GOVERNO DO DISTRITO FEDERAL

HOSPITAL DA CRIANÇA DE BRASÍLIA JOSÉ ALENCAR

Compras

CHAMAMENTO PÚBLICO 031/2026

Processo Nº 04024-00016909/2025-47

EDITAL DE CHAMAMENTO PÚBLICO

O Instituto do Câncer Infantil e Pediatria Especializada – Icipe, Pessoa Jurídica de Direito Privado, sem fins lucrativos, com sede no SHS Quadra 6, Brasil 21, Bloco A, Sala 501, CEP. 70.316-102, Brasília-DF, inscrito no CNPJ/MF sob o nº.10.942.995/0001-63, qualificado como Organização Social pelo Decreto Distrital nº. 46.525/2024, publicado no DODF nº. 84-A de 14 de novembro de 2024, responsável pela gestão do **HOSPITAL DA CRIANÇA DE BRASÍLIA JOSÉ ALENCAR – HCB**, torna público, para o conhecimento dos interessados, que realizará Chamamento Público, **na forma ELETRÔNICA, do tipo menor preço por lote,** nos termos do Decreto Distrital nº 33.390, de 06 de dezembro de 2011, e do Regulamento de Compras e Contratações (RCC) do ICIPE, aprovado pela Resolução ICIPE nº. 51, de 31/10/2025.

O Edital estará disponível no endereço eletrônico oficial do HCB: **www.hcb.org.br/compras.**

1. **DO OBJETO**

1.1. Contratação de empresa para o fornecimento de solução de segurança perimetral baseada em appliance de firewall de próxima geração (NGFW), com capacidade de inspeção profunda de pacotes, prevenção de intrusão (IPS), controle de aplicações, VPN, e funcionalidades avançadas de visibilidade e resposta, incluindo suporte técnico 24x7, atualizações de assinatura e hardware, e treinamento oficial para a equipe técnica do HCB, com a finalidade de atender as necessidades do Hospital da Criança de Brasília José Alencar - HCB, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

2. **DAS CONDIÇÕES PARA PARTICIPAÇÃO NO CHAMAMENTO**

2.1. Poderão participar deste Chamamento as empresas interessadas, legalmente constituídas, com ramo de atividade pertinente ao objeto e que comprovem sua qualificação, na forma indicada neste Edital.

2.2. Não poderão participar dos processos de aquisições e contratações nem contratar com o ICIPE:

I - Dirigente ou empregado do ICIPE/HCB, incluindo os membros da Diretoria e dos Conselhos de Administração, Fiscal, dentre outros;

II - Dirigente ou empregado da ABRACE, incluindo os membros da Diretoria e dos Conselhos de Administração e Fiscal, dentre outros;

III - Servidor público detentor de cargo em comissão ou função comissionada ou gratificada, no âmbito da Secretaria de Estado de Saúde do Distrito Federal, que possa ter conflito de interesse com o ICIPE/HCB na execução de contrato de gestão firmado com o poder público;

IV - Parentes consanguíneos ou afins até o terceiro grau das pessoas elencadas nos incisos I, II e III;

V - Empresa declarada suspensa/impedida pelo ICIPE, enquanto perdurarem os efeitos da sanção;

VI - Empresas declaradas inidôneas pelo ICIPE ou pela Administração Pública Direta e Indireta do Distrito Federal, enquanto perdurarem os efeitos da sanção; e

VII - Pessoas jurídicas nas quais as pessoas elencadas nos incisos I, II e III tenham participação societária na qualidade de sócio administrador ou gestor da empresa.

2.2.1. Entende-se por participação societária a participação individual como acionista ou sócio, nos 12 meses anteriores, respectivamente, superior a 0,3% (três décimos por cento) no capital social de sociedade por ações ou outras modalidades que admitam acionista, ou superior a 2% (dois por cento) no capital social de sociedade limitada ou outras modalidades empresariais.

2.3. Além das hipóteses acima, também não poderão participar:

I - À contratação de empregado, dirigente ou conselheiro do ICIPE, como pessoa física, bem como à participação dele em procedimentos de compras e contratações, na condição de participante do chamamento público;

II - À empresa cujo proprietário ou sócio tenha terminado seu prazo de gestão ou rompido seu vínculo empregatício com o ICIPE há menos de 12 (doze) meses.

2.4. Caso constatada qualquer situação prevista nos itens 2.2 e 2.3 supra, ainda que "*a posteriori*", no caso de credenciamento a empresa será descredenciada, e, se contratada, terá o Contrato rescindido, ficando sujeita às sanções previstas neste Edital e em seus anexos, no contrato e na legislação vigente.

3. **DO CREDENCIAMENTO E DA REPRESENTAÇÃO**

3.1. O credenciamento de que trata este item refere-se exclusivamente ao cadastro operacional na Plataforma Apoio Cotações, que constitui o nível básico de registro necessário para participação no Chamamento, não se confundindo com a habilitação jurídica ou com a comprovação de poderes de representação, as quais serão verificadas nos termos deste Edital. O cadastro deverá ser realizado no sítio eletrônico https://site.apoiocotacoes.com.br/.

3.2. O credenciamento para acesso ao sistema ocorrerá mediante a atribuição de usuário e senha pessoal e intransferível, de responsabilidade exclusiva do proponente, inclusive quanto às transações realizadas diretamente ou por seu representante, não cabendo ao provedor do sistema nem ao ICIPE, promotor do Chamamento, qualquer responsabilidade por danos decorrentes do uso indevido da senha, ainda que por terceiros.

3.3. A perda da senha ou a quebra de sigilo deverá ser comunicada imediatamente ao provedor do sistema, para fins de bloqueio imediato de acesso.

3.4. O credenciamento junto ao provedor do sistema implica a responsabilidade legal do proponente ou de seu representante legal e a presunção de sua capacidade para realizar as transações inerentes às fases de cotação e negociação previstas neste Chamamento.

3.5. É de responsabilidade do cadastrado conferir a exatidão dos dados informados na Plataforma Apoio Cotações e mantê-los atualizados, devendo promover, de imediato, a correção ou alteração sempre que identificar incorreção ou desatualização.

3.6. A inobservância do disposto no subitem anterior poderá ensejar a desclassificação do proponente no momento da habilitação.

3.7. A participação em qualquer processo de aquisição de bens e contratação de serviços realizado pelo ICIPE implica para o interessado: (*i*) a aceitação plena e irrevogável de todos os termos, cláusulas e condições estabelecidas nos respectivos documentos; (*ii*) a observância dos preceitos legais e regulamentares em vigor; e (*iii*) a responsabilidade pela fidelidade e legitimidade das informações e dos documentos apresentados em qualquer fase dos processos pertinentes.

4. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

4.1. Qualquer pessoa é parte legítima para impugnar edital de chamamento público por irregularidade na aplicação do Regulamento de Compras ou Contratações (RCC) ou para solicitar esclarecimento sobre os seus termos, devendo protocolar o pedido até 3 (três) dias úteis anteriores à data fixada para recebimento das propostas.

4.1.1. As impugnações e os pedidos de esclarecimento deverão ser enviados ao setor de compras, por meio eletrônico: compras2@hcb.org.br.

4.1.2. Os pedidos de esclarecimento apresentados em prazo inferior ao estabelecido no item 4.1 serão considerados intempestivos e não serão objeto de análise.

4.1.3. A resposta às impugnações e aos pedidos de esclarecimentos será divulgada no prazo de até 2 (dois) dois dias úteis, contado da data de recebimento do pedido de impugnação ou esclarecimento, limitado ao último dia útil anterior à data de abertura das propostas.

4.2. Até a publicação de resultado no DODF, todo e qualquer contato deverá ser feito exclusivamente através do Setor de Compras.

4.3. O processo de contratação é público, nos termos do art. 8º do Regulamento de Compras e Contratações do ICIPE, sendo resguardado o sigilo do conteúdo das propostas e das informações estratégicas até o encerramento da fase de negociação.

4.3.1. O acesso aos autos e a concessão de vistas observarão esses limites, de modo a não comprometer a isonomia entre os participantes nem a efetividade da negociação.

4.4. Eventuais modificações no edital implicarão nova divulgação na mesma forma de sua divulgação inicial, além do cumprimento dos mesmos prazos dos atos e procedimentos originais, exceto quando a alteração não comprometer a formulação das propostas.

5. DA APRESENTAÇÃO DAS PROPOSTAS E DOS DOCUMENTOS DE HABILITAÇÃO

5.1. Os interessados deverão apresentar proposta de preços exclusivamente por meio do sistema APOIO COTAÇÕES, no endereço https://site.apoiocotacoes.com.br/, no prazo estabelecido no extrato de publicação no Diário Oficial do Distrito Federal – DODF, anexando concomitantemente os documentos exigidos neste Edital, descritos no item – Da Habilitação.

5.1.1. Além da proposta, os interessados deverão anexar, de forma concomitante, os documentos de habilitação exigidos no item 6 deste ato convocatório.

5.2. O prazo para envio da documentação supracitada encerrar-se-á automaticamente na data e horário indicados no seu aviso de publicação no DODF e na plataforma Apoio.

5.3. Nos valores propostos deverão estar inclusos todos os custos operacionais, frete, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente no fornecimento do produto.

5.3.1. Sendo ofertada uma única cotação, com uma única apresentação, com preços unitários e totais por item;

5.3.2. O item ofertado deve estar em conformidade com as especificações do Anexo I, devendo ser informado uma única marca e/ou fabricante e quando couber, informar modelo e/ou referência;

5.4. Não haverá admissão de lances sucessivos por parte dos participantes.

5.5. Não haverá sessão pública para abertura das propostas recebidas.

5.6. A proposta deverá obedecer aos termos deste Edital e seus Anexos, não sendo considerada aquela que não corresponda às especificações ali contidas ou que estabeleça vínculo à proposta de outra empresa participante.

5.7. O proponente será responsável por todas as transações que forem efetuadas em seu nome no Sistema Eletrônico, assumindo suas propostas como firmes e verdadeiras.

5.8. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências para que a empresa comprove a exequibilidade da proposta.

5.8.1. Entenda-se por preços inexequíveis os que forem inferiores ao custo de produção, acrescidos dos encargos legais, hipótese em que o proponente será convocado para demonstrar a exequibilidade do preço ofertado. Omisso o proponente ou não demonstrada a viabilidade do preço, a proposta será desclassificada em decisão fundamentada.

5.9. Encerrada a análise das propostas e definida a ordem de classificação, proceder-se-á à verificação da documentação de habilitação do proponente classificado em primeiro lugar. Na hipótese de inabilitação, por descumprimento das condições previstas neste Edital, será analisada a documentação do segundo colocado, e assim sucessivamente, observada a ordem de classificação.

6. DA HABILITAÇÃO

6.1. Para fins deste Chamamento, a habilitação observará o procedimento descrito nos itens a seguir, em conformidade com o Regulamento de Compras e Contratações do ICIPE.

6.1.1. A documentação de Habilitação Jurídica e de Qualificação Técnica deverá ser apresentada concomitantemente à proposta, por meio da Plataforma Apoio Cotações, como condição para participação no Chamamento.

6.1.2. A documentação de Regularidade Fiscal e Trabalhista, embora integrante da fase de habilitação, será exigida exclusivamente do(s) proponente(s) vencedor(es), como condição para a assinatura do Instrumento Contratual.

6.1.3. A apresentação e verificação da documentação de Regularidade Fiscal e Trabalhista observará o disposto no item 9.4.1 e 9.4.2 deste Edital, sem prejuízo das verificações posteriores previstas no Regulamento de Compras e Contratações do ICIPE.

6.2. Para habilitação dos proponentes, será exigida a seguinte documentação:

6.3. **Habilitação Jurídica:**

6.3.1. Cédula de Identidade, quando se tratar de empresa Pessoa Física;

6.3.2. Registro comercial, no caso de empresa individual;

6.3.3. Ato Constitutivo, Estatuto ou Contrato Social em vigor devidamente registrado e/ou alteração, em se tratando de Sociedades Comerciais e, no caso de Sociedades por Ações, acompanhado de documentos de eleição de seus administradores;

6.3.4. Inscrição do Ato Constitutivo, no caso de Sociedades Civis, acompanhada de prova de diretoria em exercício;

6.3.5. Cópia do Documento de Identidade e CPF do Representante Legal da empresa.

6.3.6. Se a empresa se fizer representar por procurador, faz-se necessário o encaminhamento do instrumento público ou particular, neste último caso, com firma reconhecida em cartório.

6.3.7. Os documentos de identidade e CPF do Representante Legal da empresa exigido no item 6.3.5 do Edital, bem como o instrumento de procuração previsto no item 6.3.6 do Edital poderão ser apresentados pelo proponente declarado vencedor no momento da assinatura do contrato. **A ausência desses documentos na fase de habilitação não será, por si só, motivo para inabilitação do proponente.**

6.4. **Qualificação técnica:**

6.4.1. Conforme definido no Termo de Demanda.

6.5. Se o participante for a matriz, todos os documentos deverão estar em nome da matriz, e se participante for a filial, todos os documentos deverão estar em nome da filial, exceto aqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

6.5.1. O Setor de Compras poderá, no julgamento das propostas e da habilitação, sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível aos proponentes.

6.5.2. No caso de dúvidas sobre a veracidade de qualquer documento apresentado, o ICIPE poderá solicitar o documento original ou a sua cópia autenticada, em consonância com o parágrafo único do art. 21 do Regulamento de Compras e Contratações do ICIPE.

7. DO JULGAMENTO DAS PROPOSTAS:

7.1. Finalizado o prazo para cadastramento das propostas no site APOIO COTAÇÕES, o Setor de Compras analisará e poderá, desde logo, desclassificar aquelas que não estejam em conformidade com os requisitos estabelecidos neste Edital, contenham vícios insanáveis, ilegalidades ou não apresentem as especificações exigidas no Termo de Demanda.

7.1.1. Sempre que houver desclassificação da proposta, a empresa será automaticamente comunicada por meio de mensagem eletrônica (e-mail) encaminhada pela Plataforma Apoio Cotações, contendo a indicação dos motivos da desclassificação.

7.2. Os Critérios de Aceitação da Proposta são os seguintes:

7.2.1. As propostas deverão ter prazo de validade de 60 (sessenta) dias, contados a partir da data de encerramento da cotação;

7.2.2. O julgamento das propostas será realizado **POR LOTE**, adotando-se o critério de **MENOR PREÇO**.

7.2.3. Os itens da proposta deverão apresentar plena compatibilidade com as especificações técnicas e os requisitos de desempenho estabelecidos no Edital e em seus Anexos;

7.2.4. Serão desclassificadas as propostas de preços que não atendam às exigências do presente Chamamento e de seus Anexos, que sejam omissas ou apresentem irregularidades insanáveis, inclusive aquelas que contenham valores manifestamente inexequíveis, exorbitantes ou incompatíveis com os preços praticados no mercado;

7.2.5. A avaliação da exequibilidade e da aceitabilidade dos preços será realizada com base na análise do preço global, dos quantitativos e dos preços unitários, bem como na compatibilidade com os custos necessários à execução do objeto, mediante análise técnica e, quando necessário, realização de diligências para aferir a exequibilidade das propostas ou exigir dos proponentes que ela seja demonstrada, nos termos do art. 56, § 2º, do Regulamento de Compras e Contratações do ICIPE.

7.3. A oferta de objeto com características mais vantajosas que as exigidas não será considerada para efeito de ordenação das propostas, mas vinculará a empresa participante na execução contratual.

7.4. Para fins de análise da proposta quanto ao cumprimento das especificações do objeto, deverá ser colhido o Parecer Técnico do setor requisitante ou da área especializada no objeto.

7.5. O prazo para credenciamento das propostas poderá ser prorrogado no site APOIO COTAÇÕES e no site oficial do HCB quando o Chamamento restar deserto, após a publicação feita no Diário Oficial do Distrito Federal, a fim de que se obtenha sucesso na aquisição.

7.6. No caso de o processo permanecer total ou parcialmente deserto após a prorrogação do prazo, ou ser total ou parcialmente fracassado no decurso do procedimento, e desde que demonstrada a impossibilidade de sua repetição sem prejuízo ao ICIPE/HCB ou aos pacientes, poderá ser adotada a dispensa de chamamento público, nos termos do art. 97, inciso IX, do Regulamento de Compras e Contratações do ICIPE, mantendo-se as condições originalmente estabelecidas.

7.7. Na hipótese de adoção da dispensa de chamamento público, o procedimento observará o disposto no art. 99 do Regulamento de Compras e Contratações do ICIPE, inclusive quanto aos prazos e à forma de divulgação, aplicando-se a dispensa apenas aos itens não contemplados ou não homologados no chamamento, quando for o caso.

7.8. A apresentação de uma única proposta no Chamamento Público, por si só, não impede a continuação do certame, desde que a proposta atenda a todos os requisitos do edital, inclusive quanto à compatibilidade com o valor estimado adotado como referência.

7.9. Definida a ordem de classificação das propostas, o setor de compras deverá negociar condições mais vantajosas com o primeiro colocado., em consonância com o art. 57 do Regulamento de Compras e Contratações do ICIPE.

7.10. Nos casos em que a empresa participante com a proposta mais vantajosa não atender às exigências e condições deste Chamamento Público, o setor de Compras examinará a proposta subsequente na ordem de classificação, sucessivamente, até a apuração de uma proposta que atenda completamente a todos os requisitos exigidos.

7.11. Quando houver empate entre duas ou mais empresas qualificadas, será encaminhado Termo de Negociação às interessadas. Permanecendo a situação de empate, serão utilizados ordenadamente os seguintes critérios:

I - Maior quantidade de itens com menor preço aprovados no Chamamento;

II - Empresa nacional;

III - Empresa com maior tempo de atividade no mercado;

IV - Sorteio.

7.11.1. O sorteio será realizado por comissão composta por, no mínimo, 03 (três) membros, empregados do ICIPE/HCB, a qual registrará o resultado em Ata, que passará a integrar o processo.

7.12. Na fase de negociação com a empresa selecionada, poderá ser solicitada a prorrogação da validade da proposta apresentada.

7.13. Todos os avisos, comunicados e informações pertinentes a este Chamamento Público serão divulgados no sítio oficial do HCB, no endereço eletrônico www.hcb.org.br/compras, cabendo exclusivamente aos participantes o acompanhamento de tais publicações, não sendo admitida a alegação de desconhecimento das informações, sob pena de preclusão de seus direitos.

8. DA DIVULGAÇÃO DO RESULTADO, DA FASE RECURSAL E DA HOMOLOGAÇÃO

8.1. Concluídas as fases de julgamento das propostas, negociação e análise de habilitação, o resultado preliminar será anexado ao processo administrativo e divulgado no site oficial do ICIPE, nos termos do art. 66 do Regulamento de Compras e Contratações do ICIPE.

8.1.1. Após a divulgação do resultado preliminar, será aberto prazo para interposição de Recurso Administrativo de até 3 (três) dias úteis, contra: (i) o julgamento das propostas; (ii) habilitação ou inabilitação, sob pena de preclusão do direito de recorrer.

8.1.1.1. Os recursos administrativos deverão ser encaminhados para o e-mail compras2@hcb.org.br, contendo, obrigatoriamente, a identificação do número do Chamamento no campo “assunto”.

8.1.2. Admitido o recurso, poderão ser intimados os demais interessados para, querendo, apresentarem contrarrazões, concedendo-lhes o mesmo prazo de 3 (três) dias úteis, que começará a ser contado do término do prazo recursal, nos termos do § 2º. do art. 68 do Regulamento de Compras e Contratações do ICIPE.

8.1.3. Encerrado o prazo recursal, e não havendo interposição de recursos, ou sendo estes julgados improcedentes sem alteração do resultado preliminar, este será considerado resultado definitivo do Chamamento, procedendo-se à homologação do Chamamento pela autoridade competente e à respectiva publicação no Diário Oficial do Distrito Federal e divulgação no site oficial do HCB.

9. DA CELEBRAÇÃO DO CONTRATO

9.1. Após a homologação do processo, o vencedor será convocado para a assinatura do instrumento de formalização da contratação, devendo observar os prazos e condições que lhe foram estabelecidos no instrumento convocatório, nos termos do art. 72 do Regulamento de Compras e Contratações do ICIPE.

9.2. A empresa vencedora será comunicada por e-mail ou telefone para apresentação dos documentos referentes à regularidade fiscal e trabalhista.

9.3. O Contrato implicará compromisso de fornecimento nas condições estabelecidas.

9.4. O vencedor deverá apresentar a documentação abaixo apenas na celebração do Contrato:

9.4.1. Certidão Negativa de Falência e de Recuperação Judicial expedida pelo distribuidor da sede da pessoa jurídica, ou de execução patrimonial, expedida no domicílio da pessoa física, exceto nos casos de fornecimento único e imediato.

9.4.2. Regularidade Fiscal e Trabalhista:

I - prova de inscrição no CPF ou no CNPJ;

II - prova de inscrição no cadastro de contribuintes estadual ou municipal, se houver, relativa ao domicílio ou sede do proponente, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

III - prova de regularidade perante a Fazenda Federal, Estadual/Distrital e Municipal do domicílio ou sede do proponente;

IV - prova de regularidade relativa à Seguridade Social e ao Fundo de Garantia por Tempo de Serviço - FGTS demonstrando situação regular no cumprimento dos encargos sociais;

V - prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa, nos termos do Título VII-A da CLT - Consolidação das Leis do Trabalho, Decreto-Lei nº 5.452/1943;

9.4.2.1. A empresa cadastrada no Sistema de Cadastro Unificado de Fornecedores do Ministério do Planejamento poderá encaminhar declaração do SICAF/SIASG em substituição às certidões elencadas nas alíneas "**II**", "**III**", "**IV**" e "**V**".

9.5. Poderá ser dispensada, total ou parcialmente, a apresentação da documentação de regularidade fiscal e trabalhista nas aquisições para entrega imediata e nas contratações de pequeno vulto cujo valor seja inferior a 1/4 (um quarto) do limite para dispensa de Chamamento Público, desde que não envolvam obrigações futuras ou fornecimento continuado, mediante decisão motivada da autoridade competente, nos termos do art. 65do Regulamento de Compras e Contratações do ICIPE.

9.6. Quando exigida, a documentação de regularidade fiscal e trabalhista deverá estar válida na data da assinatura do Contrato ou do instrumento contratual, devendo essa condição ser mantida durante toda a sua vigência.

9.7. A empresa a ser contratada deverá assinar o Contrato em até 5 (cinco) dias úteis a partir da convocação, sob pena de decair o direito à contratação.

9.7.1. Ocorrendo impedimento justificado e acolhida a justificativa pelo ICIPE, o prazo referido no caput poderá ser prorrogado 1 (uma) vez, por igual período.

9.7.2. É facultado ao ICIPE, quando o convocado não assinar o termo de contrato ou não aceitar o instrumento equivalente no prazo e nas condições estabelecidas:

I - Convocar os fornecedores remanescentes, na ordem de classificação, para fazê-lo em igual prazo e nas mesmas condições propostas pelo primeiro colocado, inclusive quanto aos preços atualizados em conformidade com o instrumento convocatório;

II - Revogar o chamamento público.

9.8. Na hipótese de recusa injustificada pelo vencedor do certame em assinar o instrumento contratual, ou na ausência de apresentação de documentos essenciais para sua formalização, é facultado ao ICIPE convocar os demais participantes, seguindo a ordem de classificação, nos termos do Regulamento de Compras e Contratações do ICIPE.

9.8.1. A recusa injustificada do vencedor do certame em assinar o contrato ou em aceitar o instrumento equivalente no prazo estabelecido pelo ICIPE caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades estabelecidas no instrumento convocatório e neste Regulamento, bem como à perda do direito à contratação.

10. **DAS SANÇÕES**

10.1. Comete infração administrativa a empresa que:

I - Não assinar o termo de contrato ou aceitar/retirar o instrumento equivalente, quando convocado dentro do prazo concedido;

II - Apresentar documentação falsa;

III - Deixar de entregar os documentos exigidos no certame;

IV - Ensejar o retardamento da execução do objeto;

V - Não mantiver a proposta;

VI - Cometer fraude fiscal;

VII - Comportar-se de modo inidôneo.

10.2. As sanções descritas no item 10.1 também se aplicam à vencedora e às empresas classificadas, integrantes do cadastro de reserva, que, caso convocadas, não honrarem o compromisso assumido sem justificativa ou com justificativa recusada pelo ICIPE/HCB.

10.3. A empresa que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

10.3.1. Multa de 5% (cinco por cento) sobre o valor ofertado na proposta;

10.3.2. Suspensão do direito de participar de chamamento público e/ou contratar com o ICIPE pelo prazo de até dois anos.

10.3.3. A penalidade de multa pode ser aplicada cumulativamente com a sanção de suspensão.

10.4. A penalidade de multa pode ser aplicada cumulativamente com as demais sanções, facultada a defesa prévia do interessado, no respectivo processo.

10.5. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Instituição, observado o princípio da proporcionalidade.

10.6. A multa eventualmente imposta à Proponente será executada após regular processo, oferecida a oportunidade de defesa prévia.

10.7. O pagamento da multa que trata o item anterior deverá ser depositado em banco, em nome do Instituto do Câncer Infantil e Pediatria Especializada – ICIPE, no prazo estabelecido neste Edital.

10.8. As multas previstas neste Chamamento não eximem a interessada/vencedora da reparação dos eventuais danos, perdas ou prejuízos que seu ato punível venha causar ao ICIPE/HCB.

10.9. Toda sanção aplicada será anotada no histórico cadastral da empresa.

10.10. A penalidade de suspensão será publicada no Diário Oficial do Distrito Federal.

10.11. A aplicação das sanções administrativas observará o disposto no Regulamento de Compras e Contratações do ICIPE, sendo a análise jurídica realizada, quando exigida, pela Gerência Jurídica nos casos e na forma previstos no referido Regulamento, especialmente quando se tratar de sanções que impliquem restrição ao direito de contratar com a instituição.

11. **DAS OBRIGAÇÕES DO CONTRATANTE**

11.1. As obrigações da Contratante e da Contratada são as estabelecidas no Termo de Demanda e na minuta de Contrato.

12. **DA RESCISÃO**

12.1. As hipóteses de rescisão do Contrato são as estabelecidas na minuta de Contrato.

13. **DO TRATAMENTO DE DADOS DOS REPRESENTANTES**

13.1. As partes resguardam o direito de tratar os dados pessoais dos seus respectivos representantes conforme necessário para os fins de cumprimento do presente certame. Caso o representante demande seus direitos inerentes à proteção de dados pessoais, as partes assegurarão o pleno exercício destes nos termos da "LGPD".

14. **DAS DISPOSIÇÕES FINAIS**

14.1. Não serão levados em consideração os documentos e propostas que não estiverem de acordo com as condições deste Edital de Chamamento Público e seus anexos, quer por omissão, quer por discordância.

14.2. Considerando que o art. 2º, inciso III, do Decreto Distrital nº 33.390/2011 e o Regulamento de Compras e Contratações do ICIPE condicionam a exigência e a verificação documental às previsões expressas do ato de chamamento, o ICIPE está legalmente autorizado a tratar os dados pessoais constantes da documentação apresentada pelas participantes, estritamente na medida necessária ao cumprimento das exigências estabelecidas neste Edital, nos termos do art. 7º, incisos II e V, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados), sendo dispensado o consentimento dos participantes.

14.3. É facultada à Autoridade Competente, em qualquer fase do processo, a promoção de diligência destinada a esclarecer e/ou complementar a sua instrução.

14.4. A autoridade competente poderá, em qualquer fase do processo de chamamento desclassificar a proposta da empresa que for declarada suspensa de participar ou contratar com o ICIPE/HCB ou que for declarada inidônea pela Administração Pública do Distrito Federal.

14.5. A Autoridade Competente poderá revogar, por conveniência e oportunidade, ou anular, por ilegalidade, qualquer ato constitutivo ou derivado deste Chamamento Público.

14.5.1. As empresas participantes não terão direito à indenização em decorrência da revogação ou anulação do Chamamento, ressalvado o direito da Contratada de boa-fé de ser ressarcido pelos encargos que tiver suportado no cumprimento das obrigações.

14.6. O resultado final do presente Chamamento Público será publicado no Diário Oficial do Distrito Federal conforme art. 2°, inciso VI, do Decreto Distrital nº. 33.390/11.

14.7. É terminantemente proibida a utilização de mão-de-obra infantil na execução dos serviços, sendo que o descumprimento deste dispositivo implicará na rescisão imediata do contrato e aplicação de multa, sem prejuízo das sanções legais cabíveis, conforme estabelecido na Lei Distrital nº 5061, de 8 de março de 2013.

14.8. Na contagem dos prazos, excluir-se-á o dia do início e incluir-se-á o do vencimento, e considerar-se-ão os dias corridos, exceto quando for explicitamente disposto em contrário.

14.9. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça o recebimento das propostas e documentações na data marcada, o prazo será automaticamente transferido para o primeiro dia útil subsequente, no mesmo horário e local, anteriormente estabelecidos, desde que não haja comunicação da Autoridade Competente em contrário.

14.10. Em caráter excepcional, e apenas para fins de saneamento formal, o ICIPE poderá solicitar à empresa vencedora esclarecimentos pontuais sobre informações já apresentadas, vedada qualquer complementação ou alteração do conteúdo analisado, devendo a resposta ser encaminhada no prazo de até 3 (três) dias úteis, sob pena de desclassificação.

14.11. O foro para dirimir questões relativas ao presente edital será o de Brasília – Distrito Federal.

15. **ANEXOS DO EDITAL:**

15.1. Anexo I – Termo de Demanda;

15.2. Anexo II – Planilha de Formação de Custos

15.3. Anexo III – Minuta do Contrato.

ANEXO I

TERMO DE DEMANDA

1. **OBJETO**

Contratação de empresa para o fornecimento de solução de segurança perimetral baseada em appliance de firewall de próxima geração (NGFW), com capacidade de inspeção profunda de pacotes, prevenção de intrusão (IPS), controle de aplicações, VPN, e funcionalidades avançadas de visibilidade e resposta, incluindo suporte técnico 24x7, atualizações de assinatura e hardware, e treinamento oficial para a equipe técnica do HCB.

2. **JUSTIFICATIVA**

O presente Termo de Demanda visa substituição/renovação do Parque Tecnológico do HCB, aquisição de **solução de segurança integrada de perímetro para proteção de rede e servidores.**

O Hospital da Criança de Brasília José Alencar- HCB, é a unidade de referência distrital da Secretaria de Estado de Saúde do Distrito Federal (SES/DF) para atendimento de média e alta complexidade para o público pediátrico, sob regime ambulatorial e de internação, envolvendo diversas especialidades clínicas. Considera-se que, para a execução qualificada e mais segura aos pacientes, seja necessária manter o alto desempenho dos sistemas administrativos e institucionais, assegurando a continuidades das atividades.

O firewall é um dispositivo de segurança imprescindível em uma organização. Ele pode ser uma unidade de hardware ou software que filtra o tráfego de entrada e saída em uma rede privada, de acordo com um conjunto de regras para detectar e prevenir ataques cibernéticos. Utilizando um conjunto de regras bem planejadas, protege a rede impedindo o acesso não autorizado. A ausência de um firewall na infraestrutura de TI faz com que o órgão fique altamente vulnerável, facilitando ataques como DDoS, sendo um tipo de invasão cibernética que tenta indisponibilizar um website ou recurso de rede inundando-o com tráfego mal-intencionado e deixando-o incapaz de operar, como diversos outros ataques. Atualmente necessitamos de um firewall que possua módulo IDS (Intrusion Detection System), responsável por detectar a tentativa de exploração de vulnerabilidades e conectar tal tentativa em um sistema de alerta. Por ele ser um sistema de monitoramento, ele alerta o administrador de rede de que uma intrusão está acontecendo. Essa intrusão pode ser considerada qualquer atividade que comprometa o sistema nos quesitos de confiabilidade, confidencialidade, integridade e disponibilidade dos recursos de modo geral, porém não vai prevenir que o ataque ocorra. Além desse sistema de monitoramento, é necessário a adição do módulo IPS (Intrusion Prevention System), que ao detectar (IDS) uma tentativa de ataque, será disparada uma ação com intuito de bloquear tal tentativa de intrusão baseado nas configurações realizadas pelo administrador.

Atualmente o HCB possui uma infraestrutura de TI de alta disponibilidade onde são geridos a maioria dos processos em saúde por meio eletrônico, seja em sistemas desenvolvidos pelo próprio serviço, seja em plataformas integradas com os demais órgãos ou departamentos. Esse fato, aliado à constante atualização do parque tecnológico contribui para gerar economia dos recursos públicos e maior segurança da informação necessária à continuidade e à eficiência das atividades assistenciais. Neste contexto, Em 2012 o HCB adquiriu seu primeiro equipamento AKER (Axiomtek) NA-820 e licenças de uso do sistema de solução de segurança integrada, renovando o uso destas licenças em 2015. Em 2018 uma nova renovação e atualização de solução de segurança, AKER BOX (Firewall Modelo:AFW8137) e desde então estamos utilizando a solução que possui suporte técnico e atualizações limitados, pois são equipamento considerados obsoletos por alguns fornecedores e com forte tendencia a entrar no hall de obsolescências perceptiva.

A Gerencia de Tecnologia tem a responsabilidade de manter seguras as informações sob sua guarda e com soluções que consigam processamento das informações do atual ambiente de TIC. Desta forma, é de amplo conhecimento que atualmente os órgãos públicos e privados estão sofrendo ataques em seus ambientes e com isso causando perda parcial ou total das informações, além do supracitado, o crescimento exponencial do parque computacional e número de usuários, se tornando necessário uma atualização tecnológica da solução de segurança integrada de perímetro da Instituição.

Esta substituição/atualização da solução atual de proteção de rede, que atualmente é composta por hardware e software da marca AKER e FortiGate, se faz necessária devido ao crescimento do parque computacional e à necessidade de se prover um ambiente em alta disponibilidade com pelo menos dois ou mais equipamentos, do tipo appliance, trabalhando de forma redundante. Desta forma é possível alinhar a infraestrutura de segurança de perímetro do ambiente de TIC ao negócio que se encontram em rápida expansão e crescimento, provendo maior desempenho e segurança, pois trata-se de informações e dados sensíveis e de propriedade da instituição e dos usuários dos sistemas. A não aquisição de uma nova solução de segurança integrada de perímetro pode resultar nos seguintes impactos:

- Riscos de ataques e invasões no sítio do HCB;
- Roubo ou sequestro de dados sensíveis;
- Indisponibilidade total e/ou parcial em função de falta de capacidade de processamento;
- Lentidão no acesso aos sistemas e informações disponíveis na Internet;
- Paralisações por prazos indeterminados dos sistemas das áreas negociais;
- Interrupções nos atendimentos ao público externo e interno;
- Vazamento de dados pessoais e corporativos do HCB;

- Dentro outros.

Considerando que o negócio fim do Hospital da Criança de Brasília está cada vez mais depende dos sistemas de informação, da capacidade de processamento dos dados e acessos dos usuários e que estes cada vez mais são objeto de tentativas de ataques, sequestros de dados e invasões no ambiente operacional, torna-se imprescindível a substituição por uma solução de segurança de perímetro para proteção de rede moderna.

2.1. Incluir embasamento técnica/legal para a contratação, correlacionando com os objetivos estratégicos do ICIPE/HCB. Devendo ser contempladas abordagens aos requisitos a seguir relacionados:

2.1.1. Informar se é serviço recorrente, ou se trata de implantação de novo serviço.

A solução se trata de um novo serviço contemplando aquisição de novos equipamentos e licenças (hardware e software), subscrição de licenças e serviços de manutenção e treinamento (Serviços).

2.1.2. Indicar como foi apurada a estimativa dos serviços.

2.1.3. Informar a relevância da contratação dos serviços, indicando os impactos positivos da contratação (ou, sejam, os resultados esperados).

2.1.4. Registrar o impacto da não contratação para o ICIPE/HCB, face aos indicadores previstos no contrato de gestão e aos objetivos estratégicos do Instituto.

Indisponibilidade dos serviços e das operações do hospital devido a ataques cibernéticos.

2.1.5. Informar à legislação que rege o serviço.

2.2. Por todas as colocações, justifica-se a contratação pretendida neste Termo.

3. **CONDIÇÕES GERAIS PARA EXECUÇÃO DOS SERVIÇOS**

3.1. O serviço a ser executado **consistirá em:**

3.2. O prazo para a entrega, instalação, migração e configuração da solução será de no máximo 30 (trinta) dias consecutivos, contados a partir do primeiro dia útil após a data da assinatura da Ordem de Serviço;

3.3. Deverá ser realizado um cronograma/planejamento prévio de todas as ações a serem executadas, em conjunto com a equipe da GTI, bem como a definição do plano de trabalho para a execução dos serviços de instalação e configuração;

4. **DESCRIÇÃO E DETALHAMENTO DOS SERVIÇOS**

4.1. Os serviços a serem executados relacionados a este Termo de Demanda consistirá em:

4.1.1. **Quadro 01:** Quantitativo estimado

LOTE ÚNICO	CÓDIGOS	**Descrição**	**Qtde.**	**UN**
	SERVIÇO-3197	**Solução de Proteção de Perímetro do tipo Next Generation Firewall NGFW** - Solução de proteção de perímetro baseada em firewalls de próxima geração, responsável pela inspeção do tráfego em camadas 3 a 7, controle de aplicações, prevenção de intrusões, filtragem de URLs, proteção contra malware e estabelecimento de túneis VPN para 36 meses de licenciamento e suporte.	2	Unidades
	SERVIÇO-3198	**Solução de Gerenciamento Centralizado Inteligente** - Plataforma de gerenciamento centralizado dos firewalls NGFW, em nuvem do fabricante ou appliance dedicado, permitindo administração unificada de políticas, correlação e visualização de logs, geração de relatórios, análise de ameaças e acompanhamento da postura de segurança de todo o ambiente para 36 meses de licenciamento e suporte.	1	Unidade
	SERVIÇO-3199	**Serviço de Suporte da CONTRATADA -** Serviço de suporte técnico especializado para os firewalls NGFW e para a solução de gerenciamento centralizado, incluindo atendimento remoto, apoio na operação da solução, abertura e acompanhamento de chamados junto ao fabricante, bem como manutenção corretiva e evolutiva e atualização de software e assinaturas de segurança durante o período contratual de 36 meses	36	(meses)
	SERVIÇO-3200	**Serviço de Instalação da CONTRATADA -** Serviço de instalação, configuração inicial e comissionamento dos firewalls NGFW e da solução de gerenciamento centralizado, incluindo integração à rede da CONTRATANTE, configuração de alta disponibilidade, ajustes de políticas básicas de segurança, realização de testes de aceitação e entrega de documentação técnica do ambiente implantado.	2	Unidades
	SERVIÇO-3201	**Serviço de Treinamento da CONTRATADA -** Treinamento remoto de administração básica da solução de Firewall de Próxima Geração (NGFW), com carga horária total de 20 (vinte) horas para até 5 (cinco) alunos, abordando conceitos fundamentais da plataforma, interfaces e zonas, objetos e políticas de segurança, NAT, controle de aplicações e usuários, perfis de segurança e VPN. O objetivo é capacitar a equipe da CONTRATANTE para realizar a operação diária do firewall, incluindo monitoramento,	5	Alunos

		interpretação de logs, procedimentos básicos de troubleshooting, alta disponibilidade e gerenciamento de configuração.		

4.2. **ITEM 01: SOLUÇÃO DE PROTEÇÃO DE PERIMETRO**

4.2.1. **DISPOSIÇÃO GERAL**

4.2.1.1. Deve ser instalado em HA, justificando a contratação de 2 (duas) unidades.

4.2.1.2. Deve possuir throughput de, no mínimo, 9 de Gbps de Next Generation Firewall considerando no mínimo as funcionalidades de Firewall e Controle de Aplicação, sendo comprovado com documentação de domínio público.

4.2.1.3. Deve possuir throughput de, no mínimo, 6 Gbps com as funcionalidades de controle de aplicação, IPS, Antivírus, Anti-Spyware, Sandbox e log habilitadas simultaneamente na solução. A comprovação se dará através de documentação técnica do fabricante de acesso público informando os throughput aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real.

4.2.1.4. Deve suportar, no mínimo, 1.300.000 sessões simultâneas.

4.2.1.5. Deve suportar, no mínimo, 130.000 novas sessões por segundo.

4.2.1.6. Deve possuir, no mínimo, 4 interfaces físicas de rede de 10 / 100/ 1000 Mbps do tipo RJ-45.

4.2.1.7. Deve possuir, no mínimo, 4 interfaces físicas de rede de 1 / 2.5 / 5 Gbps do tipo RJ-45.

4.2.1.8. Deve possuir, no mínimo, 8 interfaces físicas de rede de 10 Gbps do tipo SFP+.

4.2.1.9. Deve ser entregue com redundância em HA ativo-passivo.

4.2.1.10. Deve ter fonte redundante.

4.2.1.11. Deve ser entregue com trilho para instalação em rack de servidores, tamanho padrão.

4.2.1.12. Caso não exista trilho, deve ser entregue bandeja ou solução similar.

4.2.1.13. Deve possuir porta de gerência out-of-band 10/100/1000 RJ45.

4.2.1.14. Deve permitir pelo menos 6 sistemas virtuais sendo que deve vir 1 (um) já licenciado.

4.3. **ITEM 02: SOLUÇÃO DE PROTEÇÃO DE PERIMETRO**

4.3.1. **FUNCIONALIDADES BASE**

4.3.1.1. A solução deve consistir em appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW) e console de gerência e monitoração.

4.3.1.2. As funcionalidades de proteção de rede que compõem a plataforma de segurança podem funcionar em múltiplos appliances, desde que obedeçam a todos os requisitos desta especificação.

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

4.3.1.4. A solução de segurança deve possuir nativamente funcionalidade de Machine Learning capaz de bloquear grande volume dos ataques nas suas redes.

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

4.3.1.6. O hardware e software que executem as funcionalidades de proteção de rede devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistemas operacionais de uso genérico.

4.3.1.7. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

4.3.1.8. Agregação de links 802.3ad e LACP para o equipamento do tipo I.

4.3.1.9. Policy based routing ou policy based forwarding.

4.3.1.10. Roteamento multicast (PIM-SM).

4.3.1.11. DHCP Relay.

4.3.1.12. DHCP Server.

4.3.1.13. Jumbo Frames.

4.3.1.14. Suporte à criação de objetos de rede que possam ser utilizados como endereço IP de interfaces L3.

4.3.1.15. Suportar sub-interfaces ethernet lógicas.

4.3.1.16. Deve suportar os seguintes tipos de NAT:

4.3.1.17. NAT dinâmico (Many-to-1).

4.3.1.18. NAT dinâmico (Many-to-Many).

4.3.1.19. NAT estático (1-to-1).

4.3.1.20. NAT estático (Many-to-Many).

4.3.1.21. NAT estático bidirecional 1-to-1.

4.3.1.22. Tradução de porta (PAT).

4.3.1.23. NAT de Origem.

4.3.1.24. NAT de Destino.

4.3.1.25. Suportar NAT de Origem e NAT de Destino simultaneamente.

4.3.1.26. Deve implementar Network Prefix Translation (NPTv6).

4.3.1.27. Enviar log para sistemas de monitoração externos.

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

4.3.1.29. Deve permitir configurar certificado, caso necessário, para autenticação no sistema de monitoração externo de logs.

4.3.1.30. Proteção contra anti-spoofing.

4.3.1.31. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2).

4.3.1.32. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3).

4.3.1.33. Suportar a OSPF graceful restart.

4.3.1.34. Deve suportar o protocolo MP-BGP (Multiprotocol BGP), permitindo que o firewall possa anunciar rotas multicast para IPv4 e rotas unicast para IPv6.

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

4.3.1.36. Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede.

4.3.1.37. Modo Camada 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação.

4.3.1.38. Modo Camada 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação, operando como default gateway das redes protegidas.

4.3.1.39. Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas.

4.3.1.40. Suporte à configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo:

4.3.1.41. Em modo transparente.

4.3.1.42. Em Layer 3.

4.3.1.43. A configuração em alta disponibilidade deve sincronizar:

4.3.1.44. Sessões.

4.3.1.45. Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QoS e objetos de rede.

4.3.1.46. Certificados de-criptografados.

4.3.1.47. Associações de Segurança das VPNs.

4.3.1.48. Tabelas FIB.

4.3.1.49. No modo HA (modo de Alta Disponibilidade), deve possibilitar monitoração de falha de link.

4.3.1.50. Deve ser capaz de analisar o comportamento de dispositivos IoT com base em CVEs conhecidas.

4.3.1.51. A ferramenta deve possuir console centralizada, apresentando graficamente o inventário de todos os dispositivos detectados pela ferramenta.

4.3.1.52. Deve ser capaz de realizar avaliação de segurança nos dispositivos descobertos e sua classificação de riscos de segurança.

4.3.1.53. A solução deve ser capaz de apresentar opção de regra baseada em boas práticas de segurança.

4.3.1.54. Deve ser possível aplicar regras de segurança limitando o acesso do dispositivo (asset) identificado com outros dispositivos de rede.

4.3.1.55. Aplicar inspeção através de funcionalidades de segurança e bloqueio de tráfego dos dispositivos (assets) identificados para conter qualquer acesso indevido ou ameaça baseada em portas/serviços não autorizados.

4.3.1.56. Caso a solução não possua essas funcionalidades, será permitido a integração com ferramentas que executam esta função para, pelo menos, 15 mil dispositivos.

4.3.2. **SD-WAN**

4.3.2.1. Deve operacionalizar, no mínimo, os seguintes critérios de SD-WAN.

4.3.2.2. A plataforma de segurança deverá recuperar pacotes perdidos antes que seja necessário alterar o caminho principal.

4.3.2.3. As configurações de perfis de SD-WAN devem partir de um ponto central, permitindo alteração e criação dos elementos primordiais para o funcionamento da solução. Deve também entregar a criação automática dos túneis IPSEC entre as localidades.

4.3.2.4. A solução deve permitir operar em caráter de diagrama hub-spoke.

4.3.2.5. É considerado diferencial dispositivos que tenham a capacidade de exibir impactos por aplicação.

4.3.2.6. A solução deve permitir ao administrador métricas de utilização de banda por circuito disponível e, desta forma, exibir no mínimo os seguintes itens em porcentagem ou contadores: jitter, latência e perda de pacote.

4.3.2.7. O dispositivo deve compreender o que está causando desempenho de degradação para as aplicações e serviços ativos, garantindo que a experiência do usuário sofra o menor impacto possível.

4.3.2.8. O SD-WAN deve suportar os seguintes tipos de conexões WAN: ADSL/DSL, Cable Modem com Ethernet ou fibra, LT/3G/4G/5G, MPLS, Link de rádio e Link satélite, desde que a sua terminação permita conectividade com interfaces Ethernet.

4.3.2.9. A solução deve ter inteligência para executar, no mínimo, as seguintes lógicas de operação:

4.3.2.10. Distribuição de tráfego por prioridade de circuito; circuitos exclusivos de contingenciamento em 3G/4G/5G devem ser utilizados apenas em caso de falha geral dos circuitos ADSL/MPLS.

4.3.2.11. Distribuição de tráfego de acordo com métricas definidas por origem e destino. O dispositivo deve permitir ao administrador criar perfis com base em latência, jitter ou perda de pacotes.

4.3.2.12. Distribuição de tráfego com balanceamento de sessão entre os circuitos existentes.

4.3.2.13. Quando ambos os pontos de extremidade dos túneis SD-WAN estiverem ativos, deve haver a duplicação de pacotes (PD) para manter a experiência dos usuários, mesmo em condição de perda de pacotes. A duplicação de pacotes deve criar uma cópia do fluxo de tráfego do aplicativo e enviá-la em ambos os túneis disponíveis, que estão orientados ao mesmo destino.

4.3.2.14. O dispositivo de SD-WAN deve utilizar "Forward Error Correction" (FEC) habilitado para permitir que aplicativos sensíveis à perda de pacotes não sejam impactados em caso de perda de pacote e recupere os pacotes perdidos ou corrompidos usando pacotes de paridade incorporados no fluxo da comunicação. O objetivo é reparar o fluxo antes que ele precise fazer failover para outro caminho.

4.3.2.15. O SD-WAN deve permitir combinar vários serviços ISP em uma interface Ethernet Agregada (AE) para redundância de link. A interface agregada deve oferecer suporte a subinterfaces para que seja possível marcar diferentes serviços ISP usando tags de VLAN de camada 3 a fim de obter segmentação de tráfego de ponta a ponta.

4.3.2.16. O SD-WAN deve permitir o monitoramento de integridade do caminho de aplicativos SaaS para garantir decisões com base em confiabilidade e experiência do usuário. Nos cenários onde o SD-WAN possui link de acesso direto à Internet (DIA), deve permitir o failover para um caminho de desempenho mais alto com base em medições precisas da qualidade da aplicação.

4.3.2.17. Distribuição orientada à qualidade: o dispositivo deve validar o melhor caminho disponível e utilizar esse "path" para manter sessões ativas. Caso o melhor caminho entre em degradação por fatores anômalos, o dispositivo deverá entender esses fatores e distribuir para os demais circuitos existentes.

4.3.3. **CONTROLE POR POLÍTICA DE FIREWALL**

4.3.3.1. Deverá suportar controles por zona de segurança.

4.3.3.2. Controles de políticas por porta e protocolo.

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

4.3.3.4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.

4.3.3.5. Deve suportar a consulta a fontes externas de endereços IP, domínios e URLs, podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego.

4.3.3.6. Deve permitir autenticação segura através de certificado nas fontes externas de endereços IP, domínios e URLs.

4.3.3.7. Deve permitir consultar e criar exceção para objetos das listas externas a partir da interface de gerência do próprio firewall.

4.3.3.8. Controle de políticas por código de país (por exemplo: BR, USA, UK, RUS).

4.3.3.9. Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e saída (Outbound).

4.3.3.10. Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound).

4.3.3.11. Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com HTTP/2, TLS 1.2 e TLS 1.3.

4.3.3.12. Controle de inspeção e de-criptografia de SSH por política.

4.3.3.13. A de-criptografia de SSH deve possibilitar a identificação e bloqueio de tráfego caso o protocolo esteja sendo usado para tunelar aplicações como técnica evasiva para burlar os controles de segurança.

4.3.3.14. Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif e reg.

4.3.3.15. Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo).

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

4.3.3.17. Suporte a objetos e regras IPv6.

4.3.3.18. Suporte a objetos e regras multicast.

4.3.3.19. Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

4.3.3.20. Deve possuir ferramenta que indique as regras sobrepostas e objetos não utilizados para otimização das regras. Caso não possua essa funcionalidade, será permitido a integração com ferramentas que executam esta função.

4.3.4. **CONTROLE DE APLICAÇÕES**

4.3.4.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

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

4.3.4.3. Reconhecer pelo menos 3000 aplicações diferentes, incluindo, mas não limitado: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, atualização de software, protocolos de rede, VoIP, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail.

4.3.4.4. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e ataques mediante a porta 443.

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

4.3.4.6. Deve permitir a utilização de aplicativos para um determinado grupo de usuários e bloquear para o restante, incluindo, mas não limitado a Skype. Deve permitir também a criação de políticas de exceção, concedendo o acesso a aplicativos como Skype apenas para alguns usuários.

4.3.4.7. Identificar o uso de táticas evasivas via comunicações criptografadas.

4.3.4.8. Atualizar a base de assinaturas de aplicações automaticamente.

4.3.4.9. Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP/AD.

4.3.4.10. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários.

4.3.4.11. Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente à possibilidade de habilitar controle de aplicações em algumas regras.

4.3.4.12. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos e análise heurística.

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

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

4.3.4.15. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações.

4.3.4.16. Deve alertar o usuário quando uma aplicação for bloqueada.

4.3.4.17. Deve possibilitar que o controle de portas seja aplicado para todas as aplicações.

4.3.4.18. Deve permitir criar filtro na tabela de regras de segurança para exibir somente:

4.3.4.19. Regras que permitem a passagem de tráfego baseado na porta e não por aplicação, exibindo quais aplicações estão trafegando nas mesmas, o volume em bytes trafegado por cada aplicação pelos últimos 30 dias e o primeiro e último registro de log de cada aplicação trafegada por esta determinada regra.

4.3.4.20. Aplicações permitidas em regras de forma desnecessária, pois não há tráfego da mesma na determinada regra.

4.3.4.21. Regras de segurança onde não houve passagem de tráfego nos últimos 90 dias.

4.3.5. **FILTRO DE URL**

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

4.3.5.2. Deve ter a capacidade de bloquear ameaças desconhecidas em tempo real.

4.3.5.3. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado com a última base de assinatura instalada no momento em que a licença expirou, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.

4.3.5.4. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo.

4.3.5.5. As assinaturas podem ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração.

4.3.5.6. Exceções por IP de origem ou de destino devem ser possíveis nas regras, de forma geral e assinatura a assinatura.

4.3.5.7. Deve permitir o bloqueio de vulnerabilidades.

4.3.5.8. Deve permitir o bloqueio de exploits conhecidos.

4.3.5.9. Deve incluir proteção contra ataques de negação de serviços.

4.3.5.10. Deverá possuir os seguintes mecanismos de inspeção de IPS:

4.3.5.11. Análise de padrões de estado de conexões.

4.3.5.12. Análise de decodificação de protocolo.

4.3.5.13. Análise para detecção de anomalias de protocolo.

4.3.5.14. Análise heurística.

4.3.5.15. IP Defragmentation.

4.3.5.16. Remontagem de pacotes de TCP.

4.3.5.17. Bloqueio de pacotes malformados.

4.3.5.18. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPflood etc.

4.3.5.19. Detectar e bloquear a origem de port scans com possibilidade de criar exceções para endereços IPs de ferramentas de monitoramento da organização.

4.3.5.20. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões.

4.3.5.21. Suportar os seguintes mecanismos de inspeção contra ameaças de rede: análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, análise heurística, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados.

4.3.5.22. Possuir assinaturas específicas para a mitigação de ataques DoS.

4.3.5.23. Possuir assinaturas para bloqueio de ataques de buffer overflow.

4.3.5.24. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto.

4.3.5.25. Identificar e bloquear comunicação com botnets.

4.3.5.26. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

4.3.5.27. O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo.

4.3.5.28. Deve suportar a captura de pacotes (PCAP), por assinatura de Malware e aplicação.

4.3.5.29. Permitir o bloqueio de vírus, pelo menos, nos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3.

4.3.5.30. Os eventos devem identificar o país de onde partiu a ameaça.

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

4.3.5.32. Bloquear proativamente os ataques sofisticados recém-descobertos em tempo real com IA e serviços avançados de proteção contra ameaças.

4.3.5.33. Proteção contra downloads involuntários usando HTTP de arquivos executáveis.

4.3.5.34. Rastreamento de vírus em PDF.

4.3.5.35. Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.).

4.3.6. **PREVENÇÃO DE AMEAÇAS AVANÇADAS DE DIA ZERO**

4.3.6.1. O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado.

4.3.6.2. Deve ser capaz de enviar para análise, arquivos do tipo Executáveis, DLLs, Arquivos de Código e MSI.

4.3.6.3. A solução deve detectar e bloquear em tempo real (inline) os artefatos maliciosos desconhecidos (zero day) no próprio gateway através de mecanismos de Machine Learning.

4.3.6.4. Suportar a análise dinâmica de arquivos maliciosos em ambiente controlado com, no mínimo, os sistemas operacionais Windows XP, Windows 7, Windows 10, Mac OS X, Android e Linux.

4.3.6.5. A análise de links em sandbox deve ser capaz de classificar sites falsos na categoria de phishing e atualizar a base de filtro de URL da solução.

4.3.6.6. Deve permitir exportar o resultado das análises de malwares de dia Zero em PDF e CSV a partir da própria interface de gerência.

4.3.6.7. Deve permitir o download dos malwares identificados a partir da própria interface de gerência.

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

4.3.6.9. Deve permitir informar ao fabricante quanto à suspeita de ocorrências de falso-positivo e falso-negativo na análise de malwares de dia Zero a partir da própria interface de gerência.

4.3.6.10. Caso sejam necessárias licenças de sistemas operacionais e softwares para execução de arquivos no ambiente controlado (sandbox), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante.

4.3.6.11. Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado.

4.3.6.12. Suportar a análise de arquivos do pacote Office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos Java (.jar e .class), Android APKs, MacOS (Mach-O, DMG e PKG), Linux (ELF), RAR e 7-ZIP no ambiente de sandbox.

4.3.6.13. A solução deve analisar os arquivos do tipo malware em bare-metal para evitar técnicas de evasão. Caso não possua essa funcionalidade, será permitido a integração com ferramentas que executam esta função. No caso de equipamento físico (appliance) do próprio fabricante, devem ser fornecidas no mínimo 28 máquinas virtuais (VM) simultaneamente por appliance.

4.3.6.14. As funcionalidades de sandbox têm como objetivo analisar e bloquear em tempo real Ameaças Avançadas Persistentes (APT). Essas funcionalidades têm o objetivo de proteger o ambiente contra a entrada de malwares não conhecidos, e para que sejam

efetivas, é necessário que a inspeção e bloqueio sejam feitas em linha (inline), através de features de machine learning.

4.3.6.15. Permitir o envio de arquivos e links para análise no ambiente controlado de forma automática via API.

4.3.6.16. Deve permitir o envio para análise em sandbox de malwares bloqueados pelo antivírus da solução.

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

4.3.6.18. Deve prevenir contra ataques sem arquivo, buscando por atividade maliciosa em pelo menos nas seguintes linguagens de scripts: PowerShell e JavaScript.

4.3.6.19. Deve ser capaz de aplicar, de forma complementar às assinaturas de antivírus, a inspeção inline através de Machine Learning em tempo real em arquivos do tipo PE (Portable Executable), ELF (Executable and Linked Format) e Arquivos Microsoft Office, bem como scripts PowerShell e shell script em tempo real para malwares desconhecidos.

4.3.6.20. A solução de prevenção de ameaças deve identificar e bloquear links maliciosos dentro de e-mails (SMTP e POP3).

4.3.7. **IDENTIFICAÇÃO DE USUÁRIOS**

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

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

4.3.7.3. Deve possuir integração com RADIUS para identificação de usuários e grupos, permitindo granularidade de controle e políticas baseadas em usuários e grupos de usuários.

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

4.3.7.5. Deve suportar o recebimento de eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via syslog, para a identificação de endereços IP e usuários.

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

4.3.7.7. Suporte à autenticação Kerberos.

4.3.7.8. Deve suportar autenticação via Kerberos para administradores da plataforma de segurança, Captive Portal e usuários de VPN SSL.

4.3.7.9. 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 nesses serviços.

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

4.3.8. **SOLUÇÃO DE SEGURANÇA PARA DNS**

4.3.8.1. A solução deve mostrar nos logs as seguintes informações sobre domínios DGA:

4.3.8.2. Domínio suspeito identificado.

4.3.8.3. ID de assinatura de detecção.

4.3.8.4. Usuário logado na estação/servidor que originou o tráfego.

4.3.8.5. Aplicação.

4.3.8.6. Porta de destino.

4.3.8.7. IP de origem.

4.3.8.8. IP de destino.

4.3.8.9. Horário.

4.3.8.10. Ação do firewall.

4.3.8.11. Severidade.

4.3.8.12. A solução deve possuir sistema de análise automático para detectar e bloquear encapsulamento de DNS com fins de roubo de dados e comunicações de comando e controle.

4.3.8.13. A análise automática deve incluir, no mínimo, as seguintes características:

4.3.8.14. Padrões de consulta.

4.3.8.15. Entropia.

4.3.8.16. Análise de frequência n-gram de domínios.

4.3.8.17. Taxa de consultas.

4.3.9. **QOS**

4.3.9.1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo (como YouTube, Ustream, etc.) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter

a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming.

4.3.9.2. Suportar a criação de políticas de QoS por:

4.3.9.3. Endereço de origem.

4.3.9.4. Endereço de destino.

4.3.9.5. Por usuário e grupo do LDAP/AD.

4.3.9.6. Por aplicações.

4.3.9.7. Por porta.

4.3.9.8. O QoS deve possibilitar a definição de classes por:

4.3.9.9. Banda Garantida.

4.3.9.10. Banda Máxima.

4.3.9.11. Fila de Prioridade.

4.3.9.12. Suportar priorização Real-Time de protocolos de voz (VoIP), como H.323, SIP, SCCP, MGCP e aplicações como Skype.

4.3.9.13. Suportar marcação de pacotes Diffserv, inclusive por aplicação.

4.3.9.14. Deve implementar QoS (traffic-shaping) para pacotes marcados por outros ativos na rede (DSCP). A priorização e limitação do tráfego deve ser efetuada nos dois sentidos da conexão (inbound e outbound).

4.3.9.15. Disponibilizar estatísticas Real-Time para classes de QoS.

4.3.9.16. Deve suportar QoS (traffic-shaping) em interfaces agregadas.

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

4.3.10. **VPN**

4.3.10.1. A solução de VPN client-to-site deverá ser atendida apenas para o equipamento do tipo II.

4.3.10.2. Suportar VPN Site-to-Site e Client-To-Site.

4.3.10.3. Suportar IPSec VPN.

4.3.10.4. Suportar SSL VPN.

4.3.10.5. A VPN IPSec deve suportar:

4.3.10.6. 3DES.

4.3.10.7. Autenticação MD5 e SHA-1.

4.3.10.8. Diffie-Hellman Group 1, Group 2, Group 5 e Group 14.

4.3.10.9. Algoritmo Internet Key Exchange (IKEv1 e v2).

4.3.10.10. AES 128 e 256 (Advanced Encryption Standard).

4.3.10.11. Autenticação via certificado IKE PKI.

4.3.10.12. Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSec a partir da interface gráfica da solução, facilitando o processo de troubleshooting.

4.3.10.13. Deve permitir criar políticas de controle de aplicações, IPS, Antivírus, Anti-Spyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL.

4.3.10.14. Suportar autenticação via AD/LDAP, OTP (One Time Password), certificado e base de usuários local.

4.3.10.15. Deve suportar a distribuição de certificado para o usuário remoto através do portal de VPN de forma automatizada.

4.3.10.16. Deve suportar a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL.

4.3.10.17. O cliente da solução de VPN client-to-site deve suportar a instalação nos seguintes tipos de sistemas operacionais:

4.3.10.18. Microsoft Windows.

4.3.10.19. Apple macOS e iOS.

4.3.10.20. Android.

4.3.10.21. Linux.

4.3.10.22. A solução de VPN client-to-site deve estar devidamente licenciada para criar perfis customizados de conformidade dos clientes das VPNs client-to-site para, no mínimo, as seguintes opções:

4.3.10.23. Sistema operacional.

4.3.10.24. Antivírus instalado.

4.3.10.25. Firewall no host.

4.3.10.26. Chaves de registros (quando aplicável).

4.3.10.27. Processos ativos.

4.3.10.28. Os mecanismos de conformidade da solução de VPN client-to-site deverão monitorar durante a conexão do usuário remoto qualquer tipo de atividade não autorizada pelo administrador em tempo real. Por exemplo: após o usuário ser conectado e admitido pela VPN client-to-site, o seu acesso ao ambiente corporativo pode ser negado caso ele manualmente desative alguma funcionalidade especificada nos testes de conformidade da solução.

4.3.10.29. Deve haver a opção do cliente remoto escolher manualmente o gateway de VPN e, de forma automática, através da melhor rota entre os gateways disponíveis com base no tempo de resposta mais rápido.

4.3.11. **NECESSIDADES TÉCNICAS DE REFERÊNCIA DE GERÊNCIA CENTRALIZADA PARA NGFW**

4.3.11.1. **FUNCIONALIDADES BASE**

I - Deverá permitir nativamente ou, através de composição com ferramentas líderes de mercado, avaliar através de uma única interface de gerenciamento o seguinte:

II - Configuração dos NGFW;

III - Utilização das subscrições de Segurança;

IV - Recomendação de ações e/ou comandos via CLI para remediar os gaps de segurança;

V - Alertas de hardware e limites de configuração;

VI - Identificação e notificação de anormalidades no estado geral de funcionamento da solução.

4.3.11.2. **FUNCIONALIDADES AVANÇADAS**

I - Deve ser hospedada na nuvem do fabricante em datacenter com no mínimo certificação SOC2 ou em dispositivos dedicados no ambiente físico do órgão.

II - Deve ser capaz de controlar todos os equipamentos da plataforma de segurança em uma única console.

III - Deve permitir a criação de dashboards customizados para exibir informações de no mínimo:

IV - Prevenção de Ameaças;

V - Uso de aplicações;

VI - Segurança de DNS;

VII - Uso de Rede;

VIII - Informações de Sandbox.

IX - Deve possuir dashboard capaz de apresentar a saúde dos dispositivos gerenciados através de escores, estatísticas e tendências.

X - Deve possuir dashboard capaz de apresentar informações de rede sumarizadas bem como por tráfego, usuários e endereços IPs.

XI - Deve prover visão de 360 graus relativa a atividades de ameaças bem como suas tendências.

XII - Deve, em relação a ameaças, apresentar dashboards de ameaças para:

XIII - Aplicações mais impactadas;

XIV - Usuários mais impactados;

XV - Políticas de segurança mais impactadas.

XVI - Deve apresentar sumário executivo contendo:

XVII - Aplicações de maiores riscos;

XVIII - Atividades web maliciosas;

XIX - Atividades de Sandbox.

XX - Deve permitir gerar relatórios de boas práticas.

XXI - Deve apresentar resumo da adoção de serviços de segurança pelos equipamentos gerenciados.

XXII - Deve ser capaz de forma centralizada criar políticas de segurança contendo:

XXIII - Regras de Antivirus e antispyware;

XXIV - Segurança de DNS;

XXV - Filtro de URLs;

XXVI - Proteção de vulnerabilidades;

XXVII - Regras de descriptografia;

XXVIII - Regras de Rede e QoS;

XXIX - Regras de NAT.

XXX - Deve ser capaz de configurar autenticação.

XXXI - Deve permitir a criação de listas externas a serem utilizadas pelas políticas de segurança.

XXXII - Deve permitir a criação de agendamentos.

XXXIII - Deve trazer informações relativas à postura de segurança e recomendações de upgrade de software.

XXXIV - Deve analisar a necessidade de criação de novas regras de segurança.

XXXV - Deve trazer informações relativas à capacidade dos dispositivos gerenciados contendo:

XXXVI - Métricas de utilização;

XXXVII - Mapa de calor do uso de recursos.

XXXVIII - O analisador de capacidade deve ser capaz de emitir alertas contendo no mínimo:

XXXIX - Recursos de criptografia;

XL - Anomalias;

XLI - Capacidade da Tabela ARP;

XLII - Capacidade de Objetos e grupos;

XLIII - Capacidade máxima de CPU;

XLIV - Capacidade máxima de Memória;

XLV - Capacidade máxima de tabelas de sessões;

XLVI - Capacidade máxima de configurações;

XLVII - HA Status;

XLVIII - Aumento de latência.

XLIX - Dashboard contendo informações relativas ao SD-WAN contendo:

L - Saúde das aplicações;

LI - Aplicações mais impactadas;

LII - Saúde dos links;

LIII - Lista de piores links.

LIV - Deve apresentar lista dos dispositivos impactados pelos CVEs.

LV - Análise de causas prováveis relativas a alta de processamento.

LVI - O gerenciamento do ambiente deve permitir, a partir de um ponto único, gerenciar firewalls físicos, firewalls virtualizados e soluções de SASE. Caso não seja possível gerenciar a partir de um ponto único, deverá ser entregue soluções terceiras que permitam essa consolidação.

LVII - A central de gerenciamento, tal qual os dispositivos por ela gerenciados, deve permitir lidar com objetos dinâmicos, permitindo e estando apta a agrupar endereços IPs para serem utilizados em políticas de segurança.

LVIII - A central de gerenciamento, tal qual os dispositivos por ela gerenciados, deve permitir lidar com usuários dinâmicos, permitindo o seu agrupamento em objeto dinâmico para serem utilizados em políticas de segurança.

LIX - Deverá suportar e permitir o agrupamento de configurações baseados em snippets para simplificar e permitir a reusabilidade de configurações, a fim de otimizar o tempo dos analistas no tocante ao gerenciamento dos dispositivos.

LX - Deve permitir a automação e a gerência da plataforma via REST API.

LXI - Deverá suportar e permitir a configuração de envio de logs dos dispositivos gerenciados para serviços de armazenamento externos.

LXII - A central de gerenciamento deverá suportar também a criação, configuração e operabilidade de dispositivos SD-WAN.

LXIII - Deverá suportar a criação automatizada de VPNs sem custos extras.

LXIV - A ferramenta deverá possuir capacidade de análise de otimização de políticas ou "Controle de qualidade de políticas com o objetivo de otimização das políticas de segurança", facilitando assim a manutenção do ambiente.

LXV - Deverá manter em tempo real as estatísticas de uso de políticas de segurança, permitindo a contagem de dias em que a política de segurança não é utilizada.

LXVI - A central de gerenciamento deverá mostrar as estatísticas de políticas de segurança não usadas e também que nunca receberam qualquer tipo de tráfego.

LXVII - A central de gerenciamento deverá mostrar as estatísticas de objetos nunca utilizados.

LXVIII - A solução deverá permitir o envio de relatórios agendados.

LXIX - A solução deverá permitir a criação de dashboards customizados.

LXX - A central de gerenciamento deverá ser capaz de gerenciar todas as funcionalidades de segurança dos dispositivos por ela gerenciados de maneira unificada para:

LXXI - Segurança para Internet das Coisas (IoT);

LXXII - Prevenção de Perda de Dados (DLP);

LXXIII - Segurança de aplicações SaaS;

LXXIV - Segurança para tráfego de DNS criptografado ou não;

LXXV - Prevenção contra ameaças avançadas tais como 0-day e APT;

LXXVI - Filtragem de URLs.

LXXVII - A plataforma de segurança deverá possuir mecanismos de avaliação de boas práticas por meio de análise das configurações atuais.

LXXVIII - Deve mostrar o estado atual da solução e a adoção de práticas recomendadas de segurança com sugestões de adequações específicas alinhadas com práticas recomendadas.

LXXIX - Deve mostrar onde melhorar a postura de segurança e definir uma linha de base para comparação posterior, fornecendo links para documentação técnica que mostram como configurar as recomendações.

LXXX - Os mecanismos de avaliação de gerenciamento devem garantir e estar licenciados para criar uma visão com base em frameworks de segurança como CIS (Critical Security Controls) e NIST Security Controls (National Institute of Standards and Technology) sobre as configurações atuais da solução, identificando os riscos e fornecendo recomendações. Exemplo: a solução deverá apontar quais são as configurações que deverão ser ajustadas e indicar local com exemplo de configuração a ser realizada para melhorar a adoção e elevar o grau de segurança.

4.4. **ITEM 03: SERVIÇO DE SUPORTE TÉCNICO ESPECIALIZADO DAS SOLUÇÕES DE SEGURANÇA**

4.4.1. A CONTRATADA deverá disponibilizar uma equipe de pessoas tecnicamente capacitadas, as quais serão responsáveis pelo suporte e manutenção das soluções durante todo o contrato de forma remota.

4.4.2. A equipe deverá estar disponível em regime 24 horas, 7 dias na semana e 365 dias ao ano.

4.4.3. Responsabilidades e atividades da Equipe:

4.4.4. Realizar todos os serviços de suporte e manutenção da solução quando solicitado pela CONTRATANTE.

4.4.5. Realizar o atendimento de tickets/chamados abertos pela contratante no sistema da CONTRATADA quando solicitado pela CONTRATANTE.

4.4.6. Realizar a interface entre as necessidades da contratante e os profissionais do fabricante por executar as atividades, em caso de necessidade de intervenção do fabricante em soluções de problemas.

4.4.7. A CONTRATADA deverá disponibilizar ferramenta de acompanhamento de chamados, de sua propriedade e de sua responsabilidade, que atendam aos seguintes requisitos:

4.4.8. O acesso às informações deverá ser protegido por senha e conexão segura ou outro método equivalente;

4.4.9. A contratante deverá ter acesso à ferramenta via interface WEB através da internet;

4.4.10. A ferramenta deverá manter identificação do projeto ou demanda, data e hora de abertura do chamado, início e término do atendimento, identificação e resolução do escopo, documentação da solução, status, recursos alocados e outras informações pertinentes;

4.4.11. A ferramenta deverá ser capaz de exportar seus dados em formato .csv;

4.4.12. A ferramenta deverá ser capaz de permitir a emissão de relatórios diários e/ou mensais para o controle de todas as solicitações abertas e encaminhadas pela contratante;

4.4.13. A ferramenta deverá ser capaz de gerir e garantir que os níveis de serviços de atendimento sejam monitorados, de forma que o tempo de atendimento de uma solicitação comece a ser contado a partir do envio da mesma pelo usuário solicitante e seja finalizado no momento de fechamento da solicitação no sistema.

4.4.14. **DA GLOSA POR DESCUMPRIMENTO DE SLA**

4.4.14.1. Os pagamentos mensais estarão condicionados ao Índice de Conformidade Mensal (ICM). O descumprimento dos níveis de serviço pactuados (Tempo de Resposta e Tempo de Solução) implicará em glosas sobre o valor da fatura mensal, conforme as tabelas abaixo:

4.4.14.2. O ICM é calculado pela razão entre os chamados atendidos dentro do prazo e o total de chamados abertos no mês: (ICM = (Chamados em conformidade / Total de chamados) x 100). Glosas por ICM (Disponibilidade e Desempenho Geral).

Índice de Conformidade Mensal (ICM)	**Impacto Financeiro (Glosa)**
95% a 100% (Meta Esperada)	Pagamento Integral (0% de desconto)
90% a 94,9%	Desconto de 2% sobre a fatura mensal

Índice de Conformidade Mensal (ICM)	Impacto Financeiro (Glosa)
85% a 89,9%	Desconto de 5% sobre a fatura mensal
80% a 84,9%	Desconto de 10% sobre a fatura mensal
Abaixo de 80%	Desconto de 15% + Abertura de Processo Administrativo

4.5. **ITEM 04: SERVIÇO DE IMPLEMENTAÇÃO DA SOLUÇÃO DE PROTEÇÃO DE PERÍMETRO**

4.5.1. Os serviços de instalação e configuração das soluções serão supervisionados pela contratante, através de funcionário (os) designado (s) para esta atividade, preliminarmente ao início da execução, durante a execução até o término da execução da instalação e ser acompanhada por gerente de projetos da CONTRATADA visando atender os prazos definidos e suas entrega de todo lote.

4.5.2. A instalação e configuração das soluções deverá ser realizada pela equipe da própria CONTRATADA.

4.5.3. A instalação e configuração da solução não poderá ocorrer por empresa, equipe ou profissional diferente da CONTRATADA neste processo.

4.5.4. A instalação e configuração contempla toda parte de hardware e software conforme item e arquitetura da solução Segurança para Defesa Cibernética.

4.5.5. Entende-se como instalação e configuração, conferência física dos itens, instalação física de hardware e software adquiridos, energização em estrutura pré-existente e ativação dos equipamentos adquiridos pela contratante.

4.5.6. A CONTRATADA executará os serviços sem qualquer interferência no funcionamento regular das atividades normalmente realizadas pela contratante, garantindo a continuidade dos serviços, ou seja, não poderá haver interrupção não programada do serviço de dados atual para a entrada do novo serviço. Desta forma, executará serviços em finais de semana, feriados e horário noturno, sempre que houver necessidade para atendimento das condições expostas pela contratante nesta especificação;

4.5.7. Todas as instalações e configurações serão realizadas em conformidade com a recomendação do fabricante do equipamento e os requisitos fornecidos pela contratante para o ambiente em questão;

4.5.8. Instalação física em rack padrão 19” disponibilizado pelo contratante;

4.5.9. Instalação lógica em ambiente virtual da contratante e/ou em nuvem do fabricante;

4.5.10. Ao término da instalação e configuração poderá ser considerado uma sessão de perguntas e respostas no local, com o objetivo de ser abordado os pontos principais e de funcionalidades chaves dos produtos instalados.

4.5.11. A CONTRATADA deverá seguir sua metodologia própria no processo de instalação e as melhores práticas indicadas pelo fabricante.

4.5.12. A CONTRATADA deverá responsabilizar-se pela conformidade e qualidade dos serviços e bens, bem como de cada material, matéria-prima ou componente individualmente considerado, mesmo que não sejam de sua fabricação, garantindo seu perfeito desempenho;

4.6. **ITEM 05: SERVIÇO DE TREINAMENTO TÉCNICO**

4.6.1. A CONTRATADA deverá fornecer serviço de treinamento técnico voltado à administração da solução de Firewall de Próxima Geração (NGFW) objeto desta contratação, observando, no mínimo, as seguintes características:

4.6.2. **CARACTERÍSTICAS GERAIS**

4.6.2.1. **Carga horária e público-alvo**

4.6.2.2. O treinamento deverá possuir carga horária mínima de 20 (vinte) horas.

4.6.2.3. O treinamento deverá ser destinado a até 5 (cinco) participantes indicados pelo CONTRATANTE.

4.6.2.4. A turma deverá ser exclusiva do CONTRATANTE, não sendo admitida a participação de profissionais de outros clientes.

4.6.3. **Modalidade do treinamento**

4.6.3.1. O treinamento deverá ser ministrado exclusivamente na modalidade remota, em formato online e síncrono (ao vivo).

4.6.3.2. A CONTRATADA deverá disponibilizar plataforma de videoconferência adequada, com recursos de compartilhamento de tela, quadro virtual e interação por voz e chat.

4.6.3.3. O treinamento deverá ser integralmente gravado pela CONTRATADA, sendo o(s) arquivo(s) de gravação disponibilizado(s) ao CONTRATANTE em até 5 (cinco) dias úteis após a conclusão do treinamento, em formato digital acessível (ex.: MP4 ou equivalente).

4.6.3.4. As gravações deverão permanecer disponíveis ao CONTRATANTE por, no mínimo, 90 (noventa) dias, seja por link de download ou ambiente de compartilhamento definido pela CONTRATADA e aceito pelo CONTRATANTE.

4.6.4. **Idioma e material didático**

4.6.4.1. O treinamento deverá ser ministrado em língua portuguesa.

4.6.4.2. A CONTRATADA deverá fornecer material didático em formato eletrônico (slides, apostila ou equivalente), contemplando, no mínimo, o conteúdo apresentado durante o treinamento.

4.6.4.3. Quando utilizados materiais em idioma estrangeiro, o instrutor deverá realizar a devida contextualização e explicação em português.

4.6.5. **Instrutor**

4.6.5.1. A CONTRATADA deverá disponibilizar instrutor que atenda, no mínimo, aos seguintes requisitos:

4.6.5.2. Experiência comprovada em implantação e administração de NGFW do mesmo fabricante da solução ofertada.

4.6.5.3. Certificação técnica relevante do fabricante do firewall ou equivalente, quando aplicável.

4.6.5.4. Experiência prévia em capacitações ou treinamentos técnicos na área de segurança de redes.

4.6.6. **Metodologia e abordagem**

4.6.7. O treinamento deverá combinar aulas expositivas e demonstrações práticas, preferencialmente utilizando ambiente de laboratório ou ambiente de demonstração do próprio firewall proposto.

4.6.8. Sempre que possível, deverão ser apresentados exemplos práticos relacionados ao ambiente típico do CONTRATANTE, incluindo boas práticas de configuração, operação e troubleshooting.

4.6.9. **Planejamento e controle**

4.6.9.1. A CONTRATADA deverá apresentar, previamente ao início do curso, plano de aulas ou cronograma detalhado, contendo a distribuição dos tópicos ao longo das 20 (vinte) horas de treinamento.

4.6.9.2. Deverá ser mantida lista de presença dos participantes, a ser encaminhada ao CONTRATANTE ao término do treinamento.

4.6.9.3. A CONTRATADA deverá aplicar avaliação de satisfação ao final do treinamento, consolidando os resultados em relatório a ser enviado ao CONTRATANTE.

4.6.10. **Certificação de participação**

4.6.10.1. Ao final do treinamento, a CONTRATADA deverá emitir certificado de conclusão individual para cada participante que tenha cumprido a carga horária mínima definida, contendo: nome do participante, nome do local de trabalho do participante, nome do curso, carga horária, data(s) de realização, nome do instrutor, razão social e CNPJ da CONTRATADA.

4.6.11. **EMENTA**

4.6.11.1. A ementa mínima do treinamento em administração de firewall NGFW deverá contemplar, no mínimo, os seguintes tópicos:

4.6.12. **Introdução à plataforma de Firewall NGFW**

4.6.12.1. Conceitos de segurança de perímetro e de borda;

4.6.12.2. Arquitetura da solução de NGFW proposta;

4.6.12.3. Componentes principais do sistema (appliance, console de gerenciamento, serviços em nuvem, etc.).

4.6.13. **Interfaces, zonas e roteamento**

4.6.13.1. Configuração de interfaces físicas e lógicas;

4.6.13.2. Criação e utilização de zonas de segurança;

4.6.13.3. Roteamento estático e, quando aplicável, dinâmico;

4.6.13.4. Modos de operação do firewall (Camada 2, Camada 3, virtual wire ou equivalente).

4.6.14. **Objetos e políticas de segurança**

4.6.14.1. Criação e gestão de objetos de rede (endereços IP, ranges, FQDN, grupos);

4.6.14.2. Criação e gestão de objetos de serviço (portas, protocolos, grupos de serviços);

4.6.14.3. Boas práticas para organização e reutilização de objetos;

4.6.14.4. Criação, ordenação e boas práticas de políticas de segurança (regras de firewall).

4.6.15. **Controle de aplicações e usuários**

4.6.15.1. Conceito de identificação de aplicações (App-ID ou equivalente);

4.6.15.2. Criação de políticas baseadas em aplicações e categorias de aplicações;

4.6.15.3. Integração com serviços de diretório (ex.: Active Directory / LDAP) para controle por usuário e grupos;

4.6.15.4. Políticas de acesso baseadas em usuário, grupo, aplicação e zona.

4.6.16. **NAT – Tradução de Endereços de Rede**

4.6.16.1. Conceitos de NAT de origem e NAT de destino;

4.6.16.2. NAT estático, dinâmico e PAT (quando suportado);

4.6.16.3. Boas práticas de configuração de NAT em ambientes corporativos;

4.6.16.4. Troubleshooting básico de problemas de NAT.

4.6.17. **Perfis de segurança e prevenção de ameaças**

4.6.17.1. Configuração e uso de perfis de IPS, Antivírus, Anti-Spyware e proteção contra ameaças avançadas;

4.6.17.2. Configuração de filtro de URLs e segurança de DNS, quando disponíveis;

4.6.17.3. Conceitos de sandboxing / análise de malware, quando aplicável à solução;

4.6.17.4. Criação de políticas de segurança combinando firewall + perfis de segurança.

4.6.18. **Inspeção de tráfego criptografado (SSL/TLS)**

4.6.18.1. Conceitos de inspeção SSL/TLS (outbound e inbound);

4.6.18.2. Importação/geração de certificados para inspeção;

4.6.18.3. Criação de regras de exceção e boas práticas para minimizar impacto em usuários e aplicações.

4.6.19. **VPN – Acesso Remoto e Interconexão de Redes**

4.6.19.1. Conceitos de VPN Site-to-Site e Client-to-Site;

4.6.19.2. Configuração básica de túneis IPSec (parâmetros principais, fases 1 e 2);

4.6.19.3. Configuração básica de VPN SSL para acesso remoto de usuários;

4.6.19.4. Aplicação de políticas de segurança para tráfego dentro dos túneis de VPN.

4.6.20. **Alta disponibilidade (HA) e resiliência**

4.6.20.1. Conceitos de HA ativo/passivo e, quando aplicável, ativo/ativo;

4.6.20.2. Sincronismo de configuração e sessões;

4.6.20.3. Testes de failover e boas práticas de operação em HA.

4.6.21. **Monitoramento, logs e troubleshooting**

4.6.21.1. Utilização da console de monitoramento;

4.6.21.2. Consulta e interpretação de logs de tráfego, ameaças e sistema;

4.6.21.3. Geração de relatórios básicos;

4.6.21.4. Fluxo recomendado de troubleshooting para incidentes de conectividade e segurança.

4.6.22. **Gerenciamento de configuração e boas práticas operacionais**

4.6.22.1. Backup e restore de configuração;

4.6.22.2. Versionamento e comparação de mudanças de política;

4.6.22.3. Boas práticas de revisão periódica de regras e objetos;

4.6.22.4. Boas práticas de atualização de software e assinaturas de segurança.

5. **ACORDO DE NÍVEL DE SERVIÇO**

5.1. Um acordo de nível de serviço define os índices a serem atingidos para o cumprimento do conjunto de compromissos acordados entre CONTRATANTE e CONTRATADA;

5.2. Tais índices serão medidos e aplicados aos serviços contratados pelo CONTRATANTE e prestados pela CONTRATADA;

5.3. Semestralmente os dados de Nível de Serviço deverão ser apresentados ao CONTRATANTE, incluindo informações sobre ações e necessidades para a correção de desvios, visando atingir, manter e melhorar os níveis desejados.

5.4. A abrangência e o nível de detalhamento dos demonstrativos serão definidos conforme as necessidades identificadas pela CONTRATADA, podendo sofrer alterações ao longo do tempo, as quais serão encaminhadas ao CONTRATANTE via os processos de Gerenciamento do Nível de Serviço e de Mudanças do mesmo;

5.5. Para a medição dos índices de nível de serviços, serão considerados os seguintes conceitos:

5.6. Requisição: solicitação do CONTRATANTE para intervenção no ambiente gerenciado e previsto no escopo desta proposta. Cada requisição será identificada unicamente por meio de um código e será classificada conforme seu nível de severidade no momento da sua comunicação a CONTRATADA;

5.7. Severidade: nível de prioridade/emergência atribuído ou solicitado para a realização de um atendimento a uma requisição do CONTRATANTE ou do ambiente, conforme critérios descritos a seguir. Solicitações de alteração do nível de severidade

poderão ser submetidas à CONTRATADA e, quando julgadas pertinentes pela mesma, serão prontamente atendidas.

5.7.1. SEVERIDADE CRÍTICO: A Plataforma de Segurança para Defesa Cibernética está totalmente parada ou inoperante;

5.7.2. SEVERIDADE ALTO: A Plataforma de Segurança para Defesa Cibernética está ativa, mas com inoperância da maioria de suas funcionalidades, causando um impacto negativo no ambiente de produção;

5.7.3. SEVERIDADE MÉDIO: A Plataforma de Segurança para Defesa Cibernética está operativa, mas suas funcionalidades são executadas com restrições;

5.7.4. SEVERIDADE BAIXO: A Plataforma de Segurança para Defesa Cibernética está operativa e a falha não compromete suas funcionalidades ou questões não tratadas pela documentação;

5.7.5. SEVERIDADE AGENDADO: O atendimento está relacionado apenas a esclarecimentos de dúvidas ou necessidade de informações da Plataforma de Segurança para Defesa Cibernética;

5.8. A cada chamado de suporte categorizado como Severidade Crítico ou Alto, o recurso humano designado para fornecer assistência na CONTRATADA deverá ser notificado e iniciará o auxílio na condução do processo internamente junto a CONTRATANTE;

5.9. Referente aos chamados categorizados como Severidade Crítico ou Alto, cabe a CONTRATADA dar início, junto ao CONTRATANTE, às providências que serão adotadas para a solução do chamado;

5.10. Para os chamados de suporte categorizado como Severidade Crítico ou Alto, o atendimento não pode ser interrompido até o completo restabelecimento de todas as funções do sistema paralisado (indisponível), mesmo que para isso tenham que se estender por períodos noturnos e dias não úteis (sábados, domingos e feriados), de acordo com a disponibilidade do CONTRATANTE.

5.11. Tempo de Notificação: O tempo máximo para a NOTIFICAÇÃO da CONTRATANTE pela CONTRATADA, conforme a severidade de incidentes Críticos e Altos: (ANEXO I).

5.12. Tempo de Atendimento (Resposta): O tempo máximo para INÍCIO de um ATENDIMENTO pela CONTRATADA após a notificação, conforme a severidade do incidentes Críticos e Altos: (ANEXO I).

5.13. Não se encaixam nos prazos descritos nos itens referentes aos níveis de criticidade, problemas cuja solução dependa de correção de falhas (bugs) ou da liberação de novas versões e patches de correção, desde que comprovados pelo fabricante da solução;

5.14. Os chamados escalados para o fabricante e em tratamento por aquele não se encaixam nos prazos descritos.

5.15. Serão excluídos do cálculo, os tempos de paralisação, decorrentes dos seguintes eventos:

5.16. anela de manutenção acordada entre CONTRATADA e CONTRATANTE;

5.17. Falhas na infraestrutura provisionada pelo CONTRATANTE decorrentes de eventos como:

5.17.1. Perda de conexão com a rede corporativa;

5.17.2. Acidentes operacionais internos;

5.17.3. Falhas elétricas que prejudiquem o funcionamento da solução;

5.17.4. Falhas de Arquitetura do ambiente que impeçam o funcionamento da solução;

5.17.5. Falta de energia elétrica;

5.17.6. Incêndios, vazamentos e outros intempéries que envolvam o ambiente físico da CONTRATANTE;

5.18. Entende-se que haverá uma fase inicial de transição e adequação dos processos de atendimento por parte da CONTRATADA. Sendo assim, os níveis de serviço (SLAs) não serão exigidos contratualmente durante os primeiros 60 (sessenta) dias úteis de duração do contrato. Os índices deverão ser apurados e apresentados ao CONTRATANTE, no entanto, a CONTRATADA não estará sujeita a penalidades pelo seu descumprimento durante este período.

6. APRESENTAÇÃO DA PROPOSTA

6.1. A proposta de preço apresentada pela proponente, de forma clara e detalhada, deverá seguir a forma definida em Edital.

6.2. A apresentação da proposta implicará plena aceitação, por parte do proponente, das condições estabelecidas neste Termo de Demanda.

7. QUALIFICAÇÃO TÉCNICA

7.1. Para habilitação no presente Chamamento Público, a participante deverá apresentar atestado(s) de capacidade técnica emitido(s) por pessoa jurídica de direito público ou privado, que comprove(m) a execução de serviços ou fornecimento de bens de natureza semelhante ao objeto deste chamamento.

7.1.1. O(s) atestado(s) deverá(ão) comprovar que a participante executou, de forma satisfatória, serviços ou forneceu bens compatíveis em características, quantidades e prazos com aqueles previstos no Edital e no Termo de Demanda.

7.1.2. O(s) atestado(s) deverá(ão) conter, no mínimo, as seguintes informações:

I - Nome da contratante;

II - Descrição detalhada do serviço ou bem fornecido;

III - Prazo de execução/fornecimento;

IV - Local de execução/fornecimento;

V - Declaração expressa de que o serviço ou fornecimento foi realizado de forma satisfatória;

VI - Assinatura do responsável pela entidade emitente.

7.1.3. A ausência ou a insuficiência de comprovação técnica poderá implicar na inabilitação da participante".

7.1.4. **SERVIÇO DE INSTALAÇÃO**

7.1.4.1. A CONTRATADA deverá ter em seu quadro de funcionários, profissional com certificação nível Profissional e/ou Engenheiro que será responsável técnico pela instalação e configuração lógica do equipamento.

7.1.4.2. Não será necessária a presença física do responsável técnico, para instalação física do equipamento, porém a CONTRATADA deverá disponibilizar alguém de seu quadro técnico para efetuar as devidas atividades.

7.1.4.3. Apesar de não ser necessário a presença física do responsável técnico, ele deverá acompanhar 100% das atividades referentes à instalação física e lógica da solução.

7.1.5. **SERVIÇO DE SUPORTE**

7.1.5.1. A CONTRATADA deverá ter em seu quadro de funcionários com certificação nível Profissional e/ou Engenheiro que deverá ser escalado para atendimento de chamados em caso de problemas de severidade Alta e Crítica.

7.1.5.2. A CONTRATADA será responsável pela comunicação com o fabricante da solução contratada em caso de problemas que exijam esta necessidade.

7.1.6. **SERVIÇO DE TREINAMENTO**

7.1.6.1. A CONTRATADA deverá ter em seu quadro de funcionários, profissional com certificação nível Profissional e/ou Engenheiro que será responsável técnico pelo treinamento e repasse de conhecimento.

8. **CRITÉRIOS DE JULGAMENTO DAS PROPOSTAS**

8.1. Será considerada como mais vantajosa para o HCB e, consequentemente, declarada vencedora a proposta que, satisfeitas todas as condições exigidas do Chamamento Público, apresentar o **MENOR PREÇO POR LOTE ÚNICO.**

8.2. A busca por lotes justifica-se por conta de que o fornecimento de itens por meio de CONTRATADAS distintas trariam relevantes riscos ao projeto, como a necessidade contínua de comunicação entre os diferentes fornecedores o que, historicamente, não ocorre com fluidez, muito menos de forma satisfatória, sendo a parte mais lesada o CONTRATANTE. Além do mais, sempre existe a necessidade de ocorrer perfeita integração técnica entre os itens do objeto, e o fornecimento parcial dos itens por diferentes fornecedores traria não apenas maior complexidade, mas maiores custos de integração e riscos de uma execução inadequada.

8.3. Serão desclassificadas as propostas que não atendam às exigências formais ou técnicas deste Termo de Demanda.

8.4. A participação no processo de contratação implica aceitação integral e irretratável do Termo de Demanda e outros documentos disponibilizados aos interessados pelo ICIPE/HCB, e observará a legislação aplicável.

8.5. Não poderão participar da Seleção de Fornecedores nem contratar com o ICIPE/HCB:

8.6. Dirigente ou empregado do ICIPE;

8.7. Servidor público detentor de cargo em comissão ou função comissionada ou gratificada, no âmbito da Secretaria de Estado de Saúde, que possa ter conflito de interesse com a entidade;

8.8. Pessoas jurídicas nas quais as pessoas elencadas nos incisos I a II tenha participação societária.

8.9. Entende-se por participação societária a participação individual direta como acionista ou sócio, nos 12 (doze) meses anteriores, respectivamente, superior a 0,3% (três décimos por cento) no capital social da sociedade por ações ou outras modalidades que admitam acionista ou superior a 2% (dois por cento) no capital social de sociedade limitada ou outras modalidades empresariais.

9. **LOCAL DE EXECUÇÃO DOS SERVIÇOS**

9.1. Os serviços serão realizados, sempre que for possível, remotamente. Caso contrário o serviço deverá ser prestado nos locais da Contratada no Hospital da Criança de Brasília - HCB, situado no AENW 3, Lote A - Bairro Noroeste - CEP 70.684-831 – Brasília-DF, devendo ser respeitado o horário de atendimento administrativo que é das 08:00-12:00 às 14:00-17:00 de segunda-feira a sexta-feira.

10. **CONTRATO E INÍCIO DA PRESTAÇÃO DOS SERVIÇOS**

10.1. A vigência do Contrato será de 36 (trinta e seis) meses, a contar da data de assinatura, podendo ser prorrogados sucessivamente por meio de Termo Aditivo mediante acordo entre as partes interessadas, observado o limite máximo de 10 (dez) anos, nos termos do Regulamento de Compras e Contratações do Icipe.

10.2. O início da prestação dos serviços dar-se-á em até 30 (trinta) dias corridos, contados da data de assinatura do instrumento contratual, mediante o envio da ordem de serviço emitida pela Contratante.

10.3. Para o reajuste dos preços contratados deverá ser observada a legislação vigente, bem como o interregno de, no mínimo, 12 (doze) meses contados a partir da assinatura do instrumento contratual.

10.4. Prazo de Implantação: Máximo de 50 dias consecutivos para entrega, instalação, migração e configuração da solução.

11. **CONDIÇÕES DE PAGAMENTO**

11.1. O serviço a ser contratado é prestado de forma contínua com pagamento em parcelas mensais mediante ateste das faturas de prestação do serviço.

11.2. Os pagamentos à empresa Contratada pela prestação dos serviços serão feitos nos termos previstos no Instrumento Contratual, consoante os preços estabelecidos e demais disposições deste Termo de Demanda, no prazo máximo de 30 (trinta) dias após o recebimento do serviço a contento e emissão do documento fiscal válido em nome do ICIPE/HCB, com todos os campos preenchidos discriminando valor unitário e total do item, sem rasuras, devidamente atestados pelo funcionário responsável pelo recebimento do serviço executado, constando, ainda, dados bancário onde deseja receber seu crédito.

11.3. A Contratada deverá encaminhar ao fiscal do contrato, nota fiscal contendo a descrição dos serviços realizados no mês anterior, até o 5º dia útil do mês subsequente à realização dos procedimentos. Após a conferência pelo fiscal do contrato, o documento será encaminhado ao setor responsável pelo pagamento.

11.4. Não haverá, sob hipótese alguma, pagamento antecipado.

12. **OBRIGAÇÕES DA CONTRATANTE**

É dever do CONTRATANTE:

12.1. Atestar a efetiva realização dos serviços e fiscalizar o cumprimento do contrato, podendo, a qualquer momento, solicitar relatórios, informações e esclarecimentos que julgar cabíveis, bem como determinar que a CONTRATADA sane as falhas ocorridas que sejam de sua competência e/ou responsabilidade.

12.2. Permitir o acesso dos representantes ou profissionais da CONTRATADA ao local de prestação dos serviços, desde que devidamente identificados, proporcionando todas as facilidades para que a empresa CONTRATADA possa desempenhar, por meio dos profissionais, os serviços contratados.

12.3. Prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATADA.

12.4. Promover o acompanhamento e fiscalização dos serviços sob os aspectos qualitativos, comunicando à CONTRATADA toda e qualquer ocorrência relacionada com a sua execução.

12.5. Indicar o gestor e/ou o fiscal para acompanhamento da execução contratual.

12.6. Atestar a execução do objeto do contrato, por meio do fiscal designado.

12.7. Rejeitar os serviços executados em desacordo com as obrigações assumidas pela empresa CONTRATADA, exigindo sua correção, no prazo previsto, sob pena de suspensão e/ou multa do contrato, ressalvadas os casos fortuitos ou de força maior, devidamente justificado e aceito pela CONTRATANTE.

12.8. Relacionar-se com a CONTRATADA através de pessoa por ela credenciada (preposto).

12.9. Comunicar à CONTRATADA qualquer descumprimento de obrigações e responsabilidades previstas neste Termo de Demanda e no respectivo contrato, determinando as medidas necessárias à sua imediata regularização.

12.10. Aplicar, por atraso ou inexecução parcial ou total dos serviços, as cláusulas penais contratuais previstas no contrato.

12.11. Elaborar o Acordo de Nível de Serviço - ANS para as atividades consideradas críticos.

12.12. Realizar acompanhamento do SLA, com classificação do atingimento das metas, segundo critérios classificatórios dos níveis de serviços prestados definidos conforme ANEXO I do Termo de Demanda.

12.13. Efetuar o pagamento à CONTRATADA de acordo com as condições estabelecidas no contrato.

13. **OBRIGAÇÕES DA CONTRATADA**

É dever da CONTRATADA:

13.1. Manter durante toda a execução contratual, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas no edital;

13.2. Prestar o serviço conforme especificações técnicas;

13.3. Submeter previamente, por escrito, ao CONTRATANTE para verificação, quaisquer mudanças nos métodos executivos que fujam às especificações descritas;

13.4. Indicar um gerente técnico do projeto, responsável pelo planejamento e acompanhamento de todas as atividades referentes à implantação e migração da solução contratada.

13.5. Realizar o acesso ao ambiente computacional do CONTRATANTE somente mediante autorização prévia e permitindo o acompanhamento pela equipe do CONTRATANTE se assim ela desejar e pelo tempo que julgar necessário;

13.6. Prover todos os meios necessários para garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações do CONTRATANTE hospedadas na solução contratada.

13.7. Responsabilizar-se técnica e administrativamente pelo objeto contratado, não sendo aceito, sob qualquer pretexto, a transferência de responsabilidade a terceiros, sejam fabricantes, técnicos ou quaisquer outros.

13.8. Propiciar a seus técnicos todas as condições necessárias à execução dos serviços.

13.9. Manter atualizado o seu cadastro e do seu responsável legal junto ao HCB, notificando oficialmente qualquer mudança de endereço, telefone, alteração no quadro de profissionais ou qualquer informação que seja útil à adequada manutenção do presente instrumento.

13.10. Prestar as informações e os esclarecimentos que venham a ser solicitados pelo CONTRATANTE, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidas no prazo de 24 (vinte e quatro) horas.

13.11. Assinar o Termo de Confidencialidade (ANEXO II) deste documento, que se estenderá aos seus empregados e prestadores de serviços, estabelecendo o compromisso de não divulgar nenhum assunto tratado na prestação de serviços objeto

deste documento.

13.12. Informar um e-mail e telefone ou sistema de abertura de chamado/ticket para que o CONTRATANTE possa acionar o suporte ao sistema e/ou equipamento.

13.13. Emitir relatório mensal contendo a quantidade de tickets atendimentos no período e destes tickets resolvidos, quantos estavam em acordo com o prazo SLA definido.

13.14. Responder pelas despesas relativas a encargos trabalhistas, seguro de acidentes, impostos, contribuições previdenciárias e quaisquer outras que forem devidas e referentes aos serviços executados por seus empregados, uma vez que eles não têm nenhum vínculo empregatício com o CONTRATANTE.

13.15. Não vincular o pagamento de salários e demais vantagens de seus funcionários aos pagamentos das Notas Fiscais/Faturas pelo CONTRATANTE.

13.16. Responsabilizar-se civil e criminalmente por danos ou prejuízos que vier a causar ao HCB, propriedade ou pessoa de terceiros, em decorrência do fornecimento do objeto do presente Termo de Demanda, correndo por suas expensas, sem quaisquer ônus para o HCB, ressarcimento ou indenizações que tais danos ou prejuízos possam causar.

13.17. Manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse do CONTRATANTE ou de terceiros de que tomar conhecimento em razão da execução do objeto deste Termo de Demanda, devendo orientar seus empregados nesse sentido.

13.18. Arcar com o pagamento de eventuais multas aplicadas por quaisquer autoridades federais, estaduais e municipais, em consequência de fato a ela imputável e relacionada com a contratação.

13.19. Arcar com todos os prejuízos advindos de perdas e danos. Incluindo despesas judiciais e honorários advocatícios resultantes de ações judiciais, a que o CONTRATANTE for compelida a responder em decorrência da contratação.

13.20. Manter seus empregados, quando nas dependências do CONTRATANTE, sujeitos às normas internas desta (segurança, disciplina).

13.21. Aceitar os acréscimos(s) ou supressão(ões) que se fizer(em) necessário(s), em até 25% (vinte e cinco por cento) do valor do objeto contratado, devendo as supressões acima deste limite, ser resultantes de acordo entre as partes.

14. **SUBCONTRATAÇÃO**

14.1. Não será permitida a subcontratação, cessão ou transferência parcial ou total do objeto deste contrato.

15. **DA GARANTIA**

15.1. A contratada prestará garantia no valor correspondente a 5% (cinco por cento) do valor do Contrato, conforme Art. 14 do Decreto Distrital nº 33.390/2011.

15.2. A garantia prestada pela Contratada será liberada ou restituída após a execução total do Contrato, devendo ser automaticamente prorrogada se houver aditivo contratual de prorrogação.

16. **SANÇÕES**

16.1. Em caso de descumprimento das condições estabelecidas neste instrumento, não veracidade das informações prestadas e/ou inexecução parcial ou total do objeto, a CONTRATADA estará sujeita às penalidades previstas em Edital, sendo garantida a prévia e ampla defesa.

17. **FISCALIZAÇÃO**

17.1. Os funcionários designados à fiscalização do contrato poderão recusar, sustar, mandar refazer ou fazer quaisquer falhas ou problemas inerentes ao fornecimento do serviço, que estejam em desacordo com o preestabelecido.

17.2. As comunicações necessárias serão feitas por intermédio do Fiscal do Contrato, indicado pela CONTRATANTE.

17.3. O HCB se reserva o direito, a qualquer momento durante a vigência do contrato, de aferir a solução contratada, realizando testes, auditorias por meio de ferramentas e recursos próprios ou empresas contratadas para este fim.

18. **APLICAÇÃO DA LGPD EM RELAÇÃO AO OBJETO**

18.1. Em conformidade com a LGPD, que assegura a privacidade e a segurança dos dados pessoais, especialmente nos termos do artigo 6º, a CONTRATADA deve manter absoluto sigilo sobre todos os dados e informações contidos em quaisquer documentos, mídias e equipamentos, bem como em seus meios de armazenamento, aos quais tenha acesso durante a execução dos serviços. É estritamente proibido divulgar, reproduzir ou utilizar tais dados e informações para qualquer finalidade, sob pena de sanções legais, independentemente da classificação de sigilo atribuída pelo Icipe/HCB.

18.2. O Icipe/HCB emitirá o Termo de Confidencialidade (ANEXO II), que contém a declaração de sigilo e o compromisso de conformidade com as normas de segurança vigentes na entidade. Este Termo deverá ser assinado pelo representante legal da CONTRATADA.

19. **ANEXOS**

ANEXO I: ACORDO DE NÍVEIS DE SERVIÇO (SLA)

ANEXO II: TERMO DE CONFIDENCIALIDADE

ANEXO I:

ACORDO DE NÍVEIS DE SERVIÇO (SLA)

Severidade	Descrição
Agendado	Esclarecimento de dúvidas ou similares.
Baixo	A Plataforma de Segurança para Defesa Cibernética opera sem impacto no negócio.
Médio	A Plataforma de Segurança para Defesa Cibernética opera com degradação de desempenho.
Alto	A Plataforma de Segurança para Defesa Cibernética opera com paralisação parcial.
Crítico	A Plataforma de Segurança para Defesa Cibernética inoperante ou paralisação total.

Tempo de Notificação:

Descrição	Meta para tempo de Notificação
Tempo máximo para notificação de eventos Críticos e Altos.	30 Minutos

Tempo de Atendimento (Resposta):

Severidade	Descrição	Meta para tempo de resposta	Penalidade por gravidade
Agendado	Esclarecimento de dúvidas ou similar.	32 horas	0,1% do valor mensal
Baixo	A Plataforma de Segurança para Defesa Cibernética opera sem impacto de negócio.	16 horas	0,1% do valor mensal
Médio	A Plataforma de Segurança para Defesa Cibernética opera com degradação de desempenho.	5 horas	0,1% do valor mensal
Alto	A Plataforma de Segurança para Defesa Cibernética opera com paralisação parcial.	3 horas	0,2% do valor mensal
Crítico	A Plataforma de Segurança para Defesa Cibernética inoperante ou paralisação total.	2 horas	0,5% do valor mensal

ANEXO II:

TERMO DE CONFIDENCIALIDADE

A empresa _____, por intermédio de seu representante legal _____, se compromete, por intermédio do presente TERMO DE CONFIDENCIALIDADE, a não divulgar sem autorização, quaisquer informações de propriedade do Icipe/HCB, em conformidade com as seguintes condições:

A empresa _____ reconhece que, em razão da sua prestação de serviços ao Icipe/HCB, conforme contrato nº _____, celebrado em ___/___/___, tem acesso a informações da CONTRATANTE., que devem ser conceituadas como sigilosas. Estas informações devem ser tratadas confidencialmente sob qualquer condição e não podem ser divulgadas sem a expressa e escrita autorização do representante legal do Icipe/HCB, signatário do contrato acima referido.

Serão consideradas como informação sigilosa, toda e qualquer informação escrita ou oral, revelada a outra parte, contendo ou não a expressão confidencial e/ou reservada. O TERMO informação abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, ativos de infraestrutura de rede, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades do Icipe/HCB e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao contrato, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do contrato celebrado entre as partes.

A CONTRATADA compromete-se a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do Contrato, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas informações, que se restringem estritamente ao cumprimento do Contrato.

A CONTRATADA compromete-se ao término do contrato ou rescisão do mesmo, após 30 dias em excluir os dados da CONTRATADA.

A CONTRATADA responsabiliza-se integralmente pelos atos de seus empregados, subcontratados ou de terceiros por ela indicados, praticados nas dependências do Icipe/HCB, ou mesmo fora delas, que venham a causar danos a esta ou a seus funcionários e servidores ou colocar em risco o patrimônio do Icipe/HCB, comprometendo-se a promover a substituição imediata daqueles que não corresponderem ao padrão de comportamento exigido.

O não cumprimento da obrigação do compromisso de sigilo, estabelecido neste Contrato, possibilitará a imediata rescisão do contrato firmado entre as partes, sem qualquer ônus para o Icipe/HCB. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos comprovadamente sofridos pelo Icipe/HCB, ou terceiro prejudicado, sem prejuízo das demais sanções legais cabíveis.

Brasília-DF, XXXXX de 2026.

Responsável legal da CONTRATADA

ANEXO II

Planilha de Formação de Custos

PLANILHA DE FORMAÇÃO DE CUSTOS							
Item	Descrição do Item / Serviço	Unidade	Quantidade Máxima Estimada	Valor Unitário Estimado (R$)	Valor Total Estimado (R$)	Composição de Custos	Observações

ANEXO III

Minuta do Contrato

(Será disponibilizado digitalmente à parte)

Documento assinado eletronicamente por **ALINE SILVA SANTOS - Matr. 0000272-5**, **Analista de Compras**, em 16/04/2026, às 15:23, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

Documento assinado eletronicamente por **RENATO DA SILVA - Matr.0000043-2**, **Coordenador(a) de Compras**, em 16/04/2026, às 16:06, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

A autenticidade do documento pode ser conferida no site: http://sei.df.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 verificador= **200502714** código CRC= **AF1F182A**.

*** MINUTA DE DOCUMENTO**

CONTRATO Nº XXX/20XX

CHAMAMENTO PÚBLICO Nº XXX/XXXX

CONTRATO DE PRESTAÇÃO DE SERVIÇOS, QUE CELEBRAM ENTRE SI O INSTITUTO DO CÂNCER INFANTIL E PEDIATRIA ESPECIALIZADA - ICIPE, GESTOR DO HOSPITAL DA CRIANÇA DE BRASÍLIA JOSÉ ALENCAR - HCB, E A EMPRESA XXXXXXXXX.

CONTRATANTE.

INSTITUTO DO CÂNCER INFANTIL E PEDIATRIA ESPECIALIZADA – ICIPE, pessoa jurídica de direito privado legalmente constituída, sem fins econômicos ou lucrativos, com sede no Setor Hoteleiro Sul (SHS), Complexo Brasil 21, Quadra 06, Conjunto A, Bloco A, Sala 501, Asa Sul, Brasília - DF, CEP 70.316-102, inscrito no CNPJ/MF sob o nº 10.942.995/0001-63 e qualificado como Organização Social pelo Decreto Distrital nº 46.525/2024, publicado no DODF de 14/11/2024, na qualidade de Gestor do **HOSPITAL DA CRIANÇA DE BRASÍLIA JOSÉ ALENCAR – HCB**, localizado na Área Especial Noroeste (AENW), nº 03, Lote A, Setor de Habitações Coletivas Noroeste (SHCNW), Brasília - DF, CEP 70.684-831, neste ato representado pela Diretora Executiva do Hospital da Criança de Brasília José Alencar, Sr.ª **xxxxxxxxxx**, brasileira, residente e domiciliada nesta Capital Federal, portadora do documento de identidade nº xxxxx e inscrita no CPF MF sob o nº xxx.xxx.xxx-xx, e pela Diretora de Práticas Assistenciais, Sra. **xxxxxxxxxx**, brasileira, residente e domiciliada nesta Capital Federal, portadora do documento de identidade nº xxxxx e inscrita no CPF MF sob o nº xxx.xxx.xxx-xx.

CONTRATADA.

XXXXXXX, pessoa jurídica de direito privado, inscrita no CNPJ sob o nº XXX, sediada na XXXXXXX, CEP XX.XXX-XXX, telefone (xx) xxxx-xxxx, e-mail xxxxxxxxxxx, neste ato representada pelo Sr. **xxxxxxxxxx**, brasileiro, portador do documento de identidade nº xxxxx SSP XX e inscrito no CPF MF sob nº xxx.xxx.xxx-xx, conforme Contrato Social, que confere ao qualificado poder para representá-la na assinatura do Contrato, daqui por diante designada simplesmente **CONTRATADA**.

As partes acima identificadas ajustaram, e por este instrumento celebram um **CONTRATO DE PRESTAÇÃO DE SERVIÇOS**, decorrente do **Chamamento Público nº XXX/20XX**, consoante às disposições do Regulamento de Compras e Contratações (RCC) do Icipe, aprovado pela **Resolução Icipe nº 51, de 31 de outubro de 2025,** e do **Processo SEI nº XXXXXX**, mediante as cláusulas e condições dispostas a seguir.

1. **CLÁUSULA PRIMEIRA – DO OBJETO**

1.1. O objeto do presente instrumento é a Contratação de empresa para o fornecimento de solução de segurança perimetral baseada em appliance de firewall de próxima geração (NGFW), com capacidade de inspeção profunda de pacotes, prevenção de intrusão (IPS), controle de aplicações, VPN, e funcionalidades avançadas de visibilidade e resposta, incluindo suporte técnico 24x7, atualizações de assinatura e hardware, e treinamento oficial para a equipe técnica do HCB, visando a proteção de rede e servidores, no âmbito do Hospital da Criança de Brasília José Alencar - HCB.

1.2. Vinculam-se a esta contratação e integram este instrumento para todos os fins, independentemente de transcrição:

a) Termo de Demanda, Anexo I do edital

b) Chamamento Público nº XXX/XXXX (XXXXXX), aqui denominado Edital;

c) A Proposta da CONTRATADA;

d) Eventuais anexos dos documentos supracitados.

2. **CLÁUSULA SEGUNDA – DA VIGÊNCIA**

2.1. A vigência do Contrato será de **36 (trinta e seis) meses**, a contar da data de assinatura, podendo ser prorrogados sucessivamente por meio de Termo Aditivo mediante acordo entre as partes interessadas, observado o limite máximo de 10 (dez) anos, nos termos do Regulamento de Compras e Contratações do Icipe.

2.2. O início da prestação dos serviços dar-se-á em **até 30 (trinta) dias corridos,** contados da data de assinatura do instrumento contratual, mediante o envio da ordem de serviço emitida pela CONTRATANTE.

2.3. O CONTRATADO não tem direito subjetivo à prorrogação contratual.

2.4. Nas eventuais prorrogações contratuais, os custos não renováveis já pagos ou amortizados ao longo do primeiro período de vigência da contratação deverão ser reduzidos ou eliminados como condição para a renovação

3. **CLÁUSULA TERCEIRA – DO LOCAL DE EXECUÇÃO DOS SERVIÇOS**

3.1. Os serviços serão realizados, sempre que for possível, remotamente. Caso contrário o serviço deverá ser prestado nos locais da Contratada no Hospital da Criança de Brasília - HCB, situado no AENW 3, Lote A - Bairro Noroeste - CEP 70.684-831 – Brasília-DF, devendo ser respeitado o horário de atendimento administrativo que é das 08:00-12:00 às 14:00-17:00 de segunda-feira a sexta-feira.

4. **CLÁUSULA QUARTA - DOS MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAIS**

4.1. Os serviços executados deverão estar de acordo com as especificações, quantificações e prazos contidos no Termo de Demanda e Edital, devendo ser sempre de boa qualidade, segundo os padrões definidos pelos órgãos de controle de qualidade e padronização do CONTRATANTE, atender as Normas Regulamentadoras, recomendações do fabricante bem como as recomendações dos órgãos fiscalizadores (VISA, ANVISA, MS, ABNT) e especialmente relacionados à área de saúde, no que couber.

4.2. O prazo para a entrega, instalação, migração e configuração da solução será de no máximo 50 (cinquenta) dias consecutivos, contados a partir do primeiro dia útil após a data da assinatura da Ordem de Serviço;

4.3. Caberá à área técnica do CONTRATANTE responsável pelo Contrato, emitir “aceite” do serviço executado, certificando-se que estes foram realizados dentro dos objetivos a que se destinam e estavam previstos em Termo de Demanda e no Edital.

4.4. O detalhamento quanto ao regime de execução contratual, os modelos de gestão e de execução, assim como o Acordo de Nível de Serviço e os prazos e condições de conclusão, prazos de entrega, especificações e condições de recebimento do objeto constam no Termo de Demanda.

5. **CLÁUSULA QUINTA – DA SUBCONTRATAÇÃO**

5.1. Não será permitida a subcontratação, cessão ou transferência parcial ou total do objeto deste contrato.

6. **CLÁUSULA SEXTA – DO PREÇO**

6.1. O valor total da contratação é de R$ XXXXXXXXXX, conforme tabela a seguir:

Nº do item no mapa de preços	Código	Descrição do Serviço	Apresentação	Quantidade Total	Marca/Fabricante	Valor Unitário (R$ XX)	Valor Total (R$ XX)
xx	xx	**Solução de Proteção de Perímetro do tipo Next Generation Firewall NGFW** - Solução de proteção de perímetro baseada em firewalls de próxima geração, responsável pela inspeção do tráfego em camadas 3 a 7, controle de aplicações, prevenção de intrusões, filtragem de URLs, proteção contra malware e estabelecimento de túneis VPN para 36 meses de licenciamento e suporte.	Unidades	2			
xx	xx	**Solução de Gerenciamento Centralizado Inteligente** - Plataforma de gerenciamento centralizado dos firewalls NGFW, em nuvem do fabricante ou appliance dedicado, permitindo administração unificada de políticas, correlação e visualização de logs, geração de relatórios, análise de ameaças e acompanhamento da postura de segurança de todo o ambiente para 36 meses de licenciamento e suporte.	Unidades	1			
xx	xx	**Serviço de Suporte da CONTRATADA -** Serviço de suporte técnico especializado para os firewalls NGFW e para a solução de gerenciamento centralizado, incluindo atendimento remoto, apoio na operação da solução, abertura e acompanhamento de chamados junto ao fabricante, bem como manutenção corretiva e evolutiva e atualização de software e assinaturas de segurança durante o período contratual de 36 meses	Meses	36			
xx	xx	**Serviço de Instalação da CONTRATADA -** Serviço de instalação, configuração inicial e comissionamento dos firewalls NGFW e da solução de gerenciamento centralizado, incluindo integração à rede da CONTRATANTE, configuração de alta disponibilidade, ajustes de políticas básicas de segurança, realização de testes de aceitação e entrega de documentação técnica do ambiente implantado.	Unidades	2			
xx	xx	**Serviço de Treinamento da CONTRATADA -** Treinamento remoto de administração básica da solução de Firewall de Próxima Geração (NGFW), com carga horária total de 20 (vinte) horas para até 5 (cinco) alunos, abordando conceitos fundamentais da plataforma, interfaces e zonas, objetos e políticas de segurança, NAT, controle de aplicações e usuários, perfis de segurança e VPN. O objetivo é capacitar a equipe da CONTRATANTE para realizar a operação diária do firewall, incluindo monitoramento, interpretação de logs, procedimentos básicos de troubleshooting, alta disponibilidade e gerenciamento de configuração.	Alunos	5			
As especificações e detalhamentos dos serviços estão definidos no Edital, no Termo de Demanda e seus anexos.							

6.2. Estão inclusos no valor total todas e quaisquer despesas, taxas e impostos aplicáveis, referente ao fornecimento, inclusive as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

6.3. As quantidades e valores acima são meramente estimativos e não indicam qualquer compromisso futuro para o CONTRATANTE, de forma que os pagamentos devidos à CONTRATADA dependerão dos quantitativos de serviços efetivamente prestados.

7. **CLÁUSULA SÉTIMA – DA GARANTIA DE EXECUÇÃO DO CONTRATO**

7.1. Será exigida prestação de garantia de execução do contrato, correspondente a 5% (cinco por cento) do valor do contrato, a ser apresentada no prazo de até 10 (dez) dias úteis da assinatura do contrato.

7.2. A garantia poderá ser prestada, à escolha da CONTRATADA, por meio de uma das seguintes modalidades:

a) Caução em dinheiro;

b) Fiança bancária;

c) Seguro garantia.

7.2.1. O atraso injustificado do prazo para apresentação da garantia por período superior a 15 (quinze) dias poderá ensejar a rescisão contratual por inadimplemento, sem prejuízo da aplicação das demais sanções cabíveis.

7.3. A garantia assegurará, qualquer que seja a modalidade escolhida e observada a legislação que rege a matéria, sob pena de não aceitação, o pagamento de:

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

b) Prejuízos diretos causados ao CONTRATANTE, decorrentes de culpa ou dolo durante a execução do Contrato;

c) multas moratórias e punitivas aplicadas pelo CONTRATANTE à CONTRATADA;

d) Obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pela CONTRATADA, quando couber.

7.4. A prestação de garantia, qualquer que seja a modalidade adotada, deverá abranger todo o período contratual, acrescida de 120 (cento e vinte) dias.

7.5. Quando a garantia for prestada sob a forma de fiança bancária ou seguro garantia, a apólice, carta de fiança ou instrumento equivalente deverá conter:

a) indicação expressa do CONTRATANTE como beneficiário;

b) identificação completa da CONTRATADA;

c) especificação do objeto garantido, conforme instrumento convocatório ou contratual ou o respectivo termo aditivo a que se vincula;

d) valor correspondente ao montante da garantia exigida.

7.6. A apólice de seguro garantia deverá ser emitida por instituição autorizada a operar pela Superintendência de Seguros Privados – SUSEP e estar devidamente registrada perante a referida Autarquia.

7.7. Quando prestada em dinheiro, a garantia deverá ser depositada em conta bancária específica, vinculada ao contrato, com movimentação autorizada exclusivamente para as finalidades previstas neste Contrato e no Regulamento de Compras e Contratações do Icipe.

7.8. No caso de garantia na modalidade de fiança bancária, esta deverá ser emitida por banco ou instituição financeira devidamente autorizada a operar no País pelo Banco Central do Brasil, e deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

7.9. Na hipótese de alteração do valor do contrato ou de prorrogação de sua vigência, a garantia deverá ser ajustada ou renovada, conforme o caso, no prazo de até 10 (dez) dias úteis, contado da assinatura do respectivo termo aditivo ou da emissão do apostilamento, mantidas as condições originalmente pactuadas.

7.10. Na hipótese de suspensão do Contrato por ordem ou inadimplemento do CONTRATANTE, a CONTRATADA ficará desobrigada de renovar a garantia ou de promover o endosso da apólice de seguro garantia até a ordem de reinício da execução contratual ou a regularização do inadimplemento

7.11. Caso o valor da garantia seja utilizado pelo CONTRATANTE, total ou parcialmente, para satisfação de quaisquer obrigações contratuais, a CONTRATADA deverá recompô-la no prazo de até 30 (trinta) dias, contado da comunicação do fato.

7.12. O CONTRATANTE poderá executar a garantia na forma prevista neste Contrato e no Regulamento de Compras e Contratações do Icipe, observada a legislação que rege a matéria.

7.13. A garantia somente será liberada após a execução integral do contrato ou sua rescisão, desde que não haja pendências financeiras ou administrativas a serem solucionadas e observado o prazo previsto no subitem 7.4.

7.13.1. Quando prestada em dinheiro, a garantia será atualizada monetariamente, na forma da legislação aplicável.

7.14. A garantia será considerada extinta:

a) com a restituição da apólice, carta fiança ou autorização para a liberação de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração do CONTRATANTE, mediante termo circunstanciado, de que a CONTRATADA cumpriu integralmente todas as obrigações contratuais;

b) após o decurso de 120 (cento e vinte) dias do término da vigência do contratual, caso não haja comunicação formal de ocorrência de sinistro pelo CONTRATANTE.

7.15. A modalidade de garantia poderá ser alterada por solicitação da CONTRATADA, desde que autorizada pela CONTRATANTE e mantidos o valor e a cobertura originalmente pactuados.

7.16. O garantidor não é parte legítima para figurar em processo administrativo instaurado pelo CONTRATANTE com a finalidade de apurar prejuízos e (ou) aplicar sanções à CONTRATADA.

7.17. A CONTRATADA autoriza expressamente o CONTRATANTE a reter e executar a garantia, a qualquer tempo, nas hipóteses previstas neste Contrato e no Regulamento de Compras e Contratações do Icipe.

7.18. A garantia de execução é independente e não substitui de eventual garantia técnicas de produtos ou serviços previstas no Termo de Demanda.

8. **CLÁUSULA OITAVA – DO PAGAMENTO**

8.1. O pagamento pelos serviços efetivamente prestados será realizado mensalmente, no valor correspondente ao período faturado, mediante a apresentação da respectiva Nota Fiscal devidamente atestada pelo Fiscal do Contrato.

8.2. A CONTRATADA deverá encaminhar ao Fiscal do Contrato, até o 5º (quinto) dia útil do mês subsequente ao da prestação dos serviços, o relatório de execução acompanhado da respectiva Nota Fiscal.

8.3. O pagamento será efetuado em até 30 (trinta) dias corridos, contados da data do ateste final da nota fiscal pelo Fiscal do Contrato. Após o ateste, o Fiscal encaminhará o documento ao setor responsável pelo pagamento.

8.4. Para fins de pagamento, a nota fiscal deverá ser acompanhada da comprovação da regularidade fiscal, bem como quaisquer outras exigidas e descritas no Edital e/ou no Termo de Demanda.

8.5. É vedada, sob qualquer pretexto, a antecipação de pagamentos pela CONTRATANTE.

8.6. A área do CONTRATANTE responsável pelo pagamento verificará se a nota fiscal apresentada expressa os elementos necessários e essenciais do documento, tais como:

a) descrição do serviço;

b) quantidade;

c) a data da emissão;

d) os dados do Contrato e do CONTRATANTE;

e) o período de prestação dos serviços;

f) o valor a pagar; e

g) eventual destaque do valor de retenções tributárias cabíveis.

8.7. A nota fiscal deve conter ainda: valor unitário, valor total, número do Chamamento, número do Contrato, Número da Ordem de Execução de Serviço (quando houver), número do banco, da agência e da conta corrente onde deseja receber seu crédito.

8.8. A consulta relativa à regularidade Fiscal, exigida quando da habilitação, será feita previamente a cada pagamento, devendo seu resultado ser juntado aos autos do processo próprio e a Contratada notificada, em caso de irregularidade constatada, sob pena de aplicação de penalidades e rescisão contratual.

8.9. Recebida a documentação de regularidade Fiscal, o Fiscal do Contrato deverá apor a data de entrega e assiná-la.

8.10. O descumprimento reiterado das disposições anteriores e a manutenção da CONTRATADA em situação irregular perante as obrigações fiscais, trabalhistas e previdenciárias implicarão rescisão contratual, sem prejuízo da aplicação das penalidades e demais cominações legais.

8.11. Havendo erro na apresentação da nota fiscal, ou circunstância que impeça a liquidação da despesa, o pagamento ficará suspenso até que a CONTRATADA providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para o CONTRATANTE.

8.12. Qualquer atraso ocorrido por parte da CONTRATADA na apresentação da nota fiscal ou dos documentos exigidos como condição para pagamento importará na interrupção da contagem do prazo de vencimento do pagamento, iniciando novo prazo após a regularização da situação.

8.13. Constatando-se a situação de irregularidade da CONTRATADA, será providenciada sua notificação formal, via plataforma SEI ou por e-mail, para que, no prazo de 03 (três) dias corridos, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do CONTRATANTE.

8.14. O pagamento será calculado e efetuado em conformidade com a efetiva prestação dos serviços, não estando o CONTRATANTE obrigado a executar integralmente o valor estimado do Contrato.

8.15. O prazo de pagamento poderá ser suspenso se o serviço não estiver de acordo com as especificações estipuladas no Termo de Demanda e/ou neste instrumento, caso em que o prazo referido no item 8.3. será contado a partir da efetiva regularização das pendências por parte da CONTRATADA.

8.16. Do montante devido à CONTRATADA poderão ser deduzidos os valores correspondentes a multas e (ou) indenizações previstas no Termo de Demanda e/ou neste instrumento.

8.17. Será indicada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a CONTRATADA:

a) não produziu os resultados acordados;

b) deixou de executar, ou não executou com a qualidade mínima exigida os serviços contratadas; ou

c) deixou de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou os empregou com qualidade ou quantidade inferior à demandada.

8.18. Não serão efetuados quaisquer pagamentos enquanto perdurar pendência de liquidação de obrigações, em virtude de penalidades impostas à empresa CONTRATADA ou inadimplência contratual.

8.19. Havendo atraso no pagamento em razão de ausência e (ou) atraso de repasse financeiro pela SES/DF ao CONTRATANTE, não incidirá multa e juros em favor da CONTRATADA.

9. **CLÁUSULA NONA – DO REAJUSTE E DA REVISÃO DE PREÇOS**

9.1. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de 12 (doze) meses contado da data de assinatura do contrato.

9.2. Após o interregno de 12 (doze) meses contados da data de assinatura do contrato, os preços poderão ser reajustados, mediante solicitação da CONTRATADA e aplicação, pelo CONTRATANTE, do índice INPC (Índice Nacional de Preço ao Consumidor*),* correspondente à variação acumulada nos 12 (doze) meses imediatamente anteriores ao mês do protocolo do pedido de reajuste, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade, ficando expressamente vedado qualquer pagamento, indenização ou compensação retroativa relacionada ao período em que a CONTRATADA se manteve inerte.

9.3. Nos reajustes subsequentes ao primeiro, o interregno mínimo de 12 (doze) meses será contado a partir dos efeitos financeiros do último reajuste.

9.4. No caso de atraso ou não divulgação do índice de reajustamento, o CONTRATANTE pagará à CONTRATADA a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo.

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

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

9.7. Ocorrerá a preclusão do direito ao reajustamento quando este for requerido após a extinção do contrato.

9.8. O reajuste de preços dos contratos será concedido observando-se os limites orçamentários anuais disponibilizados conforme os repasses realizados pela Secretaria de Saúde do Distrito Federal-SESDF, nos termos estabelecidos no Contrato de Repasse/Gestão respectivo.

9.9. O reajuste de preços será formalizado por meio de termo de apostilamento.

9.10. Na hipótese de revisão de valores, a CONTRATADA deverá apresentar dossiê, contemplando: (i) justificativa fundamentada; (ii) planilha detalhada de custos e documentos relativos aos itens que determinem e comprovem o desequilíbrio econômico financeiro do Contrato, quando aplicável; (iii) contratos firmados com entes públicos/notas fiscais; (iv) habilitação fiscal; (v) regularidade jurídica; (vi) no caso de fornecedor exclusivo, declaração de preço praticado no mercado com entes públicos ou empresas privadas e (vii) declaração de exclusividade vigente.

9.11. Os preços que sofrerem revisão não poderão ultrapassar os valores praticados no mercado, mantendo-se a diferença percentual apurada entre o valor originalmente constante da proposta e aquele vigente no mercado à época da contratação.

9.12. Consideram-se compatíveis com os preços de mercado aqueles contratados que sejam iguais ou inferiores, de acordo com a metodologia aplicada à média, diante de dados homogêneos, ou à mediana dos valores apurados pelo CONTRATANTE, diante de dados heterogêneos.

10. **CLÁUSULA DÉCIMA – DA REPETIÇÃO DO INDÉBITO**

10.1. Na hipótese de a CONTRATADA receber valores indevidos, o indébito será apurado em moeda corrente na data do recebimento do valor indevido e atualizado pelo índice IGP-M, calculado pela Fundação Getúlio Vargas (FGV), "*pro rata temporis*", desde a data da apuração até o efetivo recolhimento.

10.2. A quantia recebida indevidamente será descontada dos pagamentos devidos à CONTRATADA, devendo o CONTRATANTE notificá-la do desconto e apresentar a correspondente memória de cálculo.

10.3. Previamente aos referidos descontos, permitir-se-á a CONTRATADA manifestar sobre o pagamento superior apurado pelo CONTRATANTE.

10.4. Na hipótese de inexistirem pagamentos a serem efetuados, o CONTRATANTE deverá notificar a CONTRATADA para que recolha, no prazo máximo de 05 (cinco) dias úteis da data do recebimento do comunicado, a quantia paga indevidamente, por meio de deposito em banco, em nome do Instituto do Câncer Infantil e Pediatria Especializada - ICIPE ou por outro meio a ser informado pelo CONTRATANTE.

10.5. Efetuado o recolhimento de que trata o item anterior, a CONTRATADA encaminhará ao CONTRATANTE o respectivo comprovante, no prazo máximo de 24 (vinte e quatro) horas.

10.6. Caso o índice de atualização estabelecido não possa mais servir aos fins a que se propõe, ficam, desde já, acertadas as partes em avençar outro para substituí-lo.

11. **CLÁUSULA DÉCIMA PRIMEIRA – DAS OBRIGAÇÕES DO CONTRATANTE**

11.1. São obrigações do CONTRATANTE, além dos encargos de ordem legal e dos demais assumidos em outras cláusulas e documentos integrantes deste Contrato:

11.1.1. Cumprir e fazer cumprir as disposições deste Contrato, bem como de seus anexos e instrumentos que o integrem;

11.1.2. Relacionar-se com a CONTRATADA exclusivamente por intermédio de preposto ou representante formalmente por ela indicado;

11.1.3. Emitir, quando aplicável, a Ordem de Serviço, nos termos e prazos estabelecidos no Termo de Demanda e neste Contrato;

11.1.4. Prestar à CONTRATADA as informações, orientações e esclarecimentos que esta venha a solicitar, necessários à adequada execução dos serviços contratados;

11.1.5. Assegurar, quando necessário e previamente justificado, o acesso da CONTRATADA às dependências e/ou sistemas do CONTRATANTE estritamente indispensáveis à execução do objeto contratual, observadas as normas internas aplicáveis;

11.1.6. Acompanhar e fiscalizar a execução do Contrato, diretamente ou por intermédio de gestor e fiscal formalmente designados, verificando a conformidade da prestação dos serviços com as condições pactuadas;

11.1.7. Registrar e notificar a CONTRATADA, por escrito, sobre a ocorrência de falhas, vícios, defeitos ou irregularidades na execução dos serviços, fixando prazo razoável para sua correção, quando cabível;

11.1.8. Receber o objeto contratual nas condições e prazos estabelecidos no Termo de Demanda e neste Contrato;

11.1.9. Efetuar o pagamento devido à CONTRATADA, no prazo, forma e condições estabelecidos neste Contrato e no Termo de Demanda, após o cumprimento das exigências contratuais pertinentes;

11.1.10. Decidir, de forma expressa e motivada, quanto às solicitações, reclamações ou requerimentos formulados pela CONTRATADA relacionados à execução do Contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste;;

11.1.11. Responder aos pedidos de reajuste e/ou revisão de preços eventualmente apresentados pela CONTRATADA, nos prazos e condições previstos neste Contrato e na regulamentação aplicável;

11.1.12. Aplicar à CONTRATADA, quando cabível, as sanções previstas neste Contrato e/ou no Termo de Demanda, assegurados o contraditório e a ampla defesa;

11.1.13. Comunicar, quando necessário, aos garantidores o início de procedimento administrativo destinado à apuração de eventual descumprimento contratual;

11.1.14. Manter arquivados, durante toda a vigência do Contrato e após o seu encerramento, os documentos relacionados à contratação e à execução contratual, nos termos da regulamentação aplicável;

11.1.15. Isentar-se de qualquer responsabilidade por obrigações assumidas pela CONTRATADA perante terceiros, inclusive aquelas relacionadas a seus empregados, prepostos ou subcontratados, bem como por danos decorrentes de atos praticados por estes;

11.1.16. Abster-se de praticar atos que caracterizem ingerência na administração, organização ou gestão da CONTRATADA, especialmente no que se refere à direção, supervisão ou comando de seus empregados, ressalvadas as hipóteses expressamente previstas neste Contrato ou no Termo de Demanda.

12. **CLÁUSULA DÉCIMA SEGUNDA – DAS OBRIGAÇÕES DA CONTRATADA**

12.1. São obrigações da CONTRATADA, além dos encargos de ordem legal e dos demais assumidos em outras cláusulas e documentos integrantes deste Contrato:

12.1.1. Executar o objeto contratual em conformidade com as condições estabelecidas neste Contrato, no Termo de Demanda e no Edital, observando a legislação aplicável e as boas práticas relacionadas à natureza do serviço contratado;

12.1.2. Responder integralmente pela adequada execução dos serviços, assumindo todos os riscos inerentes à sua atividade, bem como pelos vícios, defeitos ou incorreções decorrentes da execução do objeto;

12.1.3. Reparar, corrigir, refazer ou substituir, às suas expensas, no todo ou em parte, no prazo fixado pelo CONTRATANTE, os serviços ou produtos em que se verificarem vícios, defeitos ou incorreções resultantes do fornecimento, da execução ou dos materiais empregados, em qualquer tempo e sem qualquer ônus para o CONTRATANTE;

12.1.4. Responsabilizar-se por todo e qualquer dano causado ao CONTRATANTE ou a terceiros, decorrente de ação ou omissão, dolo ou culpa, relacionados à execução do objeto contratual, não sendo a fiscalização exercida pelo CONTRATANTE causa excludente ou atenuante de responsabilidade, ficando o CONTRATANTE autorizado a descontar da garantia, caso exigida, ou dos pagamentos devidos à CONTRATADA, o valor correspondente aos danos sofridos;

12.1.5. Manter, durante toda a vigência do Contrato, em compatibilidade com as obrigações por ele assumidas, todas as condições de habilitação e qualificação exigidas no processo de contratação;

12.1.6. Cumprir integralmente as obrigações trabalhistas, previdenciárias, fiscais, comerciais e demais encargos decorrentes da execução do Contrato, inexistindo qualquer vínculo ou responsabilidade solidária ou subsidiária do CONTRATANTE;

12.1.7. Disponibilizar os recursos materiais, tecnológicos e humanos necessários à adequada execução dos serviços, assumindo integral responsabilidade por sua organização, gestão e funcionamento;

12.1.8. Prestar ao CONTRATANTE, sempre que solicitado, os esclarecimentos e informações pertinentes à execução do Contrato, no prazo e na forma estabelecidos, ressalvadas as hipóteses de natureza técnica que demandem prazo específico;

12.1.9. Comunicar prontamente ao CONTRATANTE a ocorrência de qualquer fato ou situação que possa comprometer, interromper ou prejudicar a execução regular do objeto contratual;

12.1.10. Observar as normas internas, regras de segurança, políticas institucionais e demais orientações do CONTRATANTE aplicáveis à execução do objeto, quando houver acesso às suas dependências ou sistemas;

12.1.11. Guardar sigilo e confidencialidade sobre todas as informações, dados e documentos a que tiver acesso em razão da execução do Contrato, utilizando-os exclusivamente para o cumprimento do objeto contratado;

12.1.12. Não transferir a terceiros a execução do objeto contratual, total ou parcialmente, sem prévia e expressa autorização do CONTRATANTE, quando admitida no Edital ou no Termo de Demanda;

12.1.13. Submeter à prévia anuência do CONTRATANTE quaisquer alterações relevantes nos métodos, processos ou soluções empregados na execução do objeto, quando tais alterações impactarem as condições pactuadas;

12.1.14. Atender às determinações do CONTRATANTE relacionadas à correção de falhas, desconformidades ou riscos identificados na execução contratual, observados os limites do Contrato e do Termo de Demanda;

12.1.15. Abster-se de utilizar o nome, a marca ou a imagem do CONTRATANTE em qualquer material de divulgação, publicidade ou comunicação externa, sem prévia e expressa autorização do CONTRATANTE;

12.1.16. Manter atualizados seus dados cadastrais e canais de comunicação, especialmente endereço eletrônico e telefone, para fins de notificações e comunicações formais relativas ao Contrato;

12.1.17. Cumprir as demais obrigações que lhe sejam atribuídas por força deste Contrato, do Termo de Demanda, do Edital do Chamamento Público e da regulamentação aplicável;

12.1.18. Garantir a prestação dos serviços objeto do contrato, nas mesmas condições estabelecidas no Termo de Demanda e no preço pactuado por, no mínimo, 90 (noventa) dias ou até a celebração de Contrato com outro fornecedor, em caso de risco de vida para pacientes.

13. **CLÁUSULA DÉCIMA TERCEIRA – DAS NOTIFICAÇÕES PELO CONTRATANTE**

13.1. A CONTRATADA deverá manter e acessar regularmente um correio eletrônico informado para o CONTRATANTE, para onde serão endereçadas todas as correspondências e notificações, observando que:

13.1.1. As notificações e correspondências enviadas para o correio eletrônico informado pela CONTRATADA equivalem às notificações feitas sob qualquer outra forma prevista em lei, e delas constarão o conteúdo integral da notificação;

13.1.2. As notificações e correspondências encaminhadas conforme o subitem precedente serão dadas como recebidas e lidas pela CONTRATADA a contar da data de seu envio.

14. **CLÁUSULA DÉCIMA QUARTA – DAS ALTERAÇÕES CONTRATUAIS**

14.1. Eventuais alterações contratuais reger-se-ão pela disciplina do Regulamento de Compras e Contratações (RCC) do Icipe e poderão ser realizadas nas seguintes hipóteses:

I - Quando for necessário modificar o valor contratual em decorrência de acréscimos ou supressões de seu objeto, respeitados os limites previstos neste Contrato;

II - Para substituição do objeto por outro correlato ou similar, mediante justificativa da área técnica, desde que demonstrada vantagem para a gestão e operação das atividades do CONTRATANTE;

III - Para ajustar os prazos de início, conclusão ou entrega do objeto contratado, em razão de fatos supervenientes devidamente justificados;

IV - Para redistribuir os quantitativos contratados, mediante justificativa, vedada a ampliação dos valores unitários;

V - Quando houver interesse do CONTRATANTE na substituição da garantia contratual, se exigida;

VI - Quando se fizer necessária a alteração do projeto ou das especificações técnicas, visando melhor adequação aos objetivos institucionais;

VII - Para alteração do modo de fornecimento ou do regime de execução, desde que comprovada a inviabilidade da execução conforme originalmente pactuado;

VIII - Para o restabelecimento do equilíbrio econômico-financeiro do contrato, sempre que houver a ocorrência de fatos que alterem substancialmente os encargos assumidos pelas partes.

14.2. Podem ser registradas por simples apostilamento as situações que não caracterizam alteração do contrato e de seu objeto, tais como as abaixo:

I - A variação do valor contratual para fazer face ao reajuste de preços previsto no próprio contrato;

II - As atualizações, compensações ou penalizações financeiras decorrentes das condições de pagamento previstas no contrato;

III - Atualização de endereço da contratada;

IV - Alteração da execução do objeto contratado entre matriz e filial;

V - Outras situações que se enquadrem no caput.

14.3. A CONTRATADA poderá aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários nas aquisições/compras, em até 25% (vinte e cinco por cento) do valor inicial atualizado do Contrato.

14.3.1. O limite percentual previsto no subitem precedente deverá ser calculado conforme a forma de contratação adotada: por item ou sobre o valor global.

14.3.2. Nenhum acréscimo ou supressão poderá exceder o limites estabelecido no subitem 13.3, salvo as supressões resultantes de acordo celebrado entre as partes.

14.4. As alterações contratuais não poderão suprimir a vantagem econômica obtida originalmente pelo CONTRATANTE.

14.4.1. Nos casos de alterações que envolvam simultaneamente acréscimos e supressões, é vedada a compensação entre ambos os ajustes, de forma a evitar a descaracterização do objeto inicialmente contratado.

14.5. Os contratos celebrados poderão ser revisados ou ajustados a qualquer momento, mediante termo aditivo, com a finalidade de otimizar resultados em termos de qualidade e preço, em compatibilidade com a realidade de mercado, desde que seja vantajoso para o CONTRATANTE.

14.6. Aditivos relacionados à quantidade deverão observar os ajustes já aplicados, devendo a soma respeitar os limites previstos no Art.10 do Decreto Distrital nº 33.390/11.

14.7. As alterações contratuais serão formalizadas por meio de termo aditivo.

15. **CLÁUSULA DÉCIMA QUINTA – DA RESCISÃO CONTRATUAL**

15.1. O contrato se extingue naturalmente com o cumprimento das obrigações contratuais ou pelo término do prazo de vigência, podendo ocorrer a sua extinção antecipada, a qual deverá ser formalmente motivada nos autos do processo respectivo, sem que seu objeto seja concluído e antes do prazo previsto de duração nos casos e hipóteses previstas neste Contrato.

15.2. A extinção antecipada do instrumento contratual realizada através de rescisão poderá ser formalizada:

I - Por ato unilateral e escrito do CONTRATANTE, nos casos previstos nos itens 15.3 a 15.5 deste Contrato, sem prejuízo de demais consequências contratuais e legais;

II - De forma consensual, mediante acordo entre as partes, desde que não cause prejuízos à continuidade do serviço público e haja motivação justificada.

15.2.1. A rescisão unilateral implicará, sem prejuízo das sanções aplicáveis:

I - Execução da garantia contratual, quando existente, para ressarcimento de eventuais prejuízos ou penalidades;

II - Retenção de créditos eventualmente devidos à contratada, limitados ao valor dos prejuízos apurados

15.3. Poderão ensejar a rescisão do contrato, entre outras hipóteses:

I - Descumprimento reiterado de cláusulas contratuais, prazos, especificações técnicas ou demais condições pactuadas;

II - Atraso injustificado na execução dos serviços, de modo a comprometer os objetivos da contratação;

III - Paralisação da execução contratual sem justificativa e sem prévia comunicação à Organização Social;

IV - Decretação de falência ou insolvência da contratada;

V - Dissolução da pessoa jurídica ou falecimento do contratado, se pessoa física;

VI - Alteração societária que afete negativamente a capacidade de execução contratual;

VII - Ocorrência de fato superveniente de interesse público devidamente motivado que torne a manutenção do contrato desvantajosa à instituição;

VIII - Situação de caso fortuito ou força maior, devidamente comprovada, que impossibilite a continuidade da execução;

IX - Descumprimento da obrigação de prestar garantia contratual, quando exigida, dentro do prazo estabelecido;

X - Desaparecimento do objeto contratual, tornando sua execução inviável.

15.4. O presente Contrato poderá ser rescindido unilateralmente pelo CONTRATANTE, com efeitos imediatos, mediante ato formal devidamente motivado, sempre que a inexecução contratual ou a conduta da CONTRATADA representar risco ao atendimento do interesse público e/ou continuidade da assistência à saúde.

15.4.1. Formalizada a rescisão, o CONTRATANTE poderá adotar as medidas necessárias à salvaguarda do atendimento ao interesse público e à continuidade da assistência à saúde, nos termos do Regulamento de Compras e Contratações do Icipe e demais normativos internos, inclusive reter valores eventualmente devidos à CONTRATADA, até o limite necessário à apuração e ao ressarcimento de prejuízos comprovadamente causados.

15.4.2. Considerando a situação de urgência, em razão do risco ao atendimento do interesse público ou à continuidade da assistência à saúde, o exercício do contraditório e da ampla defesa será assegurado à CONTRATADA em procedimento próprio, a ser instaurado após a adoção da medida rescisória, sem prejuízo da validade e eficácia da rescisão.

15.5. O CONTRATANTE executa sua atividade mediante Contrato de Gestão firmado com ente público e, portanto, a sua rescisão ou não renovação importará em rescisão automática deste instrumento, sem que caiba, a qualquer das partes, direito a multa, indenização, retenção, compensação, perdas e danos então decorrentes do mencionado encerramento contratual, sem qualquer ônus para as partes e que, caso seja de interesse do poder público, os contratos vigentes no momento da rescisão ou não renovação do contrato de gestão poderão ser sub-rogados em seu favor.

15.6. A alteração social ou a modificação da finalidade ou da estrutura da empresa não ensejará a rescisão se não restringir sua capacidade de concluir o Contrato.

15.6.1. O CONTRATANTE avaliará a possibilidade da manutenção do Contrato, de acordo com sua conveniência e oportunidade e, devidamente justificado.

15.6.2. Se a operação implicar mudança da pessoa jurídica CONTRATADA, deverá ser formalizado termo aditivo para alteração subjetiva.

15.7. Os casos de rescisão contratual serão formalmente motivados nos autos do respectivo processo, assegurando-se à CONTRATADA o contraditório e à ampla defesa.

15.8. A extinção do Contrato não configura óbice para o reconhecimento do desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório ou instrumento semelhante.

15.9. O termo de rescisão, sempre que possível, será precedido de:

a) Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

b) Relação dos pagamentos já efetuados e ainda devidos; e

c) Indenizações e multas.

16. **CLÁUSULA DÉCIMA SEXTA – DA DECLARAÇÃO UNIFICADA**

16.1. A CONTRATADA declara, sob as penas da lei e para todos os fins de direito, que:

I - EXERCÍCIO DAS ATIVIDADES: Exerce suas atividades em conformidade com a legislação vigente;

II - CUMPRIMENTO DE REQUISITOS DE HABILITAÇÃO: Cumpre plenamente os requisitos de habilitação exigidos e atende a todos os requisitos descritos no Edital e seus anexos;

III - FATOS IMPEDITIVOS: Não se enquadra em quaisquer das situações de impedimento previstas no item 2.2 e 2.3 do Edital;

IV - IMAGEM e REPUTAÇÃO: Não prejudica a imagem e reputação do CONTRATANTE;

V - ORDEM PÚBLICA: Não atenta contra a ordem pública;

VI - PRECONCEITO: Não evidencia e nem compactua com preconceito ou discriminação de qualquer natureza

VII - NEPOTISMO: Não compactua com situações que possam configurar nepotismo no âmbito do CONTRATANTE ou da administração pública federal, nos termos do Decreto nº 7.203, de 04.06.2010;

VIII - TRABALHO ILEGAL E/OU ANÁLOGO AO ESCRAVO: Não se utiliza direta ou indiretamente, inclusive por meio de seus fornecedores de produtos e serviços, de trabalho ilegal e/ou análogo ao escravo;

IX - INEXISTÊNCIA DE EMPREGADO MENOR NO QUADRO DA EMPRESA: Não emprega, direta ou indiretamente, por meio de seus fornecedores de produtos e serviços, menores de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre, e nem menor de 16 (dezesseis) anos em qualquer trabalho, salvo na condição de aprendiz, a partir dos 14 (quatorze) anos, e, neste caso, o trabalho não poderá ser perigoso ou insalubre, ocorrer em horário noturno e/ou de modo a não permitir a frequência escolar, conforme Decreto 4.358, de 05/09/2002;

X - DISCRIMINAÇÃO NEGATIVA: Não se utiliza de práticas de discriminação negativas e limitativas para o acesso e manutenção do emprego, tais como por motivo de sexo, origem, raça, cor, condição física, religião, estado civil, idade, situação familiar, estado gravídico etc.;

XI - SUSTENTABILIDADE: Protege e preserva o meio ambiente, prevenindo práticas danosas na execução de seus serviços, principalmente no que se refere aos crimes ambientais, observa a legislação referente à promoção do desenvolvimento nacional sustentável e adota no que é possível, as práticas de sustentabilidade ambiental;

XII - PREVENÇÃO E COMBATE À CORRUPÇÃO (Lei 12.846/13): Conhece a referida lei, comprometendo-se em:

a) não utilizar de práticas corruptas e/ou antiéticas visando obter ou dar vantagem indevida, de forma direta ou indireta, perante o CONTRATANTE; e

b) cumpri-la(s) e fazê-la(s) cumprir por seus empregados e prepostos, em especial, mas não se limitando às situações descritas em seu Capítulo II – Dos Atos Lesivos à Administração Pública Nacional ou Estrangeira controles e procedimentos voltados à prevenção e ao tratamento de incidentes.

XIII - CÓDIGO DE CONDUTA: Conhece e respeita o Código de Conduta do ICIPE e o Código de Conduta do HCB, disponível na internet, endereço: https://icipe.org.br/wp-content/uploads/Codigo-de-Conduta-agosto-2024.pdf e https://www.hcb.org.br/governanca_e_compliance/codigo_de_conduta/;

XIV - INEXISTÊNCIA DE FATO SUPERVENIENTE: Até a presente data, inexiste fato superveniente impeditivo para a sua habilitação, na forma da legislação vigente, estando ciente da obrigatoriedade de declarar ocorrências posteriores;

XV - LEI DE PROTEÇÃO DE DADOS (Lei 13.709/18): Conhece a referida regulamentação e legislação, comprometendo-se em cumpri-la(s) e fazê-la(s) cumprir por seus empregados e prepostos, em especial, mas não se limitando, aos controles e procedimentos descritos em cláusula contratual;

XVI - LEIS SOBRE CRIMES DE LAVAGEM DE DINHEIRO e FINANCIAMENTO AO TERRORISMO (Leis 9.613/1998 e 13.260/2016) – Prevenção e Combate à Lavagem de Dinheiro e ao Financiamento do Terrorismo-PCLDFT: Conhece e respeita as referidas legislações que dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos, e sobre o financiamento ao terrorismo previstos nas citadas leis, sendo vedado à CONTRATADA e a seus empregados realizar qualquer negócio em nome da CONTRATANTE ou em razão deste Contrato de maneira imprópria, que configure atos criminosos ou ilícitos, tais como: corrupção, lavagem de dinheiro, financiamento do terrorismo e fraudes.

16.2. Esta declaração é prestada de forma contínua e permanente, aplicando-se no momento da assinatura do Contrato, durante toda a fase de execução contratual e enquanto perdurar a sua vigência, inclusive em eventuais prorrogações;

16.3. A CONTRATADA obriga-se a manter todas as condições ora declaradas válidas, íntegras e plenamente atendidas ao longo de toda a vigência contratual, inclusive em eventuais prorrogações, comprometendo-se a comunicar imediatamente ao CONTRATANTE a ocorrência de qualquer fato superveniente que possa comprometer a veracidade das declarações prestadas.

16.4. A inobservância do disposto nesta cláusula ensejará a rescisão unilateral imediata do Contrato, sem prejuízo da aplicação das demais sanções contratuais, bem como das responsabilidades civis, administrativas e penais cabíveis.

17. **CLÁUSULA DÉCIMA SÉTIMA – DAS INFRAÇÕES E SANÇÕES ADMINISTRATIVAS**

17.1. Comete infração administrativa, sem prejuízo de outras previstas neste Contrato, no Termo de Demanda, no Edital e na legislação aplicável, a CONTRATADA que:

a) der causa à inexecução parcial do Contrato;

b) der causa à inexecução parcial do Contrato que cause grave dano ao CONTRATANTE ou ao funcionamento dos serviços públicos ou ao interesse coletivo;

c) der causa à inexecução total do Contrato;

d) ensejar o retardamento da execução do objeto da contratação sem motivo justificado;

e) apresentar documentação falsa ou prestar declaração falsa durante a execução do Contrato;

f) praticar ato fraudulento na execução do Contrato;

g) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

h) praticar ato lesivo previsto no Artigo 5º da Lei nº 12.846/2013.

17.2. Serão aplicadas à CONTRATADA que incorrer nas infrações acima descritas as seguintes sanções:

I - **Advertência**, quando a CONTRATADA der causa à inexecução parcial do Contrato, sempre que não se justificar a imposição de penalidade mais grave ou por faltas leves, assim entendidas como aquelas que não acarretarem prejuízos significativos ao objeto da contratação;

II - **Multa**:

a) moratória, em caso de atraso injustificado na execução do objeto, no percentual de 0,1% (um décimo por cento) por dia de atraso, incidente sobre o valor da parcela em atraso ou do serviço afetado, limitada a 30 (trinta) dias;

b.1) decorrido o prazo de 30 (trinta) dias de atraso injustificado, restará caracterizado inadimplemento contratual parcial de natureza grave, podendo, a critério do CONTRATANTE, ensejar a rescisão unilateral do Contrato, observado o contraditório e a ampla defesa;

b.2) o inadimplemento referido no parágrafo anterior poderá ser caracterizado como inadimplemento total, para fins de aplicação das sanções cabíveis, quando, no caso concreto, o atraso tornar inútil, inviável ou destituída de finalidade a execução do objeto contratual, devidamente motivado pelo CONTRATANTE;

b) compensatória de até 5% (cinco por cento), incidente sobre o valor da parcela inadimplida ou do serviço afetado, nos casos de inexecução parcial prevista na alínea "a" do item 17.1. Quando, pela natureza da obrigação descumprida, não for possível determinar objetivamente o valor da parcela inadimplida ou do serviço afetado, a multa incidirá sobre o valor do Contrato;

c) compensatória de até 10% (dez por cento), incidente sobre o valor da parcela inadimplida ou do serviço afetado, nos casos de inexecução parcial prevista na alínea "b" do item 17.1. Quando, pela natureza da obrigação descumprida, não for possível determinar objetivamente o valor da parcela inadimplida ou do serviço afetado, a multa incidirá sobre o valor do Contrato;

d) compensatória de 10% (dez por cento) sobre o valor do Contrato, nos casos de inexecução total do contrato;

e) compensatória de até 10% (dez por cento) sobre o valor do Contrato, por qualquer das infrações previstas nas alíneas de "e" até "h" do item 17.1;

f) compensatória de 10% (dez por cento) sobre o valor total da homologação do resultado em caso de recusa em assinar o Contrato ou em prestar garantia de execução contratual, quando exigida;

III - **Suspensão temporária** de participação de outros procedimentos de aquisição de bens e serviços do CONTRATANTE, e impedimento de contratar com o hospital, por prazo não superior a 02 (dois) anos, e dosada segundo a natureza e a gravidade da falta cometida.

17.3. A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao CONTRATANTE.

17.4. Todas as sanções previstas neste Contrato poderão ser aplicadas juntamente com a multa, facultada à CONTRATADA a apresentação de defesa prévia no prazo estabelecido no Regulamento de Compras e Contratações do Icipe, contado da data de sua intimação.

17.5. A aplicação da sanção de multa não impede a rescisão do contrato e nem a aplicação de outras sanções previstas neste Contrato.

17.6. Se a multa aplicada for superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou cobrada judicialmente.

17.7. Caso a CONTRATADA não tenha nenhum valor a receber do CONTRATANTE, a multa poderá ser recolhida administrativamente no prazo máximo de 5 (cinco) dias úteis, a contar da data de sua intimação para efetuar o pagamento da multa.

17.7.1. O pagamento da multa que trata o item anterior deverá ser depositado em banco, em nome do CONTRATANTE.

17.8. As penalidades aplicadas poderão ser relevadas, com fundamentação sumária:

a) na hipótese de caso fortuito, força maior, devidamente justificada e comprovada, a juízo do CONTRATANTE;

b) quando ocorrer atraso não superior a 5 (cinco) dias; e

c) a execução de multa seja inferior ao dos respectivos custos de cobrança.

17.9. Toda sanção aplicada será anotada no histórico cadastral da empresa junto ao CONTRATANTE.

17.10. A penalidade de suspensão temporária será publicada no Diário Oficial do Distrito Federal.

17.11. Na aplicação das sanções serão consideradas:

a) a razoabilidade e proporcionalidade entre a sanção, a gravidade do descumprimento das condições pactuadas e o vulto econômico da contratação;

b) os danos resultantes do descumprimento das condições pactuadas;

c) a reincidência, assim entendida a repetição de descumprimento das condições pactuadas de igual natureza;

d) outras circunstâncias gerais agravantes ou atenuantes em face do caso concreto.

17.12. A aplicação de glosas por descumprimento dos níveis de serviço (SLA) previstos no Termo de Demanda possui natureza de adequação do pagamento ao efetivo desempenho técnico e à qualidade do serviço entregue, não se confundindo com as sanções previstas nesta cláusula, podendo ser aplicada cumulativamente com estas sempre que a conduta da CONTRATADA configurar infração às obrigações contratuais.

17.13. A personalidade jurídica da CONTRATADA poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com a CONTRATADA, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia.

18. **CLÁUSULA DÉCIMA OITAVA – DA FISCALIZAÇÃO**

18.1. A fiscalização do presente Contrato será realizada pela Gerência de Tecnologia da Informação– DIRAO/GTI**,** a qual competirá dirimir as dúvidas que surgirem no curso da prestação dos fornecimentos e de tudo dará ciência à Administração do CONTRATANTE.

18.2. A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade da CONTRATADA, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, e, na ocorrência desta, não implica em corresponsabilidade do CONTRATANTE ou de seus agentes e prepostos.

18.3. A aplicação das penalidades previstas no Contrato poderá ser reconsiderada, ou aplicada no todo ou em parte, a exclusivo critério do CONTRATANTE.

18.4. Os funcionários designados para fiscalização do contrato poderão recusar, sustar, mandar refazer ou fazer quaisquer falhas ou problemas inerentes à prestação do serviço, que estejam em desacordo com o preestabelecido.

18.5. O CONTRATANTE se reserva o direito, a qualquer momento durante a vigência do Contrato, de aferir os serviços contratados, realizando testes, auditorias por meio de ferramentas e recursos próprios ou empresas contratadas para este fim.

19. **CLÁUSULA DÉCIMA NONA – DO *COMPLIANCE* E COMBATE À CORRUPÇÃO**

19.1. As Partes Contratantes declaram conhecer as normas de prevenção à corrupção previstas na legislação brasileira, dentre elas, a Lei de Improbidade Administrativa (Lei nº 8.429/1992) e a Lei Anticorrupção (Lei nº 12.846/2013) e se comprometem a cumpri-las fielmente, por si e por seus sócios, administradores e colaboradores, bem como exigir o seu cumprimento pelos terceiros por elas contratados.

19.2. As Partes Contratantes declaram que manterão até o final da vigência deste Contrato conduta ética e máximo profissionalismo na execução do objeto do presente instrumento.

19.3. A CONTRATADA se obriga a, no exercício dos direitos e obrigações previstos neste Contrato:

a) Não dar, oferecer ou prometer qualquer bem de valor ou vantagem de qualquer natureza a agentes públicos ou a pessoas a eles relacionadas ou ainda quaisquer outras pessoas, empresas e (ou) entidades privadas, com o objetivo de obter vantagem indevida, influenciar ato ou decisão ou direcionar negócios ilicitamente;

b) Adotar as melhores práticas de monitoramento e verificação do cumprimento das leis anticorrupção, com o objetivo de prevenir atos de corrupção, fraude, práticas ilícitas ou lavagem de dinheiro por seus sócios, administradores, colaboradores e (ou) terceiros por elas contratados;

c) Não empregar, direta ou mediante Contrato de serviços ou qualquer outro instrumento, trabalho escravo ou infantil;

d) Obedecer e garantir que o fornecimento contratado se dará de acordo com todas as normas internas do CONTRATANTE;

e) Zelar pelo bom nome do CONTRATANTE e a abster-se ou omitir-se da prática de atos que possam prejudicar a reputação do CONTRATANTE. Em caso de uso indevido do nome do CONTRATANTE, ou de qualquer outro nome, marca, termo ou expressão vinculados direta ou indiretamente ao CONTRATANTE, responderá a CONTRATADA pelas perdas e danos daí decorrentes;

f) Participar de todos e quaisquer treinamentos eventualmente oferecidos pelo CONTRATANTE que sejam relativos a qualquer aspecto que consta da lei anticorrupção ou políticas internas do CONTRATANTE, bem como aqueles relativos ao Código de Conduta desta.

19.4. A CONTRATADA declara que não esteve envolvida com qualquer alegação de crime de lavagem de dinheiro, delito financeiro, financiamento de atividades ilícitas ou atos contra a Administração Pública, corrupção, fraude em licitações ou suborno.

19.5. A CONTRATADA concorda em notificar prontamente ao CONTRATANTE, caso tome conhecimento de que algum pagamento impróprio tenha sido realizado, direta ou indiretamente, por um de seus colaboradores ou terceiros por esta contratados.

19.6. A comprovada violação de qualquer das obrigações previstas nesta cláusula é causa para a rescisão unilateral motivada deste Contrato, independentemente de qualquer notificação, sem prejuízo da cobrança das perdas e danos causados à parte inocente e das demais penalidades previstas no presente instrumento.

19.7. O CONTRATANTE recomenda à CONTRATADA a implantação de Programa de Integridade, caso esse ainda não possua.

20. **CLÁUSULA VIGÉSIMA – DO QUESTIONÁRIO DE *DUE DILIGENCE***

20.1. Quando solicitado pelo CONTRATANTE, a CONTRATADA deverá preencher, assinar e encaminhar o Questionário de *Due Diligence* de Fornecedores e Prestadores de Serviços – Integridade, demonstrado no Anexo II, com as devidas evidências, no prazo máximo de 15 (quinze) dias úteis, contados da solicitação. O questionário será encaminhado posteriormente à CONTRATADA, via e-mail, pela área de *Compliance* e Riscos do HCB.

20.2. A CONTRATADA fica ciente de que, ao critério do CONTRATANTE, poderá ser efetuado o *Background Check* (Análise Reputacional).

21. **CLÁUSULA VIGÉSIMA PRIMEIRA – DAS OBRIGAÇÕES RELACIONADAS À PRIVACIDADE E PROTEÇÃO DE DADOS**

21.1. A CONTRATADA declara conhecer e cumprir todas as leis vigentes envolvendo proteção de dados pessoais, em especial a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), comprometendo-se, assim, a limitar a utilização dos dados pessoais a que tiver acesso apenas para execução dos serviços a serem prestados, abstendo-se de utilizá-los em proveito próprio ou alheio, para fins comerciais ou quaisquer outros.

21.2. A CONTRATADA se compromete a respeitar as políticas e regras editadas ou que vierem a ser editadas pelo CONTRATANTE no tocante ao armazenamento e tratamento de dados e informações, sem prejuízo do estrito respeito à Lei nº 12.965/2014 (Marco Civil da Internet), Decreto nº 8.771/2016 (Regulamento do Marco Civil da Internet), Lei nº 12.527/2011 (Lei de Acesso à Informação), bem como quaisquer outras leis relativas à proteção de dados pessoais que vierem a ser promulgadas ou entrarem em vigor no curso da vigência.

21.3. Havendo o compartilhamento de dados pelo CONTRATANTE, para a execução do objeto previsto no documento, a CONTRATADA assumirá a função de operadora e efetuará o tratamento tão somente para o atingimento das finalidades previstas neste documento e em conformidade com as Leis de Dados Aplicáveis e com as instruções apresentadas pelo CONTRATANTE, quando for o caso, que terá a posição de controlador.

21.4. As partes resguardam o direito de tratar os dados pessoais dos seus respectivos representantes conforme necessário para os fins de cumprimento do presente Contrato. Caso o representante demande seus direitos inerentes à proteção de dados pessoais, as partes assegurarão o pleno exercício destes nos termos da "LGPD".

22. **CLÁUSULA VIGÉSIMA SEGUNDA - DA MATRIZ DE RISCOS**

22.1. Integra o presente Contrato, para todos os fins de direito, a Matriz de Riscos constante no Termo de Demanda, que estabelece a alocação objetiva de responsabilidades entre as Partes quanto aos eventos supervenientes que possam impactar a execução e o equilíbrio econômico-financeiro do ajuste.

22.2. A responsabilidade por cada risco atribuído na Matriz inclui o dever de arcar com os custos financeiros e operacionais decorrentes de sua materialização, sem direito a qualquer compensação adicional.

22.3. Não serão admitidos termos aditivos ou pleitos de reequilíbrio econômico-financeiro decorrentes de eventos supervenientes que, conforme previsto na Matriz de Riscos, estejam expressamente alocados como de responsabilidade da CONTRATADA.

23. **CLÁUSULA VIGÉSIMA TERCEIRA – DOS FUNDAMENTOS E DOS CASOS OMISSOS**

23.1. O Contrato fundamenta-se:

a) Nos autos do Processo SEI nº XXXXXXXXXX, Edital nº XXX/XXXX;

b) Nas disposições do Decreto Distrital nº 33.390/2011;

c) Regulamento de Compras e Contratações (RCC) do Instituto do Câncer Infantil e Pediatria Especializada (Icipe); e,

d) Nos princípios de Direito Público e supletivamente, nos princípios da Teoria Geral dos Contratos e nas disposições do Direito Privado.

23.2. Os casos omissos serão decididos pelo CONTRATANTE, segundo as disposições contidas no Regulamento de Compras e Contratações (RCC) do Icipe, subsidiariamente, segundo as disposições contidas na Lei nº 8.078/1990 (Código de Defesa do Consumidor) e Normas e Princípios Gerais dos Contratos.

24. **CLÁUSULA VIGÉSIMA QUARTA – DO SIGILO E CONFIDENCIALIDADE**

24.1. A CONTRATADA se compromete a guardar sigilo absoluto sobre as atividades decorrentes da execução do objeto e sobre as informações a que venha a ter acesso por força da execução deste Contrato.

24.2. A CONTRATADA, por seus dirigentes, prepostos ou empregados, compromete-se, mesmo após o término do presente Contrato, a manter completa confidencialidade e sigilo sobre quaisquer dados ou informações obtidas em razão do presente Contrato, reconhecendo que não poderão ser divulgados ou fornecidos a terceiros, salvo com expressa autorização, por escrito, do CONTRATANTE.

24.3. A CONTRATADA será responsável, civil e criminalmente, por quaisquer danos causados ao CONTRATANTE e (ou) a terceiros, em virtude da quebra da confidencialidade e sigilo a que está obrigada.

25. **CLÁUSULA VIGÉSIMA QUINTA – DAS DISPOSIÇÕES GERAIS**

25.1. É facultada à Autoridade Competente em qualquer fase do processo, a promoção de diligência destinada a esclarecer ou complementar a instrução do mesmo.

25.2. A CONTRATADA não terá direito à indenização em decorrência da revogação ou anulação do Chamamento Público, ressalvado o direito do contratado de boa-fé de ser ressarcido pelos encargos que tiver suportado no cumprimento das obrigações.

25.3. É facultado ao CONTRATANTE, em qualquer etapa da vigência deste Contrato, promover diligências para esclarecer fatos ou complementar a instrução processual.

25.4. Na hipótese de qualquer cláusula ou disposição deste Contrato ser declarada nula, ilegal, inexigível ou inaplicável, no todo ou em parte, tal circunstância não afetará a validade, a eficácia ou a exequibilidade das demais cláusulas, que permanecerão plenamente vigentes.

25.5. A eventual não utilização, por qualquer das Partes, de direitos ou faculdades assegurados neste Contrato ou na legislação aplicável, bem como a tolerância quanto ao descumprimento de quaisquer de suas disposições, não constituirá novação, renúncia ou alteração contratual, nem impedirá que a Parte prejudicada, a qualquer tempo, exija o fiel e integral cumprimento do avençado.

25.6. Na hipótese de fusão, cisão, incorporação ou outra forma de reorganização societária da CONTRATADA, o CONTRATANTE reserva-se o direito de promover a rescisão do Contrato ou de autorizar a sua continuidade com a sociedade resultante, desde que mantidas, integralmente, as condições contratuais originalmente pactuadas e observada a legislação aplicável.

25.7. Nenhuma das Partes poderá ceder ou transferir, no todo ou em parte, ainda que em função de reestruturação societária, fusão, cisão e incorporação, os direitos e obrigações decorrentes do Contrato, inclusive seus créditos, sem a prévia e expressa autorização por escrito da outra Parte.

25.8. O CONTRATANTE não se responsabilizará pelo pagamento de quaisquer serviços executados pela CONTRATADA sem a devida autorização prévia, ou em desacordo com as condições estabelecidas neste Contrato e no Termo de Demanda.

25.9. Cada Parte será exclusivamente responsável pelas infrações que cometer quanto ao uso de materiais, equipamentos, softwares, tecnologias, processos de execução ou quaisquer outros bens protegidos por direitos de propriedade intelectual, tais como marcas, patentes ou direitos autorais, respondendo diretamente por eventuais indenizações, taxas, royalties ou reclamações decorrentes de sua utilização indevida.

25.10. Em caso de conflito de interpretação entre as cláusulas deste Contrato e os seus anexos, prevalecerão as disposições do Contrato, sem prejuízo da aplicação das normas legais e regulamentares pertinentes.

25.11. O CONTRATANTE fica autorizado a realizar a retenção preventiva de créditos devidos à CONTRATADA quando necessário para evitar o prejuízo decorrente de inadimplemento quanto aos encargos trabalhistas, previdenciários, comerciais e fiscais resultantes da execução do Contrato.

26. **CLÁUSULA VIGÉSIMA SEXTA – DO FORO**

26.1. Fica eleito o foro de Brasília - Distrito Federal, para dirimir quaisquer dúvidas relativas ao cumprimento do presente Contrato.

E, por estarem justas e acordadas, as partes contratantes assinam o presente instrumento.

(INSERIR NOME COMPLETO DA DIRETORA) DIRETORA EXECUTIVA ICIPE/HCB CONTRATANTE	**(INSERIR NOME COMPLETO DA DIRETORA)** DIRETOR DE APOIO OPERACIONAL ICIPE/HCB CONTRATANTE

(INSERIR NOME COMPLETO) GERENTE DE CONTRATOS E SERVIÇOS ICIPE/HCB TESTEMUNHA DA CONTRATANTE	**(INSERIR NOME COMPLETO)** GERENTE DO JURÍDICO ICIPE/HCB

(INSERIR NOME COMPLETO DO REPRESENTANTE LEGAL) REPRESENTANTE LEGAL/PROCURADOR (INSERIR NOME COMPLETO DA EMPRESA CONTRATADA) CONTRATADA	**(INSERIR NOME COMPLETO DA TESTEMUNHA)** TESTEMUNHA DA CONTRATADA (INSERIR NOME COMPLETO DA EMPRESA CONTRATADA)

ANEXO I - RELAÇÃO DE SERVIÇOS/EXAMES

Nº do item no mapa de preços	Código	Descrição do Serviço	Apresentação	Quantidade Total
xx	xx	**Solução de Proteção de Perímetro do tipo Next Generation Firewall NGFW** - Solução de proteção de perímetro baseada em firewalls de próxima geração, responsável pela inspeção do tráfego em camadas 3 a 7, controle de aplicações, prevenção de intrusões, filtragem de URLs, proteção contra malware e estabelecimento de túneis VPN para 36 meses de licenciamento e suporte.	Unidades	2
xx	xx	**Solução de Gerenciamento Centralizado Inteligente** - Plataforma de gerenciamento centralizado dos firewalls NGFW, em nuvem do fabricante ou appliance dedicado, permitindo administração unificada de políticas, correlação e visualização de logs, geração de relatórios, análise de ameaças e acompanhamento da postura de segurança de todo o ambiente para 36 meses de licenciamento e suporte.	Unidades	1
xx	xx	**Serviço de Suporte da CONTRATADA -** Serviço de suporte técnico especializado para os firewalls NGFW e para a solução de gerenciamento centralizado, incluindo atendimento remoto, apoio na operação da solução, abertura e acompanhamento de chamados junto ao fabricante, bem como manutenção corretiva e evolutiva e atualização de software e assinaturas de segurança durante o período contratual de 36 meses	Meses	36
xx	xx	**Serviço de Instalação da CONTRATADA -** Serviço de instalação, configuração inicial e comissionamento dos firewalls NGFW e da solução de gerenciamento centralizado, incluindo integração à rede da CONTRATANTE, configuração de alta disponibilidade, ajustes de políticas básicas de segurança, realização de testes de aceitação e entrega de documentação técnica do ambiente implantado.	Unidades	2
xx	xx	**Serviço de Treinamento da CONTRATADA -** Treinamento remoto de administração básica da solução de Firewall de Próxima Geração (NGFW), com carga horária total de 20 (vinte) horas para até 5 (cinco) alunos, abordando conceitos fundamentais da plataforma, interfaces e zonas, objetos e políticas de segurança, NAT, controle de aplicações e usuários, perfis de segurança e VPN. O objetivo é capacitar a equipe da CONTRATANTE para realizar a operação diária do firewall, incluindo monitoramento, interpretação de logs, procedimentos básicos de troubleshooting, alta disponibilidade e gerenciamento de configuração.	Alunos	5

ANEXO II - QUESTIONÁRIO DE *DUE DILIGENCE*

QUALIFICAÇÃO DA EMPRESA E IDENTIFICAÇÃO DO(S) RESPONSÁVEL(IS) LEGAL(IS)	
RAZÃO SOCIAL:	
NOME FANTASIA:	
CNPJ:	INSCRIÇÃO ESTADUAL:
DATA DE CONSTITUIÇÃO DA EMPRESA:	
DESCRIÇÃO DO OBJETO SOCIAL:	
ENDEREÇO:	
QUADRO SOCIAL:	
QUANTIDADE DE FUNCIONÁRIOS:	
RELACIONE O(S) REPRESENTANTE(S) LEGAL (IS) DA EMPRESA CONFORME CONTRATO SOCIAL/ESTATUTO SOCIAL:	
TELEFONE(S) E E-MAIL(S) DO(S) REPRESENTANTE(S) LEGAL(IS) DA EMPRESA:	
SITE DA EMPRESA:	
RESPONSÁVEL PELO PREENCHIMENTO (NOME COMPLETO):	
CONTATO (TELEFONE/E-MAIL):	
DEPARTAMENTO/FUNÇÃO:	

Porte da Empresa

- ☐ Microempresa – Faturamento menor ou igual a R$ 360 mil.
- ☐ Pequena empresa – Faturamento maior que R$ 360 mil e menor ou igual a R$ 4,8 milhões.
- ☐ Média empresa – Faturamento maior que R$ 4,8 milhões e menor ou igual a R$ 300 milhões.
- ☐ Grande empresa – Faturamento maior que R$ 300 milhões.

Ramo principal de atividade da empresa

- ☐ Comercial
- ☐ Industrial
- ☐ Prestação de Serviços

CLASSIFICAÇÃO DO CONTRATO QUANTO AOS RISCOS DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

1. A empresa já iniciou o processo de adequação à Lei Geral de Proteção de Dados Pessoais (LGPD)?
   ☐ Sim ☐ Não
2. A empresa realiza o tratamento de dados pessoais sensíveis? (dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural)
   ☐ Sim ☐ Não
   Especifique:
   _____
3. Os dados sensíveis são compartilhados com terceiros?
   ☐ Sim ☐ Não
4. A empresa realiza o tratamento de dados de crianças e adolescentes?
   ☐ Sim ☐ Não
5. A empresa já designou um Encarregado (DPO)?Em caso positivo, informe o nome e contato
   ☐ Sim ☐ Não
   Nome: _____
   Contato: _____
6. Os contratos com terceiros da empresa possuem cláusulas compatíveis com os termos e condições das leis de proteção de dados em vigor?
   ☐ Sim ☐ Não ☐ Em adequação
7. A empresa já identificou as bases legais para justificar o(s) tratamento(s) de dados que realiza?
   ☐ Sim ☐ Não ☐ Em adequação
8. A empresa possui registro das atividades de tratamento de dados que realiza, conforme dispõe o art. 37 da LGPD?
   ☐ Sim ☐ Não ☐ Em adequação
9. Em caso de atividades de tratamento de dados pessoais que resultem em um alto risco para os titulares de dados, a empresa possui um Relatório de Impacto à Proteção de Dados Pessoais?
   ☐ Sim ☐ Não ☐ Em adequação
10. A empresa tem a intenção de subcontratar outra empresa para a realização do serviço? Se a resposta for positiva, especifique.
    ☐ Sim ☐ Não
    Especifique:
    _____
11. A empresa já possui algum procedimento para atender os direitos dos titulares de dados?
    ☐ Sim ☐ Não ☐ Em adequação
12. A empresa possui algum canal de comunicação com o titular de dados?
    ☐ Sim ☐ Não ☐ Em adequação

13. A empresa possui políticas de privacidade (interna e externa) e boas práticas com relação a proteção de dados pessoais alinhadas com as regras da LGPD?
    ☐ Sim ☐ Não ☐ Em adequação
14. A empresa possui Política de Segurança da Informação?
15. ☐ Sim ☐ Não ☐ Em adequação
16. A empresa possui plano de resposta a incidentes envolvendo dados pessoais?
    ☐ Sim ☐ Não ☐ Em adequação
17. O tratamento dos dados será realizado apenas no Brasil?
    ☐ Sim ☐ Não
18. A empresa possui algum tipo de metodologia para fins de acompanhamento das alterações jurídicas, legais e jurisprudenciais relacionadas à LGPD e proteção de dados pessoais no Brasil?
    ☐ Sim ☐ Não
19. A empresa possui sistema operacional legalizado e registrado em seus computadores?
    ☐ Sim ☐ Não
20. A empresa possui um antivírus padrão instalado nos computadores?
    ☐ Sim ☐ Não
21. A empresa possui Firewall? Quais?
    ☐ Sim ☐ Não
    Especifique:
    _____
22. A empresa utiliza sistemas de colaboração em nuvem (Ex: Office 365 ou G-Suite)?
    ☐ Sim ☐ Não
    Especifique:
    _____
23. Os servidores da sua empresa estão em ambiente físico ou em Nuvem?
    ☐ Físico ☐ Nuvem ☐ Híbrido
24. Se os servidores estão armazenados em nuvem ou híbrido, em qual país estão hospedados?
    _____
25. A empresa possui rotina de backup? Onde são armazenados?
    ☐ Não tem backup
    ☐ Sim, armazenados na nuvem
    ☐ Sim, armazenados em servidor local
    ☐ Sim, armazenados no servidor local e na nuvem
26. A empresa possui políticas, procedimentos e medidas protetivas (controles de acesso, criptografia, modificação de dados, mascaramento de dados) que proporcionam segurança e garantem a conformidade com os regulamentos/leis de privacidade?
    ☐ Sim ☐ Não ☐ Em adequação
27. A empresa conduz, periodicamente, avaliações de vulnerabilidade e testes de penetração em seus sistemas de tratamento de dados pessoais?
    ☐ Sim ☐ Não
28. A empresa é certificada em algum padrão ou framework de segurança?
    ☐ Sim ☐ Não

Especifique:

_____

29. A empresa é capaz de detectar rapidamente incidentes de segurança (incluindo acesso não autorizado, destruição, perda, alteração e violação de dados)?

☐ Sim ☐ Não

30. A empresa possui uma política de revisão regular das permissões de acesso aos dados pessoais que garanta o acesso somente aos funcionários e contratados que precisam ter acesso, bem como um procedimento para prevenir prontamente funcionários e contratados desligados de acesso a dados pessoais?

☐ Sim ☐ Não

31. A empresa exige que seus funcionários e prestadores de serviços assinem acordos de confidencialidade e sigilo das informações?

☐ Sim ☐ Não

32. A empresa passou por algum incidente de segurança nos últimos 2 (dois) anos? Se a resposta for positiva, relate qual(is) incidente(s) e qual(is) providência(s) foram adotadas.

☐ Sim ☐ Não

Especifique:

_____

33. A empresa possui procedimentos para atender as solicitações para eliminar dados pessoais de seus sistemas, se necessário e legal?

☐ Sim ☐ Não

RESPONSABILIDADES E CONDIÇÕES

1. A empresa assume a responsabilidade de manter procedimento para efetivação dos direitos dos titulares dos dados pessoais.

☐ Concorda ☐ Não concorda

2. A empresa reconhece que na hipótese de tratamento de dados pessoais sensíveis, estes, serão tratados com um maior rigor legal e, portanto, deve garantir que as proteções técnicas e organizacionais sejam implementadas, a fim de manter a segurança dos dados pessoais.

☐ Concorda ☐ Não concorda

3. A empresa assume a responsabilidade de manter medidas de segurança capazes de proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, ou qualquer forma de tratamento inadequado ou ilícito, como previsto na legislação.

☐ Concorda ☐ Não concorda

4. A empresa está ciente que deve seguir as instruções exclusivas do controlador (quando o Icipe ocupar respectiva posição) sobre o tratamento de dados pessoais.

☐ Concorda ☐ Não concorda

5. A empresa está ciente que deve garantir que seus funcionários que tratam dados pessoais estão sujeitos a um dever de sigilo e confidencialidade.

☐ Concorda ☐ Não concorda

6. A empresa está ciente que nos casos nos quais seja necessário envolver um subcontratado, deverá obter, primeiramente, autorização prévia do Icipe e de acordo com o estipulado em contrato firmado entre as Partes?

☐ Concorda ☐ Não concorda

7. A empresa concorda e assume o compromisso de realizar o tratamento dos dados pessoais envolvidos na contratação, em consonância com as determinações da LGPD.

☐ Concorda ☐ Não concorda

8. A empresa concorda e assume o compromisso de tratar os dados pessoais exclusivamente em razão do objeto do contrato firmado entre as partes, e conforme as indicações do Icipe, aplicando todas as medidas de segurança necessárias, sejam elas organizacionais, técnicas e/ou operacionais, além de manter a confidencialidade das informações pessoais.

☐ Concorda ☐ Não concorda

9. A empresa concorda e assume o compromisso de notificar imediatamente o Icipe quando da ocorrência de qualquer incidente que tenha potencial de afetar a segurança dos dados pessoais, incluindo, mas sem se limitar a: (i) recebimento de qualquer solicitação de uma autoridade que tiver como objeto a divulgação de dados pessoais; e/ou (ii) ocorrência de qualquer incidente de segurança que afete, ou possa afetar, os dados pessoais.

☐ Concorda ☐ Não concorda

10. A empresa concorda e assume o compromisso de notificar o Icipe ao receber qualquer solicitação ou queixa por parte dos titulares de dados a respeito dos dados pessoais, abstendo- se de contestar o titular sem a prévia autorização, por escrito do Icipe, sempre que esses titulares tenham relação com o objeto do contrato firmado entre as partes.

☐ Concorda ☐ Não concorda

11. A empresa concorda e assume o compromisso de excluir e/ou anonimizar os dados pessoais, após o término do prazo legal para seu armazenamento, assim como em quaisquer dos seguintes casos, salvo se existir algum impedimento legal para tanto: (i) quando tenha terminado a relação contratual com o Icipe, ou (ii) por instruções expressas e/ou por escrito do Icipe.

☐ Concorda ☐ Não concorda

12. A empresa concorda e assume o compromisso de auxiliar o Icipe, no que for necessário, para: (i) o atendimento de solicitações de titulares de dados pessoais, bem como requisições de informações, (ii) atendimento à Autoridade Nacional de Proteção de Dados (ANPD), e (iii) cooperar com o Icipe em eventuais procedimentos judiciais e/ou extrajudiciais que envolvam os dados pessoais.

☐ Concorda ☐ Não concorda

13. A empresa está ciente que deve se submeter a auditorias e inspeções por parte do Icipe em relação à proteção de dados e segurança da informação.

☐ Concorda ☐ Não concorda

Declaro, sob as penas da lei, que as informações prestadas neste questionário são verdadeiras, completas e atualizadas.

Local e data: _____, ___, _____ de 2024.

_____

Assinatura