, efetuará análise nos documentos apresentados pela CONTRATADA, e aprovará os procedimentos executados e valores correspondentes, solicitando que a CONTRATADA emita a nota fiscal para o devido pagamento;

14.3. A CONTRATADA deverá emitir uma nota fiscal para cada unidade discriminando detalhadamente os serviços prestados e deverá enviar para o endereço de e-mail notafiscalsmsp@smfuabc.org.br.

14.4. Em hipótese alguma será aceito boleto bancário como meio de cobrança;

14.5. O pagamento será efetuado mediante a apresentação, pela CONTRATADA, dos seguintes documentos, que serão arquivados pela CONTRATANTE:

a) Cartão CNPJ e Nota Fiscal constando discriminação detalhada do serviço prestado;

b) CND válida, provando regularidade do prestador de serviço contínuo de contrato formal, junto à Previdência Social;

c) Prova de regularidade perante o FGTS.

d) CNDT – Certidão Negativa de Débitos Trabalhistas, emitida pela Justiça do Trabalho;

e) Cópia de guia de recolhimentos do INSS, acompanhada da folha resumo da GEFIP correspondente. Quando isento, o prestador deverá apresentar justificativa e comprovante, nos termos da instrução normativa RFB N 971/2009;

f) Relação nominal atualizada de todos os profissionais que trabalham na empresa, prestando serviços diretamente nas dependências da CONTRATANTE;

g) Demonstrativos dos pagamentos realizados a todos os empregados (salário, vale transporte e benefícios), acompanhado do respectivo recibo firmado pelo empregado.

14.6. A CONTRATANTE poderá, a seu critério, solicitar outras documentações de regularidade não citadas acima;

14.7. Qualquer atraso ocorrido na apresentação da Nota Fiscal/Fatura por parte da Contratada importará em prorrogação automática do prazo de vencimento da obrigação da Contratante.

14.8. A CONTRATADA deverá indicar no corpo da nota fiscal as exigências contidas na resolução 23/2022, que aprova as alterações as instruções n 1/2020, do Tribunal de contas do Estado de São Paulo, as notas fiscais deverão obrigatoriamente conter:

a) Indicação da Contratante: Fundação do ABC – Contrato de Gestão de

São Mateus, CNPJ/MF sob o nº 57.571.275/0023-08;

b) Número do Contrato de Gestão: Contrato de Gestão 009/2015 - SMS/NTCSS.;

c) Número do processo.

14.9. Caso não haja tal informação o pagamento não será efetuado até sua regularização.

14.10. Caso seja detectado algum problema na documentação entregue anexada à nota fiscal, será concedido, pela Contratante, prazo para regularização.

14.11. A CONTRATADA deverá fazer constar na Nota Fiscal, o número do Banco, Agência e da conta corrente bancária, a fim de agilizar o pagamento.

14.12. Em hipótese alguma será aceito boleto bancário como meio de cobrança.

14.13. A CONTRATADA ficara responsável pelo pagamento dos encargos trabalhistas, previdenciários, fiscais, comerciais e outros que resultarem dos compromissos no contrato.

14.14. A CONTRATANTE não assumira responsabilidade alguma por pagamento de impostos e encargos que competirem a CONTRATADA, nem estará obrigado a restituir-lhe valores, principais e acessórios, que por ventura despender com pagamento dessa natureza.

14.15. O pagamento pelos serviços prestados, serão realizados, mensalmente, entre o décimo quinto ao vigésimo dia do mês subsequente ao da prestação dos serviços, mediante a emissão de nota fiscal/fatura e a sua devida atestação pela CONTRATANTE, com resalvas as cláusulas 14.5.

14.16. As notas fiscais, referentes aos serviços prestados, deverão ser entregues em tempo considerável (primeiro dia útil do mês) juntamente com relatório pré aprovado, para que a CONTRATANTE possa proceder com as análises devidas e o subsequente pagamento dos valores;

14.17. A CONTRATANTE procederá a retenção tributária, referente aos serviços prestados, nas alíquotas legalmente devidas, incidentes sobre o valor destacado em nota fiscal.

14.18. A CONTRATADA, neste ato declara estar ciente de que os recursos utilizados para o pagamento dos serviços ora contratados serão aqueles repassados pelo ente público, em razão do Contrato de Gestão 009/2015 - SMS/NTCSS, firmado entre a CONTRATANTE e a Prefeitura de São Paulo – Secretaria Municipal da Saúde para Gestão do Contrato de São Mateus/SP.

14.19. A CONTRATANTE compromete-se em pagar o preço irreajustável constante na proposta da CONTRATADA, desde que não ocorram atrasos e ou paralisação dos repasses pela Prefeitura Municipal de São Paulo - Secretaria Municipal de Saúde para a CONTRATANTE, relativo ao custeio do objeto do Contrato de Gestão 009-2015- SMS/NTCSS.

14.20. No caso de eventuais atrasos, os valores serão atualizados de acordo com a legislação vigente, salvo quando não decorram de atrasos e ou paralisação dos repasses pela Prefeitura de São Paulo – Secretaria Municipal da Saúde para a CONTRATANTE, em consonância com o disposto nas cláusulas deste CONTRATO.

15. DO REAJUSTE DOS PREÇOS

15.1. Havendo prorrogação do presente contrato de prestação de serviços, após ocorrido 12 (doze) meses, poderá haver reajuste de preços, da seguinte forma:

15.2. Será utilizado o IGP-M (Índice Geral de Preços do Mercado) ou o IPCA (Índice Nacional de Preço ao Consumidor Amplo – IBGE) a ser utilizado, observando os seguintes critérios:

Obs: Em casos específicos poderá ser utilizado o reajuste da categoria disposto em Convenção Coletiva de Trabalho.

15.2.1. Na eleição do Índice:
15.2.1.1. Dois meses de retroação da data base (mês da proposta);
15.2.1.2. Na periodicidade:

15.3. Será considerada a variação ocorrida no período de 12 (doze) meses, a contar do mês da proposta, observada a retroação de dois meses na eleição dos índices.
15.3.1. Na incidência:
15.3.2. A variação verificada no período de 12 (doze) meses apurada na forma citada nos itens 15.2.1.1. e 15.2.2.1, será aplicada sobre o preço inicial (da proposta).

15.4. A Contratada ficará responsavel pelo pagamento dos encargos trabalhistas, previdenciarios, fiscais, comerciais e outros que resultarem dos compromissos no contrato.

15.5. A Contratante não assumira responsabilidade responsabilidade alguma pelo pagamento de impostos e encargos que competirem a CONTRATADA, nem estará obrigada a restituir-lhe valores, principais e acessórios, que porventura despender com pagamento dessa natureza.

16. DO REGIME DE EXECUÇÃO

16.1. A Prestação de serviços/locação deverá ser executada de acordo com o ANEXO I do presente Ato convocatório;

16.2. Os produtos/serviços/locação deverão ser fornecidos nos padrões técnicos recomendados e atender os descritivos mínimos descritos;

17. DA RESCISÃO

17.1. O presente Contrato poderá ser rescindido unilateralmente, desde que haja conveniência para a CONTRATANTE mediante autorização escrita e fundamentada da autoridade superior, com antecedência mínima de (30) trinta dias, sem que caiba à CONTRATADA o direito de indenização de qualquer espécie;

17.2. Este instrumento poderá ser rescindido por ato unilateral da CONTRATANTE, verificando-se a ocorrência de descumprimento de cláusulas contratuais, assegurados, no entanto, o contraditório e a ampla defesa.

17.3. O não cumprimento das obrigações contratuais pela CONTRATANTE poderá ensejar rescisão contratual pela CONTRATADA, assegurados, no entanto, o contraditório e a ampla defesa. Configurado o justo motivo para rescisão, a CONTRATADA deverá permanecer por até (90) noventa dias na execução dos serviços.

17.4. A presente avença extinguir-se-á automaticamente em caso de rescisão do contrato de gestão/convênio celebrado entre a CONTRATANTE e a Administração Pública, não cabendo indenização de qualquer natureza às partes. – para contratos de serviços contínuos.

17.5. A presente avença poderá ser rescindida em caso de extinção do estado de necessidade que ensejou a contratação ou em caso de conclusão de tomada de preços, realizada nos termos do Regulamento de Compras e Contratação de Serviços de Terceiros e Obras da Fundação do ABC, que objetive a substituição da contratação emergencial por serviços contínuos. – para contratos emergenciais.

17.6. No caso de não interesse de renovação do contrato por parte da CONTRATADA, ela deverá comunicar à CONTRATANTE, em um prazo mínimo de 90 (noventa) dias, ou manter o serviço contratado em funcionamento por igual período, após o vencimento do mesmo;

18. DISPOSIÇÕES GERAIS

18.1. Quaisquer esclarecimentos poderão ser obtidos na Fundação do ABC-, situado na Avenida Lauro Gomes, n° 2000 – Príncipe de Gales – Santo André/SP – CEP 09060-650, no horário das 08hs00min às 17hs00min;

18.2. Todas as dúvidas eventualmente surgidas deverão ser apresentadas por escrito e encaminhadas ao endereço mencionado na cláusula 18.1 deste Ato convocatório.

18.3. Segue anexo ao presente Ato convocatório:

- ANEXO I – TERMO DE REFERÊNCIA;
- ANEXO II – MODELO DE PROPOSTA;
- ANEXO III – MODELO DE ETIQUETA PARA PROPOSTA/DOCUMENTAÇÃO;
- ANEXO IV – MODELO DE DECLARAÇÃO DE ANTICORRUPÇÃO;
- ANEXO V – MODELO DE DECLARAÇÃO QUADRO SOCIETÁRIO;
- ANEXO VI – MODELO DE DECLARAÇÃO DE NÃO IMPEDIMENTO;
- ANEXO VII – MODELO DE DECLARAÇÃO DE PERFEITAS CONDIÇÕES;
- ANEXO VIII - DECLARAÇÃO DE ACEITAÇÃO DO REGULAMENTO DE COMPRAS E CONTRATAÇÃO DA FUNDAÇÃO DO ABC (ENVELOPE Nº 1 – PROPOSTA);
- ANEXO IX – QUESTIONARIO DUE DILIGENCE DE COMPLIENCE DE FORNECEDORES;
- ANEXO X – DECLARAÇÃO DE CUMPRIMENTO AO CÓDIGO DE CONDUTA ÉTICA DA FUABC;
- ANEXO XI – MODELO DE ATESTADO DE VISTORIA;
- ANEXO XII – MODELO DE DECLARAÇÃO DE DECLINIO DE VISTORIA;
- ANEXO XIII- MODELO DE DECLARAÇÃO DE QUE NÃO EMPREGA MENOR;
- ANEXO XIV – DECLARAÇÃO DE RESPONSABILIDADE, QUE ASSUME INTEGRALMENTE POR QUAISQUER AÇÕES TRABALHISTA MOVIDA PELO OS SEUS EMPREGADOS.
- ANEXO XV – MINUTA DE CONTRATO.

DIRETOR GERAL

ANEXO I
TERMO DE REFERÊNCIA

CONTRATAÇÃO DE EMPRESA PARA FORNECIMENTO DE EQUIPAMENTO DE SEGURANÇA DO TIPO FIREWALL NGFW, COM SERVIÇO DE SUPORTE, CONFIGURAÇÃO E MONITORAMENTO.

1. Objeto

Contratação de empresa para fornecimento de infraestrutura firewall NGFW com Appliance físicos como serviço e serviços de monitoramento e suporte 24X7 durante a vigência do contrato.
Contratação de empresa para fornecimento de infraestrutura de Firewall como HaaS, incluindo instalação e configuração, com o objetivo de reforçar a segurança da rede e implementar VPNs site-to-site, integração na Nuvem e assegurando comunicação segura, tráfego entre as unidades da Sede Administrativa e Sede Assistencial.

2. Justificativa

A contratação de dois firewalls de próxima geração para a Fundação do ABC – Contrato São Mateus visa garantir proteção avançada contra ameaças cibernéticas, assegurando segurança abrangente para dados e sistemas. A solução permitirá a gestão eficaz do tráfego de rede, prevenção de acessos não autorizados e otimização do desempenho.

Os firewalls deverão suportar redes complexas e grandes volumes de dados, além de viabilizar a implementação de VPNs site-to-site para comunicação segura entre unidades. Também oferecerão monitoramento contínuo do tráfego e estarão preparados para integração futura com soluções em nuvem, garantindo continuidade operacional e escalabilidade.

A escolha dessa tecnologia demonstra o compromisso da instituição com a segurança da informação, protegendo seus ativos digitais e adotando medidas preventivas e proativas contra ameaças emergentes no cenário cibernético.

3. Benefícios Esperados

Os seguintes benefícios são esperados mediante a presente contratação:

- ✓ **Proteção Avançada Contra Ameaças**: Segurança contra-ataques DDoS, ransomware, malware e tentativas de acesso não autorizado, garantindo a integridade dos dados.
- ✓ **Gestão Eficiente do Tráfego**: Controle e otimização do uso da rede, priorizando aplicações críticas e assegurando alto desempenho para usuários e sistemas.
- ✓ **VPNs Site-to-Site Seguras:** Comunicação criptografada entre unidades, proporcionando conectividade estável e segura para transferência de dados.
- ✓ **Integração com a Nuvem**: Suporte a ambientes híbridos, permitindo a continuidade dos serviços mesmo em caso de falha na infraestrutura local.

- ✓ **Monitoramento Contínuo e Resposta a Incidentes**: Supervisão 24x7 da rede, identificação de anomalias em tempo real e mitigação proativa de riscos.
- ✓ **Suporte Técnico Especializado**: Atendimento rápido e eficiente para a resolução de problemas, reduzindo impactos operacionais.

4. Descrição Técnicas dos Firewalls e Abrangência dos locais

LOCAL	ENDEREÇO	Quantidade de Firewall
SEDE ADMINISTRATIVA	Rua Suíça, 95. Parque das Nações – Santo André (SP). CEP: 09210-000	2
SEDE ASSISTENCIAL	Av. Cláudio Augusto Fernandes, 518, Cidade São Mateus, São Paulo – SP, CEP: 03962-120	1

As atividades de instalação, configuração e suporte técnico deverão ser realizadas prioritariamente no ambiente atual. Caso ocorra uma mudança de endereço, a empresa contratada será responsável por todos os custos relacionados à remoção e relocação dos equipamentos.

4.1 Especificações Técnicas do Firewall para Sede Administrativa

TERMOS TÉCNICOS	REQUISITOS
Throughput de Firewall	Deve ser capaz de manipular no mínimo até 7 Gbps.
Throughput de IPS	Deve suportar no mínimo até 1,4 Gbps com a funcionalidade de IPS ativa.
Throughput de NGFW	Deve suportar no mínimo até 1 Gbps com funcionalidades de firewall, IPS e controle de aplicativos ativos.
Throughput de Proteção contra Ameaças	Deve ser capaz de suportar no mínimo até 900 Mbps com proteção ativa contra malware.
Throughput de VPN IPsec	Deve ser capaz de alcançar no mínimo até 6,5 Gbps para conexões seguras de alta velocidade.
Throughput de Inspeção SSL	Deve ser capaz no mínimo de processar até 950 Mbps para sessões HTTPS com cifra média.
Túneis VPN IPsec	Deve suportar no mínimo até 200 túneis de VPN IPsec Site-to-Site simultâneos.
Usuários SSL-VPN	Deve suportar no mínimo até 200 usuários SSL-VPN simultâneos.
Sessões Simultâneas	Deve suportar no mínimo até 1.500.000 de conexões TCP simultâneas.
Novas Sessões por Segundo	Deve suportar no mínimo até 45.000 novas sessões por segundo.
Políticas de Firewall	Deve permitir a criação de até 5.000 regras distintas.
CARACTERÍSTICAS DE HARDWARE	**ESPECIFICAÇÕES**

Portas 10 Gigabit Combo	Deve possuir 2 portas 10 Gigabit SFP+.
Portas GE RJ45	Deve possuir 8 portas GE RJ45 configuráveis para uso como LAN, WAN ou DMZ.
Portas USB	Deve dispor de 1 porta USB para conectividade adicional.
Porta de Console	Deve possuir 1 porta de console RJ45 para gerenciamento.
Armazenamento de Logs	Deve prover armazenamento seguro em nuvem.
CARACTERÍSTICAS AMBIENTAIS	**ESPECIFICAÇÕES**
Fixação e Dimensões	O dispositivo deve ser compacto com opção para fixação em rack. Dimensões de 1.6 x 8.5 x 7.0 polegadas e peso de 1,1 kg.
Requisitos de Energia	Deve operar com fonte de alimentação de 12V DC, 3A, com plugue no formato padrão NBR 14136.
Faixa de Temperatura Operacional	Deve funcionar de forma adequada em temperaturas entre 0°C e 40°C.
CARACTERÍSTICAS DE RECURSOS	**ESPECIFICAÇÕES**
Domínios Virtuais	Deve suportar até no mínimo 10 domínios virtuais para gerenciamento de ambientes multi-tenant.
Opções de Alta Disponibilidade	Deve suportar configurações em modos Ativo-Ativo, Ativo-Passivo e Clustering, garantindo redundância e disponibilidade contínua.
Unidade de Processamento de Segurança	Deve utilizar unidades de processamento de segurança especializadas para desempenho aprimorado em tarefas de detecção de ameaças e criptografia.

4.2 Especificações Técnicas do Firewall para Sede Assistencial.

TERMOS TÉCNICOS	REQUISITOS
Throughput de Firewall	Deve ser capaz de manipular no mínimo até 6 Gbps.
Throughput de IPS	Deve suportar no mínimo até 1,4 Gbps com a funcionalidade de IPS ativa.
Throughput de NGFW	Deve suportar no mínimo até 1 Gbps com funcionalidades de firewall, IPS e controle de aplicativos ativos.
Throughput de Proteção contra Ameaças	Deve ser capaz de suportar no mínimo até 700 Mbps com proteção ativa contra malware.
Throughput de VPN IPsec	Deve ser capaz de alcançar no mínimo até 6,5 Gbps para conexões seguras de alta velocidade.
Throughput de Inspeção SSL	Deve ser capaz no mínimo de processar até 630 Mbps para sessões HTTPS com cifra média.
Túneis VPN IPsec	Deve suportar no mínimo até 200 túneis de VPN IPsec Site-to-Site simultâneos.
Usuários SSL-VPN	Deve suportar no mínimo até 200 usuários SSL-VPN simultâneos.

Sessões Simultâneas	Deve suportar no mínimo até 700.000 de conexões TCP simultâneas.
Novas Sessões por Segundo	Deve suportar no mínimo até 30.000 novas sessões por segundo.
Políticas de Firewall	Deve permitir a criação de até 2.000 regras distintas.
CARACTERÍSTICAS DE HARDWARE	**ESPECIFICAÇÕES**
Portas GE RJ45	Deve possuir no mínimo 8 portas GE RJ45 configuráveis para uso como LAN, WAN ou DMZ.
Portas USB	Deve dispor de no mínimo 1 porta USB para conectividade adicional.
Porta de Console	Deve possuir no mínimo 1 porta de console RJ45 para gerenciamento.
Armazenamento de Logs	Deve prover armazenamento seguro em nuvem.
CARACTERÍSTICAS AMBIENTAIS	**ESPECIFICAÇÕES**
Fixação e Dimensões	O dispositivo deve ser compacto, com dimensões de 1.5 x 8.5 x 6.3 polegadas e peso de 1 kg para posicionamento em bandeja ou fixação em rack.
Requisitos de Energia	Deve operar com fonte de alimentação de 12V DC, 3A, com plugue no formato padrão NBR 14136.
Faixa de Temperatura Operacional	Deve funcionar de forma adequada em temperaturas entre 0°C e 40°C.
CARACTERÍSTICAS DE RECURSOS	**ESPECIFICAÇÕES**
Domínios Virtuais	Deve suportar no mínimo até 10 domínios virtuais para gerenciamento de ambientes multi-tenant.
Opções de Alta Disponibilidade	Deve suportar configurações em modos Ativo-Ativo, Ativo-Passivo e Clustering, garantindo redundância e disponibilidade contínua.
Unidade de Processamento de Segurança	Deve utilizar unidades de processamento de segurança especializadas para desempenho aprimorado em tarefas de detecção de ameaças e criptografia.

5. REQUISITOS TÉCNICOS GERAIS

5.1 Filtro de pacote, controle de aplicação, administração de largura de banda (QoS), VPN.

5.2 IPsec e SSL, IPS, prevenção contra ameaças como vírus, spywares e malwares "Zero Day".

5.3 Filtro de Conteúdo Web (Webfilter) e controle de transmissão de dados e acesso à internet, compondo uma plataforma robusta e integrada de segurança.

5.4 Deve ser um appliance físico específico para proteção de rede, integrando funcionalidades de um Firewall de Nova Geração (NGFW).

5.5 Deve garantir um throughput mínimo de 1 Gbps com todas as funcionalidades de segurança habilitadas (controle de aplicações, prevenção de intrusões, antimalware, antivírus, antispyware, sandboxing e filtragem de URLs).
5.6 Suporte para pelo menos 1.500.000 conexões simultâneas para a Sede Administrativa e
750.000 para a Sede Assistencial, com capacidade de até 100.000 novas conexões HTTP por segundo para a Sede Administrativa e 55.000 para a Sede Assistencial.
5.7 O firewall deve ser fornecido com software dedicado, não sendo aceitável o uso de sistemas operacionais de propósito geral.

5.1. Funcionalidades de SD-WAN

5.1.1. A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação.
5.1.2. Possibilidade de criar políticas para modelagem do tráfego com os seguintes parâmetros: IP de origem, VLAN de origem, IP de destino, Porta TCP/UDP de destino, Domínio e URL de destino.
5.1.3. Aplicação de camada 7 utilizada (O365 Exchange, AWS, Dropbox, etc).
5.1.4. Capacidade de monitorar e identificar falhas com health check, permitindo testes de resposta por ping, HTTP, TCP/UDP echo, DNS, TCP-connect e TWAMP.
5.1.5 O SD-WAN deve balancear o tráfego das aplicações entre múltiplos links simultaneamente.
5.1.6. Deve ser capaz de analisar o tráfego em tempo real e realizar balanceamento de pacotes do mesmo fluxo entre múltiplos links, com reordenação dos pacotes caso necessário.
5.1.7. Criação de políticas de roteamento com base nos seguintes critérios: Latência, Jitter, Perda de pacote e Banda ocupada ou todos ao mesmo tempo.
5.1.8. A solução deve permitir a definição de roteamento para cada aplicação.
5.1.9. Diversas formas de escolha de link, incluindo: Melhor link, Menor custo e Definição de níveis máximos de qualidade.
5.1.10. Possibilidade de definir o link de saída para uma aplicação específica.
5.1.11. Implementar balanceamento de link por hash do IP de origem e destino.
5.1.12. A solução de SD-WAN deve oferecer suporte a roteamento baseado em políticas (Policy Based Routing) ou encaminhamento baseado em políticas.
5.1.13. Deve suportar roteamento estático e dinâmico (BGP e OSPF).
5.1.14. Possibilidade de realizar balanceamento por pacote entre túneis IPsec.
5.1.15. Deve possuir recurso de correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões.
5.1.16. Deve permitir a customização dos timers para detecção de queda de link, com tempo necessário para restabelecimento.
5.1.17. Deve possibilitar políticas para controlar o uso de aplicações e tráfego intenso (como YouTube, Facebook) que possam impactar as aplicações de negócio e deve permitir bloqueio ou limitação de tráfego excessivo para evitar impacto nas aplicações de negócios.

5.1.18. Suporte para criar políticas de QoS e Traffic Shaping por endereço de origem, endereço de destino, usuário ou grupo de usuários, aplicações e porta, permitir definição de tráfego com banda garantida (banda mínima disponível para aplicações de negócio) e definição de tráfego com banda máxima para aplicativos best-effort (ex. YouTube, Facebook).
5.1.19. Possibilidade de marcar pacotes com DSCP para reserva de banda ao longo do backbone.
5.1.20. Configuração de filas de prioridade para aplicações específicas.
5.1.21. Possibilidade de definir banda máxima e garantida por aplicação, com suporte para categorias de URL, IPs de origem e destino, logins e portas.
5.1.22. Definição de Bandas Distintas para Download e Upload.
5.1.23. Capacidade de agendar intervalos de tempo para aplicar políticas de banda, como horários mais permissivos durante o almoço.
5.1.24. Visualização em tempo real de ocupação de banda (upload e download), bem como latência, jitter e perda de pacote.
Suporte a IPv6: Compatibilidade com IPv6.
5.1.25. Possibilidade de definir roteamento específico por grupo de usuário.
5.1.26. Suporte para configuração em modos Ativo/Passivo e Ativo/Ativo.
5.1.27. O SD-WAN deverá possuir serviço de Firewall Stateful;
5.1.28. A solução SD-WAN deverá fornecer criptografia AES de 128 bits ou AES de 256 bits em sua VPN;
5.1.29 A solução SD-WAN deverá simplificar a implantação de túneis criptografados de site para site;
5.1.30. Deve ser capaz de bloquear acesso às aplicações;
5.1.31. Deve suportar NAT dinâmico bem como NAT de saída;
5.1.32. Deve suportar balanceamento de tráfego por sessão e pacote;
5.1.33. As funcionalidades de SD-WAN podem ser fornecidas no NGFW ofertado ou em uma solução à parte, na mesma quantidade de equipamentos definida para os firewalls;
5.1.34. Em caso de composição de solução, a solução de SD-WAN deverá suportar tráfego compatível com a capacidade do equipamento de NGFW.

5.2. Controle por Política de Firewall
5.2.1. Deverá suportar controles por zonas de segurança;
5.2.2 Deverá suportar controles de políticas por porta e protocolo;
5.2.3. Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;
5.2.4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
5.2.5. Controle de políticas por código de país (Por exemplo: BR, US, UK, RU);
5.2.6. Controle, inspeção e descriptografia de SSL por política para tráfego de saída (Outbound);
5.2.7. Deve descriptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3;

Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;
5.2.8. Suporte a objetos e regras IPv6;
5.2.9. Suporte a objetos e regras multicast;
5.2.10. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

5.3. Controle de Aplicações
5.3.1. Capacidade de identificar e controlar o acesso a aplicações, permitindo a definição de políticas específicas para permitir ou bloquear aplicações com base em categorias ou comportamentos identificados.
5.3.2. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos.
Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado a: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, VoIP, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos e e-mail.
5.3.3. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linkedin, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-doc, sisqual.
5.3.4. Inspecionar o payload de pacotes para detectar assinaturas de aplicações conhecidas, independentemente de porta e protocolo.
5.3.5. Identificar o uso de táticas evasivas, visualizando e controlando aplicações e ataques que utilizam táticas evasivas como comunicações criptografadas (e.g., Skype e rede Tor).
Para tráfego criptografado SSL, descriptografar pacotes para verificar assinaturas de aplicações.
5.3.6. Decodificar protocolos para detectar aplicações encapsuladas e validar se o tráfego corresponde ao protocolo especificado.
5.3.7. Identificar funcionalidades específicas de aplicações, bem como táticas evasivas em comunicações criptografadas.
5.3.8. Atualizar a base de assinaturas de aplicações automaticamente.
Dispositivos de proteção de rede devem identificar o usuário de rede via integração com o Microsoft Active Directory sem a necessidade de agentes ou Domain Controller.
5.3.9. Permitir controle de aplicações em múltiplas regras de segurança, possibilitando habilitar controle de aplicações em regras específicas.
5.3.10. Suportar métodos de identificação de aplicações por assinaturas e decodificação de protocolos.
5.3.11. Permitir criação de assinaturas personalizadas para aplicações proprietárias, com interface gráfica de configuração.
5.3.12. Alertar o usuário quando uma aplicação for bloqueada.
5.3.13. Possibilitar diferenciação de tráfegos Peer2Peer com granularidade de controle.

5.3.14. Diferenciar e controlar tráfego de aplicações como Peer2Peer (ex.: BitTorrent) por políticas.
5.3.15. Deve possibilitar a diferenciação e controle de partes das aplicações, como por exemplo, permitir o Hangouts e bloquear a chamada de vídeo.
5.3.16. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc.), possuindo granularidade de controle/políticas para os mesmos.
5.3.17. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol etc.).
5.3.18. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características como: nível de risco da aplicação e categoria da aplicação.
5.3.19. Deve ser possível a criação de grupos estáticos de aplicações baseados em características como: categoria da aplicação.

5.4 Prevenção de Ameaças

5.4.1. Detectar e prevenir ameaças em tempo real, incorporando mecanismos de prevenção de intrusões (IPS) e sistemas antivírus, bloqueando ataques antes de atingirem os recursos internos da rede.
5.4.2. Incluir proteção contra vírus em conteúdo HTML e JavaScript, software espião (spyware) e Worms.
5.4.3. Proteção contra downloads indesejados via HTTP de arquivos executáveis e maliciosos.
5.4.4. Permitir configuração de políticas baseadas em usuários, grupos de usuários, origem, destino e zonas de segurança, podendo ser aplicadas diferentes políticas para um mesmo perfil.
5.4.5. Capacidade de mitigar APTs, através de análises dinâmicas e identificação de malwares desconhecidos.
5.4.6. Capacidade de analisar malware desconhecido (Zero-Day) em ambiente isolado (sandbox) e bloquear o acesso a arquivos suspeitos.
5.4.7. Analisar o comportamento de arquivos suspeitos em ambiente controlado.

5.5. Filtro de URL

5.5.1. O firewall deve possuir um sistema de filtragem de URLs que permita bloquear ou acessar sites com base em listas de categorias pré-definidas, contribuindo para a segurança e conformidade com políticas de uso da internet.
5.5.2. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora).
5.5.3. Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança.
5.5.4. Deve permitir a criação de políticas com base na visibilidade e controle de quem está utilizando quais URLs, através de integração com serviços de diretório, Active Directory e base de dados local.
5.5.5. A identificação pela base do Active Directory deve permitir SSO, para que os usuários não precisem logar novamente na rede para navegar pelo firewall.

5.5.6. Suportar a criação de políticas baseadas no controle por URL ou categoria de URL.
5.5.7. Deve possuir pelo menos 70 categorias de URLs, definidas pelo fabricante e atualizáveis a qualquer tempo.
5.5.8. Deve permitir a exclusão de URLs específicas do bloqueio.
5.5.9. Permitir a customização da página de bloqueio.
5.5.10. Permitir a restrição de acesso a canais específicos do YouTube, configurando uma lista de canais permitidos ou bloqueados.
5.5.11. Deve bloquear o acesso a conteúdo inadequado em sites de busca, como Google, Bing e Yahoo, implementando o Safe Search para restringir resultados.

5.6. Identificação de Usuários
5.6.1. Deve ser capaz de identificar usuários de forma precisa para aplicar políticas de segurança personalizadas, utilizando-se de integração com sistemas de autenticação existentes, como LDAP ou Active Directory, para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on (SSO). Essa funcionalidade não deve possuir limites licenciados de usuários.
5.6.2. Deve possuir integração com Radius para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários.
5.6.3. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída à internet para que antes iniciem a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal).
5.6.4. Deve possuir suporte à identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços.
5.6.5. Deve permitir a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD.
5.6.6. A solução deve suportar autenticação de usuários com credenciais de mídias sociais de terceiros como Facebook, Twitter, LinkedIn e Google+.
5.6.7. A solução deve permitir que usuários sem conta local ou em mídias sociais se autentiquem através de um rápido cadastro, garantindo o mínimo de rastreabilidade, com validação de endereços de e-mail ou número de telefone.
5.6.8. Permitir o login automático de usuários visitantes depois de se registrarem com sucesso.
5.6.9 Agir como um Provedor de Identidade (Identity Provider - IDP), estabelecendo um relacionamento com o Provedor de Serviços (Service Provider - SP) para autenticação segura de usuários tentando acessar o Provedor de Serviços.
5.6.10 Deve suportar nativamente a integração e autenticação de switches e outros dispositivos compatíveis com o padrão 802.1X.
5.6.11. Oferecer integração de clientes finais para autenticação 802.1X, permitindo que qualquer cliente com Windows possa configurar seu equipamento para o suporte 802.1X.
5.6.12. Suportar os seguintes métodos 802.1X EAP: PEAP (MSCHAPv2), EAP-TTLS, EAP-TLS e EAP-GTC.

5.6.13. Suporte à interoperabilidade com equipamentos de acesso de outros fabricantes para autenticação de portas junto à solução, através dos padrões 802.1X.
5.6.14. Permitir bypass de autenticação 802.1X para dispositivos conhecidos que não suportem 802.1X.
5.6.15. A liberação deverá ser feita baseada no endereço MAC dos dispositivos previamente cadastrados, permitindo o acesso à rede sem necessidade de autenticação adicional por parte do usuário do dispositivo.

5.7. QoS (Quality of Service)
5.7.1. O dispositivo deve suportar funcionalidades de Qualidade de Serviço (QoS), permitindo a priorização de tráfego de dados na rede, assegurando que aplicações críticas tenham a largura de banda necessária para operar eficientemente.

5.8. VPN (Virtual Private Network)
5.8.1. Deve suportar a criação de redes privadas virtuais utilizando protocolos IPSec e SSL, garantindo comunicações seguras e criptografadas entre diferentes locais ou para usuários remotos.
5.8.2. VPN IPSec Site-to-Site
5.8.3. Suporte à criptografia 3DES, AES128, AES192 e AES256 (Advanced Encryption Standard).
5.8.4. Suporte para autenticação MD5, SHA1, SHA256, SHA384 e SHA512.
5.8.5. Suporte para Diffie-Hellman Groups 1, 2, 5, 14, 15, 21, 27 e 32.
5.8.6. Suporte para Algoritmo Internet Key Exchange (IKEv1 e v2).
5.8.7. Suporte para autenticação via certificado IKE PKI.
5.8.8. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet e SonicWall.

5.9. Controlador de Switch
5.9.1. Gerenciamento e operação centralizada e integrada no mesmo appliance, com inventário de hardware, software e configuração dos switches.
5.9.2. Interface gráfica para configuração, administração e monitoramento dos switches.
5.9.3 Exibição da topologia da rede com todos os switches administrados para monitoramento, incluindo status dos uplinks e equipamentos para identificação de problemas na rede.

5.10. Console de Gerência e Monitoração
5.10.1. Uma plataforma centralizada para gerenciamento e monitoramento do firewall, incluindo funcionalidades para a configuração de políticas, SD-WAN, atualizações de segurança, revisão de logs de segurança e geração de relatórios detalhados.

5.11. CASB (Cloud Access Security Broker)
5.11.1. Fornece visibilidade, controle e segurança para interações entre usuários e serviços em nuvem.

5.11.3. A plataforma deve suportar implementação futura de licenciamento para ativação da funcionalidade de CASB.

5.12. ZTNA (Zero Trust Network Access)
5.12.1. Ter suporte ao de "Nunca Confiar, Sempre Verificar": Baseado no princípio de "nunca confiar, sempre verificar", o ZTNA assegura que apenas usuários autenticados e dispositivos validados tenham acesso a aplicações e recursos específicos.
5.12.2. Acesso é verificado antes de qualquer conexão, minimizando a superfície de ataque.
5.12.3. A plataforma deve suportar implementação futura de licenciamento para ativação da funcionalidade de ZTNA.

5.13. Inspeção Profunda de Pacotes (Deep Packet Inspection, DPI)
5.13.1. Analisa profundamente o conteúdo dos pacotes de dados que atravessam a rede para detectar e bloquear tráfego malicioso ou não autorizado, fornecendo uma compreensão detalhada do tipo de tráfego processado.

5.14. Controle de Acesso Baseado em Identidade (Identity-Based Access Control)
5.14.1. Dar suporte para integrar sistemas de autenticação para controlar o acesso a recursos da rede com base na identidade dos usuários ou dispositivos, tolerando as políticas de segurança internas.

5.15. Proteção Contra-ataques Distribuídos de Negação de Serviço (DDoS)
5.15.1. Implementa estratégias para detectar e mitigar ataques DDoS, preservando a disponibilidade e operacionalidade dos serviços de rede.

5.16. Geolocalização
5.16.1. Políticas por Geolocalização: Suportar a criação de políticas por geolocalização, permitindo que o tráfego de determinados países seja bloqueado.
5.16.2. Visualização nos Logs: Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.

5.17. Gerenciamento de Acesso Wireless
5.17.1. Gerenciamento Centralizado de Pontos de Acesso: Gerenciamento e operação centralizada dos pontos de acesso wireless, integrada no mesmo appliance da solução ofertada.

6. Garantia, Suporte e Acordos de Níveis de Serviços (SLA)

6.1. Os serviços poderão ser prestados pela CONTRATADA ou por representante indicada pela CONTRATADA ou pelo fabricante da solução;

6.2. Entende-se por "Garantia" ou" Suporte" ou "Manutenção", doravante denominada unicamente como "Garantia", 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. Esta "Garantia" inclui os procedimentos destinados a recolocar em perfeito estado de operação os serviços e produtos ofertados, tais como:

6.2.1 **Do hardware**: desinstalação, reconfiguração ou reinstalação decorrente de falhas de fabricação no hardware, fornecimento de peças de reposição, substituição de hardware por defeito de fabricação, atualização da versão de drivers e firmwares, ajustes e reparos necessários, de acordo com os manuais e as normas técnicas específicas para os recursos utilizados;

6.2.2 **Do software**: desinstalação, reconfiguração ou reinstalação decorrente de falhas de desenvolvimento do software, atualização da versão de software, correção de defeitos de desenvolvimento do software, de acordo com os manuais e as normas técnicas específicas do fabricante para os recursos utilizados; 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, reinstalação e reconfiguração quando necessário.

6.3 A CONTRATADA fornecerá e aplicará pacotes de correção, em data e horário a serem definidos pela CONTRATANTE, sempre que forem encontradas falhas de laboratório (bugs) ou falhas comprovadas de segurança em software ou firmware dos aparelhos que integrem o objeto do contrato.

6.4 O atendimento deste requisito está condicionado a liberação pelo fabricante dos pacotes de correção e/ou novas versões de software.

6.5 É facultado a CONTRATADA a execução, ao seu planejamento e disponibilidade, de "Garantia" do tipo "preventiva" que pela sua natureza reduza a incidência de problemas que possam gerar "Garantia" do tipo "corretiva". As manutenções do tipo "preventiva" não podem gerar custos a CONTRATANTE.

6.6 A manutenção técnica do tipo "corretiva" será realizada sempre que solicitada pelo CONTRATANTE por meio da abertura de chamado técnico diretamente à empresa CONTRATADA (ou a outra informada pela CONTRATADA) via telefone ou Internet ou e-mail ou outra forma de contato;

7. ACORDOS DE NÍVEIS DE SERVIÇOS (SLA) E PRAZOS DE ATENDIMENTO

7.1 Os serviços contratados devem estar disponíveis 24 horas por dia, 7 dias por semana, 365 dias por ano e possuir Suporte Técnico, em igual disponibilidade, durante toda a vigência contratual;

7.1. SEVERIDADE URGENTE

- Prazo máximo de início de atendimento de até 02 hora útil contadas a partir do horário de abertura do chamado; Prazo máximo de resolução do problema de até 08 horas úteis contadas a partir do início do atendimento.

7.2. SEVERIDADE IMPORTANTE

- Necessidade de suporte na solução com a necessidade de interrupção de funcionamento da solução.
- Prazo máximo de início de atendimento de até 04 horas úteis contadas a partir do horário de abertura do chamado;
- Prazo máximo de resolução do problema de até 12 horas úteis contadas a partir do início do atendimento.

7.3. SEVERIDADE NORMAL

- Necessidade de suporte na solução sem a necessidade de interrupção de funcionamento da solução.
- Prazo máximo de início de atendimento de até 8 horas úteis contadas a partir do horário de abertura do chamado;
- Prazo máximo de resolução do problema de até 24 horas úteis contadas a partir do início do atendimento.

7.4. 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. Caso seja necessária a reinstalação da solução, a reinstalação será realizada através dos serviços compatíveis do "Catálogo de Serviços".

7.5. SEVERIDADE INFORMAÇÃO

- Solicitações de informações diversas ou dúvidas sobre a solução.
- Prazo máximo de resposta de até 3 dias úteis, contados a partir da data de abertura da ocorrência.

7.6. 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;

7.7. 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.

7.8. 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;

7.9. 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. Os tempos de "início de atendimento" e "solução do problema" se aplicam para chamados com atendimento na cidade de São Paulo – SP.

8. Vistoria Técnica

A visita técnica PRÉVIA é FACULTATIVA, podendo a(s) empresa(s) interessada(s) em participar desta Coleta de Preços, comparecerem **a Fundação do ABC – Contrato São Mateus**, para conhecimento de todas as informações e condições locais para o cumprimento das obrigações.

8.1 A visita técnica deverá ser previamente agendada em horário comercial, junto a equipe de TI da Fundação da ABC – Contrato São Mateus, pelo e-mail marcelo.netto@smfuabc.org.br , considerando a data e horário disponível.

8.2 A visita técnica prévia tem por finalidade permitir que a Proponente obtenha, para a sua utilização e exclusiva responsabilidade, toda a informação necessária à elaboração de sua proposta, sendo que todas as despesas e os custos associados à visita correrão por sua única e inteira responsabilidade.

8.3 Caso a Proponente opte pela não realização da visita técnica, não serão admitidas alegações posteriores de desconhecimento dos serviços e de dificuldades não previstas.

9. TREINAMENTO TÉCNICO FORNECIDO PELA CONTRATADA

A CONTRATADA deverá fornecer treinamento base para os usuários, conforme necessidade e solicitação do CONTRATANTE, garantindo suporte adequado para o uso e operação dos serviços fornecidos. Esse treinamento deverá ser disponibilizado em até 7 dias úteis após a solicitação formal.

9.1. O treinamento será prestado para um grupo de no máximo 03 (três) participantes a ser realizado nas instalações da CONTRATANTE OU DE FORMA REMOTA devendo ser ministrados em língua portuguesa e por profissionais qualificados para este fim.

9.2. O treinamento deverá ser realizado de acordo com a disponibilidade de agenda das equipes da CONTRATADA e CONTRATANTE;

9.3. Os treinamentos deverão ser ministrados em dias úteis (de segunda a sexta-feira) das 08:00h às 17:00h;

10.OBRIGAÇÕES DA CONTRATADA

10.1. A CONTRATADA será responsável por fornecer equipamento como serviço, licenciamento e todo o serviço de suporte e monitoramento especializado dos equipamentos, bem como sua saúde, disponibilidade dos links de internet, detecção de ameaças e gestão de consumo de banda, além de suporte contínuo reativo e proativo.

10.2 A CONTRATADA será responsável por prover TODO o licenciamento necessário para a aplicação das funcionalidades de segurança da solução de firewall de nova geração, bem como providenciar sempre sua renovação, de forma antecipada, quando necessários, durante toda a vigência do contrato.

10.3 A CONTRATADA efetuará toda a implantação física e lógica dos recursos da solução, bem como a instalação física no ambiente da CONTRATANTE, configurações iniciais da solução, integrações com sistemas de autenticação LDAP, implementação das regras solicitadas, criação de VPN's Site-to-Site e Client-to-Site, implementação completa da solução de Webfilter de acordo com as políticas definidas, configuração do serviço de SD-WAN para melhor aproveitamento dos links de dados, configurações de failover para links de internet, configurações de roteamento necessários, configurações de inspeção SSL, DPI, configuração do serviço de Sandbox, criação e parametrização de serviços de relatórios.

10.4. A CONTRATADA deve garantir o monitoramento constante da parametrização dos serviços de firewall e da disponibilidade dos links de internet.

10.5 A CONTRATADA deverá apresentar relatórios mensais sobre indicadores de ameaças, eventos críticos de segurança, alertas de alto consumo de banda, variações na latência e status de desempenho dos links de internet.

10.6 A CONTRATADA deverá realizar análises preditivas que antecipam problemas e comportamentos anormais, combinadas com atuações proativas para resolver questões antes que se transformem em problemas significativos.

10.7 A CONTRATADA será responsável por manter o sistema atualizado com as últimas atualizações de segurança, garantindo proteção contra as mais recentes vulnerabilidades e exploits.

10.8 A CONTRATADA deverá fornecer de forma regular e/ou sob demanda relatórios detalhados que documentam as ameaças identificadas e a atividade de navegação por usuário, site e aplicação, apoiando a tomada de decisão e a gestão estratégica de TI.

10.9 Cumprir fielmente toda a execução do objeto, de acordo com as condições e exigências previamente estabelecidas;

10.10 A CONTRATADA Deve fornecer os Firewalls, cada qual respeitando as especificações abaixo descritas. Ressaltamos as especificações de acordo deste Termo de Referência apresentam, não somente os itens a serem entregues, como também as capacidades esperadas.

10.11 A CONTRATADA deve realizar a montagem física dos Firewalls nos locais estratégicos, assegurando a correta fixação e organização dos cabos.

10.12 A CONTRATADA deve fornecer a configuração inicial e customização do hardware e software dos Firewalls para atender às necessidades específicas do ambiente e instituição.

10.13 A CONTRATADA deve efetuar a configuração total do equipamento ou solução em nuvem

de controladora centralizada, garantindo que todas as funcionalidades de gerenciamento estejam completamente disponíveis para pronto uso e conforme orientação da CONTRATANTE.

10.14 A CONTRATADA será responsável pela gestão e execução dos serviços contratados, gestão dos recursos humanos e físicos necessários à execução do objeto contratual e fornecimento dos bens e materiais solicitados de acordo com o cronograma de execução;

10.15 Fornecer garantia e substituição do equipamento durante toda vigência Contratual;

10.16 Prestar serviços de suporte e assistência técnica aos bens pelo período de vigência do contrato, de acordo com a forma e regime estabelecidos;

10.17 A CONTRATADA deverá disponibilizar o planejamento e entregas dos serviços solicitados nos dias e horários definidos pelo CONTRATANTE, podendo ser realizados fora de horário comercial, incluindo sábados, domingos e feriados, caso o CONTRATANTE julgue necessário, sem nenhum ônus adicional a CONTRATATE

10.18 Observar rigorosamente todos os prazos de atendimento e resolução de chamados estabelecidos, bem como as datas de manutenções preventivas, sob pena de aplicação de multa e demais cominações pelo CONTRATANTE;

10.19 Agir de forma proativa, objetivando prevenir a ocorrência de erros e defeitos, por meio das inspeções nos equipamentos, componentes, dispositivos e softwares de configuração, bem como a coleta e avaliação de logs, atualização, verificação e inspeção visual das condições de funcionamento dos equipamentos, seus componentes e dispositivos;

10.20 Reparar eventuais falhas apresentadas nos equipamentos, compreendendo serviços de conserto, reparos e/ou substituição de bens, componentes e dispositivos, bem como sua configuração e gerenciamento, com vistas a normalidade da operação dos serviços prestados;

10.21 Prover toda e qualquer evolução de software, incluindo correções, patches, fixes, updates, service packs, novas releases, versões, builds e upgrades às suas expensas;

10.22 Comunicar à CONTRATANTE qualquer anormalidade que esteja impedindo a execução contratual dos serviços de suporte, prestando os esclarecimentos julgados necessários;

10.23 Responsabilizar-se por todos os tributos, contribuições fiscais e parafiscais que incidam ou venham a incidir, direta ou indiretamente, sobre os serviços fornecidos, bem como pelo custo do frete e outros inerentes à execução do objeto, apresentando os documentos fiscais em conformidade com a legislação vigente;

10.24 Assumir todas as despesas com transporte, hospedagem e outros custos operacionais decorrentes da execução do objeto, inexistindo qualquer possibilidade de pedido de desembolso à CONTRATANTE;

10.25 Responsabilizar-se pela fiel execução contratual, respondendo civil e criminalmente pelos danos diretos, que, por dolo ou culpa sua ou de seus empregados, causarem a CONTRATANTE ou a terceiros, sendo admitido o direito à ampla defesa;

10.26 Manter seus profissionais identificados com crachá em decorrência de acesso as dependências do CONTRATANTE, para prestação das atividades previstas para a execução do Contrato;

10.27 Fornecer equipamento de redundância, com características iguais ou superiores, sempre que precisar desativar hardware, software ou quaisquer recursos computacionais da CONTRATANTE, até que o problema seja sanado;

10.28 Responsabilizar-se pelo sigilo e confidencialidade, por si e seus empregados, dos documentos e/ou informações que lhe chegarem ao conhecimento por força da execução do contrato, e tenham sido definidas como confidenciais, não podendo divulgá-lo, sob qualquer pretexto, conforme as diretrizes estabelecidas pela Política de Segurança da Informação e Comunicações da CONTRATANTE e Lei Geral de Proteção de Dados;

10.29 Manter durante o período de vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação quanto à situação de regularidade da empresa (artigo 27, § 2º, do Decreto nº 5.540/2005), exigidas no ato da contratação;

10.30 Disponibilizar uma infraestrutura de atendimento via telefone ou web, para recebimento

registro dos chamados técnicos realizados pela CONTRATANTE, disponibilizando sempre um número de protocolo para controle de atendimento;

10.31 Entregar à CONTRATANTE, às suas expensas, toda documentação técnica (relatórios técnicos) gerada em função da execução do Contrato;

10.32 Responder por quaisquer acidentes de que possam sofrer os seus profissionais, quando em serviço nas dependências da CONTRATANTE;

10.33 Obedecer às normas internas da CONTRATANTE relativas à segurança,

identificação, ao trânsito e permanência de pessoas em suas dependências;

10.34 Acatar as orientações do Gestor e Fiscais do Contrato, sujeitando-se a fiscalização destes e prestando-lhes os esclarecimentos solicitados;

10.35 Observar a vedação de subcontratação parcial ou total da execução do objeto, de veiculação de publicidade acerca do Contrato, como também, de contratar servidor do quadro de pessoal da CONTRATANTE durante a vigência contratual;

10.36 Velar para que todos os privilégios de acesso a sistemas, dados ou informações do FUABC sejam utilizados exclusivamente na execução contratual e, pelo período estritamente essencial à realização de serviços

10.37 Refazer ou corrigir serviços às suas expensas, no todo ou em parte, sempre que identificado pela FUABC ter sido realizado em desacordo com o estabelecido no Termo de Referência;

10.38 Realizar a execução do objeto atendendo aos critérios de sustentabilidade ambiental, nos termos da Instrução Normativa SLTI/MPOG nº 01/2010, onde couber;

10.39 Informar e manter atualizados os números de telefone e endereço eletrônico (e-mail), bem como nome da pessoa autorizada para contatos que se fizerem necessários por parte da CONTRATANTE, bem como os dados do responsável pela assinatura do contrato e seus respectivos aditivos;

11 . DA FISCALIZAÇÃO

11.1 A gestão do presente contrato ficará sob a responsabilidade de Tiago Henrique Pezzo, Gerente de Informação, Saúde e Tecnologia RE:3504, RG:30.496.995-3, CPF:047.210.836-02 e Marcelo Teixeira da Dalt Netto, Coordenador de Rede Infra RE:5647, RG:14.087.035, CPF:074.800.576-52. Estes gestores atuarão na supervisão e acompanhamento das atividades relacionadas ao cumprimento das obrigações contratuais, garantindo que os serviços prestados estejam em conformidade com os requisitos estabelecidos neste Termo de Referência.

12. DO PREÇO E CONDIÇÕES DE PAGAMENTOS

12.1 Este contrato será executado sob regime de preço fixo e irreajustável, durante os primeiros 12 (doze) meses;

13. DA VIGÊNCIA E EFICÁCIA DO CONTRATO

13.1 O prazo de vigência do contrato será de 12 (doze) meses consecutivos e ininterruptos, contados a partir da data da assinatura do Contrato, podendo ser prorrogado por iguais e sucessivos períodos até o limite de 60 (sessenta) meses a critério da CONTRATANTE.

13.2 O início do serviço deverá ser executado a partir da data da assinatura do contrato entre as partes, tendo prazo máximo de 60 dias para implantação e configuração dos novos serviços podendo ser negociado em prazos excepcionais

Tiago Pezzo
GERENTE DE INFORMAÇÃO EM SAÚDE
REDE ASSISTENCIAL DE SÃO MATEUS – FUABC

ANEXO II

MODELO DE PROPOSTA COMERCIAL
(em papel timbrado da empresa participante)

À
REDE ASSISTENCIAL DA SUPERVISÃO TÉCNCIA DE SÃO MATEUS – FUNDAÇÃO DO ABC.

Ref. PROCESSO N° 133/25 - CONTRATAÇÃO DE EMPRESA PARA FORNECIMENTO DE INFRAESTRUTURA DE FIREWALL COMO HAAS, INCLUINDO INSTALAÇÃO E CONFIGURAÇÃO, COM O OBJETIVO DE REFORÇAR A SEGURANÇA DA REDE E IMPLEMENTAR VPNS SITE-TO-SITE, INTEGRAÇÃO NA NUVEM E ASSEGURANDO COMUNICAÇÃO SEGURA, TRÁFEGO ENTRE AS UNIDADES DA SEDE ADMINISTRATIVA E SEDE ASSISTENCIAL DA FUNDAÇÃO DO ABC – CONTRATO DE GESTÃO DE SÃO MATEUS, PARA O PERÍODO DE 12 (DOZE) MESES.

1. A empresa (razão social da participante), inscrita no CNPJ n.º xx.xxx.xxx/xxxx-xx, com sede no (endereço completo), por intermédio de seu representante legal, o(a) Sr.(a) (nome do representante Legal), infra-assinado, para os fins do Processo N° 133/25, apresenta a seguinte proposta de preço:

Item	LOCAL	LOCAL	ENDEREÇO	Quantidade de Firewall	Valor uni	Valor mensal
1	FORNECIMENTO DE EQUIPAMENTO DE SEGURANÇA TIPO FIRE WALL SERVIÇOS MONITORAMENTO	SEDE ADMINISTRATIVA	Rua Suíça, 95. Parque das Nações – Santo André (SP). CEP: 09210-000	2		
2	FORNECIMENTO DE EQUIPAMENTO DE SEGURANÇA TIPO FIRE WALL SERVIÇOS MONITORAMENTO	SEDE ASSISTENCIAL	Av. Cláudio Augusto Fernandes, 518, Cidade São Mateus, São Paulo – SP, CEP: 03962-120	1		
				Valor mensal		
				Valor global (12) meses		

VALOR MENSAL R$ (XXX.XXX, XX)
VALOR MENSAL POR EXTENSO:_____

VALOR PARA 12 (DOZE) MESES R$ (XXX.XXX, XX)
VALOR PARA 12 (DOZE) MESES POR EXTENSO:_____

1.1. Serviços de **SEGURANÇA DA REDE E IMPLEMENTAR VPNS SITE-TO-SITE**, de acordo com o termo de referência.

1.2. **DA VALIDADE DA PROPOSTA**: A proposta deverá conter prazo de validade mínimo de 60 (sessenta) dias.

1.3. A simples apresentação da proposta, implicará que a proponente considerou para fins da **FORMULAÇÃO DOS CUSTOS DA PROPOSTA**, todos os custos necessários para o atendimento do objeto desta contratação, preço tais como: custos com mão de obra, equipamentos, materiais, utensílios e transporte, impostos, encargos trabalhistas, previdenciários, fiscais, comerciais, taxas, fretes, seguros, deslocamentos de pessoal, garantia e quaisquer outros que incidam ou venham a incidir sobre o objeto licitado.

1.4. O pagamento será realizado de acordo com os serviços efetivamente atestados por profissionais designado pela Fundação do ABC;

(Local), ... de ..... de 2025.

REPRESENTANTE LEGAL DA EMPRESA
(Nome, assinatura)

ANEXO III

MODELOS DE ETIQUETAS PARA CAPA DOS ENVELOPES

ENVELOPE N° 01 – PROPOSTA COMERCIAL

FUNDAÇÃO DO ABC

SEGURANÇA DA REDE E IMPLEMENTAR VPNS SITE-TO-SITE

COLETA DE PREÇOS Nº 133/25

Razão Social: _____

CNPJ N°_____

Endereço do Proponente: _____

Nome do Representante Legal/Responsável_____

E-mail:_____

Telefone:_____

Data de Recebimento_____.

Horário_____hrs_____min.

ENVELOPE N° 02 – DOCUMENTAÇÃO

FUNDAÇÃO DO ABC

SEGURANÇA DA REDE E IMPLEMENTAR VPNS SITE-TO-SITE

COLETA DE PREÇOS Nº 133/25

Razão Social: _____

CNPJ N°_____

Endereço do Proponente: _____

Nome do Representante Legal/Responsável_____

E-mail:_____

Telefone:_____

Data de Recebimento_____

Horário_____hrs_____min.

ANEXO IV
[logotipo da empresa]
MODELO DE DECLARAÇÃO DE ANTICORRUPÇÃO

Eu, _____ , portador do CPF/MF n. _____ , representante legal da empresa (Razão Social da Empresa), estabelecida na _____.(endereço completo), inscrita no CNPJ/MF sob n.°_____, no uso de minhas atribuições, **DECLARO** que a pessoa jurídica conduz seus negócios de forma a coibir fraudes, corrupção e a prática de quaisquer outros atos lesivos à Administração Pública, direta ou indireta, nacional ou estrangeira, em atendimento à Lei Federal nº 12.846/ 2013 , ao Decreto Estadual nº 60.106/2014, tais como:

I – Prometer, oferecer ou dar, direta ou indiretamente, vantagem indevida a agente público, ou a terceira pessoa a ele relacionada;

II – Comprovadamente, financiar, custear, patrocinar ou de qualquer modo subvencionar a prática dos atos ilícitos previstos em Lei;

III – Comprovadamente, utilizar-se de interposta pessoa física ou jurídica para ocultar ou dissimular seus reais interesses ou a identidade dos beneficiários dos atos praticados;

IV – No tocante a licitações e contratos:

a) Frustrar ou fraudar, mediante ajuste, combinação ou qualquer outro expediente, o caráter competitivo de procedimento licitatório público;

b) Impedir, perturbar ou fraudar a realização de qualquer ato de procedimento licitatório público;

c) Afastar ou procurar afastar licitante, por meio de fraude ou oferecimento de vantagem de qualquer tipo;

d) Fraudar licitação pública ou contrato dela decorrente;

e) Criar, de modo fraudulento ou irregular, pessoa jurídica para participar de licitação pública ou celebrar contrato administrativo;

f) Obter vantagem ou benefício indevido, de modo fraudulento, de modificações ou prorrogações de contratos celebrados com a administração pública, sem autorização em lei, no ato convocatório da licitação pública ou nos respectivos instrumentos contratuais; ou;

g) Manipular ou fraudar o equilíbrio econômico-financeiro dos contratos celebrados com a administração pública;

V – Dificultar atividade de investigação ou fiscalização de órgãos, entidades ou agentes públicos, ou intervir em sua atuação, inclusive no âmbito das agências reguladoras e dos órgãos de fiscalização do sistema financeiro nacional.

[LOCAL] [DATA]

_____

Representante legal:
Empresa:
CNPJ:

ANEXO V

[logotipo da empresa]

DECLARAÇÃO

Eu, _____ , portador do CPF/MF n. _____ , representante legal da empresa (Razão Social da Empresa), estabelecida na _____.(endereço completo), inscrita no CNPJ/MF sob n.°_____, **DECLARO**, para todos os fins de direito, sob as penas da lei, não possuir no quadro da Empresa pessoa que figure como dirigente ou sócio cônjuge, companheiro, parente em linha reta, colateral ou por afinidade, até terceiro grau inclusive de profissionais integrantes de órgãos de deliberação ou direção da Fundação do ABC, exceto o previsto nos parágrafos 3º e 4º do artigo 6º do Regulamento Interno de Compras da Fundação do ABC.

Ainda, declaro que no quadro da empresa não possui sócios que sejam agentes políticos de Poder, membros do Ministério Público, ou dirigentes de órgão ou entidade da Administração Pública celebrante, bem como seus respectivos cônjuges, companheiros ou parentes, até o segundo grau, em linha reta, colateral ou por afinidade

[LOCAL] [DATA]

_____

Representante legal:
Empresa:
CNPJ:

ANEXO VI

[logotipo da empresa]

DECLARAÇÃO NÃO IMPEDIMENTOS

Eu, _____, portador do CPF/MF n. _____, representante legal da empresa (Razão Social da Empresa), estabelecida na _____. (endereço completo), inscrita no CNPJ/MF sob n.°_____, **DECLARO**, para todos os fins de direito, sob as penas da lei, de que inexiste impedimento em contratar com a Fundação do ABC ou com a Administração Pública.

[LOCAL] [DATA]

_____

Representante legal:
Empresa:
CNPJ:

ANEXO VII

[logotipo da empresa]

DECLARAÇÃO DE PERFEITAS CONDIÇÕES

Declaro, para todos os fins de direito, que de acordo com as especificações fornecidas pela CONTRATANTE, há perfeitas condições para execução completa dos serviços.

[LOCAL] [DATA]

_____

Representante legal:
Empresa:
CNPJ:

ANEXO VIII

[logotipo da empresa]

DECLARAÇÃO DE ACEITAÇÃO DO REGULAMENTO DE COMPRAS E CONTRATAÇÃO DA FUNDAÇÃO DO ABC

À FUNDAÇÃO DO ABC

Prezados Senhores,

Pelo presente, informamos que analisamos atentamento o Regulamento de Compras e Contratação da Fundação do ABC – FUABC e manifestamos plena aceitação aos termos e condições previstas no documento, não reputando qualquer vício ou discordância expressa e/ou tácita com as suas condições renunciando expressamente a qualquer discussão acerca de suas cláusulas, e concordando expressamente com o seu conteúdo.

Declaramos outrossim que o sócio/representante que abaixo assina tem plenos poderes para celebrar tal declaração.

Sem mais para o momento.

Atenciosamente,

[LOCAL] [DATA]

_____

Representante legal:
Empresa:
CNPJ:

ANEXO IX

FUNDAÇÃO DO ABC Desde 1967	**FORMULÁRIO**	**CÓDIGO: FOR.RHU.009**	**PÁG: 1 de 3**
		ELABORADO: 16/07/2021	**REVISADO: 28/06/2023**
		VIGÊNCIA: NA	**VERSÃO: 01**
TÍTULO: QUESTIONÁRIO DE *DUE DILIGENCE* DE *COMPLIANCE* DE FORNECEDORES			

IDENTIFICAÇÃO DO FORNECEDOR - DADOS CADASTRAIS BÁSICOS		
Razão social	CNPJ ou equivalente	
Nome fantasia		Data de constituição / /
Endereço	Número	Complemento
Cidade	Estado	CEP

INFORMAÇÕES SOBRE A PARTICIPAÇÃO SOCIETÁRIA E GESTÃO DA EMPRESA

Apresentar os dados das pessoas físicas e jurídicas que detém participação societária. Se houver alguma pessoa jurídica nesta lista, por favor, indicar os beneficiários finais, até o nível em que haja somente pessoas físicas.

Nome/Razão social	CPF/CNPJ	Nacionalidade	% Participação

As pessoas listadas nos itens anteriores possuem relação de parentesco com algum colaborador em cargo de confiança – Conselheiro, dirigente, diretor, gerente ou coordenador da Fundação do ABC?	☐ Sim ☐ Não
Em caso afirmativo informar os seguintes dados:	Nome: Função: Unidade:

RAMO DE ATIVIDADE	
1. Segmento	☐ Indústria ☐ Comércio e Serviços
Principais atividades (CONFORME DESCRIÇÃO NO CNAE):	Atividades secundárias:

PORTE	
2. Receita bruta anual: ☐ Até R$ 60 mil e 1 até empregado (Microempreendedor individual - MEI) ☐ Até R$ 360 mil (Microempresa) ☐ De R$ 360 mil a R$ 3,6 milhões (Pequena empresa) ☐ De R$ 3,6 milhões a R$ 300 milhões (Média empresa) ☐ Acima de R$ 300 milhões (Grande empresa)	3. Nº de empregados: ☐Até 19 ☐De 20 a 99 ☐De 100 a 499 ☐Acima de 500 Cobertura geográfica:

POLÍTICAS E PROCEDIMENTOS	
Programa de Integridade	☐ Sim ☐ Não
Em caso positivo, fornecer uma cópia.	
Código de ética	☐ Sim ☐ Não
Em caso positivo, fornecer uma cópia.	

FUNDAÇÃO DO ABC Desde 1967	FORMULÁRIO	CÓDIGO: FOR.RHU.009	PÁG: 2 de 3
		ELABORADO: 16/07/2021	REVISADO: 28/06/2023
		VIGÊNCIA: NA	VERSÃO: 01

TÍTULO: QUESTIONÁRIO DE *DUE DILIGENCE* DE *COMPLIANCE* DE FORNECEDORES

A empresa possui política de recebimento e apuração de denúncias de irregularidades por parte de seus steackholders (Canal de Denúncias)?	☐ Sim ☐ Não
Política de seleção e contratação de funcionários	☐ Sim ☐ Não
Prevenção e combate à fraude e corrupção	☐ Sim ☐ Não
Oferta e recebimento de brindes, presentes e hospitalidades	☐ Sim ☐ Não
Política de registros contábeis e financeiros	☐ Sim ☐ Não
Proteção de dados	☐ Sim ☐ Não
Segurança da Informação	☐ Sim ☐ Não
Due diligence de terceiros	☐ Sim ☐ Não
Os funcionários recebem treinamentos sobre Código de Ética e/ou outros temas relacionados com ética, integridade e anticorrupção?	☐ Sim ☐ Não
Em caso positivo, com qual frequencia?	

SUPORTE E COMPROMETIMENTO DA ALTA ADMINISTRAÇÃO E LIDERANÇA

O fornecedor possui um órgão ou área responsável pela coordenação ou gestão de suas atividades de *Compliance* (integridade e conformidade)	☐ Sim ☐ Não
Este órgão ou área está subordinado à(o):	☐Presidência ☐Jurídico ☐Financeiro ☐Outro:
O fornecedor possui canal de denúncias? Caso positivo, identificar o fluxo de tratamento das ocorrências, se é garantida a confidencialidade dos dados e a proteção do anonimato aos denunciantes	☐ Não ☐ Sim. Resposta:
O fornecedor promove treinamentos periódicos sobre suas normas internas, inclusive a seus empregados e demais públicos pertinentes	☐ Sim ☐ Não
São mantidos registros dos treinamentos, incluindo controle dos participantes e do material utilizado	☐ Sim ☐ Não

QUESTÕES OPERACIONAIS E REPUTACIONAIS

O fornecedor possui algum tipo de conflito de interesses que impossibilitaria a prestação de serviços a FUABC?	☐ Não ☐ Sim, qual impedimento:
O fornecedor subcontrata algum de seus serviços ou utiliza intermediários?	☐ Sim ☐ Não
O fornecedor possui controles financeiros, de tesouraria e contábeis adequados, precisos e atualizados?	☐ Sim ☐ Não
Possui registros contábeis submetidos à auditoria independente (em caso positivo, informa a empresa de auditoria):	☐ Sim ☐ Não

A empresa, seus acionistas, conselheiros ou diretores estatutários ou quaisquer empresas em seu grupo econômico estão ou estiveram nos últimos 05 (cinco) anos, de qualquer forma, envolvidos em processos administrativos ou judiciais fundados nas legislações abaixo:

Leis anticorrupção brasileira ou internacionais	☐ Sim ☐ Não
Lei de improbidade administrativa	☐ Sim ☐ Não
Lei de licitações	☐ Sim ☐ Não
Lei de Defesa da Concorrência	☐ Sim ☐ Não
Processos criminais	☐ Sim ☐ Não

Em caso de afirmativo à questão anterior, justificar e identificar o andamento do(s) processo(s).

Nome da pessoa envolvida	Justificativa	Andamento

FUNDAÇÃO DO ABC Desde 1967	FORMULÁRIO	CÓDIGO: FOR.RHU.009	PÁG: 3 de 3
		ELABORADO: 16/07/2021	REVISADO: 28/06/2023
		VIGÊNCIA: NA	VERSÃO: 01

TÍTULO: QUESTIONÁRIO DE *DUE DILIGENCE* DE *COMPLIANCE* DE FORNECEDORES

PESSOA EXPOSTA POLITICAMENTE AO CONFLITO DE INTERESSE
Algum proprietário, sócio, acionista majoritário, membro do Conselho de Administração, Diretor e/ou representante da empresa enquadra-se na na condição de PEP, conforme definido no § 1º, artigo 1º, da Resolução COAF n.° 40, de 22 de novembro de 2021?
☐ Sim ☐ Não - Em caso positivo, informe quem é a pessoa, a posição ocupada e o órgão do governo:

DECLARAÇÃO
Declaro e atesto para os devidos fins que as informações fornecidas anteriormente, bem como os documentos disponibilizados são verdadeiros e não ocultaram quaisquer dados. Se em algum momento as informações ou documentos apresentados neste questionário não representarem mais a realidade, comprometo-me em comunicar imediatamente a Fundação do ABC e fornecer um relatório complementar detalhando referida mudança.
_____ _____/_____/_____ _____
Local (cidade) Data Assinatura do responsável

ANEXO X

DECLARAÇÃO DE CUMPRIMENTO AO CÓDIGO DE CONDUTA ÉTICA DA FUABC

A empresa_____, CNPJ_____, declara, para os devidos fins legais, estar ciente e de acordo com as normas institucionais, preceitos éticos e de anticorrupção previstos no Código de conduta Ética da Fundação do ABC, comprometendo-se a cumpri-lo fielmente, durante todo o período de vigência do presente contrato, em especial, atender as práticas de antissuborno voltadas aos seus representantes ou por terceiras pessoas a eles relacionadas, independentemente do valor envolvido, não efetuando qualquer tipo de pagamento, dação, doação, presente, entretenimento, transporte, patrocínio, doação beneficente dentre outros que possam ser caracterizados como subornos, propinas ou ainda prometer, oferecer ou dar, direta ou indiretamente qualquer vantagem indevida para garantir negócios com as empresas interessadas em adquirir nossos produtos e serviços.

Atenciosamente,

[LOCAL] [DATA]

_____

Representante legal:
Empresa:
CNPJ:

ANEXO XI

[logotipo da empresa]

ATESTADO DE VISTORIA (obs.: emitir um para cada unidade visitada)

Declaramos que a empresa _____, CNPJ nº _____, esteve presente através de seu representante Sr(a) _____,portador do documento de identidade nº _____ realizando vistoria na unidade _____, onde deverá ser executado os serviços constantes no Anexo I – TERMO DE REFERENCIA.

Estando a mesma ciente das obrigações, natureza e vulto dos serviços, bem como, informados a respeito de todas as condições locais que direta e indiretamente se relacionem com a execução dos trabalhos e serviços.

____ de _____ de 2025.

_____

FUNDAÇÃO DO ABC - REDE ASSISTENCIAL DA SUPERVISÃO TÉCNICA DE SAÚDE DE SÃO MATEUS– Unidade Visitada

De acordo:

_____

Representante legal:
Empresa:
CNPJ:

ANEXO XII

[logotipo da empresa]
MODELO DE OPÇÃO POR NÃO REALIZAR A VISITA TÉCNICA

Eu, _____, portador do RG nº _____ e do CPF nº_____, na condição de representante legal de _____ (nome Empresa), inscrita no CNPJ sob o nº_____, com sede no endereço _____, interessado em participar da Coleta de Preços nº, DECLARO que a Empresa não realizou a visita técnica prevista no Ato convocatório e que, mesmo ciente da possibilidade de fazê-la e dos riscos e consequências envolvidos, optou por formular a proposta sem realizar a visita técnica que lhe havia sido facultada. A Empresa está ciente desde já que, em conformidade com o estabelecido no Ato convocatório, não poderá pleitear em nenhuma hipótese modificações nos preços, prazos ou condições ajustadas, tampouco alegar quaisquer prejuízos ou reivindicar quaisquer benefícios sob a invocação de insuficiência de dados ou informações sobre os locais em que serão executados os serviços.

Local, data.

_____

Representante legal:
Empresa:
CNPJ:

ANEXO XIII

logotipo da empresa]

MODELO DE DECLARAÇÃO DE QUE NÃO EMPREGA MENOR

Processo nº:
Objeto:

A Empresa_____, devidamente inscrita, no CNPJ/MF sob o nº_____, com sede_____, nº_____, Bairro_____, na cidade de _____, por intermédio de seu representante legal, o Sr._____, portador do CPF/MF nº_____, DECLARA, nos termos da Lei nº 9.854/1999, que não emprega menor de 18 (Dezoito) anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 (Dezesseis) anos, salvo na condição de aprendiz.

[LOCAL] [DATA]

_____

Empresa

Representante Legal
CNPJ:

_____

Empresa

Representante Legal
CNPJ:

ANEXO XIV

MODELO DE DECLARAÇÃO DE RESPONSABILIDADE

Processo nº:

A Empresa_____, devidamente inscrita, no CNPJ/MF sob o nº_____, com sede_____, nº_____, Bairro_____, na cidade de _____, por meio de seu representante legal, vem, por me o desta ,declarar, sob as penas da lei, que assume integral responsabilidade por quaisquer ações trabalhistas, cíveis ou de qualquer outra natureza que venham a ser propostas por seus funcionários, prepostos, contratados ou terceiros a ela vinculados, relacionados às atividades desempenhadas no âmbito do contrato firmado com a Fundação do ABC.

A _____, compromete-se a adotar todas as medidas necessárias para garantir o cumprimento das obrigações trabalhistas, previdenciárias, fiscais e cíveis, isentando a Fundação do ABC de qualquer responsabilidade solidária ou subsidiária, seja no polo passivo de eventuais demandas judiciais ou extrajudiciais, seja em relação a quaisquer encargos ou ônus decorrentes de tais ações.

Esta declaração é firmada em observância às disposições legais aplicáveis, em especial à Lei n11 13.429/2017, à Consolidação das Leis do Trabalho (CLT) e ao Código Civil Brasileiro, com o objetivo de resguardar a Fundação do ABC de qualquer vinculação ou responsabilidade por atos ou omissões da _____.

Por ser verdade, firmamos a presente declaração para que produza os devidos efeitos legais.

[LOCAL] [DATA]

_____

Empresa

Representante Legal
CNPJ:

ANEXO XV
MINUTA DE CONTRATO.

CONTRATAÇÃO DE EMPRESA PARA FORNECIMENTO DE INFRAESTRUTURA DE FIREWALL COMO HAAS, INCLUINDO INSTALAÇÃO E CONFIGURAÇÃO, COM O OBJETIVO DE REFORÇAR A SEGURANÇA DA REDE E IMPLEMENTAR VPNS SITE-TO-SITE, INTEGRAÇÃO NA NUVEM E ASSEGURANDO COMUNICAÇÃO SEGURA, TRÁFEGO ENTRE AS UNIDADES DA SEDE ADMINISTRATIVA E SEDE ASSISTENCIAL DA FUNDAÇÃO DO ABC – CONTRATO DE GESTÃO DE SÃO MATEUS, PARA O PERÍODO DE 12 (DOZE) MESES - PROCESSO Nº 133/25.

EMENTA: FORNECIMENTO DE INFRAESTRUTURA DE FIREWALL COMO HAAS, INCLUINDO INSTALAÇÃO E CONFIGURAÇÃO, COM O OBJETIVO DE REFORÇAR A SEGURANÇA DA REDE E IMPLEMENTAR VPNS SITE-TO-SITE, INTEGRAÇÃO NA NUVEM E ASSEGURANDO COMUNICAÇÃO SEGURA, TRÁFEGO ENTRE AS UNIDADES DA SEDE ADMINISTRATIVA E SEDE ASSISTENCIAL DA FUNDAÇÃO DO ABC – CONTRATO DE GESTÃO DE SÃO MATEUS, PARA O PERÍODO DE 12 (DOZE) MESES, VISANDO ATENDER AS NECESSIDADES DO MUNICÍPIO DE SÃO PAULO – 133/25

CONTRATADA: _____

Por este instrumento, as partes, de um lado a **FUNDAÇÃO DO ABC- REDE ASSISTENCIAL DA SUPERVISÃO TÉCNICA DE SAÚDE DE SÃO MATEUS**, inscrita no Cadastro Nacional de Pessoas Jurídicas do Ministério da Fazenda sob o n° 57.571.275/0023-08, estabelecida na Rua Bandeira de Aracambi, n° 704, Jardim Rodolfo Pirani, São Paulo - SP, CEP: 08310-010, neste ato representada por seu Diretor Geral, _____, brasileiro, , estado civil , RG nº _____e CPF/MF nº _____, doravante denominada simplesmente **"CONTRATANTE",** e de outro lado, a empresa _____, estabelecida _____, regularmente inscrita no Cadastro Nacional de Pessoas Jurídicas do Ministério da Fazenda sob o nº _____, representada na forma de seu contrato social, doravante designada **"CONTRATADA**", tendo em vista o Processo Administrativo nº 133/25, tem por justo e acordado as seguintes condições:

1. DO OBJETO

1.1 O presente contrato tem por objeto a CONTRATAÇÃO DE EMPRESA PARA FORNECIMENTO DE INFRAESTRUTURA DE FIREWALL COMO HAAS, INCLUINDO INSTALAÇÃO E CONFIGURAÇÃO, COM O OBJETIVO DE REFORÇAR A SEGURANÇA DA REDE E IMPLEMENTAR VPNS SITE-TO-SITE, INTEGRAÇÃO NA NUVEM E ASSEGURANDO COMUNICAÇÃO SEGURA, TRÁFEGO ENTRE AS UNIDADES DA SEDE ADMINISTRATIVA E SEDE ASSISTENCIAL DA FUNDAÇÃO DO ABC – CONTRATO DE GESTÃO DE SÃO MATEUS, PARA O PERÍODO DE 12 (DOZE) MESES, visando atender as necessidades do Município de São Paulo, rigorosamente conforme Termo de Referência, processo de compras nº 133/25, proposta comercial e anexos, partes integrantes desta avença.

1.2 Os serviços deverão atender as características equivalentes ou superiores aos apresentados e ofertados na proposta comercial.

2 PRAZO

2.1 O prazo de vigência do contrato é de 12 (doze) meses consecutivos e ininterruptos, contados a partir da assinatura do presente instrumento contratual, podendo ser prorrogado por igual e sucessivo período, no limite de 60 (sessenta) meses, nos termos e condições permitidos pela legislação vigente.

3 CONDIÇÕES DE EXECUÇÃO

3.1 Os serviços serão iniciados pela CONTRATADA após a assinatura do Contrato de Prestação de Serviços.

3.2 A CONTRATANTE fiscalizará obrigatoriamente a execução do contrato, a fim de verificar se no seu desenvolvimento estão sendo observadas as especificações e demais requisitos nele previstos, reservando-se o direito de rejeitar os serviços que, a seu critério, não forem considerados satisfatórios, ressalvado o direito de defesa da CONTRATADA;

3.3 Deverá a CONTRATADA, tendo ciência do valor global disposto na Cláusula 9.0 deste contrato, manter controle próprio da execução do objeto, não ultrapassando o limite financeiro global estipulado.

3.4 O valor global poderá ser ultrapassado única e exclusivamente mediante solicitação

da CONTRATANTE e desde que devidamente motivado, sendo acompanhado do respectivo Termo Aditivo.

3.5 Havendo solicitação da CONTRATANTE e aditamento de acréscimo ao valor do contrato, poderá a CONTRATADA continuar a execução do objeto observando o novo valor estipulado.

3.6 Sendo ultrapassado o valor mensal estimado na Cláusula 9.0, deverá a CONTRATADA informar imediatamente a CONTRATANTE, a fim de que esta redistribua execução do contrato ou solicite o aditamento de valor devido, limitando-se ao disposto na Cláusula 4.7 do presente instrumento.

3.7 O descumprimento das Cláusulas 3.3 a 3.6 sujeitará a CONTRATADA ao não recebimento dos valores executados que ultrapassem o valor global do Contrato.

3.8 Os serviços serão realizados prestados paras as unidades constantes no Anexo II do presente contrato.

3.9 Em cumprimento à Lei Geral de Proteção de Dados Pessoais - Lei nº 13.709/2018 - as partes se obrigam a respeitar os termos e condições estabelecidos no Anexo I do presente contrato.

3.10 A CONTRATADA deverá realizar os serviços condizente com a proposta comercial, devendo este atender o descritivo técnico mínimo descrito no Termo de Referência.

3.10.1 Havendo discrepância dos serviços, a CONTRATADA será notificada via e-mail para apuração e substituição dos produtos e/ou serviços e/ou locações em até 05 (cinco) dias.

3.11 Os responsáveis pelos acessos que ingressar nas unidades devem estar uniformizados, identificado com crachá e portando todo e qualquer EPI necessário.

4 DAS OBRIGAÇÕES DA CONTRATADA

São obrigações da CONTRATADA:

4.1 Deverá iniciar os serviços apenas após a assinatura do presente contrato, conforme

termos prazos e condições neste instrumento estabelecidos;

4.2 Prestar os serviços observando as melhores préticas e técnicas aplicadas no mercado.

4.3 Cumprir todas as normas, regras e leis aplicaveis a execução do objeto do Contrato.
4.4 Obriga-se a Contratada a seguir exatamente os termos e requisitos para prestação dos serviços contemplados no termo de referência do memorial descritvo de coleta de preços.

4.5 Todos os encargos decorrentes da execução dos ajustes, tais como: obrigações civis, trabalhistas, fiscais, previdenciarias, assim como despesas com transportes, distribuição e quaisquer outras que incidão sobre a contratação, serão de exclusiva responsabilidade da Contratada.

4.6 Indenizar, imediatamente, a Contratante por quaisquer danos que seus representantes legais, prepostos, empregados ou terceirizados credenciados causem, por culpa, dolo, ação ou omissão, a Contratante ou a terceiros.

4.7 A Contratada deverá estar em condições de prestar os serviços a partir da data da assinatura do Contrato e manter essa condição durante a vigência do Contrato, atendendo a demanda contratada, incluido-se eventuais acréscimos ou supressões que não deverão ultrapassar os 25% (vinte e cinco por cento) do valor inicial atualizado do Contrato, nos termos do Regulamento de Compras da Fundação do ABC e., subsidiariamente, a lei 14.133/21.

4.8 A Contratada deverá manter durante todo o período do contrato, compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas no Certame.

4.9 Fica vedada a Contratada a subcontratação objeto do Contrato, bem como a execução deste através de terceiros sem a expressa anuência da Contratante, que deverá motivar eventual liberação.

4.10 A Contratada devera responsabilizar-se pelo fornecimento de todos os Equipamentos de Proteção Individual – EPIs, nas quantidades necessarias a perfeita execução dos serviços.

4.11 Responsabilizar-se pelo comprimento, por parte dos funcionarios, das normas diciplinares determinadas pela Contratante.

4.12 Assumir inteira responsabilidade técnica e administrativa do objeto contratado, não podendo, sob qualquer hipotese, transferir a outras empresas a responsabilidade por

problemas no fornecimento do serviço.

4.13 Responder diretamente por quaisquer perdas, danos, ou prejuisos que vier a causar a Contratante, decorrentes de sua ação ou omisão, dolosa ou culposa, na execução deste contrato, independentemente de outras cominações contratuais ou legais a que estiver sujeita.

4.14 Cumprir rigorasamente as exigencias da legislação tributaria, fiscal, trabalhista, previdenciaria assumindo todas as obrigações e encargos legais inerentes e respondendo integralmente pelo onus resultantes das infrações cometidas;

4.15 Fornecimento de dois firewalls de próxima geração para a Fundação do ABC – Contrato São Mateus garantindo proteção avançada contra ameaças cibernéticas, assegurando segurança abrangente para dados e sistemas.

4.16 A solução deverá permitir a gestão eficaz do tráfego de rede, prevenção de acessos não autorizados e otimização do desempenho.

4.17 Os firewalls deverão suportar redes complexas e grandes volumes de dados, além de viabilizar a implementação de VPNs site-to-site para comunicação segura entre unidades.

4.18 Monitoramento contínuo do tráfego e estarão preparados para integração futura com soluções em nuvem, garantindo continuidade operacional e escalabilidade.

4.19 A escolha dessa tecnologia demonstra o compromisso da instituição com a segurança da informação, protegendo seus ativos digitais e adotando medidas preventivas e proativas contra ameaças emergentes no cenário cibernético.

4.20 **Proteção Avançada Contra Ameaças**: Segurança contra-ataques DDoS, ransomware, malware e tentativas de acesso não autorizado, garantindo a integridade dos dados.

4.21 **Gestão Eficiente do Tráfego**: Controle e otimização do uso da rede, priorizando aplicações críticas e assegurando alto desempenho para usuários e sistemas.

4.22 **VPNs Site-to-Site Seguras:** Comunicação criptografada entre unidades, proporcionando conectividade estável e segura para transferência de dados.

4.23 **Integração com a Nuvem**: Suporte a ambientes híbridos, permitindo a continuidade dos serviços mesmo em caso de falha na infraestrutura local.

4.24 **Monitoramento Contínuo e Resposta a Incidentes**: Supervisão 24x7 da rede, identificação de anomalias em tempo real e mitigação proativa de riscos.

4.25 **Suporte Técnico Especializado**: Atendimento rápido e eficiente para a resolução de problemas, reduzindo impactos operacionais.

4.26 Locais:

LOCAL	ENDEREÇO	Quantidade de Firewall
SEDE ADMINISTRATIVA	Rua Suíça, 95. Parque das Nações – Santo André (SP). CEP: 09210-000	2
SEDE ASSISTENCIAL	Av. Cláudio Augusto Fernandes, 518, Cidade São Mateus, São Paulo – SP, CEP: 03962-120	1

4.27 As atividades de instalação, configuração e suporte técnico deverão ser realizadas prioritariamente no ambiente atual. Caso ocorra uma mudança de endereço, a empresa contratada será responsável por todos os custos relacionados à remoção e relocação dos equipamentos.

4.28 Especificações Técnicas do Firewall para Sede Administrativa:

TERMOS TÉCNICOS	REQUISITOS
Throughput de Firewall	Deve ser capaz de manipular no mínimo até 7 Gbps.
Throughput de IPS	Deve suportar no mínimo até 1,4 Gbps com a funcionalidade de IPS ativa.
Throughput de NGFW	Deve suportar no mínimo até 1 Gbps com funcionalidades de firewall, IPS e controle de aplicativos ativos.
Throughput de Proteção contra Ameaças	Deve ser capaz de suportar no mínimo até 900 Mbps com proteção ativa contra malware.
Throughput de VPN IPsec	Deve ser capaz de alcançar no mínimo até 6,5 Gbps para conexões seguras de alta velocidade.
Throughput de Inspeção SSL	Deve ser capaz no mínimo de processar até 950 Mbps para sessões HTTPS com cifra média.
Túneis VPN IPsec	Deve suportar no mínimo até 200 túneis de VPN IPsec Site-to-Site simultâneos.
Usuários SSL-VPN	Deve suportar no mínimo até 200 usuários SSL-VPN simultâneos.
Sessões Simultâneas	Deve suportar no mínimo até 1.500.000 de conexões TCP simultâneas.
Novas Sessões por Segundo	Deve suportar no mínimo até 45.000 novas sessões por segundo.
Políticas de Firewall	Deve permitir a criação de até 5.000 regras distintas.
CARACTERÍSTICAS DE HARDWARE	**ESPECIFICAÇÕES**
Portas 10 Gigabit Combo	Deve possuir 2 portas 10 Gigabit SFP+.
Portas GE RJ45	Deve possuir 8 portas GE RJ45 configuráveis para uso como LAN, WAN ou DMZ.
Portas USB	Deve dispor de 1 porta USB para conectividade adicional.
Porta de Console	Deve possuir 1 porta de console RJ45 para gerenciamento.
Armazenamento de Logs	Deve prover armazenamento seguro em nuvem.
CARACTERÍSTICAS AMBIENTAIS	**ESPECIFICAÇÕES**
Fixação e Dimensões	O dispositivo deve ser compacto com opção para fixação em rack. Dimensões de 1.6 x 8.5 x 7.0 polegadas e peso de 1,1 kg.
Requisitos de Energia	Deve operar com fonte de alimentação de 12V DC, 3A, com plugue no formato padrão NBR 14136.
Faixa de Temperatura Operacional	Deve funcionar de forma adequada em temperaturas entre 0°C e 40°C.
CARACTERÍSTICAS DE RECURSOS	**ESPECIFICAÇÕES**
Domínios Virtuais	Deve suportar até no mínimo 10 domínios virtuais para gerenciamento de ambientes multi-tenant.
Opções de Alta Disponibilidade	Deve suportar configurações em modos Ativo-Ativo, Ativo-Passivo e Clustering, garantindo redundância e disponibilidade contínua.
Unidade de Processamento de Segurança	Deve utilizar unidades de processamento de segurança especializadas para desempenho aprimorado em tarefas de detecção de ameaças e criptografia.

4.29 Especificações Técnicas do Firewall para Sede Assistencial

TERMOS TÉCNICOS	REQUISITOS
Throughput de Firewall	Deve ser capaz de manipular no mínimo até 6 Gbps.
Throughput de IPS	Deve suportar no mínimo até 1,4 Gbps com a funcionalidade de IPS ativa.
Throughput de NGFW	Deve suportar no mínimo até 1 Gbps com funcionalidades de firewall, IPS e controle de aplicativos ativos.
Throughput de Proteção contra Ameaças	Deve ser capaz de suportar no mínimo até 700 Mbps com proteção ativa contra malware.
Throughput de VPN IPsec	Deve ser capaz de alcançar no mínimo até 6,5 Gbps para conexões seguras de alta velocidade.
Throughput de Inspeção SSL	Deve ser capaz no mínimo de processar até 630 Mbps para sessões HTTPS com cifra média.
Túneis VPN IPsec	Deve suportar no mínimo até 200 túneis de VPN IPsec Site-to-Site simultâneos.
Usuários SSL-VPN	Deve suportar no mínimo até 200 usuários SSL-VPN simultâneos.
Sessões Simultâneas	Deve suportar no mínimo até 700.000 de conexões TCP simultâneas.
Novas Sessões por Segundo	Deve suportar no mínimo até 30.000 novas sessões por segundo.
Políticas de Firewall	Deve permitir a criação de até 2.000 regras distintas.
CARACTERÍSTICAS DE HARDWARE	**ESPECIFICAÇÕES**
Portas GE RJ45	Deve possuir no mínimo 8 portas GE RJ45 configuráveis para uso como LAN, WAN ou DMZ.
Portas USB	Deve dispor de no mínimo 1 porta USB para conectividade adicional.
Porta de Console	Deve possuir no mínimo 1 porta de console RJ45 para gerenciamento.
Armazenamento de Logs	Deve prover armazenamento seguro em nuvem.
CARACTERÍSTICAS AMBIENTAIS	**ESPECIFICAÇÕES**
Fixação e Dimensões	O dispositivo deve ser compacto, com dimensões de 1.5 x 8.5 x 6.3 polegadas e peso de 1 kg para posicionamento em bandeja ou fixação em rack.
Requisitos de Energia	Deve operar com fonte de alimentação de 12V DC, 3A, com plugue no formato padrão NBR 14136.
Faixa de Temperatura Operacional	Deve funcionar de forma adequada em temperaturas entre 0°C e 40°C.
CARACTERÍSTICAS DE RECURSOS	**ESPECIFICAÇÕES**
Domínios Virtuais	Deve suportar no mínimo até 10 domínios virtuais para gerenciamento de ambientes multi-tenant.
Opções de Alta Disponibilidade	Deve suportar configurações em modos Ativo-Ativo, Ativo-Passivo e Clustering, garantindo redundância e disponibilidade contínua.
Unidade de Processamento de Segurança	Deve utilizar unidades de processamento de segurança especializadas para desempenho aprimorado em tarefas de detecção de ameaças e criptografia.

4.30 REQUISITOS TÉCNICOS GERAIS Filtro de pacote, controle de aplicação, administração de largura de banda (QoS), VPN.

4.31 IPsec e SSL, IPS, prevenção contra ameaças como vírus, spywares e malwares "Zero Day".

4.32 Filtro de Conteúdo Web (Webfilter) e controle de transmissão de dados e acesso à internet, compondo uma plataforma robusta e integrada de segurança.

4.33 Deve ser um appliance físico específico para proteção de rede, integrando funcionalidades de um Firewall de Nova Geração (NGFW).

4.34 Deve garantir um throughput mínimo de 1 Gbps com todas as funcionalidades de segurança habilitadas (controle de aplicações, prevenção de intrusões, antimalware,

antivírus, antispyware, sandboxing e filtragem de URLs).

4.35 Suporte para pelo menos 1.500.000 conexões simultâneas para a Sede Administrativa e 750.000 para a Sede Assistencial, com capacidade de até 100.000 novas conexões HTTP por segundo para a Sede Administrativa e 55.000 para a Sede Assistencial.

4.36 O firewall deve ser fornecido com software dedicado, não sendo aceitável o uso de sistemas operacionais de propósito geral.

4.37 Funcionalidades de SD-WAN A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação.

4.38 Possibilidade de criar políticas para modelagem do tráfego com os seguintes parâmetros: IP de origem, VLAN de origem, IP de destino, Porta TCP/UDP de destino, Domínio e URL de destino.

4.39 Aplicação de camada 7 utilizada (O365 Exchange, AWS, Dropbox, etc).

4.40 Capacidade de monitorar e identificar falhas com health check, permitindo testes de resposta por ping, HTTP, TCP/UDP echo, DNS, TCP-connect e TWAMP.

4.41 O SD-WAN deve balancear o tráfego das aplicações entre múltiplos links simultaneamente.

4.42 Deve ser capaz de analisar o tráfego em tempo real e realizar balanceamento de pacotes do mesmo fluxo entre múltiplos links, com reordenação dos pacotes caso necessário.

4.43 Criação de políticas de roteamento com base nos seguintes critérios: Latência, Jitter, Perda de pacote e Banda ocupada ou todos ao mesmo tempo.

4.44 A solução deve permitir a definição de roteamento para cada aplicação.

4.45 Diversas formas de escolha de link, incluindo: Melhor link, Menor custo e Definição de níveis máximos de qualidade.

4.46 Possibilidade de definir o link de saída para uma aplicação específica.

4.47 Implementar balanceamento de link por hash do IP de origem e destino.

4.48 A solução de SD-WAN deve oferecer suporte a roteamento baseado em políticas (Policy Based Routing) ou encaminhamento baseado em políticas.

4.49 Deve suportar roteamento estático e dinâmico (BGP e OSPF).

4.50 Possibilidade de realizar balanceamento por pacote entre túneis IPsec.

4.51 Deve possuir recurso de correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões.

4.52 Deve permitir a customização dos timers para detecção de queda de link, com tempo necessário para restabelecimento.

4.53 Deve possibilitar políticas para controlar o uso de aplicações e tráfego intenso (como YouTube, Facebook) que possam impactar as aplicações de negócio e deve permitir bloqueio ou limitação de tráfego excessivo para evitar impacto nas aplicações de negócios.

4.54 Suporte para criar políticas de QoS e Traffic Shaping por endereço de origem, endereço de destino, usuário ou grupo de usuários, aplicações e porta, permitir definição de tráfego com banda garantida (banda mínima disponível para aplicações de negócio) e definição de tráfego com banda máxima para aplicativos best-effort (ex. YouTube, Facebook).

4.55 Possibilidade de marcar pacotes com DSCP para reserva de banda ao longo do backbone.

4.56 Configuração de filas de prioridade para aplicações específicas.

4.57 Possibilidade de definir banda máxima e garantida por aplicação, com suporte para categorias de URL, IPs de origem e destino, logins e portas.

4.58 Definição de Bandas Distintas para Download e Upload.

4.59 Capacidade de agendar intervalos de tempo para aplicar políticas de banda, como horários mais permissivos durante o almoço.

4.60 Visualização em tempo real de ocupação de banda (upload e download), bem como latência, jitter e perda de pacote.

4.61 Suporte a IPv6: Compatibilidade com IPv6.

4.62 Possibilidade de definir roteamento específico por grupo de usuário.

4.63 Suporte para configuração em modos Ativo/Passivo e Ativo/Ativo.

4.64 O SD-WAN deverá possuir serviço de Firewall Stateful;

4.65 A solução SD-WAN deverá fornecer criptografia AES de 128 bits ou AES de 256 bits em sua VPN;

4.66 A solução SD-WAN deverá simplificar a implantação de túneis criptografados de site para site;

4.67 Deve ser capaz de bloquear acesso às aplicações;

4.68 Deve suportar NAT dinâmico bem como NAT de saída;

4.69 Deve suportar balanceamento de tráfego por sessão e pacote;

4.70 As funcionalidades de SD-WAN podem ser fornecidas no NGFW ofertado ou em uma solução à parte, na mesma quantidade de equipamentos definida para os firewalls;

4.71 Em caso de composição de solução, a solução de SD-WAN deverá suportar tráfego compatível com a capacidade do equipamento de NGFW.

4.72 Controle por Política de Firewall -Deverá suportar controles por zonas de segurança;

4.73 Deverá suportar controles de políticas por porta e protocolo;

4.74 Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;

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

4.76 Controle de políticas por código de país (Por exemplo: BR, US, UK, RU);

4.77 Controle, inspeção e descriptografia de SSL por política para tráfego de saída (Outbound);

4.78 Deve descriptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3;

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

4.80 Suporte a objetos e regras IPv6;

4.81 Suporte a objetos e regras multicast;

4.82 Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e

desabilitar políticas em horários pré-definidos automaticamente.

4.83 Controle de Aplicações - Capacidade de identificar e controlar o acesso a aplicações, permitindo a definição de políticas específicas para permitir ou bloquear aplicações com base em categorias ou comportamentos identificados.

4.84 Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos.

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

4.86 Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linkedin, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-doc, sisqual.

4.87 Inspecionar o payload de pacotes para detectar assinaturas de aplicações conhecidas, independentemente de porta e protocolo.

4.88 Identificar o uso de táticas evasivas, visualizando e controlando aplicações e ataques que utilizam táticas evasivas como comunicações criptografadas (e.g., Skype e rede Tor).

4.89 Para tráfego criptografado SSL, descriptografar pacotes para verificar assinaturas de aplicações.

4.90 Decodificar protocolos para detectar aplicações encapsuladas e validar se o tráfego corresponde ao protocolo especificado.

4.91 Identificar funcionalidades específicas de aplicações, bem como táticas evasivas em comunicações criptografadas.

4.92 Atualizar a base de assinaturas de aplicações automaticamente.

4.93 Dispositivos de proteção de rede devem identificar o usuário de rede via integração com o Microsoft Active Directory sem a necessidade de agentes ou Domain Controller.

4.94 Permitir controle de aplicações em múltiplas regras de segurança, possibilitando habilitar controle de aplicações em regras específicas.

4.95 Suportar métodos de identificação de aplicações por assinaturas e decodificação de protocolos.

4.96 Permitir criação de assinaturas personalizadas para aplicações proprietárias, com interface gráfica de configuração.

4.97 Alertar o usuário quando uma aplicação for bloqueada.

4.98 Possibilitar diferenciação de tráfegos Peer2Peer com granularidade de controle.

4.99 Diferenciar e controlar tráfego de aplicações como Peer2Peer (ex.: BitTorrent) por políticas.

4.100 Deve possibilitar a diferenciação e controle de partes das aplicações, como por exemplo, permitir o Hangouts e bloquear a chamada de vídeo.

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

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

4.103 Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características como: nível de risco da aplicação e categoria da aplicação.

4.104 Deve ser possível a criação de grupos estáticos de aplicações baseados em características como: categoria da aplicação.

4.105 Prevenção de Ameaças - Detectar e prevenir ameaças em tempo real, incorporando mecanismos de prevenção de intrusões (IPS) e sistemas antivírus, bloqueando ataques antes de atingirem os recursos internos da rede.

4.106 Incluir proteção contra vírus em conteúdo HTML e JavaScript, software espião (spyware) e Worms.

4.107 Proteção contra downloads indesejados via HTTP de arquivos executáveis e maliciosos.

4.108 Permitir configuração de políticas baseadas em usuários, grupos de usuários, origem, destino e zonas de segurança, podendo ser aplicadas diferentes políticas para um mesmo perfil.

4.109 Capacidade de mitigar APTs, através de análises dinâmicas e identificação de

malwares desconhecidos.

4.110 Capacidade de analisar malware desconhecido (Zero-Day) em ambiente isolado (sandbox) e bloquear o acesso a arquivos suspeitos.

4.111 Analisar o comportamento de arquivos suspeitos em ambiente controlado.

4.112 Filtro de URL - O firewall deve possuir um sistema de filtragem de URLs que permita bloquear ou acessar sites com base em listas de categorias pré-definidas, contribuindo para a segurança e conformidade com políticas de uso da internet.

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

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

4.115 Deve permitir a criação de políticas com base na visibilidade e controle de quem está utilizando quais URLs, através de integração com serviços de diretório, Active Directory e base de dados local.

4.116 A identificação pela base do Active Directory deve permitir SSO, para que os usuários não precisem logar novamente na rede para navegar pelo firewall.

4.117 Suportar a criação de políticas baseadas no controle por URL ou categoria de URL.

4.118 Deve possuir pelo menos 70 categorias de URLs, definidas pelo fabricante e atualizáveis a qualquer tempo.

4.119 Deve permitir a exclusão de URLs específicas do bloqueio.

4.120 Permitir a customização da página de bloqueio.

4.121 Permitir a restrição de acesso a canais específicos do YouTube, configurando uma lista de canais permitidos ou bloqueados.

4.122 Deve bloquear o acesso a conteúdo inadequado em sites de busca, como Google, Bing e Yahoo, implementando o Safe Search para restringir resultados.

4.123 Identificação de Usuários - Deve ser capaz de identificar usuários de forma precisa para aplicar políticas de segurança personalizadas, utilizando-se de integração com sistemas de autenticação existentes, como LDAP ou Active Directory, para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on (SSO). Essa funcionalidade não deve possuir limites

licenciados de usuários.

4.124 Deve possuir integração com Radius para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários.

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

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

4.127 Deve permitir a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD.

4.128 A solução deve suportar autenticação de usuários com credenciais de mídias sociais de terceiros como Facebook, Twitter, LinkedIn e Google+.

4.129 A solução deve permitir que usuários sem conta local ou em mídias sociais se autentiquem através de um rápido cadastro, garantindo o mínimo de rastreabilidade, com validação de endereços de e-mail ou número de telefone.

4.130 Permitir o login automático de usuários visitantes depois de se registrarem com sucesso.

4.131 Agir como um Provedor de Identidade (Identity Provider - IDP), estabelecendo um relacionamento com o Provedor de Serviços (Service Provider - SP) para autenticação segura de usuários tentando acessar o Provedor de Serviços.

4.132 Deve suportar nativamente a integração e autenticação de switches e outros dispositivos compatíveis com o padrão 802.1X.

4.133 Oferecer integração de clientes finais para autenticação 802.1X, permitindo que qualquer cliente com Windows possa configurar seu equipamento para o suporte 802.1X.

4.134 Suportar os seguintes métodos 802.1X EAP: PEAP (MSCHAPv2), EAP-TTLS, EAP-TLS e EAP-GTC.

4.135 Suporte à interoperabilidade com equipamentos de acesso de outros fabricantes para autenticação de portas junto à solução, através dos padrões 802.1X.

4.136 Permitir bypass de autenticação 802.1X para dispositivos conhecidos que não

suportem 802.1X.

4.137 A liberação deverá ser feita baseada no endereço MAC dos dispositivos previamente cadastrados, permitindo o acesso à rede sem necessidade de autenticação adicional por parte do usuário do dispositivo.

4.138 QoS (Quality of Service) - O dispositivo deve suportar funcionalidades de Qualidade de Serviço (QoS), permitindo a priorização de tráfego de dados na rede, assegurando que aplicações críticas tenham a largura de banda necessária para operar eficientemente.

4.139 VPN (Virtual Private Network) - Deve suportar a criação de redes privadas virtuais utilizando protocolos IPSec e SSL, garantindo comunicações seguras e criptografadas entre diferentes locais ou para usuários remotos.

4.140 VPN IPSec Site-to-Site - Suporte à criptografia 3DES, AES128, AES192 e AES256 (Advanced Encryption Standard).

4.141 Suporte para autenticação MD5, SHA1, SHA256, SHA384 e SHA512.

4.142 Suporte para Diffie-Hellman Groups 1, 2, 5, 14, 15, 21, 27 e 32.

4.143 Suporte para Algoritmo Internet Key Exchange (IKEv1 e v2).

4.144 Suporte para autenticação via certificado IKE PKI.

4.145 Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet e SonicWall.

4.146 Controlador de Switch

4.147 Gerenciamento e operação centralizada e integrada no mesmo appliance, com inventário de hardware, software e configuração dos switches.

4.148 Interface gráfica para configuração, administração e monitoramento dos switches.

4.149 Exibição da topologia da rede com todos os switches administrados para monitoramento, incluindo status dos uplinks e equipamentos para identificação de problemas na rede.

4.150 Console de Gerência e Monitoração - Uma plataforma centralizada para gerenciamento e monitoramento do firewall, incluindo funcionalidades para a configuração de políticas, SD-WAN, atualizações de segurança, revisão de logs de segurança e geração de relatórios detalhados.

4.151 CASB (Cloud Access Security Broker) - Fornece visibilidade, controle e segurança para interações entre usuários e serviços em nuvem.

4.152 A plataforma deve suportar implementação futura de licenciamento para ativação da funcionalidade de CASB.

4.153 ZTNA (Zero Trust Network Access) - Ter suporte ao de "Nunca Confiar, Sempre Verificar": Baseado no princípio de "nunca confiar, sempre verificar", o ZTNA assegura que apenas usuários autenticados e dispositivos validados tenham acesso a aplicações e recursos específicos.

4.154 Acesso é verificado antes de qualquer conexão, minimizando a superfície de ataque.

4.155 A plataforma deve suportar implementação futura de licenciamento para ativação da funcionalidade de ZTNA.

4.156 Inspeção Profunda de Pacotes (Deep Packet Inspection, DPI) - Analisa profundamente o conteúdo dos pacotes de dados que atravessam a rede para detectar e bloquear tráfego malicioso ou não autorizado, fornecendo uma compreensão detalhada do tipo de tráfego processado.

4.157 Controle de Acesso Baseado em Identidade (Identity-Based Access Control) - Dar suporte para integrar sistemas de autenticação para controlar o acesso a recursos da rede com base na identidade dos usuários ou dispositivos, tolerando as políticas de segurança internas.

4.158 Proteção Contra-ataques Distribuídos de Negação de Serviço (DDoS) - Implementa estratégias para detectar e mitigar ataques DDoS, preservando a disponibilidade e operacionalidade dos serviços de rede.

4.159 Geolocalização - Políticas por Geolocalização: Suportar a criação de políticas por geolocalização, permitindo que o tráfego de determinados países seja bloqueado.

4.160 Visualização nos Logs: Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.

4.161 Gerenciamento de Acesso Wireless - Gerenciamento Centralizado de Pontos de Acesso: Gerenciamento e operação centralizada dos pontos de acesso wireless, integrada no mesmo appliance da solução ofertada.

4.162 **Garantia, Suporte e Acordos de Níveis de Serviços (SLA) -** Os serviços poderão ser prestados pela CONTRATADA ou por representante indicada pela CONTRATADA ou pelo fabricante da solução;

4.163 Entende-se por "Garantia" ou" Suporte" ou "Manutenção", doravante denominada unicamente como "Garantia", 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. Esta "Garantia" inclui os procedimentos destinados a recolocar em perfeito estado de operação os serviços e produtos ofertados, tais como;

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

4.165 Do software: desinstalação, reconfiguração ou reinstalação decorrente de falhas de desenvolvimento do software, atualização da versão de software, correção de defeitos de desenvolvimento do software, de acordo com os manuais e as normas técnicas específicas do fabricante para os recursos utilizados; 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, reinstalação e reconfiguração quando necessário.

4.166 A CONTRATADA fornecerá e aplicará pacotes de correção, em data e horário a serem definidos pela CONTRATANTE, sempre que forem encontradas falhas de laboratório (bugs) ou falhas comprovadas de segurança em software ou firmware dos aparelhos que integrem o objeto do contrato

4.167 O atendimento deste requisito está condicionado a liberação pelo fabricante dos pacotes de correção e/ou novas versões de software.

4.168 É facultado a CONTRATADA a execução, ao seu planejamento e disponibilidade, de "Garantia" do tipo "preventiva" que pela sua natureza reduza a incidência de problemas que possam gerar "Garantia" do tipo "corretiva". As manutenções do tipo "preventiva" não podem gerar custos a CONTRATANTE.

4.169 A manutenção técnica do tipo "corretiva" será realizada sempre que solicitada pelo CONTRATANTE por meio da abertura de chamado técnico diretamente à empresa CONTRATADA (ou a outra informada pela CONTRATADA) via telefone ou Internet ou e-mail

ou outra forma de contato;

4.170 ACORDOS DE NÍVEIS DE SERVIÇOS (SLA) E PRAZOS DE ATENDIMENTO - Os serviços contratados devem estar disponíveis 24 horas por dia, 7 dias por semana, 365 dias por ano e possuir Suporte Técnico, em igual disponibilidade, durante toda a vigência contratual;

4.171 SEVERIDADE URGENTE - Prazo máximo de início de atendimento de até 02 hora útil contadas a partir do horário de abertura do chamado; Prazo máximo de resolução do problema de até 08 horas úteis contadas a partir do início do atendimento.

4.172 SEVERIDADE IMPORTANTE -Necessidade de suporte na solução com a necessidade de interrupção de funcionamento da solução.

4.173 Prazo máximo de início de atendimento de até 04 horas úteis contadas a partir do horário de abertura do chamado;

4.174 Prazo máximo de resolução do problema de até 12 horas úteis contadas a partir do início do atendimento.

4.175 SEVERIDADE NORMAL - Necessidade de suporte na solução sem a necessidade de interrupção de funcionamento da solução.

4.176 Prazo máximo de início de atendimento de até 8 horas úteis contadas a partir do horário de abertura do chamado;

4.177 Prazo máximo de resolução do problema de até 24 horas úteis contadas a partir do início do atendimento.

4.178 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. Caso seja necessária a reinstalação da solução, a reinstalação será realizada através dos serviços compatíveis do "Catálogo de Serviços".

4.179 SEVERIDADE INFORMAÇÃO Solicitações de informações diversas ou dúvidas sobre a solução.

4.180 Prazo máximo de resposta de até 3 dias úteis, contados a partir da data de abertura da ocorrência.

4.181 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;

4.182 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.

4.183 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;

4.184 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. Os tempos de "início de atendimento" e "solução do problema" se aplicam para chamados com atendimento na cidade de São Paulo – SP.

4.185 TREINAMENTO TÉCNICO FORNECIDO PELA CONTRATADA- A CONTRATADA deverá fornecer treinamento base para os usuários, conforme necessidade e solicitação do CONTRATANTE, garantindo suporte adequado para o uso e operação dos serviços fornecidos. Esse treinamento deverá ser disponibilizado em até 7 dias úteis após a solicitação formal.

4.186 O treinamento será prestado para um grupo de no máximo 03 (três) participantes a ser realizado nas instalações da CONTRATANTE OU DE FORMA REMOTA devendo ser ministrados em língua portuguesa e por profissionais qualificados para este fim.

4.187 O treinamento deverá ser realizado de acordo com a disponibilidade de agenda das equipes da CONTRATADA e CONTRATANTE;

4.188 Os treinamentos deverão ser ministrados em dias úteis (de segunda a sexta-feira) das 08:00h às 17:00h;

4.189 A CONTRATADA será responsável por fornecer equipamento como serviço, licenciamento e todo o serviço de suporte e monitoramento especializado dos equipamentos, bem como sua saúde, disponibilidade dos links de internet, detecção de ameaças e gestão de consumo de banda, além de suporte contínuo reativo e proativo.

4.190 A CONTRATADA será responsável por prover TODO o licenciamento necessário para a aplicação das funcionalidades de segurança da solução de firewall de nova geração, bem como providenciar sempre sua renovação, de forma antecipada, quando necessários,

durante toda a vigência do contrato.

4.191 A CONTRATADA efetuará toda a implantação física e lógica dos recursos da solução, bem como a instalação física no ambiente da CONTRATANTE, configurações iniciais da solução, integrações com sistemas de autenticação LDAP, implementação das regras solicitadas, criação de VPN's Site-to-Site e Client-to-Site, implementação completa da solução de Webfilter de acordo com as políticas definidas, configuração do serviço de SD-WAN para melhor aproveitamento dos links de dados, configurações de failover para links de internet, configurações de roteamento necessários, configurações de inspeção SSL, DPI, configuração do serviço de Sandbox, criação e parametrização de serviços de relatórios.

4.192 A CONTRATADA deve garantir o monitoramento constante da parametrização dos serviços de firewall e da disponibilidade dos links de internet.

4.193 A CONTRATADA deverá apresentar relatórios mensais sobre indicadores de ameaças, eventos críticos de segurança, alertas de alto consumo de banda, variações na latência e status de desempenho dos links de internet.

4.194 A CONTRATADA deverá realizar análises preditivas que antecipam problemas e comportamentos anormais, combinadas com atuações proativas para resolver questões antes que se transformem em problemas significativos.

4.195 A CONTRATADA será responsável por manter o sistema atualizado com as últimas atualizações de segurança, garantindo proteção contra as mais recentes vulnerabilidades e exploits.

4.196 A CONTRATADA deverá fornecer de forma regular e/ou sob demanda relatórios detalhados que documentam as ameaças identificadas e a atividade de navegação por usuário, site e aplicação, apoiando a tomada de decisão e a gestão estratégica de TI.

4.197 Cumprir fielmente toda a execução do objeto, de acordo com as condições e exigências previamente estabelecidas;

4.198 A CONTRATADA Deve fornecer os Firewalls, cada qual respeitando as especificações abaixo descritas.

4.199 Ressaltamos as especificações de acordo deste Termo de Referência apresentam, não somente os itens a serem entregues, como também as capacidades esperadas.

4.200 A CONTRATADA deve realizar a montagem física dos Firewalls nos locais estratégicos, assegurando a correta fixação e organização dos cabos.

4.201 A CONTRATADA deve fornecer a configuração inicial e customização do hardware e

software dos Firewalls para atender às necessidades específicas do ambiente e instituição.

4.202 A CONTRATADA deve efetuar a configuração total do equipamento ou solução em nuvem de controladora centralizada, garantindo que todas as funcionalidades de gerenciamento estejam completamente disponíveis para pronto uso e conforme orientação da CONTRATANTE.

4.203 A CONTRATADA será responsável pela gestão e execução dos serviços contratados, gestão dos recursos humanos e físicos necessários à execução do objeto contratual e fornecimento dos bens e materiais solicitados de acordo com o cronograma de execução;

4.204 Fornecer garantia e substituição do equipamento durante toda vigência Contratual;

4.205 Prestar serviços de suporte e assistência técnica aos bens pelo período de vigência do contrato, de acordo com a forma e regime estabelecidos;

4.206 A CONTRATADA deverá disponibilizar o planejamento e entregas dos serviços solicitados nos dias e horários definidos pelo CONTRATANTE, podendo ser realizados fora de horário comercial, incluindo sábados, domingos e feriados, caso o CONTRATANTE julgue necessário, sem nenhum ônus adicional a CONTRATATE

4.207 Observar rigorosamente todos os prazos de atendimento e resolução de chamados estabelecidos, bem como as datas de manutenções preventivas, sob pena de aplicação de multa e demais cominações pelo CONTRATANTE;

4.208 Agir de forma proativa, objetivando prevenir a ocorrência de erros e defeitos, por meio das inspeções nos equipamentos, componentes, dispositivos e softwares de configuração, bem como a coleta e avaliação de logs, atualização, verificação e inspeção visual das condições de funcionamento dos equipamentos, seus componentes e dispositivos;

4.209 Reparar eventuais falhas apresentadas nos equipamentos, compreendendo serviços de conserto, reparos e/ou substituição de bens, componentes e dispositivos, bem como sua configuração e gerenciamento, com vistas a normalidade da operação dos serviços prestados;

4.210 Prover toda e qualquer evolução de software, incluindo correções, patches, fixes, updates, service packs, novas releases, versões, builds e upgrades às suas expensas;

4.211 Comunicar à CONTRATANTE qualquer anormalidade que esteja impedindo a execução contratual dos serviços de suporte, prestando os esclarecimentos julgados necessários;

4.212 Responsabilizar-se por todos os tributos, contribuições fiscais e parafiscais que incidam ou venham a incidir, direta ou indiretamente, sobre os serviços fornecidos, bem como pelo custo do frete e outros inerentes à execução do objeto, apresentando os documentos fiscais em conformidade com a legislação vigente;

4.213 Assumir todas as despesas com transporte, hospedagem e outros custos operacionais decorrentes da execução do objeto, inexistindo qualquer possibilidade de pedido de desembolso à CONTRATANTE;

4.214 Responsabilizar-se pela fiel execução contratual, respondendo civil e criminalmente pelos danos diretos, que, por dolo ou culpa sua ou de seus empregados, causarem a CONTRATANTE ou a terceiros, sendo admitido o direito à ampla defesa;

4.215 Manter seus profissionais identificados com crachá em decorrência de acesso as dependências do CONTRATANTE, para prestação das atividades previstas para a execução do Contrato;

4.216 Fornecer equipamento de redundância, com características iguais ou superiores, sempre que precisar desativar hardware, software ou quaisquer recursos computacionais da CONTRATANTE, até que o problema seja sanado;

4.217 Responsabilizar-se pelo sigilo e confidencialidade, por si e seus empregados, dos documentos e/ou informações que lhe chegarem ao conhecimento por força da execução do contrato, e tenham sido definidas como confidenciais, não podendo divulgá-lo, sob qualquer pretexto, conforme as diretrizes estabelecidas pela Política de Segurança da Informação e Comunicações da CONTRATANTE e Lei Geral de Proteção de Dados;

4.218 Manter durante o período de vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação quanto à situação de regularidade da empresa (artigo 27, § 2º, do Decreto nº 5.540/2005), exigidas no ato da contratação;

4.219 Disponibilizar uma infraestrutura de atendimento via telefone ou web, para recebimento registro dos chamados técnicos realizados pela CONTRATANTE, disponibilizando sempre um número de protocolo para controle de atendimento;

4.220 Entregar à CONTRATANTE, às suas expensas, toda documentação técnica (relatórios técnicos) gerada em função da execução do Contrato;

4.221 Responder por quaisquer acidentes de que possam sofrer os seus profissionais, quando em serviço nas dependências da CONTRATANTE;

4.222 Obedecer às normas internas da CONTRATANTE relativas à segurança, identificação, ao trânsito e permanência de pessoas em suas dependências;

4.223 Acatar as orientações do Gestor e Fiscais do Contrato, sujeitando-se a fiscalização destes e prestando-lhes os esclarecimentos solicitados;

4.224 Observar a vedação de subcontratação parcial ou total da execução do objeto, de veiculação de publicidade acerca do Contrato, como também, de contratar servidor do quadro de pessoal da CONTRATANTE durante a vigência contratual;

4.225 Velar para que todos os privilégios de acesso a sistemas, dados ou informações do FUABC sejam utilizados exclusivamente na execução contratual e, pelo período estritamente essencial à realização de serviços;

4.226 Refazer ou corrigir serviços às suas expensas, no todo ou em parte, sempre que identificado pela FUABC ter sido realizado em desacordo com o estabelecido no Termo de Referência;

4.227 Realizar a execução do objeto atendendo aos critérios de sustentabilidade ambiental, nos termos da Instrução Normativa SLTI/MPOG nº 01/2010, onde couber;

4.228 Informar e manter atualizados os números de telefone e endereço eletrônico (e-mail), bem como nome da pessoa autorizada para contatos que se fizerem necessários por parte da CONTRATANTE, bem como os dados do responsável pela assinatura do contrato e seus respectivos aditivos;

4.229 O início do serviço deverá ser executado a partir da data da assinatura do contrato entre as partes, tendo prazo máximo de 60 dias para implantação e configuração dos novos serviços podendo ser negociado em prazos excepcionais.

5. DAS OBRIGAÇÕES DA CONTRATANTE

A Contratante compromete-se a:

5.1. Disponibilizar estrutura fisica adequada para prestação de serviços ora contratada, respeitando as especificações técnicas apresentadas pela Contratada.

5.2. Indicar responsavel para fiscalização dos serviços a serem prestados pela contratada.

5.3. Cancelar ou alterar, ao seu exclusivo critério e a qualquer tempo, a prestação de serviços nos locais que julgar conveniente, com antecedencia minima de 30 (trinta) dias.

5.4. Realizar os pagamentos na forma e condições previstas.

5.5. Fornecer e colocar a disposição da Contratada, todos os elementos e informações que se fizerem necessarios a execução do Contrato.

5.6. Prestar as informações e esclarecimentos atinentes ao objeto do contrato, que venham a ser solicitados pela Contratada.

5.7. Conferir toda documentação técnica gerada e apresentada durante a execução do contrato, efetuando sua atestação quando estiverem em conformidade com os padrões de informação e qualidade exigidos no contrato.

6. **DA FISCALIZAÇÃO**

6.1. A CONTRATANTE fiscalizará o serviço através de funcionário (s) designado (s) para esse fim, com a incumbência de relatar ao supervisor as falhas ou irregularidades que porventura verificar, as quais, se não forem sanadas, serão objetos de comunicado oficial, expedido pela Unidade, à CONTRATADA.

6.2. A execução do contrato será fiscalizada em todos os aspectos pertinentes ao objeto ajustado, inclusive, reservando o direito de resolução de quaisquer casos omissos, em especial às especificações, requisitos, sinalizações e segurança, implicando o direito de rejeitar os serviços insatisfatórios, intimando a execução das devidas modificações, quando for o caso.

6.3. O exercício de fiscalização por parte da CONTRATANTE não eximirá a CONTRATADA das responsabilidades pelos danos materiais e pessoais que vier a causar a terceiros ou à CONTRATANTE, por culpa ou dolo de seus prepostos, na execução do contrato, nos termos do Código Civil.

6.4. Para todos os efeitos, o contrato a ser firmado, bem como o processo que a ele seja correlato, têm o Sr. Tiago Henrique Pezzo, Gerente de Informação, Saúde e Tecnologia [redacted] e Marcelo Teixeira da Dalt Netto, Coordenador de Rede Infra [redacted] como gestores/fiscais do contrato.

7. **DO PREÇO E DAS CONDIÇÕES DE PAGAMENTOS**

A CONTRATANTE compromete-se a pagar o preço constante da proposta da CONTRATADA, observando-se as seguintes condições:

7.1. A CONTRATADA deverá apresentar, mensalmente, a CONTRATANTE, documento contendo a relação dos serviços efetivamente realizados;

7.2. A CONTRATANTE, efetuará análise nos documentos apresentados pela CONTRATADA, e aprovará os procedimentos executados e valores correspondentes, solicitando que a CONTRATADA emita a nota fiscal para o devido pagamento;

7.3. A CONTRATADA deverá emitir uma nota fiscal para cada unidade discriminando detalhadamente os serviços prestados e deverá enviar para o endereço de e-mail notafiscalsmsp@smfuabc.org.br.

7.4. Em hipótese alguma será aceito boleto bancário como meio de cobrança;

7.5. O pagamento será efetuado mediante a apresentação, pela CONTRATADA, dos seguintes documentos, que serão arquivados pela CONTRATANTE:

a. Cartão CNPJ e Nota Fiscal constando discriminação detalhada do serviço prestado;
b. CND válida, provando regularidade do prestador de serviço contínuo de contrato formal, junto à Previdência Social;
c. Prova de regularidade perante o FGTS.
d. CNDT – Certidão Negativa de Débitos Trabalhistas, emitida pela Justiça do Trabalho;
e. Cópia de guia de recolhimentos do INSS, acompanhada da folha resumo da GEFIP correspondente. Quando isento, o prestador deverá apresentar justificativa e comprovante, nos termos da instrução normativa RFB N 971/2009;
f. Relação nominal atualizada de todos os profissionais que trabalham na empresa, prestando serviços diretamente nas dependências da CONTRATANTE;
g. Demonstrativos dos pagamentos realizados a todos os empregados (salário, vale transporte e benefícios), acompanhado do respectivo recibo firmado pelo empregado.

7.6. A CONTRATANTE poderá, a seu critério, solicitar outras documentações de regularidade não citadas acima;

7.7. Qualquer atraso ocorrido na apresentação da Nota Fiscal/Fatura por parte da Contratada importará em prorrogação automática do prazo de vencimento da obrigação da Contratante.

7.8. A CONTRATADA deverá indicar no corpo da nota fiscal as exigências contidas na resolução 23/2022, que aprova as alterações as instruções n 1/2020, do Tribunal de contas do Estado de São Paulo, as notas fiscais deverão obrigatoriamente conter:

a) Indicação da Contratante: Fundação do ABC – Contrato de Gestão de São Mateus, CNPJ/MF sob o nº 57.571.275/0023-08;

b) Número do Contrato de Gestão: Contrato de Gestão 009/2015 - SMS/NTCSS.;

c) Número do processo.

7.9. Caso não haja tal informação o pagamento não será efetuado até sua regularização.

7.10. Caso seja detectado algum problema na documentação entregue anexada à nota fiscal, será concedido, pela Contratante, prazo para regularização.

7.11. A CONTRATADA deverá fazer constar na Nota Fiscal, o número do Banco, Agência e da conta corrente bancária, a fim de agilizar o pagamento.

7.12. A CONTRATADA ficara responsável pelo pagamento dos encargos trabalhistas, previdenciários, fiscais, comerciais e outros que resultarem dos compromissos no contrato.

7.13. A CONTRATANTE não assumira responsabilidade alguma por pagamento de impostos e encargos que competirem a CONTRATADA, nem estará obrigado a restituir-lhe valores, principais e acessórios, que por ventura despender com pagamento dessa natureza.

7.14. O pagamento pelos serviços prestados, serão realizados, mensalmente, entre o décimo quinto ao vigésimo dia do mês subsequente ao da prestação dos serviços, mediante a emissão de nota fiscal/fatura e a sua devida atestação pela CONTRATANTE, com resalvas as cláusulas 7.5 desse Contrato.

7.15. As notas fiscais, referentes aos serviços prestados, deverão ser entregues em tempo considerável (primeiro dia útil do mês) juntamente com relatório pré aprovado (Fiscal do Contrato), para que a CONTRATANTE possa proceder com as análises devidas e o subsequente pagamento dos valores;

7.16. A CONTRATANTE procederá a retenção tributária, referente aos serviços prestados, nas alíquotas legalmente devidas, incidentes sobre o valor destacado em nota fiscal.

7.17. A CONTRATADA, neste ato declara estar ciente de que os recursos utilizados para o pagamento dos serviços ora contratados serão aqueles repassados pelo ente público, em razão do Contrato de Gestão 009/2015 - SMS/NTCSS, firmado entre a CONTRATANTE e a Prefeitura de São Paulo – Secretaria Municipal da Saúde para Gestão do Contrato de São Mateus/SP.

7.18. A CONTRATANTE compromete-se em pagar o preço irreajustável constante na proposta da CONTRATADA, desde que não ocorram atrasos e ou paralisação dos repasses pela Prefeitura Municipal de São Paulo - Secretaria Municipal de Saúde para a CONTRATANTE, relativo ao custeio do objeto do Contrato de Gestão 009-2015- SMS/NTCSS.

7.19. No caso de eventuais atrasos, os valores serão atualizados de acordo com a legislação vigente, salvo quando não decorram de atrasos e ou paralisação dos repasses pela Prefeitura de São Paulo – Secretaria Municipal da Saúde para a CONTRATANTE, em consonância com o disposto nas cláusulas deste CONTRATO.

8. DO REAJUSTE DOS PREÇOS

8.1. Havendo prorrogação do presente contrato de prestação de serviços, após ocorrido 12 (doze) meses, poderá haver reajuste de preços, da seguinte forma:

8.2. Será utilizado o IGP-M (Índice Geral de Preços do Mercado) ou o IPCA (Índice Nacional de Preço ao Consumidor Amplo – IBGE), observando os seguintes critérios:

Obs: Em casos especificos poderá ser utilizado o reajuste da categoria disposto em Convenção Coletiva de Trabalho.

8.2.1.1. Na eleição do Índice:
8.2.1.2. Dois Meses de retroação da data base (mês da proposta);

8.2.2. Na periodicidade:

8.2.2.1. Será considerada a variação ocorrida no período de 12 (doze) meses, a contar do mês da proposta, observada a retroação de dois meses na eleição dos índices.

8.2.3. Na incidência:

8.2.3.1. A variação verificada no período de 12 (doze) meses apurada na forma citada nos itens 8.2.1.1. e 8.2.2.1, será aplicada sobre o preço inicial (da proposta).

8.3. A CONTRATADA ficará responsável pelo pagamento dos encargos trabalhistas, previdenciários, fiscais, comerciais e outros que resultarem dos compromissos no contrato.

8.4. A CONTRATANTE não assumirá responsabilidade alguma pelo pagamento de impostos e encargos que competirem à CONTRATADA, nem estará obrigada a restituir-lhe valores, principais e acessórios, que porventura despender com pagamento dessa natureza.

9. DO VALOR

9.1. Dá ao presente contrato o valor mensal de **R$ XXXXXXX** (_____) e valor total de **R$ XXXXXXX** (_____).

10. DO RECEBIMENTO

10.1. No recebimento dos produtos e/ou serviços e/ou locação, serãos observados os preceitos pertinentes ao Regulamento Interno de Compras da Fundação do ABC;

11. DAS PENALIDADES

11.1. As penalidades serão propostas pela fiscalização da CONTRATANTE e aplicadas, se for o caso, pela autoridade competente, garantindo o contraditório administrativo com defesa prévia.

11.2. Multa de 3% (três por cento) sobre o valor do contrato, na recusa da empresa vencedora em assiná-lo dentro do prazo estabelecido.

11.3. Multa de 10% (dez por cento), sobre o valor do contrato, por inexecução parcial do contrato, podendo a CONTRATANTE autorizar a continuação do mesmo.

11.4. Multa de 20% (vinte por cento) sobre o valor do contrato, por inexecução total do mesmo.

11.5. Multa de 10% (dez por cento) sobre o valor do contrato, do valor do faturamento do mês em que ocorrer a infração, se o serviço prestado estiver em desacordo com as especificações propostas e aceitas pela CONTRATANTE.

11.6. Multa de 1% (um por cento), sobre o valor do contrato, por dia de atraso no cumprimento dos prazos estipulados em contrato.

11.7. As multas são independentes entre si, podendo ser aplicadas cumulativamente. A aplicação de uma não exclui a das outras, bem como a das demais penalidades previstas em lei.

11.8. O valor relativo, às multas eventualmente aplicadas, será deduzido de pagamentos que a CONTRATANTE efetuar, mediante a emissão de recibo.

11.9. As penalidades serão propostas pela fiscalização da CONTRATANTE e aplicadas, se for o caso, pela autoridade competente, garantindo o contraditório administrativo com defesa prévia.

12. DA RESCISÃO

12.1. O presente Contrato poderá ser rescindido unilateralmente, desde que haja conveniência para a CONTRATANTE mediante autorização escrita e fundamentada da autoridade superior, com antecedência mínima de (30) trinta dias, sem que caiba à CONTRATADA o direito de indenização de qualquer espécie;

12.2. Este instrumento poderá ser rescindido por ato unilateral da CONTRATANTE, verificando-se a ocorrência de descumprimento de cláusulas contratuais, assegurados, no entanto, o contraditório e a ampla defesa.

12.3. O não cumprimento das obrigações contratuais pela CONTRATANTE poderá ensejar rescisão contratual pela CONTRATADA, assegurados, no entanto, o contraditório e a ampla defesa. Configurado o justo motivo para rescisão, a CONTRATADA deverá permanecer por até (90) noventa dias na execu-ção dos serviços.

12.4. A presente avença extinguir-se-á automaticamente em caso de rescisão do contrato de gestão/convênio celebrado entre a CONTRATANTE e a Administração Pública, não cabendo indenização de qualquer natureza às partes. – para contratos de serviços contínuos.

12.5. A presente avença poderá ser rescindida em caso de extinção do estado de necessidade que ensejou a contratação ou em caso de conclusão de tomada de preços, realizada nos termos do Regulamento de Compras e Contratação de Serviços de Terceiros e Obras da Fundação do ABC, que objetive a substituição da contratação emergencial por serviços contínuos. – para contratos emergenciais.

12.6. No caso de não interesse de renovação do contrato por parte da CONTRATADA, ela deverá comunicar à CONTRATANTE, em um prazo mínimo de 90 dias, ou manter o serviço contratado em funcionamento por igual período, após o vencimento do mesmo;

13. **DISPOSIÇÕES FINAIS**

13.1. Este ajuste regular-se-á pelas suas disposições e partes integrantes tais como seus anexos, processo administrativo, proposta da CONTRATADA, legislação vigente e demais normas de direito aplicáveis.

13.2. Fica eleito o foro da Comarca de Santo André para dirimir quaisquer questões oriundas do presente contrato.

E, por estarem as partes de comum acordo sobre as estipulações, termos e condições deste instrumento, firmam-no em 03 (três) vias, na presença de 02 (duas) testemunhas.

Santo André, xx de xxxxxx de 2025.

_____

FUNDAÇÃO DO ABC

Nome:
CPF:

_____

Nome:
CPF:

Testemunhas:

1- _____ Nome:
CPF:

2- _____ Nome:
CPF:

ANEXO I – AO CONTRATO

CONTRATO DE PRESTAÇÃO DE SERVIÇO - PROCESSO Nº 133/25
PROTEÇÃO DE DADOS

1.1. Quando utilizados neste Contrato os seguintes termos, no singular ou no plural, terão o significado atribuído a eles abaixo, exceto se expressamente indicado ou acordado entre as Partes de outra forma:

Dado(s) Pessoal(ais)" significa qualquer informação que identifique ou possa identificar uma pessoa física, como, por exemplo, nome, CPF, endereço, e-mail, número de IP, número de conta corrente, dentre outras.

"Dado(s) Pessoal(ais) Sensível(eis)" significa qualquer informação que revele, ou qualquer tratamento que venha revelar, em relação a uma pessoa física, sua origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a Organização de caráter religioso, filosófico ou político, dados referentes a saúde ou a vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

"Titular(es)" significa qualquer pessoa física identificada ou que possa vir a ser identificada a partir dos Dados Pessoais.

"Tratamento" significa toda e qualquer atividade realizada com os Dados Pessoais, incluindo (mas não se limitando à/ao), coleta, armazenamento, compartilhamento, destruição, agregação, dentre outros.

"Violação de Dados" significa um incidente de segurança não autorizado que provoque (i) destruição, (ii) perda, (iii) alteração, (iv) divulgação ou (v) acesso acidental ou ilegal a Dados Pessoais.

LEGISLAÇÃO DE Proteção de Dados: significa qualquer lei sobre privacidade e proteção a dados, incluindo a Lei Geral de Proteção de Dados Pessoais (LGPD), à(s) qual(is) a CONTRATADA esteja sujeita em conexão com o Contrato (incluindo, sem limitação, e a título de exemplo, interpretações, decisões, acordos ou diretrizes de qualquer autoridade governamental);

LGPD: significa a Lei Geral de Proteção de Dados, Lei 13.709 de 14 de agosto de 2018, assim como suas eventuais alterações, regulamentações ou substituições.

Todos os demais termos não definidos neste Contrato que possuem definição na Lei Geral

de Proteção de Dados (Lei Federal nº 13.709/2018) serão compreendidos como ali descritos.

1.2. As Partes, neste ato, se comprometem a cumprir toda a legislação aplicável sobre a segurança da informação, privacidade e proteção de dados, inclusive (sempre e quando aplicáveis) a Constituição Federal, o Código de Defesa do Consumidor, o Código Civil, o Marco Civil da Internet (Lei Federal nº 12.965/2014), seu decreto regulamentar (Decreto 8.771/2016), a Lei Geral de Proteção de Dados (Lei Federal nº 13.709/2018) (LGPD), e as demais normas setoriais ou gerais sobre o tema, se comprometendo a tratar os dados pessoais e sensíveis ("Dados") de acordo com as melhores práticas de proteção de dados utilizadas no mercado, se comprometendo a:

(i) Atender eventuais solicitações de autoridades brasileiras, incluindo a Autoridade Nacional de Proteção de Dados ("ANPD");

(ii) Respeitar, no Tratamento de Dados, os princípios descritos no artigo 6º da LGPD, disponibilizando aos Titulares todas as informações obrigatórias previstas na LGPD e nas demais legislações aplicáveis;

(iii) Manter um programa de segurança da informação apropriado, razoável e por escrito, que inclua medidas físicas, técnicas e organizacionais proporcionais à natureza do dado pessoal tratado sob este Contrato, medidas que correspondam ou superem padrões e boas práticas industriais e que sejam adequadas a prevenir a Violação de Dados Pessoais;

(iv) As Partes cumprirão a Legislação de Proteção de Dados que tenha conexão com este Contrato;

(v) Não reter quaisquer Dados por período superior ao necessário para o cumprimento das suas obrigações ou para cumprimento de prazo fixado em lei específica, salvaguardas e hipóteses em sentido contrário;

(vi) Respeitar os direitos dos Titulares previstos na LGPD, e responder às solicitações dos Titulares;

(vii) Manter registro dos Tratamentos realizados e

(viii) Notificar, quando exigido pela legislação, as autoridades competentes e os Titulares sobre eventual a Violação de Dados, nos termos do artigo 48 da LGPD.

1.3. As Partes declaram que têm compromisso com a privacidade de seus clientes, parceiros e empregados, sendo sua atuação guiada pelos seguintes princípios: (a) limitação

de uso de dados pessoais ao extremamente necessário para atender aos propósitos empresariais; (b) acesso aos dados pessoais apenas por pessoas imprescindíveis e eliminação de dados quando não mais necessários; (c) cuidado adicional no tratamento de dados pessoais sensíveis; (d) transparência com clientes, parceiros e empregados; (e) segurança dos dados pessoais.

1.4. A parte prejudicada terá o direito de ser reembolsada pela parte infratora por quaisquer perdas, danos, multas, custos ou despesas (incluindo despesas e desembolsos legais) incorridos pela parte prejudicadas e que resultem de uma Violação de Dados Pessoais, falha na adoção de medidas de segurança exigidas pelo artigo 46 da LGPD ou da violação de algum item desta cláusula em relação a quaisquer dados pessoais tratados em conexão com o Contrato, e que tais valores serão considerados perdas diretas e serão devidos pela arte infratora à parte prejudicada, mediante comprovação.

Santo André, XX de XXXXX de 20XX.

_____

FUNDAÇÃO DO ABC

_____

Representante legal:
Empresa:
CNPJ:

ANEXO II – AO CONTRATO
Planilha de valores contratados

Item	LOCAL	LOCAL	ENDEREÇO	Quantidade de Firewall	Valor uni	Valor mensal
1	FORNECIMENTO DE EQUIPAMENTO DE SEGURANÇA TIPO FIRE WALL SERVIÇOS MONITORAMENTO	SEDE ADMINISTRATIVA	Rua Suíça, 95. Parque das Nações – Santo André (SP). CEP: 09210-000	2		
2	FORNECIMENTO DE EQUIPAMENTO DE SEGURANÇA TIPO FIRE WALL SERVIÇOS MONITORAMENTO	SEDE ASSISTENCIAL	Av. Cláudio Augusto Fernandes, 518, Cidade São Mateus, São Paulo – SP, CEP: 03962-120	1		
				Valor mensal		
				Valor global (12) meses		