PREGÃO PRESENCIAL Nº 07/2023
PROCESSO Nº 0544/2023
ANO VIGENTE - 2023

CONTRATAÇÃO DE COMPUTAÇÃO EM NUVEM, LINK DEDICADO E BACKUP PARA O CENTRO UNIVERSITÁRIO FMABC.

1. PREÂMBULO.

1.1. O Centro Universitário FMABC, com sede na Avenida Lauro Gomes, 2.000, Vila Sacadura Cabral, Santo André, São Paulo/SP, CEP 09060-870, inscrita no CNPJ sob nº 57.571.275/0007-98, torna público que fará realizar licitação na modalidade PREGÃO PRESENCIAL, do tipo menor preço global, visando a CONTRATAÇÃO DE COMPUTAÇÃO EM NUVEM, LINK DEDICADO E BACKUP PARA O CENTRO UNIVERSITÁRIO FMABC, nas condições e especificações constantes do Anexo I - Termo de Referência, de acordo com a nova Lei Geral de Licitações e Contratos nº 14.133 de 1º de abril de 2021, e, subsidiariamente, pela Lei Complementar 123, de 14 de dezembro de 2006, suas alterações posteriores e demais normas legais pertinentes.

1.2. **LOCAL E DATA.**

1.2.1. **Da Entrega dos envelopes de Documentos de Habilitação e de Proposta de Preços: DATA/HORA:** Dia 19 de setembro de 2023, até as 10h00min.

LOCAL: Salão Nobre - Prédio Administrativo do Centro Universitário FMABC, Avenida Lauro Gomes, 2.000, Vila Sacadura Cabral, Santo André, São Paulo/SP, CEP 09060-870.

1.2.2. Da abertura da sessão:

DATA/HORA: Dia 19 de setembro de 2023, às 10h00min.

LOCAL: Salão Nobre - Prédio Administrativo do Centro Universitário FMABC, Avenida Lauro Gomes, 2.000, Vila Sacadura Cabral, Santo André, São Paulo/SP, CEP 09060-870.

1.2.3. É vedado ao setor de compras do Centro Universitário FMABC receber as propostas além do horário acima descrito, ou fora do local determinado.

2. OBJETO

Visa o presente a contratação de empresa especializada para prestação de serviço de hospedagem, conectividade, segurança de rede e backup (cópia de segurança), incluindo todos os serviços de garantia de funcionamento e suporte técnico, visando atender às necessidades de infraestrutura desta Instituição de Ensino Superior, nas condições e especificações constantes do Termo de Referência e de acordo com a Nova Lei Geral de Licitações e Contratos nº 14.133 de 1º de abril de 2021, em seu artigo 28, Inciso I.

3. DO EDITAL E SEUS ANEXOS.

3.1. O presente edital estará disponível a qualquer interessado, à partir da data de publicação do respectivo Aviso, e poderá ser examinada e obtida com o setor de Compras do Centro Universitário FMABC, na sede da Instituição, cujo endereço consta no preâmbulo, de segunda à sexta-feira das 9:00 às 16:00, ou no sítio eletrônico: www.fuabc.org.br, no campo de “Publicações Oficiais” > “Editais”.

3.2. Incluem-se como anexo do Edital, como se nela estivessem transcritos, os seguintes Anexos:

Anexo I	ESPECIFICAÇÃO DOS SERVIÇOS – TERMO DE REFERÊNCIA;
Anexo II	MODELO DE PROPOSTA
Anexo III	MODELO DE ATESTADO DE CAPACIDADE TÉCNICA
Anexo IV	MODELO DE DECLARAÇÃO QUE NÃO EMPREGA MENOR
Anexo V	MODELO DE DECLARAÇÃO DE MANUTENÇÃO DAS CONDIÇÕES CONTRATUAIS
Anexo VI	MODELO DE DECLARAÇÃO DE PLENO ATENDIMENTO
Anexo VII	MODELO DECLARAÇÃO DE ENQUADRAMENTO COMO MICROEMPRESA OU EMPRESA DE PEQUENO PORTE
Anexo VIII	MODELO DE DECLARAÇÃO DE SUPERVENIÊNCIA DE FATO IMPEDITIVO PARA HABILITAÇÃO
Anexo IX	MODELO DE DECLARAÇÃO DE ELABORAÇÃO INDEPENDENTE DE PROPOSTA E ATUAÇÃO CONFORME AO MARCO LEGAL ANTICORRUPÇÃO
Anexo X	MINUTA DO CONTRATO
Anexo XI	TERMO DE RESPONSABILIDADE PELO TRATAMENTO DE DADOS PESSOAIS - FORNECEDOR

4. CONDIÇÕES DE PARTICIPAÇÃO

Poderão participar da presente Licitação:

4.1. Empresas estabelecidas em qualquer localidade do território nacional, identificadas com o objeto em questão, que tenham protocolado a entrega dos envelopes de Documentos de Habilitação e de Proposta de Preço na sede do Centro Universitário FMABC até a data e hora limite fixadas, com exceção dos casos relacionados no item 4.2.

4.2. Não poderão participar da presente Licitação:

a) empresas em consórcio;

b) sociedades cooperativas;

c) empresas concordatárias, em recuperação judicial ou extrajudicial, ou cuja falência tenha sido declarada, que se encontram sob concurso de credores, em dissolução ou em liquidação;

d) empresas punidas com suspensão ou que tenham sido declaradas inidôneas para licitar ou contratar com a Administração Pública Direta ou Indireta, bem como com a Fundação do ABC – Centro Universitário FMABC;

e) empresas cujos diretores, gerentes, sócios e empregados sejam servidores, empregados ou dirigentes da empresa licitante;

f) não ter sido descredenciado, nem ter contrato anterior rescindido por iniciativa do Centro Universitário FMABC, decorrente de culpa, e/ou que teve contrato anterior rescindido por iniciativa da empresa, salvo mediante apresentação de justificativa aceita pela Centro Universitário da FMABC.

Parágrafo único – As empresas que estiverem sob processo falimentar, facultada a participação de empresa que esteja em recuperação judicial, mediante apresentação, durante a fase de habilitação, do Plano de Recuperação já homologado pelo juízo competente e em pleno vigor, nos termos da Súmula 50 do TCE.

5. FORMA DE APRESENTAÇÃO DOS ENVELOPES

5.1. Os Documentos de Habilitação e de Proposta de Preços deverão ser apresentados em envelopes distintos e fechados (preferencialmente opacos e rubricados no fecho), de forma a não permitir a violação de seu conteúdo, e identificados com etiqueta conforme o modelo abaixo estabelecido no item 5.3.
5.2. Os envelopes deverão ser endereçados ao setor de Compras do Centro Universitário FMABC e ter a entrega registrada até a data e hora fixadas no subitem 1.2.1.
5.3. Os envelopes deverão ser identificados com etiqueta conforme o modelo abaixo:

I – ENVELOPE Nº 01 – HABILITAÇÃO
- Documentação
- COMPRAS – CENTRO UNIVERSITÁRIO FMABC
- Pregão nº 07/2023
- Nome completo da licitante
- CNPJ
- Contato: e-mail + telefone

II – ENVELOPE Nº 02 – PROPOSTA
- Proposta de Preços
- COMPRAS – CENTRO UNIVERSITÁRIO FMABC
- Pregão nº 07/2023
- Nome completo da licitante
- CNPJ
- Contato: e-mail + telefone

6. DO CREDENCIAMENTO.

6.1. Será admitido apenas 1 (um) representante credenciado para cada Licitante.
6.2. Para comprovar a representação legal ou a qualidade de preposto da Licitante, o representante entregará juntamente com seu documento de identidade de fé pública (será aceito o RG - Carteira de Identidade Civil ou documento de Identidade expedido por Órgão de Registro Profissional):
a) se procurador, procuração pública ou particular (acompanhada de cópia autenticada do contrato social/estatuto social da empresa), com poderes específicos para representar a empresa na licitação em todas as suas fases, e em todos os demais atos, em nome da licitante; ou
b) se representante legal, cópia autenticada do contrato social, estatuto ou ata de eleição do dirigente da licitante.

6.3. A credencial não é obrigatória, mas somente poderá manifestar-se nas sessões de abertura dos envelopes o representante devidamente credenciado.
6.4. Toda a documentação relativa ao credenciamento deverá ser apresentada fora do envelope de "Habilitação ou proposta.
6.5. A empresa licitante somente poderá se pronunciar através de seu representante credenciado e ficará obrigada pelas declarações e manifestações do mesmo.

7. DOS DOCUMENTOS DE HABILITAÇÃO

7.1. Nos Documentos de Habilitação deverão constar (i.) o nome/razão social da Licitante, (ii.) o número do CNPJ, observado que:

a) se a licitante for matriz, os documentos deverão estar em nome da matriz;

b) se a licitante for a filial, os documentos deverão estar em nome da filial, salvo situação expressa no documento válido para matriz e filiais.

7.2. As Licitantes que por sua natureza ou por força de lei estiverem dispensadas da apresentação de determinados documentos de habilitação deverão apresentar declaração identificando a situação e citando os dispositivos legais pertinentes.
7.3. Os Documentos de Habilitação devem ser apresentados no idioma nacional em 1 (uma) via rubricada em todas as suas páginas por representante legal ou preposto da licitante, e preferencialmente (i.) com furação dupla central, (ii.) com as páginas numeradas sequencialmente, e (iii.) acompanhados de um sumário de documentos.
7.4. Os Documentos de Habilitação somente poderão ser apresentados (i.) por qualquer processo de cópia autenticada por cartório competente ou por membro da Comissão Permanente de Licitação, mediante a apresentação do documento original, ou (ii.) publicação em órgão da imprensa oficial.
7.4.1. Documentos oficiais emitidos pela Internet ficam condicionados à verificação de autenticidade pela Comissão Permanente de Licitações da FUABC.
7.4.2. As cópias simples, acompanhadas dos documentos originais, deverão ser entregues para autenticação à Comissão Permanente de Licitações da FUABC durante a sessão de abertura dos Documentos de Habilitação.

7.5. Os Documentos de Habilitação compreendem:

a) **documentos relativos à habilitação jurídica;**

b) **documentos relativos à regularidade fiscal e trabalhista;**

c) **documentos relativos à qualificação econômico-financeira;**

d) **documentos relativos à qualificação técnica.**

7.6. Compõem os documentos relativos à **habilitação jurídica:**

a) Ato Constitutivo, estatuto ou contrato social e suas alterações em vigor, devidamente registrados no órgão competente, em se tratando de sociedades empresárias, e, no caso de sociedades por ações, acompanhado de documento de eleição de seus administradores, e ainda no caso de sociedade simples (civil), inscrição do ato constitutivo acompanhada de prova da diretoria em exercício. O ato constitutivo deverá comprovar, que a atividade da empresa é compatível com o objeto deste procedimento licitatório e o constante do Termo de Referência.

b) Declaração de cumprimento do disposto no inciso XXXIII, do art. 7º, da Constituição Federal, relativamente à proibição de trabalho noturno, perigoso ou insalubre a menores de dezoito e de qualquer trabalho a menores de dezesseis anos, salvo na condição de aprendiz, a partir de quatorze anos, conforme modelo **Anexo IV**.

c) Declaração de manutenção das condições contratuais, conforme modelo **Anexo V**.

d) Declaração da empresa licitante de que aceita os termos do presente Edital, em todas as fases do processo licitatório modelo **Anexo VI**.

e) Declaração da empresa licitante de superveniência de fato impeditivo para habilitação modelo Anexo **VIII**.

f) Declaração da empresa licitante de elaboração independente de proposta e atuação conforme ao marco legal anticorrupção modelo Anexo **IX**.

7.6.1 As empresas enquadradas como microempresas ou empresas de pequeno porte que desejam usufruir do tratamento favorecido estabelecido nos artigos 42 a 49 da Lei Complementar n.º 123 de 2006, nos termos do artigo 11.º do Decreto Lei n.º 6.204/2007, (conforme modelo **Anexo VII**) deverão entregar:

a) Certidão expedida pelo órgão de registro competente atestando que a empresa se enquadra na condição de ME ou EPP na forma da Lei Complementar 123/2006.

7.7. Compõem os documentos relativos à **regularidade fiscal e trabalhista**:

a) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas do Ministério da Fazenda – CNPJ/MF;

b) Prova de regularidade perante a Fazenda Federal, Dívida Ativa da União e Seguridade Social (INSS), mediante Certidão Negativa Conjunta de Débitos;

c) Prova de regularidade perante a Fazenda Estadual do Estado de São Paulo e da Unidade da Federação da sede da Licitante, mediante apresentação de Certidão(ões) Negativa(s) de Débitos expedida pelo(s) órgão(s) competente(s);

d) Prova de regularidade perante a Fazenda Municipal da sede da Licitante, mediante apresentação de Certidão Negativa de Débitos expedida pelo órgão competente;

e) Prova de Inscrição Estadual ou Municipal, relativo ao domicilio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto da licitação.

f) Prova de regularidade relativa ao Fundo de Garantia por Tempo de Serviço (FGTS), mediante apresentação de Certificado de Regularidade de Situação (CRS) expedido pela Caixa Econômica Federal, de acordo com a Lei n.° 8.036, de 11 de maio de 1990;

f) Comprovação da inexistência de débitos perante à Justiça do Trabalho, mediante a apresentação de Certidão Negativa de Débitos Trabalhistas – CNDT.

7.7.1. Os documentos devem estar válidos na data de realização da sessão, caso possuam prazo determinado de validade. Será considerada como válida pelo prazo de 90 (noventa) dias, contados a partir da data da respectiva emissão, o documento que não apresentar prazo de validade, exceto se anexada legislação específica para o respectivo documento.

7.7.2. Serão aceitas Certidões Positivas com Efeito de Negativas.

7.7.3. As microempresas e empresas de pequeno porte, por ocasião da participação deste certame licitatório ficam obrigadas a apresentar toda documentação exigida, inclusive, as pertinentes à comprovação de regularidade fiscal, mesmo que apresentem alguma restrição.

7.7.3.1. Havendo alguma restrição na comprovação da regularidade fiscal e trabalhista, será assegurado o prazo de 5 (cinco) dias úteis, cujo termo inicial corresponderá ao momento em que o licitante proponente for declarado o vencedor do certame, prorrogáveis por igual período, mediante solicitação do licitante e a critério da FUABC – Centro Universitário FMABC, para a regularização da documentação, pagamento ou parcelamento do débito, e a emissão de eventuais certidões negativas ou positivas com efeito de certidão negativa.

7.7.3.2. A não regularização da documentação relativa à regularidade fiscal e

trabalhista, no prazo previsto no subitem anterior, implicará decadência do direito à contratação, sem prejuízo das sanções previstas na Lei 14.133/2021, sendo facultado à FUABC – Centro Universitário FMABC, convocar os licitantes remanescentes, na ordem de classificação, para a assinatura do contrato, ou revogar a licitação.

7.8. Compõem os documentos relativos à **qualificação econômico-financeira:**

7.8.1. Certidão negativa de falência ou recuperação judicial expedida pelo Poder Judiciário, através da Comarca da sede do licitante, com prazo de validade determinado no documento ou com a data de emissão não superior a 90 (noventa) dias.
7.8.1.1. Caso o Poder Judiciário da sede do licitante não forneça o documento com informações unificadas da Comarca, deverá apresentar a Certidão negativa de falência ou recuperação judicial juntamente com documento emitido pelo órgão judiciário competente, que relacione o(s) distribuidor (es) que na Comarca de sua sede tem atribuição para expedir Certidões Negativas de Falência ou Recuperação Judicial.
7.8.1.2. Balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrados há mais de 3 (três) meses da data de apresentação da proposta;

7.9. Compõem os documentos relativos à **qualificação técnica:**

7.9.1 Para comprovação da qualificação técnica, a licitante deverá apresentar atestado de capacidade técnica fornecido por pessoas jurídicas de direito público ou privado, conforme **ANEXO III**, no qual deverá estar comprovado que desempenha ou desempenhou em favor dos signatários, atividade compatível em características e prazo com o Objeto pretendido pela Contratante.

8. DO VALOR E DOS RECURSOS ORÇAMENTÁRIOS

8.1. O **valor total máximo referencial estimado** aceito pelo Centro Universitário FMABC, considerando a quantidade mínima do ANEXO II,) para a prestação dos serviços é de R$ 491.630,00 (quatrocentos e noventa e um mil seiscentos e trinta reais) anual, correspondendo ao valor mensal estimado de R$ 40.969,17 (Quarenta mil novecentos e sessenta e nove reais e dezessete centavos).
8.2. Em havendo prorrogação do presente contrato de prestação de serviços, e após decorrido 12 (doze) meses, poderá haver reajustamento de preços, com a devida solicitação expressa da Contratada e anuência da Contratante, conforme descrito abaixo:
8.3. Ficará instituído o IPCA - Índice de Preços ao Consumidor Amplo, para reajustamento de preços após decorridos 12 meses de contrato com anuência da Contratante.
8.4. O Centro Universitário FMABC não assumirá responsabilidade alguma por pagamento de impostos e encargos que competirem a Contratada, nem estará obrigado a restituir-lhe valores, principais e acessórios, que porventura despender com pagamento dessa natureza.

9. DA PROPOSTA DE PREÇOS

9.1. Deverá ser entregue no envelope de Proposta de Preços:
9.1.1. A Proposta de Preço deverá ser apresentada em uma via, de acordo com o modelo constante do **Anexo II**, devendo obrigatoriamente, ser digitada ou impressa por

qualquer processo eletrônico, estar em idioma nacional, sem cotações alternativas, emendas, rasuras ou entrelinhas, estar rubricada em todas as páginas e assinada na última página pelo representante legal ou preposto da licitante. E, preferencialmente (i) em papel timbrado da companhia, e (ii) com as páginas numeradas sequencialmente.

9.1.2. A Proposta de Preço deve ser apresentada contendo obrigatoriamente:

a) a identificação do objeto ofertado, observadas as especificações constantes do **Anexo I**, e quaisquer outros elementos referentes ao produto cotado;

b) o Preço Unitário e Total, expresso em reais, com no máximo 2 (dois) algarismos decimais;

c) a validade da proposta, a qual fica estabelecida como sendo de no mínimo **60 (sessenta) dias** contados da data do protocolo de entrega das propostas.

9.1.3. No Preço Total da Proposta devem estar inclusos a remuneração e todos os custos e despesas relacionados ao material a ser adquirido por completo.

10. DO PRAZO DE INICIAÇÃO DOS SERVIÇOS E PAGAMENTO.

10.1. Os prazos de iniciação e as condições de pagamento estão definidos no Anexo I - Termo de Referência.

11. DOS PROCEDIMENTOS DA LICITAÇÃO: HABILITAÇÃO DOS LICITANTES E CLASSIFICAÇÃO DAS PROPOSTAS DE PREÇO.

11.1. No dia, horário e local indicados no preâmbulo será realizada a sessão pública de processamento do Pregão para recebimento das propostas, devendo o interessado ou seu representante apresentar identificação e se for o caso, comprovante da existência dos necessários poderes para formulação de propostas e para a prática de todos os demais atos inerentes ao certame.

11.2. Aberta a sessão, os interessados e seus representantes, entregarão ao(a) pregoeiro(a) para credenciamento declaração dando ciência de que cumprem plenamente os requisitos de habilitação, de acordo com os modelos constantes dos anexos deste Edital, e, em envelopes separados, a proposta de preços e os documentos de habilitação.

11.3. Analisado os credenciamentos, serão lançados em atas os nomes dos representantes legais e/ou procuradores dos licitantes.

11.4. Iniciada a abertura do primeiro envelope de proposta, estará encerrado o credenciamento e, por consequência, a possibilidade de admissão de novos participantes.

11.5. A análise das propostas pelo Pregoeiro visará ao atendimento das condições estabelecidas neste Edital e seus anexos, sendo desclassificadas as propostas:

a) Cujo objeto não atenda às especificações, prazos e condições fixados neste Edital;

b) Que apresentem preço baseado exclusivamente em proposta das demais licitantes;

c) Cujos preços forem excessivos ou incompatíveis com os valores de mercado;

d) Cujos preços globais forem simbólicos ou irrisórios, ou manifestamente inexequíveis. Serão considerados inexequíveis aqueles preços cuja viabilidade não tenha sido demonstrada pelo Licitante.

11.4.2. No que diz respeito aos preços, as propostas serão verificadas quanto à exatidão das operações aritméticas que conduziram ao valor total orçado, procedendo-se às correções no caso de eventuais erros, tomando-se como corretos os preços unitários. As correções efetuadas serão consideradas para apuração do valor da proposta.

11.4.2. Serão desconsideradas ofertas ou vantagens baseadas nas propostas das

demais licitantes.
11.5. Para julgamento e classificação das propostas será adotado critério de **MENOR PREÇO GLOBAL,** observadas as especificações exigidas neste Edital.
11.6. As propostas não desclassificadas serão selecionadas para a etapa de lances, com observância dos seguintes critérios:
a) seleção da proposta de menor preço e as demais com preços até 10% (dez por cento) superiores àquela;
b) não havendo pelo menos 03 (três) preços na condição definida na alínea anterior, serão selecionadas as propostas que apresentarem os menores preços, até o máximo de 3 (três). No caso de empate nos preços, serão admitidas todas as propostas empatadas, independentemente do número de licitantes.
11.7. Para efeito de seleção será considerado o valor global.
11.8. O(A) Pregoeiro(a) convidará individualmente os autores das propostas selecionadas a formular lances de forma sequencial, à partir do autor da proposta de maior preço e os demais em ordem decrescente de valor, decidindo-se por meio de sorteio no caso de empate de preços.
11.8.1. O licitante sorteado em primeiro lugar poderá escolher a posição na ordenação de lances em relação aos demais empatados, e assim sucessivamente até a definição completa da ordem de lances.
11.9. Os lances deverão ser formulados em valores distintos e decrescentes, inferiores à proposta de menor preço.
11.9.1. A desistência em apresentar lance verbal, quando convocado pelo(a) pregoeiro(a), implicará na exclusão do licitante da etapa de lances verbais e na manutenção do último preço apresentado pelo licitante, para efeito de posterior ordenação das propostas.
11.10. A etapa de lances será considerada encerrada quando todos os participantes dessa etapa declinarem da formulação de lances.
11.11. Encerrada a etapa de lances, serão classificadas as propostas selecionadas e não selecionadas para a etapa de lances, em ordem crescente de valores, considerando-se para as selecionadas o último preço ofertado.
11.12. - Não será admitida desistência da proposta inicial ou dos lances ofertados, sujeitando-se o licitante desistente às penalidades constantes neste Edital.
11.13. Se houver empate, será assegurado o exercício do direito de preferência às microempresas e empresas de pequeno porte, nos seguintes termos:
11.13.1. Entende-se por empate aquelas situações em que as propostas apresentadas pelas microempresas e empresas de pequeno porte sejam iguais ou até 5% (cinco por cento) superiores à proposta melhor classificada;
11.13.2. A microempresa ou empresa de pequeno porte cuja proposta for melhor classificada, poderá apresentar nova proposta de preço inferior àquela considerada vencedora da fase de lances, situação em que sua nova proposta será declarada a melhor oferta, dentro do intervalo estabelecido neste Edital;
11.13.3. O prazo para a formulação da proposta referida será de 05 (cinco) minutos, contados da convocação do(a) Pregoeiro(a), sob pena de preclusão;
11.13.4. Se houver equivalência dos valores das propostas apresentadas pelas microempresas e empresas de pequeno porte que se encontrem no intervalo estabelecido, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá exercer a preferência e apresentar nova proposta;
11.13.5. Entende-se por equivalência dos valores das propostas as que apresentarem igual valor, respeitada a ordem de classificação.
11.13.5.1. O exercício do direito de preferência somente será aplicado quando a melhor oferta da fase de lances não tiver sido apresentada por microempresa ou empresa de pequeno porte.
11.14. Não configurada a contratação de microempresa ou empresa de pequeno porte, será declarada a melhor oferta a proposta originalmente vencedora da fase de lances.

11.16 O(A) Pregoeiro(a) poderá negociar com o autor da oferta de menor valor com vistas à redução do preço.

11.17. Após a negociação, se houver, o(a) Pregoeiro(a) examinará a aceitabilidade do menor preço, decidindo motivadamente a respeito.

11.18. Considerada aceitável a oferta de menor preço será aberto o Envelope nº 02, contendo os documentos de habilitação de seu autor.

11.19 Eventuais falhas, omissões ou outras irregularidades nos documentos de habilitação poderão ser saneadas na sessão pública de processamento do Pregão, até a decisão sobre a habilitação, desde que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante decisão fundamentada do pregoeiro;

11.19.1. A verificação será certificada pelo(a) Pregoeiro(a) e deverá ser anexada aos autos os documentos passíveis de obtenção por meio eletrônico, salvo impossibilidade devidamente justificada.

11.19.2 A Instituição licitante não se responsabilizará pela eventual indisponibilidade dos meios eletrônicos, no momento da verificação. Ocorrendo essa indisponibilidade e não sendo apresentados os documentos alcançados pela verificação, o licitante será inabilitado.

11.20. Constatado o atendimento dos requisitos de habilitação previstos neste Edital, o licitante será habilitado e **declarado provisoriamente vencedor do certame.**

11.21. Se a oferta não for aceitável, ou se a licitante desatender as exigências para a habilitação e/ou não demonstrar o sistema integrado, de acordo com o exigido, o Pregoeiro examinará a oferta subseqüente de menor preço, observado o direito de preferência estipulado na Lei Complementar nº 123/2006, negociará com o seu autor, decidirá sobre a sua aceitabilidade e, em caso positivo, verificará as condições de habilitação e assim sucessivamente, até a apuração de uma oferta aceitável cujo autor atenda os requisitos de habilitação, caso em que será declarado vencedor.

11.22. Caso, excepcionalmente, seja suspensa ou encerrada a sessão antes de cumpridas todas as fases preestabelecidas, os envelopes, devidamente rubricados pelo pregoeiro e pelos representantes credenciados, ficarão sob a guarda do(a) pregoeiro(a), sendo exibidos aos licitantes na reabertura da sessão ou na nova sessão previamente marcada para prosseguimento dos trabalhos.

12. DO RECURSO ADMINISTRATIVO

12.1. Após declaração do vencedor, o licitante que quiser recorrer deverá manifestar imediata e motivadamente a sua intenção, abrindo-se então o prazo de 03 (três) dias úteis para apresentação de memoriais, ficando as demais licitantes desde logo intimadas para apresentar contrarrazões em igual número de dias, que começarão a correr no término do prazo do recorrente, sendo-lhes assegurada vista imediata dos autos.

12.2. A ausência de manifestação imediata e motivada do licitante importará: a decadência do direito de recurso, a adjudicação do objeto do certame pelo(a) Pregoeiro(a) ao licitante vencedor e o encaminhamento do processo à autoridade competente para a homologação.

12.3. Interposto o recurso, o(a) Pregoeiro(a) poderá reconsiderar a sua decisão ou encaminhá-lo devidamente informado à autoridade competente.

12.4. Decididos os recursos e constatada a regularidade dos atos praticados, a autoridade competente adjudicará o objeto do certame ao licitante vencedor e homologará o procedimento.

12.5. O recurso terá efeito suspensivo e o seu acolhimento importará a invalidação dos atos insuscetíveis de aproveitamento.

12.6. A adjudicação será realizada pelo pregoeiro nos termos deste Edital.

12.7. Tratando-se a adjudicatária de microempresa ou empresa de pequeno porte em

relação a qual se tenha constado restrição ou ressalva no tocante à respectiva regularidade fiscal e trabalhista ao tempo da etapa de habilitação, deverá ela demonstrar a correção da falta no prazo de cinco (5) dias úteis, que se seguirem à adjudicação, prorrogáveis por igual período a critério da Instituição licitante**,** mediante prévio pedido da interessada, sem prejuízo da imposição das sanções previstas no neste edital;

12.8. Quando a Adjudicatária se recusar a entregar a documentação exigida, bem como, se recusar a entregar o(s) item(ns) do(s) qual(is) sagrou-se vencedora, poderão ser retomados, em sessão pública, os procedimentos relativos à licitação.

12.8.1. Essa nova sessão será realizada em prazo não inferior a 03 (três) dias úteis, contados da divulgação do aviso.

13. DAS CONDIÇÕES DA PRESTAÇÃO DOS SERVIÇOS

13.1. O objeto desta contratação, deverá ser prestado em conformidade com o estabelecido no **Anexo I** – Termo de Referência, e as demais cláusulas e condições estabelecidas neste Edital e na minuta de contrato.

13.2. Os serviços, objeto do contrato decorrente da licitação, será acompanhada e fiscalizada por um funcionário especialmente designado pela Contratante.

14. DA FISCALIZAÇÃO

14.1 O Centro Unviersitário FMABC fiscalizará a prestação dos serviços através de funcionário(s) designado(s) para esse fim, com a incumbência de relatar à Contratada as falhas ou irregularidades que verificar, as quais, se não forem sanadas, serão objetos de comunicado oficial.

14.2 A prestação dos serviços será fiscalizada, em todos os aspectos pertinentes ao objeto ajustado, inclusive reservando o direito de resolução de quaisquer casos omissos ou duvidosos, não previstos no contrato, em especial as especificações, requisitos, sinalizações, segurança, implicando, o direito de rejeitar os serviços insatisfatórios.

14.3 O exercício de fiscalização por parte da Contratante não eximirá a Contratada das responsabilidades pelos danos materiais e pessoais que vier a causar a terceiros ou ao Centro Univeristário FMABC, por culpa ou dolo de seus prepostos, nos termos do Código Civil.

15. DA CONTRATAÇÃO.

15.1. Após a homologação do resultado da licitação pelo Centro Universitário FMABC, a adjudicação do objeto desta licitação, se efetivará através de CONTRATO a ser firmado com a licitante vencedora.

15.2. A celebração do contrato será formalizada com o Centro Universitário FMABC, consoante a minuta que constitui o **Anexo X** desta Licitação.

15.3. Convocação para assinatura do contrato:

15.3.1. O Centro Universitário FMABC convocará a Licitante vencedora que terá o **prazo de 5 (cinco) dias úteis**, contados da data da convocação, para assinar o termo de contrato.

15.3.2. A Licitante convocada poderá pedir prorrogação do prazo, por igual período, para assinatura do contrato, desde que formulada no curso do prazo inicial e alegado justo motivo, condicionado o atendimento do requerido, à aceitação dos motivos pela Contratante.

15.3.3. Transcorrido o prazo sem que o contrato seja assinado, a Contratante poderá, a seu critério, convocar as licitantes remanescentes, obedecida a ordem de classificação, para assinar o contrato em idêntico prazo e nas mesmas condições da proposta da Licitante Vencedora.

16. DAS DISPOSIÇÕES FINAIS

16.1 A adjudicatária, durante a execução do contrato, obriga-se a manter todas as condições de habilitação e qualificação exigidas no Pregão Nº 07/2023.

16.2. A presente licitação poderá ser revogada por razões de interesse público decorrentes de fato superveniente devidamente comprovado, ou anulada no todo ou em parte, por ilegalidade reconhecida de ofício ou provocação de terceiros, mediante parecer escrito e devidamente fundamentado, sem que seja devida qualquer indenização aos interessados.

16.3. A empresa que vier a ser contratada será responsável por executar o serviço por completo. Não se admite subcontratação.

16.4. A presente Licitação e seus anexos poderão ser alterados pela Contratante, antes de aberta a licitação, por interesse público, por sua iniciativa ou decorrente de provocação de terceiros, bem como, adiar ou prorrogar o prazo para recebimento e/ou a abertura dos documentos e propostas.

16.5. Cópia deste Edital e seus anexos poderão ser obtidos pelos interessados no endereço eletrônico (www.fuabc.org.br), no campo de “Publicações Oficiais” > “Editais” ou na sede do Centro Universitário FMABC no horário acima mencionado.

16.6. A Contratante não se responsabiliza pelo conteúdo e autenticidade de cópias desta Licitação, senão aquelas que estiverem rubricadas pela autoridade competente, ou sua cópia fiel.

16.7. As normas disciplinadoras desta licitação serão interpretadas em favor da ampliação da disputa, respeitada a igualdade de oportunidade entre as licitantes e desde que não comprometam o interesse público, a finalidade e a segurança da contratação.

16.8. Das sessões públicas de processamento do Pregão serão lavradas atas circunstanciadas, a serem assinadas pelo Pregoeiro e pelos licitantes presentes.
Os atos ocorridos na sessão pública de processamento do pregão terão efeito presuntivo, de modo que não poderão os licitantes que não se fizerem representar na sessão alegar qualquer prejuízo, em especial, quanto à formulação de lances.

16.9. Todos os documentos de habilitação cujos envelopes forem abertos na sessão e as propostas serão rubricados pelo(a) Pregoeiro(a) e pelos licitantes presentes que desejarem.

16.10. Os envelopes contendo os documentos de habilitação das demais licitantes ficarão à disposição para retirada junto ao setor de compras do Centro Universitário FMABC, até 10 (dez) dias após a publicação da homologação.

16.11. Até 2 (dois) dias úteis antes da data fixada para abertura da sessão pública, qualquer pessoa poderá impugnar o ato convocatório do Pregão (presencial).

16.12. Caberá ao(à) pregoeiro(a) e equipe de apoio, auxiliado pelo setor responsável pela elaboração do edital, decidir sobre a petição no prazo de vinte e quatro horas.

16.13. Acolhida a petição contra o ato convocatório, será designada nova data para a realização do certame.

16.14. Os pedidos de esclarecimentos referentes ao processo licitatório deverão ser enviados ao setor de compras do Centro Universitário FMABC, até 3 (três) dias úteis anteriores à data fixada para abertura da sessão pública, por meio eletrônico via internet ou através de protocolo no setor de Compras do Centro Universitário FMABC, nos endereços indicados no edital.

16.15. Os casos omissos do presente Pregão serão solucionados pelo Pregoeiro.

16.16. Fica eleito o foro da Comarca de Santo André, para apreciação judicial de quaisquer questões resultantes desta Licitação.

Santo André, 16 de agosto de 2023.

Dr. David Everson Uip
Reitor do Centro Universitário FMABC

ANEXO I

TERMO DE REFERÊNCIA PARA CONTRATAÇÃO DE COMPUTAÇÃO EM NUVEM, LINK DEDICADO E BACKUP

APRESENTAÇÃO

O Centro Universitário FMABC, registrada sob CNPJ 57.571.275/0007-98, caracteriza-se como instituição privada de Ensino Superior, tendo como sua criadora e mantenedora a Fundação do ABC - FUABC, instituição de caráter filantrópico, com sua atuação adstrita as áreas de educação e assistência a saúde, que se configura como pessoa jurídica de direito privado, registrada sob o CNPJ 57.571.275/0001-00.

O Centro Universitário FMABC é a primeira mantida pela Fundação do ABC, tendo sido a Mantenedora instituída pelas leis ns. 2.695, de 24.5.1967 e 2.741, de 10.7.1967, do município de Santo André, 1.546, de 6.9.1967, do município de São Bernardo do Campo e 1.584, de 4.7.1967, do município de São Caetano do Sul, modificadas pelas leis ns. 2.905, de 1º.3.1968; 3.732, de 12.11.1971; 3.741, de 25.11.1971; 4.014, de 9.4.1973 e 5.725, de 16.7.1980,do Município de Santo André; 1.630, de 11.6.1968; 1.907, de 6.5.1971; 2.031, de 6.4.1973; 2.186, de 30.6.1975 e 2.415, de 31.7.1980, do Município de São Bernardo do Campo e 1.661, de 9.2.1968; 1.900, de 23.6.1971; 2.024, de 11.4.1973; 2.247, de 9.5.1975 e 2.623, de 11.7.1980, do Município de São Caetano do Sul, inscrito no registro Público da Comarca de Santo André, sob n. 825, de 6 de outubro de 1967, no Livro A-2, de pessoas jurídicas, às folhas 192 com a finalidade de criar e instalar o Centro Universitário Saúde.

A Fundação do ABC - Centro Universitário FMABC é regido pelo presente Regimento, pelo Estatuto da Fundação do ABC, pelas normas do Ministério da Educação e da legislação brasileira do ensino superior.

1. OBJETO

1.1. Contratação de empresa especializada para **prestação de serviço de hospedagem, conectividade, segurança de rede e backup (cópia de segurança)** incluindo todos os serviços de garantia de funcionamento e suporte técnico, visando atender as necessidades de infraestrutura conforme condições especificadas neste termo de referência.

2. CARACTERISTICAS DA SOLUÇÃO DE CLOUD COMPUTING

2.1. Todos os equipamentos, software, infraestrutura e sustentação, necessários à implementação da solução proposta, são de inteira responsabilidade da

Contratada, que deverá realizar de forma continuada tarefas e rotinas que garantam o pleno funcionamento de toda a infraestrutura, de forma integral e ininterrupta, ou seja, "24x7x365" (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias por ano) nas dependências da Contratada, mantendo em pleno funcionamento todo objeto da contratação.

2.2. A Contratada deverá gerenciar, monitorar, sustentar e operar de forma proativa todos os recursos disponibilizados para a CONTRATATANTE, de forma a garantir o correto funcionamento de todas as funcionalidades especificadas neste Termo de Referência, a partir de seu Centro de Operações de Rede (NOC), em regime 24x7 (24 horas por dia, 7 dias por semana).

2.3. A solução de Computação em Nuvem ofertada deve permitir a criação de uma ou mais VPC´s (Virtual Private Cloud), de forma que a CONTRATADA possa provisionar uma seção da nuvem da solução ofertada isolada logicamente, onde é possível executar recursos da solução em uma rede virtual definida pela CONTRATADA, permitindo o controle total sobre seu ambiente de redes virtuais, incluindo a seleção do seu próprio intervalo de endereços IP, a criação de sub redes e a configuração de tabelas de rotas e gateways de rede, para acessar recursos e aplicações com segurança e facilidade. Além disso, a CONTRATANTE poderá criar uma conexão de Hardware Virtual Private Network (VPN) entre seu datacenter corporativo e a VPC e aproveitar a nuvem da solução ofertada como uma extensão do seu datacenter corporativo.

2.4. A solução deverá ser escalável, de forma a permitir aumentar os recursos na infraestrutura de Cloud Computing da CONTRATADA para absorver a demanda complementar oriunda de picos de acesso ou expansão natural dos usuários em ambiente Cloud Computing.

2.5. Os servidores virtuais deverão ser disponibilizados em ambiente de Cloud Computing, em ambiente seguro e separados logicamente de outros clientes, com as seguintes funcionalidades:

2.6. Implementar características de escalabilidade horizontal (novos servidores) e vertical (aumento de recursos do mesmo servidor), flexibilidade de configuração de memória, processador e disco.

2.7. Implementar a movimentação automática de servidores virtuais para redistribuição de carga e recuperação de falhas do ambiente físico.

2.8. É de responsabilidade da Contratada o monitoramento do hardware e seus componentes, bem como a manutenção dos mesmos, identificando necessidades de reposições, adaptações e melhorias, procedendo chamados aos fornecedores, acompanhando, garantindo a devida solução aos problemas

que porventura ocorram, observando os tempos definidos no Nível de Serviço Exigido e fornecendo Console de Gestão para monitoramento em tempo real de todos os recursos computacionais.

2.9. O monitoramento deverá ser feito de forma continuada, não sobrecarregando os equipamentos ou consumindo recursos da solução de cloud computing provisionada aos clientes.

3. CARACTERÍSTICAS DA INFRAESTRUTURA FÍSICA

3.1. A solução proposta deverá hospedar os dados em datacenter localizado em território nacional;

3.2. Para fins de segurança da informação os dados deverão ser replicados entre datacenters com no mínimo 40km de distância entre eles. Em caso de desastre no datacenter principal o ambiente deverá estar disponível do datacenter réplica.

3.3. Os serviços de Cloud Computing a serem prestados deverão ser baseados em infraestrutura de Datacenter, que deverá manter compatibilidade com padrões internacionais, e deverão manter compatibilidade durante toda vigência do contrato.

3.4. As instalações físicas e recursos de infraestrutura que suportarão o ambiente crítico de serviço atenderão, no mínimo, às características aqui definidas de estrutura física, instalações físicas, energia elétrica, climatização, proteção contra incêndio, segurança física, infraestrutura de acesso à internet do Datacenter e segurança lógica do Datacenter.

3.5. Os datacenters da CONTRATADA deverá possuir um ambiente com alta disponibilidade, atendendo aos seguintes requisitos mínimos:

3.6. Possuir certificação padrão TIER III;

3.7. Garantir a disponibilidade imediata de energia elétrica através do fornecimento de sistemas de nobreaks independentes e redundantes

3.8. Redundância no fornecimento de link de internet de trânsito (uplink) através da utilização de no mínimo dois links IP's de trânsito diferentes e independentes. A comprovação deste item deverá ser feita através de sites públicos na internet como o https://bgpview.io/ ou https://bgp.he.net

3.9. Redundância no anúncio de suas rotas através do protocolo BGP através da disponibilização de no mínimo dois roteadores distintos e independentes.

3.10. Redundância no fornecimento de portas de rede de acesso, através da disponibilidade de no mínimo dois switches distintos e independentes com portas Gigabit Ethernet com ao menos duas portas disponíveis em cada switch.

3.11. A fim de se comprovar o atendimento à estes requisitos mínimos, a CONTRATANTE se reserva o direito de realizar uma vistoria técnica presencial no ambiente da CONTRATADA, a qualquer momento durante a vigência deste contrato, mediante agendamento prévio.

3.12. Caso ocorram quaisquer despesas de deslocamento ou viagem para a realização desta vistoria presencial, as despesas serão de responsabilidade da CONTRATADA.

4. CONSOLE DE GESTÃO DO AMBIENTE CLOUD COMPUTING

4.1. Permitir o gerenciamento da infraestrutura de Computação em Nuvem de forma independente de softwares de cliente (VNC, Remote Desktop, SSH, etc), por meio de API (Application Programming Interface), acessada via browser, de forma segura (HTTPS), utilizando-se de recursos de autenticação.

4.2. O acesso via interface web browser não poderá permitir a visualização ou edição de qualquer componente persistente a infraestrutura física que compõe a solução.

4.3. Possibilitar o cadastramento dos colaboradores da CONTRATANTE, inclusive, por perfil de acesso para administrar, operar ou consultar o ambiente de produção da solução na infraestrutura de Computação em Nuvem disponibilizada pela Contratada.

4.4. Permitir selecionar modelos preexistentes (templates) de infraestrutura. A visualização dos modelos deve ser gráfica, por meio de diagramas e a sua edição deve ser simplificada.

4.5. Permitir personalizar modelos (templates) que melhor se adaptem às necessidades da CONTRATANTE.

4.6. Permitir modificar os recursos da Infraestrutura de Computação em Nuvem e atualizá-los de uma forma controlada e previsível, aplicando-se, quando necessário, controles de versionamento, devendo ser permitido o rastreamento das alterações históricas efetuadas no ambiente.

4.7. Disponibilizar console via interface gráfica afim de permitir o agendamento, realização de backups e horários de funcionamento por recurso (servidor; banco de dados, fileserver), por ambiente (produção) ou por etiqueta (classificação das soluções/sistemas).

5. CONSOLE DE GESTÃO DE DOMINIOS E SUBDOMINIOS

5.1. Deverá ser disponibilizado um painel de controle (software de gestão para alojamento web) com as opções mínimas de: gerenciamento FTP, gerenciamento de arquivos, gerenciamento de banco de dados, verificação de estatísticas, gerenciamento de domínios;

5.2. Deverá possuir gerenciador de arquivos web;

5.3. Deverá possuir painel de gerenciamento de DNS.

6. MONITORAMENTO DE RECURSOS

6.1. A Contratada deverá oferecer Console de Gestão de fácil utilização e que permita criar e gerenciar os recursos e/ou grupo de recursos relacionados ao serviço de Computação em Nuvem por meio de web browsers.

6.2. A solução ofertada deverá permitir o monitoramento das máquinas virtuais, provendo o monitoramento do ambiente de Computação em Nuvem (serviços e recursos), de forma automatizada e abrangendo a gama de aplicações, bancos de dados, servidores, sistemas operacionais e recursos de comunicação, em tempo real (24x7x365), visando detectar problemas (incidentes), no que tange à sustentação operacional e não a aplicação do Contratante.

6.3. Prover o monitoramento constante em amostras com granularidade mínima de 1 hora (24X7X365) dos serviços e recursos, visando detectar os problemas mais frequentes, informando a CONTRATANTE a ocorrência destes.

6.4. Deverá ser realizada pela Contratada a monitoração da qualidade e nível de utilização da infraestrutura de acesso à Internet, disponibilizada pela solução ofertada pela Contratada, bem como as resoluções em caso de problemas.

6.5. Deverá permitir a visualização dos indicadores de desempenho, falhas do ambiente e características e requisitos operacionais dos recursos gerenciados por meio do painel de apresentação (dashboard) Online (tempo real).

6.6. A solução ofertada deverá prover alarmes para a Console de Gestão de eventos, mostrando quais recursos estiveram acima do threshold, permitindo gerar relatório a partir dos eventos observados.

6.7. Para cada servidor virtual, deverá ser possível o acompanhamento e monitoramento dos seguintes recursos: vCPU, RAM, Tráfego de Rede (In/Out) e Disco.

7. PROVISIONAMENTO DO AMBIENTE CLOUD COMPUTING

7.1. A Contratada será responsável por criar os novos servidores no ambiente de Cloud Computing, com as versões do sistema operacional e dos softwares básicos especificados pela CONTRATANTE.

7.2. Será de responsabilidade da equipe técnica da Contratada, com o apoio da equipe técnica da CONTRATANTE, a migração das aplicações para o novo ambiente, sendo que a CONTRATANTE disponibilizará os recursos necessários, tanto de equipamentos quanto humanos, para apoiar a migração das aplicações.

7.3. Será de responsabilidade da equipe técnica da Contratada o acompanhamento e auxilio a instalação dos softwares básicos e a migração das aplicações da CONTRATANTE, durante a migração a CONTRATANTE disponibilizará o conhecimento da estrutura das aplicações e dos softwares básicos necessários (programas, diretórios, arquivos de configuração e demais informações) para a CONTRATADA afim de otimizar os recursos.

7.4. Após a finalização da migração das aplicações para o ambiente Cloud Computing, a CONTRATANTE disponibilizará uma equipe técnica para fazer os testes de homologação das aplicações migradas afim de atestar a conclusão da migração, sendo que os serviços contratados somente serão considerados como entregues aceitos após a conclusão dos testes.

8. RECURSOS COMPUTACIONAIS

8.1. Todos os servidores virtuais deverão ser disponibilizados em ambiente de Cloud Computing, em ambiente seguro e separados logicamente de outros clientes, com as seguintes funcionalidades:

8.2. Implementar características de escalabilidade vertical (aumento/diminuição de recursos do mesmo servidor), incluindo flexibilidade de configuração de memória, processador e disco;

8.3. Permitir a criação, pela CONTRATANTE, de pelo menos 1 (uma) imagem (snapshot) dos servidores virtuais sem custo adicional;

8.4. Assegurar a comunicação segura e encriptada entre os próprios servidores e os clientes que farão acesso aos mesmos, através de protocolo seguro HTTPS, ou seja, todos os servidores deverão ser disponibilizados com certificados digitais SSL instalados.

8.5. Os recursos computacionais adicionais, poderão ser utilizados para agregação ou distribuição entre os servidores virtualizados existentes ou para a criação de novos servidores virtuais;

8.6. Deverá ser considerado um pool de recursos computacionais para suprir a demanda das máquinas virtuais do ambiente, os recursos computacionais como memória e vCPU poderão ser utilizados e divididos entre as máquinas virtuais em nuvem conforme necessidade da CONTRATANTE.

8.7. Cada vCPU deverá fornecer uma velocidade de clock com no mínimo 2 GHz.

9. ARMAZENAMENTO

9.1. O armazenamento disponível para as máquinas virtuais deverá considerar o armazenamento dos dados de forma persistente.

9.2. Permitir o gerenciamento de discos virtuais pela CONTRANTANTE através do portal WEB, desde sua criação, exclusão, expansão e anexo as máquinas virtuais no ambiente (VPC).

9.3. O(s) volume(s) criado(s) anexado(s) às máquinas virtuais deverão ser reconhecidos(s) pelo sistema operacional como um dispositivo físico local.

9.4. A solução de armazenamento deverá permitir que a CONTRATANTE defina a política de uso dos discos virtuais das máquinas virtuais em seu ambiente (VPC).

9.5. O armazenamento disponível e não alocado deverá permitir as seguintes características.

9.5.1. Expansão dos discos existentes das máquinas virtuais no ambiente (VPC)

9.5.2. Inclusão de novos discos nas máquinas virtuais existentes no ambiente (VPC)

9.5.3. Criação de novas máquinas virtuais no ambiente (VPC)

9.6. O armazenamento disponível deverá permitir que a CONTRATANTE defina através de políticas pré existentes a seguinte carga de uso:

9.6.1. ALTA PERFORMANCE (SSD)

9.6.2. BAIXA PERFORMANCE (HDD)

9.6.3. OBJECT STORAGE

9.6.3.1. Gerenciamento de quotas e permissões de acesso via interface WEB;

9.6.3.2. Compatível com API S3;

9.7. Os dados deverão estar localizados em território nacional;

9.8. O tráfego de dados (Download e Upload) deve ser ilimitado;

9.9. Os dados deverão estar acessíveis imediatamente sem restrições de acesso;

10. CONECTIVIDADE

10.1. Link Ponto a Ponto

10.1.1. A CONTRATADA deverá prover um link de dados ponto a ponto em fibra óptica garantindo a banda dedicada para upload e download entre o site da CONTRATANTE e o datacenter da CONTRATADA onde se encontram os equipamentos que compõem a solução de datacenter virtual. Este link será utilizado exclusivamente para os serviços de comunicação entre datacenters;

10.1.2. O volume de tráfego de dados ofertado deve ser ilimitado, tanto no sentido de download como upload, permitindo a transferência, via funcionalidades de backup e restauração, de volume ilimitado de dados.

10.2. IP's públicos

10.2.1. A CONTRATADA deverá disponibilizar endereços IP fixos e públicos (válidos) para uso da CONTRATANTE de tal forma que lhe convir para uso em seu ambiente de produção.

10.2.2. A fim de garantir que o endereçamento IP utilizado pelo serviço de replicação de backup e recuperação de desastres não sofra constantes alterações e consequentes indisponibilidades, a CONTRATADA deverá possuir seu próprio bloco de endereçamento IP atribuído pelo órgão gestor dos serviços de numeração brasileira (NIC.br). A CONTRATADA deve comprovar que possui a devida alocação do bloco ofertado de seu ASN (Autonomous System Number) através de uma declaração do NIC.br.

10.3. Link de Internet VPC

10.3.1. A CONTRATADA deverá prover na VPC (Virtual Private Cloud) um link de internet dedicado para uso e comunicação das instâncias virtuais para a internet.

10.3.2. O volume de tráfego de dados ofertado deve ser ilimitado, tanto no sentido de download como upload, permitindo a transferência, via funcionalidades de backup e restauração, de volume ilimitado de dados.

11. FIREWALL E SEGURANÇA

11.1. Deverá ser fornecido uma solução de segurança com as seguintes características mínimas:

11.2. A solução deverá suportar throughput (Taxa de Transferência) de, no mínimo, 15 Gbps com a funcionalidade de firewall habilitada, independentemente do tamanho dos pacotes;

11.3. A solução deve suportar Throughput (Taxa de Transferência) de, no mínimo, 2.2 Gbps com as seguintes funcionalidades habilitadas simultaneamente: Firewall, Controle de Aplicação e Prevenção de Ameaças (Anti-Malware, IPS, Application Control URL Filtering). Esta taxa deve referenciar-se a tráfego multiprotocolo em ambiente de produção, tráfego considerado de mundo real ou tráfego misto, ou seja, aquele que não faz referência apenas a um protocolo e/ou um tamanho de pacote para teste em condição ideal;

11.4. Suportar throughput (Taxa de Transferência) de, no mínimo, 1 Gbps de VPN IPsec;

11.5. Deverá suportar e incluir licenciamento para, no mínimo, 2.000 Túneis VPN Lan-to-Lan (ou Gateway-to-Gateway) com VPN IPSec;

11.6. Deverá suportar e incluir licenciamento para, no mínimo, 32.000 usuários remotos (ou client-to-site) com VPN IPSec;

11.7. Deverá suportar e incluir licenciamento para, no mínimo, 500 usuários remotos (ou client-to-site) com VPN SSL;

11.8. Suporte a, no mínimo, 3.300.000 (três milhões e trezentos mil) conexões TCP simultâneas;

11.9. Suporte a, no mínimo, 140.000 (cento e quarenta mil) novas conexões TCP por segundo;

11.10. A solução deve possuir o licenciamento para, no mínimo, 10 sistemas virtuais lógicos (Contextos), independentes entre si e estar licenciado e/ou ter incluído sem custo adicional pelo menos 5 sistemas;

11.11. A solução deve possuir, no mínimo, 2 (duas) interfaces no padrão 10 GbE;

11.12. A solução deve possuir, no mínimo, 8 (oito) interfaces no padrão 1GbE;

11.13. A solução deve possuir console para configuração e gerenciamento por interface de linha de comando (CLI);

11.14. Todas as portas de comunicação e interfaces devem ser capazes de funcionar simultaneamente oferecendo, cada uma, a plenitude de suas capacidades;

11.15. A solução deve apresentar armazenamento interno do tipo SSD (Solid-State Drive), com no mínimo 480GB;

11.16. A solução deve consistir em plataforma para centralização do gerenciamento, dos logs e geração de relatórios dos equipamentos que compõem a solução de segurança rede (NGFW);

11.17. A solução de gerenciamento, logs e relatoria deve ser do mesmo fabricante da solução de segurança de rede (NGFW);

11.18. As funcionalidades de centralização do gerenciamento, dos logs e geração de relatórios que compõe a plataforma, podem funcionar em múltiplos equipamentos desde que obedeçam a todos os requisitos desta especificação;

11.19. Funcionalidades gerais para cluster de equipamentos

11.20. Funcionalidades gerais para Solução de Segurança de Perímetro (NGFW)

11.21. Funcionalidades Gerais e Recursos mínimos:

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

11.23. Deve suportar o protocolo padrão da indústria VXLAN;

11.24. Os dispositivos de proteção de rede devem possuir suporte a agregação de links 802.3ad e LACP;

11.25. Os dispositivos de proteção de rede devem possuir suporte a Policy based routing (PBR) ou policy based forwarding (PBF);

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

11.27. Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;

11.28. Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;

11.29. Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames;

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

11.31. Deve suportar NAT dinâmico (Many-to-1);

11.32. Deve suportar NAT dinâmico (Many-to-Many);

11.33. Deve suportar NAT estático (1-to-1);

11.34. Deve suportar NAT estático (Many-to-Many);

11.35. Deve suportar NAT estático bidirecional 1-to-1;

11.36. Deve suportar Tradução de porta (PAT);

11.37. Deve suportar NAT de Origem;

11.38. Deve suportar NAT de Destino;

11.39. Deve suportar NAT de Origem e NAT de Destino simultaneamente;

11.40. Deve poder combinar NAT de origem e NAT de destino na mesma politica

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

11.42. Deve suportar NAT64 e NAT46;

11.43. Deve implementar Equal-cost Multipath ECMP.

11.44. Deve suportar nativamente ou integração com soluções de SD-WAN;

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

11.46. Deve suportar o padrão do protocolo 'syslog' para geração e armazenamento dos logs usando o formato Common Event Format (CEF);

11.47. Deve suportar o armazenamento de logs em tempo real tanto para o ambiente de nuvem quanto o ambiente local (on-premise);

11.48. Enviar log para sistemas de monitoração externos, simultaneamente;

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

11.50. Implementar Proteção anti-spoofing;

11.51. Deve identificar e bloquear comunicação com redes botnets;

11.52. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos de usuários, permitindo que os mesmos sejam utilizados, ao menos, no acesso administrativo dos equipamentos, autenticação VPN e políticas de firewall, dando assim maior granularidade e controle.

11.53. Deve possuir integração com LDAP para identificação de usuários e grupos de usuários, permitindo que os mesmos sejam utilizados, ao menos, no acesso administrativo dos equipamentos, autenticação VPN e políticas de firewall, dando assim maior granularidade e controle.

11.54. Deve possuir integração com Radius para identificação de usuários e grupos de usuários, permitindo que os mesmos sejam utilizados, ao menos, no acesso administrativo dos equipamentos, autenticação VPN e políticas de firewall, dando assim maior granularidade e controle.

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

11.56. Deve possuir funcionalidade de Single Sign-On. Essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso

como, mas não limitado à utilização de sistemas virtuais, segmentos de rede, etc;

11.57. Deve possuir funcionalidade de Captive Portal local para autenticação de usuários que solicitem navegação através de políticas de firewall que façam o controle por usuários/grupos de usuários. Deve permitir também a customização deste Portal.

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

11.59. Deve permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso a internet e gerenciamento da solução;

11.60. Deve prover nativamente, no mínimo, licenciamento de uso de um (1) token, possibilitando autenticação de duplo fator para usuário administrador, acesso VPN e etc;

11.61. Para IPv4, deve suportar roteamento estático e dinâmico (RIP, BGP e OSPF);

11.62. Para IPv6, deve suportar roteamento estático e dinâmico (OSPF e BGP);

11.63. Suportar OSPF graceful restart;

11.64. 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);

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

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

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

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

11.69. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo transparente;

11.70. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3;

11.71. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3 e com no mínimo 3 equipamentos no cluster;

11.72. A configuração em alta disponibilidade deve sincronizar: Sessões;

11.73. A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede;

11.74. A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs;

11.75. A configuração em alta disponibilidade deve sincronizar: Tabelas FIB;

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

11.77. Deve possuir suporte a criação de sistemas virtuais lógicos (contexto) no mesmo appliance;

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

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

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

11.81. Deverá suportar controles por zona de segurança;

11.82. Controles de políticas por porta e protocolo;

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

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

11.85. Firewall deve ser capaz de aplicar a inspeção de camada 7 (Application Control e Webfiltering no mínimo) diretamente às políticas de segurança versus via perfis;

11.86. Além dos endereços e serviços de destino, objetos de serviços de Internet devem poder ser adicionados diretamente às políticas de firewall;

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

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

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

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

11.91. Suportar a criação de políticas por geolocalização, permitindo o trafego de determinado País/Países sejam bloqueados;

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

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

11.94. O gerenciamento da solução deve suportar acesso via interface WEB (HTTPS) e interface de linha de comando (SSH), incluindo, mas não limitado à, exportar configuração dos sistemas virtuais lógicos por ambas interfaces;

11.95. Controle de Aplicações

11.96. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

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

11.98. Reconhecer pelo menos 1500 aplicações diferentes, incluindo, mas não limitado a: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

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

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

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

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

11.103. 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;

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

11.105. Identificar o uso de táticas evasivas via comunicações criptografadas;

11.106. Atualizar a base de assinaturas de aplicações automaticamente;

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

11.108. 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;

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

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

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

11.112. 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;

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

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

11.115. Deve alertar o usuário quando uma aplicação for bloqueada;

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

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

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

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

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

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

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

11.123. Prevenção de Ameaças

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

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

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

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

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

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

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

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

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

11.133. Deve permitir o bloqueio de vulnerabilidades;

11.134. Deve permitir o bloqueio de exploits conhecidos;

11.135. Deve incluir proteção contra-ataques de negação de serviços;

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

11.137. Análise de padrões de estado de conexões;

11.138. Análise de decodificação de protocolo;

11.139. Análise para detecção de anomalias de protocolo;

11.140. Análise heurística;

11.141. IP Defragmentation;

11.142. Remontagem de pacotes de TCP;

11.143. Bloqueio de pacotes malformados;

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

11.145. Detectar e bloquear a origem de portscans;

11.146. Bloquear ataques efetuados por worms conhecidos;

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

11.148. Possuir assinaturas para bloqueio de ataques de buffer overflow;

11.149. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica;

11.150. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;

11.151. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

11.152. Identificar e bloquear comunicação com botnets;

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

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

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

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

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

11.158. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;

11.159. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;

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

11.161. Fornecer proteção contra-ataques de dia zero por meio de estreita integração com os componentes Sandbox (on-premise ou nuvem);

11.162. Filtro de URL

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

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

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

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

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

11.168. Possuir pelo menos 50 categorias de URLs;

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

11.170. Permitir a customização de página de bloqueio;

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

11.172. Além do Explicit Web Proxy, suportar proxy Web transparente;

11.173. QoS e Traffic Shaping

11.174. 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 máxima largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;

11.175. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;

11.176. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;

11.177. Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo;

11.178. Suportar a criação de políticas de QoS e Traffic Shaping por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube;

11.179. Suportar a criação de políticas de QoS e Traffic Shaping por porta;

11.180. Possibilitar a definição de tráfego com banda garantida;

11.181. Possibilitar a definição de tráfego com banda máxima;

11.182. Possibilitar a definição de fila de prioridade;

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

11.184. Suportar marcação de pacotes Diffserv, inclusive por aplicação;

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

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

11.187. VPN

11.188. Suportar VPN Site-to-Site e Cliente-To-Site;

11.189. Suportar IPSec VPN e VPN SSL de forma simultânea;

11.190. A VPN IPSEC deve suportar 3DES;

11.191. A VPN IPSEC deve suportar Autenticação MD5 e SHA-1;

11.192. A VPN IPSEC deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;

11.193. A VPN IPSEC deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);

11.194. A VPN IPSEC deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);

11.195. A VPN IPSEC deve suportar Autenticação via certificado IKE PKI;

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

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

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

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

11.200. Atribuição de DNS nos clientes remotos de VPN;

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

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

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

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

11.205. Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas:

11.206. Antes do usuário autenticar na estação;

11.207. Após autenticação do usuário na estação;

11.208. Sob demanda do usuário;

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

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

12. SOLUÇÃO DE DETECÇÃO E REPOSTA DE ENDPOINT

12.1. Requisitos gerais da solução:

12.1.1. Solução de proteção contra ameaças avançadas, com funcionalidades de detecção, bloqueio, investigação e resposta a incidentes, incluindo console Web ou console gráfica do próprio fabricante para administração da solução e centralização de eventos.

12.1.2. Fornecimento da console de gerência, incluindo implantação dos agentes, documentação da arquitetura da solução e repasse de conhecimento

12.1.3. A Solução de gerência deve ser fornecida pela licitante vencedora e contemplar todos os softwares e respectivas licenças necessárias ou adicionais para a instalação, configuração e funcionamento da solução de proteção.

12.1.4. A solução de proteção deve ser oferecida na última versão disponibilizada pelo fabricante.

12.1.5. Na data da proposta, nenhum dos softwares componentes da solução de proteção ofertados poderão estar listados pelo fabricante com data definida para fim de suporte (“end of support”) ou fim de vendas (“end of sale”).

12.2. Requisitos e funcionalidades técnicos da solução:

12.2.1. A solução de proteção deve ser capaz de detectar e bloquear em tempo real ameaças conhecidas e desconhecidas (zeroday), ataques file-less, ameaças persistentes avançadas (APTs), ransomwares, exploits e outros comportamentos maliciosos, sem depender exclusivamente de base de assinaturas ou heurísticas.

12.2.2. A solução de proteção deverá possuir funcionalidades especificas para prevenção contra a ação de ransomwares com capacidade de restauração dos arquivos comprometidos.

12.2.3. A solução de proteção deve ter a funcionalidade específica de impedir as técnicas de manipulação e randomização de memória impossibilitando a exploração de vulnerabilidades em aplicações.

12.2.4. A solução de proteção deve ter a capacidade de impedir os ataques direcionados mesmo que utilizando as vulnerabilidades de dia zero, mitigando no mínimo os conhecidos comportamentos de exploração de vulnerabilidades.

12.2.5. Efetuar a análise baseada em técnicas de machine learning, inteligência artificial e threat intelligence, permitindo a proteção contra ataques que

explorem vulnerabilidades, mesmo que ainda não existam patches de correção.

12.2.6. Realizar análise de comportamento com base nas táticas, técnicas e procedimentos (TTPs) listados no framework MITRE ATT&CK.

12.2.7. A análise dos artefatos deve ocorrer em pré-execução, ou seja, antes de serem executados no sistema operacional, evitando que a máquina seja infectada.

12.2.8. Detectar e bloquear ameaças que utilizem técnicas de ofuscação e sequestro de DLL.

12.2.9. Detectar e bloquear técnicas de evasão, incluindo process injection e uso de executáveis legítimos do Windows para rodar scripts e ações maliciosas.

12.2.10. Reconhecer padrões e bloquear comportamentos potencialmente maliciosos ou o possuir mecanismos automáticos preventivos ou corretivos que sejam capazes de inibir as ações maliciosas resultantes de pelo menos 5(cinco) das ações listadas abaixo:

12.2.10.1. Rodar a partir diretórios incomuns (ex: diretório de dados, temp e lixeira);

12.2.10.2. Executar elevações de privilégio inesperadas;

12.2.10.3. Tentar se passar por processos do Windows;

12.2.10.4. Estabelecer conexões de rede suspeitas (call back ou command & control);

12.2.10.5. Uso suspeito do PSEXEC;

12.2.10.6. Invocação maliciosa através do Rundll;

12.2.10.7. Exploração ou modificação do arquivo hosts;

12.2.10.8. Tentativa de invocação de Remote Shell.

12.2.11. Identificar e bloquear alterações suspeitas em chaves de registro e tarefas agendadas na máquina.

12.2.12. Proteger contra macros maliciosas, bem como scripts e comandos Powershell maliciosos.

12.2.13. Bloquear exploits e payloads suspeitos do Metasploit.

12.2.14. As análises poderão ser complementadas utilizando recursos em nuvem da solução, sem custos adicionais, onde será permitido apenas o envio de metadados dos artefatos sob análise, sem submissão do artefato em si ou seu conteúdo à nuvem.

12.2.15. O agente da solução deve realizar suas análises e bloqueios nas estações mesmo quando estiver sem conectividade com os servidores da solução e sem acesso à Internet.

12.2.16. O agente da solução deve possuir proteção contra desinstalação e/ou desativação dos seus componentes, serviços e processos de forma não autorizada.

12.2.17. Deve ser possível realizar a configuração de proxy no agente ou obter as configurações de proxy definidas no próprio sistema operacional.

12.2.18. Deve ser possível exibir ou inibir alertas ao usuário em caso de detecção de alguma ameaça, conforme definição do administrador.

12.2.19. Deve ser possível definir as seguintes ações de resposta quando uma ameaça ou comportamento malicioso for detectado:

12.2.19.1. Ignorar;

12.2.19.2. Registrar em log;

12.2.19.3. Alertar;

12.2.19.4. Bloquear;

12.2.19.5. Remover ou quarentenar;

12.2.20. Isolar a máquina, de maneira que ela perca a comunicação com a rede ou se comunique apenas com os servidores da solução ou com servidores e serviços definidos na política de isolamento.

12.2.21. I - O agente deve ter a capacidade de fazer o isolamento da máquina por si só, sem precisar de nenhuma integração com outros softwares ou dispositivos de rede para isso.

12.2.22. II - Deve ser possível ao administrador efetuar a liberação da máquina do isolamento via console de gerência ou fornecer uma chave para realizar a liberação.

12.2.23. A solução deve possuir funcionalidade de EDR e análise forense, provendo uma visão completa do fluxo do ataque e informações detalhadas sobre os comportamentos detectados, de forma a auxiliar e agilizar as ações de remediação.

12.2.24. A console deve oferecer uma linha do tempo gráfica, contendo toda a sequência de eventos que ocorreram durante a execução do malware, sendo possível ainda expandir os detalhes de cada informação.

12.2.25. Devem ser coletadas as atividades de todos artefatos analisados, contendo informações sobre interação com outros processos, arquivos e chaves de registro acessadas/modificadas, conexões de rede realizadas, dentre outras. Deve ser possível gerar relatório dessas informações.

12.2.26. A solução deve correlacionar os eventos de detecção e bloqueio de malwares, permitindo a visualização de relatório com todas as fases do ataque.

12.2.27. Deve ser possível configurar regras de exclusão (whitelists) determinando quais arquivos, diretórios, processos ou aplicativos não devem ser analisados pela solução.

12.2.28. A solução deve ser capaz de remover de forma ágil e eficaz outras soluções de antivírus instaladas nos equipamentos do CONTRATANTE ou possuir mecanismos que possibilitem essa remoção.

12.2.29. A Solução deve ter a capacidade de implementar, no mínimo, cinco das seguintes funcionalidades:

12.2.29.1. Reputação de Arquivos (Com ou sem acesso à internet no endpoint);

12.2.29.2. IPS de Próxima Geração;

12.2.29.3. Proteção de Navegadores;

12.2.29.4. Aprendizado de Máquinas;

12.2.29.5. Análise Comportamental;

12.2.29.6. Mitigação da Exploração de Memória;

12.2.29.7. Controle e isolamento de Aplicações;

12.2.29.8. Controle de Dispositivos;

12.2.29.9. Emulação para Malware;

12.2.29.10. Proteção ao ambiente de Active Directory;

12.2.29.11. Mitigação de Exploração de Vulnerabilidades em aplicações conhecidas.

12.2.30. Deve ter a capacidade de implementar a funcionalidade de “Machine Learning” utilizando como fonte de aprendizado a rede de inteligência do fabricante, correlacionando no mínimo as seguintes técnicas de proteção com os vetores de ataques, identificando não somente os aspectos maliciosos.

12.2.31. De forma opcional ou não obrigatória a solução poderá a solução poderá ser capaz de distribuir iscas no ambiente com o objetivo de detectar e interromper tentativas de infiltração, através da implementação de pelo menos:

12.2.32. Criação de entradas falsas de cache, como Cache de DNS afim de enganar um invasor e identificar ações maliciosas no ambiente;

12.2.33. Deve possibilitar a criação de arquivos falsos nas máquinas dos usuários;

12.2.34. Deve possibilitar a criação e distribuição de senhas falsas nos sistemas afim de identificar invasores no ambiente;

12.2.35.

12.2.36. Criação de compartilhamentos de rede falsos em desktops;

12.2.37. Deve ser capaz de enviar alertas quando as “Iscas” falsas são acionadas e/ou modificadas;

12.2.38. Deve ter a capacidade de revelar tentativas de ataques dentro da rede interna;

12.2.39. De forma opcional ou não obrigatória, a solução poderá ter a capacidade de impedir os ataques direcionados mesmo que utilizando as vulnerabilidades de dia zero, mitigando no mínimo um dos conhecidos comportamentos de exploração de vulnerabilidades:

12.2.39.1. SEHOP - Structured Exception Handler Overwrite Protection;

12.2.39.2. Heap Spray (Exploits que iniciam através do HEAP);

12.2.39.3. Java Exploit Protection;

12.2.40. De forma opcional ou não obrigatória, a solução poderá se capaz de:

12.2.40.1. A solução poderá ter a capacidade de bloquear exploits que trabalham em nível de “shell code”.

12.2.40.2. A solução poderá ter proteção contra técnicas de reconhecimento do domínio, sendo capaz de detectar um invasor que utilize técnicas de movimentação lateral ou roubo de credenciais válidas;

12.2.40.3. A solução poderá proteger contra intrusões por processo, usuário e terminal;

12.2.40.4. A solução poderá ser capaz de identificar vulnerabilidades, erros de configurações e possíveis Backdoors presentes no Active Directory;

12.2.40.5. A solução poderá ser capaz de proteger alterações no Active Directory sem a necessidade de instalação de agentes ou componentes adicionais nas estações de trabalho;

12.2.40.6. A solução poder ser capaz de detectar e proteger roubos de credenciais no ambiente que utilizem a técnica Pass-the-Hash e Pass-the-Ticket;

12.2.41. Instalação dos agentes:

12.2.41.1. A solução deve ser compatível com as versões de Sistema Operacionais:

12.2.41.2. Para computadores de usuários finais (estações: desktop, workstation e notebooks):

12.2.41.3. I - Microsoft Windows 7 (32-64bit) e superior em todas as suas distribuições (home, starter, professional, ultimate e enterprise).

12.2.41.4. Para servidores de rede físicos ou virtuais

12.2.41.5. I - Microsoft Windows Server 2012 (64bit) e superior.

12.2.41.6. II - Ser suportado em sistemas operacionais linux, tais como Ubuntu, CentOS, Debian, Oracle Linux, Red Hat Enterprise, SUSE Linux Enterprise (32-64bit).

12.2.41.7. III - O agente deve suportar sua instalação em Sistemas Operacionais virtualizados em ambiente Vmware.

12.2.42. O agente não deve impactar a performance das estações e servidores, gerando baixo consumo de CPU, memória, disco e rede.

12.2.43. Deve ser possível a instalação e atualização dos agentes de forma manual ou remota, com suporte à distribuição do agente por ferramentas de terceiros, incluindo o System Center Configuration Manager (SCCM) da Microsoft.

12.2.44. A instalação deve ser feita de forma silenciosa, sem interação com o usuário e sem necessidade de acesso à Internet.

12.2.45. Deve ser possível permitir a desinstalação ou alteração da configuração do agente mediante requisição de senha ou token gerados pela console de gerência.

12.2.46. Deve ser possível impedir alterações na configuração do agente por usuários ou processos não autorizados.

12.2.47. Toda a solução deverá funcionar com agente único na estação de trabalho e servidores físicos e/ou virtuais a fim de diminuir o impacto ao usuário final;

12.2.48. Para equipamentos que não podem se conectar à internet, devido a regras de negócio e/ou restrições impostas pelo próprio equipamento, a solução deve possibilitar a instalação de um componente on-premises, para que tais equipamentos possam ser gerenciados, atualizados e protegidos.

12.2.49. Toda a solução deverá funcionar com agente nas estações de trabalho e servidores físicos e/ou virtuais a fim de diminuir o impacto ao usuário final. Será permitido agentes múltiplos para o atendimento deste requisito.

12.3. Console de Gerência:

12.3.1. A solução deve oferecer console de gerência via protocolo web seguro ou console do próprio fabricante.

12.3.2. Caso a console seja Web, deve ser compatível com pelo menos dois dos seguintes navegadores: Microsoft Edge 41 ou superior; Google Chrome 70 ou superior; Mozilla Firefox 60 ou superior.

12.3.3. A console deve funcionar plenamente sem requerer a instalação de plug-ins, drivers, java e flash player.

12.3.4. Permitir no mínimo 5(cinco) acessos simultâneos.

12.3.5. A console e os agentes da solução devem possuir interface em português ou inglês.

12.3.6. Toda comunicação da solução deve ocorrer de forma criptografada usando protocolo seguro conforme padrão aceito pela indústria.

12.3.7. Permitir a configuração de perfis com permissões agrupadas que possam ser vinculados às contas de acesso à solução, para possibilitar a segregação de funções.

12.3.8. Suporte à criação de usuários, permitindo senhas de no mínimo 8 caracteres de 3 ou mais tipos, como: letras maiúsculas, letras minúsculas, dígitos numéricos e caracteres especiais.

12.3.9. A solução de console de gerência, deve ser possível configurar autenticação em múltiplos fatores.

12.3.10. Permitir ao administrador criar diferentes políticas de segurança e aplicá-las a diferentes grupos de máquinas de acordo com seus atributos.

12.3.11. Registro em log de todas as ações de detecção e bloqueio de malware e comportamento malicioso.

12.3.12. Deve ser possível efetuar busca no log pelo IP de Origem, IP de destino, nome da máquina, nome do processo, arquivo e chave de registro.

12.3.13. Deve ser possível efetuar o “drill down” das consultas realizadas a fim de avaliação mais detalhada das ocorrências.

12.3.14. A partir dos eventos exibidos na console, deve ser possível tomar ações como quarentenar a máquina, adicionar o artefato a blacklist ou lista de exclusão (whitelist), dentre outras.

12.3.15. Permitir a geração de relatórios, consulta em log ou dashboard para visualizar no mínimo as informações abaixo:

12.3.15.1. Eventos de ameaças;

12.3.15.2. Eventos de comportamentos suspeitos;

12.3.15.3. Malwares detectados e bloqueados;

12.3.15.4. Computadores infectados.

12.3.16. Deve ser possível exportar os relatórios para o formato CSV ou PDF.

12.3.17. Permitir a configuração de alertas em tempo real de ameaças com envio de e-mail a usuários pré-definidos.

12.3.18. A solução deve manter log de auditoria com registro das configurações realizadas por qualquer usuário ou administrador do sistema.

12.3.19. Permitir a visualização do inventário das máquinas que possuem o agente instalado, contendo no mínimo as seguintes informações:

12.3.19.1. Nome da máquina;

12.3.19.2. Endereço IP;

12.3.19.3. Versão do sistema operacional (incluindo a versão do Service Pack);

12.3.19.4. Versão do agente;

12.3.19.5. Política aplicada.

12.3.20. A partir do console de gerenciamento da solução, deve ser possível identificar o equipamento que está sofrendo ataques e comandar o agente de endpoint para que aquele determinado equipamento seja movido para uma área de quarentena.

12.4. Monitoramento Assistido:

12.4.1. Este serviço tem por objetivo operacionalizar as atividades de monitoração, detecção e resposta a incidentes de segurança, tratando os incidentes de forma coordenada, organizada e eficaz conforme necessidade do CONTRATANTE.

12.4.2. Deverá ser realizado de forma remota, externamente à CONTRATANTE, em dependências sob responsabilidade da CONTRATADA;

12.4.3. Deverá atuar na resposta à incidentes e ser realizado em língua portuguesa com monitoração em regime 12x5 (doze horas e cinco dias por semana);

12.4.4. Este serviço deverá ser prestado por equipe própria da CONTRATADA ou pela fabricante da solução;

12.4.5. Este serviço deverá interagir com o CONTRATANTE via sistema de gestão e orquestração de incidentes de segurança da informação, sistemas disponibilizados pelo CONTRATANTE, ligação telefônica e correio eletrônico;

12.4.6. As solicitações e respostas de informações adicionais sobre os incidentes, como logs e evidências, devem ser anexadas ao tíquete registrado na ferramenta;

12.4.7. A CONTRATADA deverá garantir a prestação de serviço com disponibilidade mensal de 97% no regime de monitoração 12x5(doze horas e cinco dias por semana). Em casos de indisponibilidade, esta não deverá atingir períodos superiores a 4 horas consecutivas;

12.4.8. A CONTRATADA deverá apresentar plano de continuidade para a prestação deste serviço; será considerado incidente de segurança qualquer ação que vise comprometer a integridade, a confidencialidade das informações ou a disponibilidade dos serviços de tecnologia da informação do CONTRATANTE;

12.4.9. O serviço deverá atender os seguintes requisitos:

12.4.9.1. Monitorar ferramentas de segurança;

12.4.9.2. Monitorar o armazenamento dos logs de eventos e e incidentes de segurança;

12.4.9.3. Monitorar sistema de gestão, orquestração e automação de incidentes de segurança da informação, controlando eventos, alertas, painéis e incidentes;

12.4.9.4. Iniciar tratamento de incidentes em até 10 min;

12.4.9.5. Realizar triagem, classificação e categorização de eventos de segurança da informação;

12.4.9.6. Realizar triagem, classificação e categorização de incidentes de segurança da informação, também identificando casos de falso positivo;

12.4.9.7. Identificar incidentes de segurança da informação; Registrar, escalar e notificar incidentes de segurança da informação;

12.4.9.8. Registrar, escalar e notificar incidentes de segurança da informação;

12.4.9.9. Realizar coleta de dados, informações e evidências para inclusão no registro do evento ou incidente;

12.4.9.10. Executar ações de mitigação, contenção, diagnóstico, resolução e outros procedimentos necessários para tratamento de incidentes de segurança da informação, solicitados pelo CONTRATANTE;

12.4.9.11. Interagir com a ETIR e demais equipes da CONTRATANTE, podendo realizar ações em conjunto;

12.4.9.12. Registrar e documentar ações e procedimentos realizados;

12.4.9.13. Emitir relatório semanal estatístico das operações realizadas;

12.4.9.14. Emitir relatórios conforme necessidade, periodicidade e padrões estabelecidos pela CONTRATANTE;

12.4.9.15. Apoiar na definição, documentação e manutenção de Política de Gerenciamento de Eventos, contendo diretrizes para geração, coleta, retenção e classificação de eventos e monitoramento de logs;

12.4.9.16. Apoiar na definição, documentação e manutenção de estratégia de visibilidade de ameaças, devendo abordar: rotinas, periodicidade, métodos para identificação de novos casos de uso, utilização de fontes de visibilidade e inteligência de ameaças;

12.4.9.17. Apoiar na definição, documentação e manutenção da normas, diretrizes e Política de Segurança da Informação e Comunicação da CONTRATANTE , visando refletir as definições instituídas por esses serviços de monitoramento;

12.4.9.18. Apoiar na Análise de Requisitos Regulatórios, Contratuais e Legais que se referem à segurança da informação e aplicáveis a CONTRATANTE;

12.4.9.19. Apoiar na avaliação de Helth Check das soluções de segurança do CONTRATANTE, validando o mesmo e apresentando recomendações;

12.4.9.20. Apoiar na definição de ajustes e configuração de ferramentas de Segurança, apresentando recomendações a serem realizadas pela equipe técnica da CONTRATANTE.

12.4.9.21. Apoiar na realização de Avaliação da Utilização de ferramentas de Segurança, observando: regras, alertas, painéis, fontes de dados, automatizações, integrações, relatórios e dimensionamento; apresentar recomendações e indicações de melhores práticas no que se refere à monitoração, análises, casos de uso de forma eficiente; e participar da implementação das recomendações quando necessário;

12.4.9.22. Realizar Avaliação de Performance, com base nas métricas e indicadores definidos;

12.4.9.23. Gerar subsídios e recomendações para elaboração de conteúdo para divulgação de definições e orientações de segurança da informação e cibernética, a serem utilizados em ações de cultura e conscientização;

12.4.9.24. Apoiar na definição, documentação e manutenção de linha base (baseline) de comportamento para monitoração do ambiente de TI da CONTRATANTE, ajustando métricas e limiares de detecção, com o objetivo de reduzir o número de falsos positivos e aumentar a precisão da detecção;

12.4.9.25. Interagir com o sistema do CONTRATANTE para o processo de Gestão de Mudanças, Gestão de Incidentes de TI Gestão de requisições.

12.5. Instalação da solução e repasse de conhecimento.

12.5.1. A disponibilização da solução de gerência e a instalação e configuração dos agentes da solução deverá ser realizada pela Contratada ou pelo fabricante da solução presencialmente na Sede do CONTRATANTE, em dias úteis, no período de 8h00 às 12h00 e de 14h00 às 18h00.

12.5.2. A disponibilização da solução de gerência e a instalação e configuração dos agentes da solução deve ser executada por pessoal especializado, qualificado e com certificação na solução.

12.5.3. A disponibilização da solução de gerência e a instalação e configuração dos agentes da solução deverá ser concluída em 30 (trinta) dias corridos para a sede do CONTRATANTE e em até 60 (sessenta) dias corridos para as unidades nas demais localidades, contados a partir da assinatura da Ordem de Serviço

12.5.4. A instalação compreenderá:

12.5.4.1. Implantação de todos os componentes em sua última versão estável.

12.5.4.2. Configuração completa da solução, incluindo o apoio na definição de políticas e melhores práticas de segurança.

12.5.4.3. Configuração de dashboards, relatórios e alertas, de maneira coordenada com o CONTRATANTE.

12.5.4.4. Customização dos pacotes de instalação dos agentes e distribuição a todas as estações do CONTRATANTE, inclusive nas unidades descentralizadas nos estados da federação.

12.5.4.5. Instrução da equipe técnica do CONTRATANTE para a integração da a solução com ferramenta SIEM ou envio para servidor de registro de logs (Syslog).

12.5.4.6. Documentação da topologia da solução, relatório das atividades e configurações realizadas.

12.5.4.7. Apresentação da solução configurada e implantada.

12.5.4.8. Deverá ser realizado repasse de conhecimento da solução de gerência para 1 grupo de até 4 pessoas, oferecido por técnico certificado na solução.

12.5.4.9. No repasse de conhecimento deve ser utilizado material em português.

12.5.4.10. Não é necessário que o repasse seja feito para um grupo fechado do CONTRATANTE e o mesmo pode ser realizado de forma remota.

12.5.4.11. O repasse de conhecimento deve conter parte teórica e prática, incluindo tópicos sobre a instalação, uso, configuração, resolução de problemas da solução, análise de relatórios, respostas a incidentes, introdução ao Framework MITRE ATT&CK e outros.

12.5.4.12. As datas dos repasses de conhecimento devem ser previamente combinadas com o CONTRATANTE.

12.5.4.13. Todas as despesas do repasse de conhecimento devem correr por conta da Contratada.

12.5.4.14. Caso o repasse de conhecimento seja ministrado presencialmente e fora de São Paulo, deverão estar incluídas as despesas com passagens aéreas, hospedagem e traslado entre aeroporto, hotel e local de treinamento.

12.5.4.15. O CONTRATANTE se reserva o direito de solicitar novo repasse caso aquele oferecido venha a ser questionado com relação à qualidade ou à carga horária. Neste caso, eventuais despesas de locomoção e estadia serão ressarcidas ao CONTRATANTE pela Contratada.

12.5.4.16. Deverá ser disponibilizado formulário de avaliação (online ou impresso) e a média das notas deverá ser superior a 80%. Caso a média das notas seja inferior a 80% a contratada deverá ministrar novo repasse.

12.5.4.17. A fornecedora e/ou fabricante da solução poderá, a qualquer tempo, durante a vigência do contrato, sem ônus extra para o CONTRATANTE, oferecer participação em seminários, conferências, visitas técnicas, eventos educacionais e treinamentos não previstos nesta especificação técnica, desde que relacionados ao objeto contratado.

13. **BACKUP**

13.1. A Contratada deverá disponibilizar serviços que permitam realizar backup e restore rápidos dos servidores virtuais com retenção em storage.

13.2. As políticas de backup deverão ser configuradas conforme necessidades de tempo de retenção e periodicidade que o cliente desejar.

13.3. A fim de manter a integridade das informações e dos dados armazenados, a solução de Cloud Computing deverá garantir o backup das

instâncias baseado nas características técnicas mínimas de uma solução de Backup conforme listadas abaixo:

13.4. Os Backups poderão ser completos do tipo imagem dos volumes, sendo executados de forma automática (agendada) ou através de comandos manuais. Os backups das bases de dados de aplicações de execução contínua deverão ser realizados sem interrupção dos serviços (backup on line), e deverá ser utilizada uma rede de alta velocidade evitando que o tráfego de backup afete a operação normal dos sistemas.

13.5. Para realização da funcionalidade Backup e Restore, a Contratada deverá disponibilizar solução completa, com todos os recursos necessários para executar as rotinas da CONTRATANTE, sendo que a solução de Backup deverá estar preparada para geração automática de imagens das máquinas virtuais /Snapshots, gravados em ambiente de armazenamento em nuvem da Contratada, que devem ser acessíveis aos recursos de Computação em Nuvem disponibilizados para a CONTRATANTE.

13.6. As políticas de backup poderão ser ajustadas para uma maior quantidade de backups diários e/ou retenção no repositório de armazenamento a ser disponibilizado para as cópias de segurança das instâncias contratadas respeitando a capacidade contratada sem considerar eventuais ganhos com compressão e deduplicação.

13.7. Não serão permitidas soluções de backup de dados baseados em cópias realizadas de forma manual, nem baseadas em scripts automatizados, devendo ser utilizado um software de uso específico e dedicado para backup.

13.8. Não serão permitidas soluções de backup de dados baseados em sistemas operacionais gratuitos ou de código aberto.

13.9. A solução proposta deverá dispor de software profissional para gerência e execução de backup e restauração de dados em nuvem, com garantia de atualizações e expansões durante o período do contrato sem ônus financeiro para a CONTRATANTE.

13.10. Deverá ter a capacidade de testar a consistência do backup e replicação (Sistema Operacional, aplicação, máquina virtual), emitindo relatório de auditoria para garantir a capacidade de recuperação, sempre que solicitado.

13.11. Deverá incluir ferramentas de recuperação, mediante as quais os administradores dos servidores de serviços de diretório Microsoft Active Directory, possam recuperar objetos individuais como usuários, grupos, contas, Objetos de Política de Grupo (GPOs), registros do Microsoft DNS integrados ao

Active Directory, sem a necessidade de recuperar os arquivos das máquinas virtuais como um todo ou reiniciar a mesma.

13.12. Deverá incluir ferramentas de recuperação, mediante as quais os administradores dos servidores de banco de dados Microsoft SQL Server, possam recuperar objetos individuais, tais como bases, tabelas, registros, entre outros, sem a necessidade de recuperar os arquivos das máquinas virtuais como um todo ou reiniciar a mesma.

13.13. Deverá ter a capacidade de realizar proteção (backup) incremental e replicação diferencial, aproveitando a tecnologia de “rastreio de blocos modificados” (CBT – changed block tracking), reduzindo ao mínimo necessário, o tempo de backup e possibilitando proteção (backup e replicação).

13.14. Deverá oferecer a possibilidade de armazenar backups de forma criptografada, bem como garantir o trânsito de informações sob esse esquema a partir do arquivo de backup, sem exigir criptografia do sistema de armazenamento.

13.15. Deverá prover acesso ao conteúdo das máquinas virtuais, para recuperação de arquivos, pastas ou anexos, diretamente do ambiente protegido (repositório de backup) ou replicados, sem a necessidade de recuperar completamente o backup e inicializar.

13.16. Deverá assegurar a consistência de aplicações transacionais de forma automática por meio da integração com Microsoft VSS, dentro de sistemas operacionais Windows.

13.17. Deverá permitir criar uma cópia da máquina virtual de produção para criação de ambiente de homologação, testes ou desenvolvimento, em qualquer estado anterior, para a resolução de problemas, provas de procedimentos ou capacitação.

13.18. Deverá permitir a recuperação de mais de uma máquina virtual e pontos de restauração simultâneo, permitindo assim, ter múltiplos pontos de tempo de uma ou mais máquinas virtuais.

13.19. O software deverá possuir painel de gerenciamento de ambiente de backup (dashboard) com suporte a visualização de todas as rotinas de backup, com opção de gerar relatórios online e enviar estes relatórios aos endereços designados pela CONTRATATANTE.

13.20. O software deverá permitir a execução de backup de arquivos abertos em Windows, mesmo que estejam sendo alterados durante a operação e backup, sem necessidade de suspender a utilização de aplicações pelos usuários nem

a conexão da rede. A cópia do arquivo salvo deverá ser idêntica ao arquivo residente em disco, quando do início da operação de backup.

13.21. A replicação dos dados deve ter funcionalidade nativa do software de backup, não podendo usar sistemas externos (appliances).

13.22. O sistema deve prover quantidade ilimitada de restaurações, conforme as solicitações da CONTRATANTE, durante a vigência deste Contrato.

13.23. O console central de administração dos backups deve ser via WEB e acessível via navegador utilizando protocolos HTTPS integrado a solução de Console de gestão do ambiente Cloud Computing (ITEM 7).

14. RECUPERAÇÃO DE DESASTRES

14.1. Deverá fornecer solução de recuperação de desastres, baseado em replicação automatizada entre os datacenters da CONTRATADA.

14.2. A solução deverá ser integrada a mesma solução de gerenciamento do ambiente de máquinas virtuais, não sendo permitido utilização de software externos.

14.3. Garantir a proteção e replicação automatizada de máquinas virtuais.

14.4. Permitir a criação de planos de recuperação personalizáveis.

14.5. Deverá possuir funcionalidade de testes de plano de recuperação sem impacto.

14.6. Permitir a recuperação orquestrada quando necessário.

14.7. Permitir a replicação e recuperação para outro ambiente de Cloud Computing.

14.8. Permitir a utilização do ambiente em nuvem como datacenter secundário ou como um ambiente de recuperação.

14.9. Fornecer o monitoramento e envio de alertas do estado de suas instâncias protegidas.

14.10. A solução deverá permitir a reconfiguração das interfaces de rede destino.

14.11. Solução de Desastre Avançada

14.11.1. A solução de desastre avançada deverá ser licenciada por máquina virtual.

14.11.2. A solução de desastre avançada deverá ser entregue com uma política de replicação para no mínimo 15 minutos de RPO (Recovery Point Object).

14.11.3. A solução de desastre avançada deverá ser entregue com a funcionalidade de retenção para os pontos no tempo, provendo no mínimo 7 dias de retenção.

15. SOFTWARES E LICENCIAMENTO

15.1. Todos os licenciamentos necessários para a prestação dos serviços de Cloud Computing, conforme descrito neste Termo de Referência, serão responsabilidade da contratada.

15.2. Durante a vigência do contrato, a Contratada deverá fornecer os seguintes softwares licenciados:

15.2.1. Windows Server na sua versão mais recente;

15.2.2. Red Hat Enterprise Linux na sua versão mais recente;

15.2.3. Windows Remote Desktop na sua versão mais recente;

15.2.4. Microsoft SQL Server Standard;

15.2.4.1. Caso haja a requisição de uso do licenciamento SQL Server Standard, deverá ser considerado o consumo mensal para no mínimo 4 vCPUs.

15.2.5. Microsoft SQL Server Enterprise;

15.2.5.1. Caso haja a requisição de uso do licenciamento SQL Server Entreprise, deverá ser considerado o consumo mensal para no mínimo 4 vCPUs.

15.3. Os softwares poderão ser atualizados pela contratada durante toda a vigência do contrato.

15.4. A solução deve permitir licenciamentos atuais de posse desta Administração, conforme os parâmetros de licenças determinados, não se limitando a estes.

16. OPERAÇÃO, SUPORTE E GERENCIAMENTO

16.1. A CONTRATADA deverá prover todo o suporte e gestão da solução ofertada.

16.2. É responsabilidade da CONTRATADA monitorar a solução 24 x 7 x 365 (vinte e quatro horas, sete dias por semana, 365 dias por ano) para garantia da disponibilidade da mesma.

16.3. A CONTRATADA será responsável por operar e gerenciar as tarefas de backup de acordo com as solicitações realizadas pelo time da CONTRATANTE,

devendo adicionar, alterar ou remover tarefas e rotinas de backup, de acordo com as solicitações.

16.4. A CONTRATADA será responsável em verificar a execução das rotinas e tarefas de backup.

16.5. Em casos de falha, a CONTRATADA deverá notificar prontamente o time da CONTRATANTE, verificar a causa raiz da falha, e sendo possível a correção, corrigir e executar novamente a tarefa.

16.6. A CONTRATANTE terá direito a um número ilimitado de alterações mensais nas políticas e rotinas vigentes em seu cenário de backup sem qualquer custo adicional.

16.7. A CONTRATADA deverá enviar mensalmente relatório estatístico das rotinas de backup.

16.8. A CONTRATADA deverá fornecer suporte técnico na modalidade 8 x 5 (8 horas por dia e 5 dias por semana) em língua portuguesa, para sanar dúvidas quanto da solução, sua configuração ou quaisquer outros assuntos relacionados à solução, através de suporte telefônico, por e-mail e através de um sistema online de chamados.

16.9. Em casos de acionamento de desastre, restaurações de bancos ou que seja necessária a restauração baremetal de um ou mais servidores, a CONTRATADA deve disponibilizar time técnico devidamente qualificado e de forma presencial nas dependências da CONTRATADA para a realização ou acompanhamento das tarefas.

16.10. A equipe técnica deverá estar alocada em até no máximo 4 horas na CONTRATANTE, após a constatação efetiva do desastre.

16.11. Durante a execução deste serviço a CONTRATADA se obriga a manter profissional(ais) com todas as qualificações.

16.12. SUPORTE A AMBIENTE MICROSOFT

16.12.1. Alguns serviços a serem executados incluem, mas não se limitam a:

16.12.1.1. Auxílio na migração de servidores Windows 2008 para Windows 2019;

16.12.1.2. Auxílio na migração de servidores Windows 2012 para Windows 2019;

16.12.1.3. Auxílio na atualização da estrutura de domínio para ambiente Windows 2019;

16.12.1.4. Auxílio no troubleshooting de problemas de operação;

16.12.1.5. Auxílio no planejamento de Life-cycle de servidores;

16.12.1.6. Auxílio na implantação de novos serviços e rotinas pertinentes ao domínio.

16.13. SUPORTE A AMBIENTE RED HAT

16.13.1. Alguns serviços a serem executados incluem, mas não se limitam a:

16.13.1.1. Auxílio na migração de servidores;

16.13.1.2. Auxílio na atualização da estrutura;

16.13.1.3. Auxílio no troubleshooting de problemas de operação;

16.13.1.4. Auxílio no planejamento de Life-cycle de servidores;

16.13.1.5. Auxílio na implantação de novos serviços e rotinas pertinentes ao ambiente.

16.14. SUPORTE A BANCO DE DADOS

16.14.1. Alguns serviços a serem executados incluem, mas não se limitam a:

16.14.1.1. Auxílio no monitoramento

16.14.1.2. Auxílio no troubleshooting de problemas de operação;

16.14.1.3. Auxílio na implantação de novos serviços e rotinas pertinentes ao banco de dados.

16.15. SUPORTE A AMBIENTE DE FIREWALL

16.15.1. O serviço deve ser prestado por profissional certificado pela solução NSE4, SNSA, JNCIP, PCNSA ou equivalentes (certificação ativa ou desativa) ou especialista em solução de segurança baseada em firewall.

16.15.2. Alguns serviços a serem executados incluem, mas não se limitam a:

16.15.2.1. Auxílio na migração das regras do firewall existente para o firewall em nuvem;

16.15.2.2. Auxílio no troubleshooting de problemas de operação;

16.15.2.3. Auxílio na implantação de novos serviços e rotinas pertinentes ao ambiente.

17. DA PRIVACIDADE E DISPONIBILIDADE

17.1. O prazo para disponibilização dos serviços para a CONTRATANTE deverá ser de até 60 dias após a assinatura do contrato

17.2. A qualquer momento durante a execução deste contrato, todos os dados e informações da CONTRATADA poderão ser solicitados pela CONTRATADA para a CONTRATANTE e deverão ser disponibilizados em até 48 horas após esta solicitação. Os dados deverão ser disponibilizados em formato de padrão de mercado, sem qualquer tipo de criptografia ou formato proprietário da CONTRATADA, de forma que permita serem lidos, acessados e modificados pela CONTRATANTE.

17.3. Após o término do contrato, todos os dados e informações da CONTRATADA devem ser disponibilizados em formato de padrão de mercado, sem qualquer tipo de criptografia ou formato proprietário da CONTRATADA, de forma que permita serem lidos, acessados ou modificados pela CONTRATANTE. Os dados deverão ser disponibilizados em um local a ser disponibilizado pela CONTRATANTE em um prazo de até 48 horas após a solicitação formal.

18. REGULAMENTO DA PROVA DE CONCEITO

18.1. Por se tratar de uma contratação de serviço em um ambiente de terceiros, não há como fazer a habilitação do licitante vencedor apenas através da análise de documentos ou da conferência física em equipamentos, pois eles estarão instalados no datacenter da empresa vencedora

18.2. A prova de conceito tem a finalidade de validar e conferir se todas as exigências técnicas serão devidamente cumpridas antes da efetivação do contrato com a empresa vencedora

18.3. A prova de conceito será realizada apenas com o licitante vencedor do certame

18.4. Todas as atividades relativas à Prova de Conceito serão realizadas dentro do horário comercial, de 10h às 16h, nas dependências da CONTRATANTE, ou através de vistoria técnica presencial na localidade onde se encontra o datacenter da empresa vencedora, a critério único e exclusivo da CONTRATANTE.

18.5. A Prova de Conceito será composta pela homologação das funcionalidades, características e demais evidências acerca da Solução Computacional de Nuvem ofertada, segundo o Roteiro apresentado neste documento (a seguir no texto).

18.6. O prazo máximo para a conclusão de todas as etapas previstas no Roteiro da Prova de Conceito será de 10 (dez) dias úteis após iniciada a atividade.

18.7. A LICITANTE deverá executar todas as atividades previstas no Roteiro da Prova de Conceito, devendo apresentar os produtos gerados para a verificação da conformidade quanto aos requisitos descritos neste Termo de Referência.

18.8. A partir da convocação do pregoeiro, a LICITANTE terá até 05 (cinco) dias úteis para iniciar a Prova de Conceito. Nesse prazo, dúvidas a respeito ao Roteiro poderão ser sanadas.

18.9. A Prova de conceito será avaliada quanto ao cumprimento dos requisitos do Roteiro e aderência ao Termo de Referência, por uma equipe de técnicos a ser nomeada pelo CONTRATANTE.

18.10. Caso a empresa vencedora não consiga comprovar o atendimento à todas as exigências da prova de conceito, sua proposta será considerada como desclassificada, sendo chamado o próximo licitante com a menor oferta durante a fase de lances para executar a mesma prova de conceito.

18.11. Só será considerada como habilitada a empresa que comprovar o atendimento à todas as exigências da prova de conceito.

19. ROTEIRO DA PROVA DE CONCEITO

19.1. O roteiro para testes desta prova de conceito deverá ocorrer conforme as tarefas a seguir, sendo executadas pela licitante vencedora em acompanhadas pela CONTRATANTE:

19.2. deverá demonstrar a capacidade de conexão lógica entre a sede da CONTRATANTE e o datacenter da licitante vencedora

19.3. deverá demonstrar a taxa de transferência obtida entre a sede da CONTRATANTE e o datacenter da licitante vencedora, não podendo ser uma taxa sustentada inferior a 50 Mbps

19.4. deverá demonstrar a latência obtida entre a sede da CONTRATANTE e o datacenter da licitante vencedora, não podendo ser um tempo superior a 200 ms (milisegundos)

19.5. deverá executar uma rotina de backup de uma máquina virtual do ambiente da CONTRATANTE

19.6. deverá demonstrar a possibilidade de operação de uma máquina virtual a partir do backup efetuado no item anterior

19.7. deverá executar uma rotina de restore (recuperação) da máquina virtual que teve o backup realizado no item anterior

19.8. deverá executar uma rotina de restore (recuperação) de apenas um objeto (arquivo ou pasta) da máquina virtual definido pela CONTRATANTE, que teve o backup realizado no item anterior.

20. IMPLANTAÇÃO E INTEGRAÇÃO

20.1. Deve compreender a instalação física e lógica da solução (desde a montagem dos equipamentos, configuração, testes, até que o a solução esteja ativa e em pleno funcionamento), além de ligações de energia elétrica. A solução deverá ser instalada e configurada em seu local de funcionamento, ligados à alimentação elétrica dos nobreaks indicados pela equipe técnica;

20.2. Caso a ligação elétrica existente não seja suficiente para ligação ou mesmo haja necessidade de complemento de material, a contratada deverá realizar o provimento desta instalação através do fornecimento e a passagem da infraestrutura e cabeamento elétrico do quadro até o rack, inclusive com o fornecimento dos plugues ou o que for necessário para a correta instalação do equipamento, conforme a recomendação do fabricante.

20.3. A Solução deverá vir com todos os acessórios, réguas e tomadas para se interligar às atuais existentes;

20.4. Realizar a instalação física e configuração lógica dos switches.

20.5. Realizar serviço de migração dos dados, servidores (limitado a 300 servidores) e serviços atuais armazenados nos storage atuais para a nova solução. Acompanhar e desenvolver solução conjunta para os problemas que houver durante a migração.

20.6. Todo cabeamento (fibras, patch cords, cabos elétricos) necessários para que o datacenter da CONTRATADA deverão ser previstas para atender suas capacidades plenas e integrado à infraestrutura da CONTRATANTE deverá ser fornecido pela CONTRATADA;

20.7. Os componentes dos equipamentos deverão ser homologados pelo fabricante. Não será aceita a adição ou subtração de qualquer componente não original de fábrica para adequação do equipamento;

20.8. Os horários de instalação, serão executados em hora e dia previstos pela equipe técnica responsável da CONTRATANTE, podendo ser requisitados fora do horário normal de expediente, estes combinados com antecedência;

20.9. Deverá ser elaborado cronograma contemplando as etapas de instalação e configurações;

20.10. Análise de ambiente, ligações de cabos, apresentação lógica e ativação da solução.

20.11. Depois de concluída a instalação e configuração dos novos equipamentos, a Contratada deverá fornecer documentação detalhada de todo o processo de instalação e configuração dos equipamentos ativos da solução;

20.12. Realização de testes da solução;

20.13. Preparação e detalhamento do ambiente a ser implantado.

20.14. Todos os equipamentos deverão ser fornecidos com manuais técnicos do usuário e de referência contendo todas as informações sobre os produtos com as instruções para instalação, configuração, operação e administração.

21. OUTROS

21.1. Quando o Licitante não for o próprio fabricante dos equipamentos ofertados, deverá apresentar declaração do Fabricante específica para o edital, autorizando a empresa licitante a comercializar os equipamentos ofertados;

21.2. Os componentes do equipamento deverão ser homologados pelo fabricante. Não será aceita a adição ou subtração de qualquer componente não original de fábrica para adequação do equipamento;

21.3. Apresentação de no mínimo um atestado emitido por pessoa jurídica de direito público ou privado, comprovando que a proponente fornece/forneceu bens compatíveis com os objetos da licitação emitidos em papel timbrado, com assinatura, identificação e telefone do emitente.

22. TREINAMENTO

22.1. A contratada deverá fornecer treinamento via web ou presencial para a equipe técnica da CONTRATANTE, habilitando-a a realizar Diagnóstico e Manutenção dos equipamentos fornecidos;

22.2. O treinamento capacitará equipe técnica a realizar diagnósticos, abrir chamados diretamente em ferramenta do fabricante, solicitar peça e se necessário realizar a troca do componente;

22.3. Esse escopo será tratado como um recurso opcional e/ou complementar, ao nível de suporte dos equipamentos visando incrementar o atendimento referente ao suporte técnico do fabricante. Tal certificação/habilitação não torna

a CONTRATANTE responsável técnica pelos atendimentos dos referidos equipamentos. Esta responsabilidade permanece do fabricante;

22.4. O treinamento deve propiciar aos técnicos da CONTRATANTE a autorização de abertura dos equipamentos para diagnóstico e acréscimo de periféricos / dispositivos homologados sem perda da garantia, bem como solicitação de peças para reposição e abertura de chamados com o fabricante.

22.5. 1 visita mensal presencial durante a vigência do contrato para manutenção preventiva, corretiva e atualização das máquinas virtuais.

23. ENTREGA

23.1. O prazo máximo de entrega deverá ser de até 30 dias a partir do recebimento do empenho, ou no caso de haver contrato formal, a partir da data de assinatura;

23.2. A entrega deverá ser realizada na sede da CONTRATANTE, observando o horário de funcionamento da Instituição.

24. DA VISITA TÉCNICA FACULTATIVA

24.1. O licitante poderá realizar visita técnica, visando o pleno conhecimento do objeto, das condições de atendimento, dos acessos, equipamentos e sistemas, das instalações físicas, bem como das demais informações necessárias para a consecução do objeto da contratação.

24.2. Para realização da visita técnica será necessário o agendamento prévio junto ao Departamento de Tecnologia da Informação, de segunda a sexta-feira, das 09:00 às 17:00 horas ou através do telefone (11) 4993-7271 ou ainda ou pelo e-mail: ti@fmabc.br

24.3. A visita técnica é facultativa.

24.4. A não realização da visita exime o direito do licitante a questionamentos posteriores e alegações de desconhecimento para o não cumprimento das obrigações contratuais.

24.5. Local para a visita - instalações da CONTRATANTE, situada na Av. Lauro Gomes, 2000 – Bairro Vila Principe de Gales – Santo André - – SP – de 2ª a 6ª feiras das 10h00min às 12h00min e das 13h00min às 16h00min, oportunidade em que lhe será fornecido Atestado de Vistoria, para averiguação e ciência da complexidade técnica que recairão na instalação dos equipamentos objeto desta licitação.

JUSTIFICATIVA DA CONTRATAÇÃO

Itens necessários para a mudança do Data Center atual para Cloud (nuvem). O Data Center atual está localizado em uma sala que deverá ser desativada no Centro Universitário FMABC.

LOCAL DE ENTREGA

A entrega do serviço deverá ser realizada no Centro Universitário FMABC, localizado na Av. Lauro Gomes, 2000 – Vila Sacadura Cabral – Santo André – SP – CEP: 09060-650 (Portaria 1), devendo ser previamente agendada utilizando como forma de comunicação oficial o e-mail ti@fmabc.br e telefone (11)4993-7271.

VIGÊNCIA

O prazo de vigência deverá ser pelo período de 12 (doze) meses, contados da assinatura do contrato, podendo ser prorrogado por iguais e sucessivos períodos a critério da Contratante até o limite de 60 (sessenta) meses, desde que:

- Esteja formalmente demonstrado que a forma de prestação dos serviços tem natureza continuada;
- Seja juntado relatório que discorra sobre a execução do contrato, com informações de que os serviços tenham sido prestados regularmente;
- Seja juntada justificativa e motivo, por escrito, de que a Instituição Contratante mantém interesse na realização do serviço.
- Seja comprovado que o valor do contrato permanece economicamente vantajoso para Instituição;
- Haja manifestação expressa da Contratada informando o interesse na prorrogação; e
- Seja comprovado que a contratada mantém as condições iniciais de habilitação.

A prorrogação de contrato deverá ser promovida mediante celebração de termo aditivo.

DO CONTRATO

A pretensa contratação será formalizada por meio de instrumento contratual e será regida pela Lei nº 14.133/2021.

Já no que diz respeito ao ulterior vencedor, aquele que não comparecer para a assinatura do contrato no prazo de 5 (cinco) dias úteis, contados da sua convocação, decairá do direito a contratação, sem prejuízo das sanções previstas neste instrumento e no termo de contrato a ser firmado entre as partes.

Na ocorrência do disposto no item acima, facultar-se-á a Contratante convocar os demais proponentes, sucessivamente e por ordem de classificação, para assinar o instrumento contratual em igual prazo e nas mesmas condições propostas pelo vencedor, inclusive quanto aos preços e prazos, independente da aplicação das

cominações previstas.

Não estão sujeitos às penalidades do item acima, *in fine*, os licitantes que convocados nos termos do citado item não aceitarem a contratação nas mesmas condições propostas pelo que apresentara o menor preço na ordem de classificação.

O contrato firmado com a vencedora poderá ser alterado nos termos do art. 124 da Lei nº 14.133/2021, mediante termo aditivo.

A Contratada ficará obrigada a aceitar, nas mesmas condições ajustadas, acréscimos ou supressões que se fizerem necessárias no objeto do contrato de acordo com o artigo 125 da Lei 14.133 de 2021.

DOS PRAZOS DE ENTREGA

O prazo de entrega do serviço descritos no objeto deste Termo de Referência, iniciar-se-á com a emissão da ordem de fornecimento no prazo de até 15 (quinze) dias úteis.

QUALIFICAÇÃO TÉCNICA

Para a comprovação da qualificação técnica, a Proponente deverá apresentar atestado fornecido por pessoas jurídicas de direito público ou privado conforme modelo contido no **ANEXO I** deste Termo de Referência, no qual deverá estar comprovado que fornece ou forneceu em favor dos signatários, material compatível em característica com o Objeto pretendido pela Contratante.

OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATADA

A Contratada além do fornecimento dos produtos, obriga-se a:

Fornecer dentro do prazo acordado os respectivos produtos relacionados neste Termo de Referência, nos horários estabelecidos pela Contratante.

Responsabilizar-se integralmente pela qualidade dos produtos fornecidos, cumprindo as disposições legais que interfiram em sua comercialização.

Designar por escrito, no ato do recebimento da Autorização de Fornecimento, preposto (s) que tenha (m) poder (es) para resolução de possíveis ocorrências durante o fornecimento dos itens contratados.

Responsabilizar-se pelos danos causados diretamente à Contratante ou a terceiros, decorrentes de sua culpa ou dolo, não excluindo ou reduzindo essa responsabilidade à fiscalização do Contratante.

Manter todas as condições que culminaram em sua habilitação desde a entrega o início da vigência contratual, durante a entrega do serviço, até o término de sua vigência com a atestação dos produtos contratados.

Comunicar, por escrito, imediatamente, a impossibilidade atendimento à qualquer

obrigação contratual, para adoção das providências cabíveis.

Reparar, corrigir, remover, refazer ou substituir, às suas expensas, imediatamente, os equipamentos em que se verificarem vícios, defeitos ou incorreções.

Permitir e facilitar a supervisão dos seus serviços pela fiscalização.

Substituir, por sua conta e responsabilidade, os equipamentos recusados pela fiscalização, em prazo a ser estabelecido pelo Contratante de acordo com cada caso.

OBRIGAÇÔES E RESPONSABILIDADES DO CONTRATANTE

O Centro Universitário fiscalizará a entrega do serviço através de funcionário designado para esse fim, com a incumbência de relatar as falhas ou irregularidades que verificar, as quais, se não forem sanadas, estarão passíveis de aplicação das sanções estabelecidas por lei, bem como as constantes deste Termo de Referência.

Indicar, formalmente, o gestor e ou fiscal para acompanhamento da entrega do serviço, objeto deste Termo de Referência.

Efetuar os pagamentos nas condições e preços pactuados no contrato.

Rejeitar no todo ou em parte, os equipamentos em desacordo com as exigências deste Termo de Referência e do contrato, atestando seu recebimento, após verificação das especificações.

Expedir Autorização de Fornecimento no prazo máximo de 15 (quinze) dias após a divulgação do vencedor.

A Contratante elegerá como responsável pela fiscalização e acompanhamento da entrega do objeto do presente contrato, **o Sr. José Roberto de Sousa Martins,** o qual poderá ser contactado em horário comercial, através dos canais abaixo descritos:

E-mail: roberto.martins@fmabc.br

Telefone: (011) 4993-5420

Aplicar as penalidades previstas para o caso do não cumprimento de cláusulas contratuais, ou aceitar as justificativas apresentadas pela empresa.

CONTROLE DA EXECUÇÃO DO SERVIÇO

A fiscalização por parte da Contratante não exime, nem diminui a completa responsabilidade da Contratada, por qualquer inobservância ou omissão às cláusulas Contratuais.

O acompanhamento quanto ao cumprimento da entrega do serviço ocorrerá por conta

da Contratada, e cabe a fiscalização por conta da Contratante, através do colaborador responsável, ao qual compete o acompanhamento, controle e avaliação dos materiais a serem entregues.

DO ENVIO DA PROPOSTA DE PREÇOS

Apresentar proposta de preços conforme ANEXO II e documentações de forma clara, contendo discriminação detalhada dos itens ofertados contendo módulos, valor unitário e total, em moeda nacional brasileira, em algarismo e por extenso, garantia, assistência técnica e demais informações relevantes.

A proposta de preços, deverá conter especificações detalhadas do objeto ofertado, e deverá ser formulada e enviada em formulário específico, exclusivamente por meio do Sistema Eletrônico.

Indicação de valores, na qual a empresa participante se propõe a fornecer, expresso numericamente e por extenso, já incluídas, discriminadamente, todas as despesas, BDI, impostos, e quaisquer encargos que incidam ou venham a incidir sobre o objeto desta contratação.

A ALTERAÇÃO DO OBJETO DO CONTRATO

O contrato poderá ser modificado no todo ou em parte, por acordo entre as partes, somente através de Termo Aditivo de acordo com a previsão contida na Lei n° 14.133/2021.

DA CESSÃO E TRANSFERÊNCIA

É vedada a cessão ou transferência total ou parcial dos direitos e/ou obrigações inerentes a este contrato, por quaisquer das partes, sem prévia e expressa autorização da outra.

DO PAGAMENTO

O Centro Universitário FMABC compromete-se a pagar o preço constante da proposta da Contratada, observadas as seguintes condições:

O pagamento será efetuado à Contratada em 12 (doze) parcelas iguais, sendo:

A **Primeira parcela** – 30 (trinta) dias após o início dos serviços e aceite da respectiva nota fiscal pelo Contratante;

Caso seja detectado algum problema na documentação entregue anexada à nota fiscal, será concedido, pela Contratante, prazo para regularização. Após o decurso deste, em permanecendo a inércia da Contratada, o contrato será rescindido com aplicação de multa prevista em capítulo próprio.

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

da Contratante.

Em caso de eventuais atrasos, os valores serão atualizados de acordo com a legislação vigente.

A Contratada deverá indicar, com a documentação fiscal, o número da conta corrente e a agência do Banco Santander S/A, a fim de agilizar o pagamento.
A Contratada deverá enviar a nota fiscal para os e-mails: compras@fmabc.br e ti@fmabc.br, na nota deverá constar o número do processo ao qual corresponde.

As notas fiscais deverão ser entregues em tempo considerável (até o quinto dia útil do mês subsequente), para que a Contratante possa proceder com as análises devidas e o subsequente pagamento dos valores.

DAS PENALIDADES E RECURSOS

Com fulcro nos artigos 155 e 156 da Lei 14.133/2021, atualizada, a Contratante poderá, garantida a prévia defesa, aplicar à Contratada as seguintes sanções:

I) advertência;

II) multa, a ser recolhida no prazo máximo de 15 (quinze) dias corridos, a contar da comunicação oficial, nas seguintes hipóteses:

II.1 – 0,3% (zero vírgula três por cento) por dia de atraso injustificado e por descumprimento das obrigações estabelecidas em contrato, até o máximo de 10% (dez por cento) sobre o valor total do contrato;

II.2 – 10% (dez por cento) sobre o valor total do contrato, no caso de inexecução total ou 5% (cinco por cento) do valor total do objeto contratado, no caso de inexecução parcial;

III) impedimento de contratar;

IV) declaração de inidoneidade para licitar ou contratar, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação perante a própria autoridade que aplicou a penalidade.

As sanções previstas nos incisos I, III, e IV do caput poderão ser aplicadas juntamente com as do inciso II.

Da aplicação das penalidades previstas nos incisos I, II e III do caput, poderão ser interpostos recursos no prazo máximo de 5 (cinco) dias úteis, a contar da intimação do ato ou da lavratura da ata.

No caso da penalidade prevista no inciso IV do caput, caberá pedido de reconsideração, no prazo de 10 (dez) dias úteis, a contar da intimação do ato, podendo a reabilitação ser requerida após 2 (dois) anos de sua aplicação.

DA RESCISÃO

A inexecução total do Contrato ensejará a sua rescisão, enquanto a inexecução parcial poderá ensejar a sua rescisão, com as consequências cabíveis, conforme penalidades do artigo anterior.

As práticas passíveis de rescisão, tratadas no inciso anterior, podem ser definidas, dentre outras, como:

a) **corrupta:** oferecer, dar, receber ou solicitar, direta ou indiretamente, qualquer vantagem com o objetivo de influenciar a ação do empregado da **CONTRATANTE** no processo administrativo ou na execução do Contrato;
b) **fraudulenta:** falsificar ou omitir fatos, com o objetivo de influenciar o processo administrativo ou de execução do Contrato;

c) **colusiva:** esquematizar ou estabelecer um acordo entre dois ou mais interessados, com ou sem conhecimento de representantes da Companhia, visando estabelecer preços em níveis artificiais e não competitivos;
d) **coercitiva:** causar dano ou ameaçar, direta ou indiretamente, as pessoas físicas ou jurídicas, visando influenciar sua participação em processo de credenciamento ou afetar a execução do Contrato;
e) **obstrutiva:** destruir, falsificar, alterar ou ocultar provas ou fazer declarações falsas, com objetivo de impedir materialmente a apuração de práticas ilícitas.

As práticas acima exemplificadas, além de acarretarem responsabilização administrativa e judicial da pessoa física e/ou jurídica, implicarão na responsabilidade individual dos dirigentes da **CONTRATADA** e dos administradores ou gestores, enquanto autores, coautores ou partícipes do ato ilícito, nos termos da lei.

São considerados motivos para a rescisão:

a) a inexecução parcial ou total das obrigações e prazos constantes nos Instrumentos Convocatórios e Contratuais;
b) a dissolução da sociedade ou o falecimento do contratado;
c) a decretação de falência ou a insolvência civil do contratado;
d) a alteração social ou a modificação da finalidade ou da estrutura da **CONTRATADA**, desde que prejudique a execução do Contrato;
e) razões de interesse público, de alta relevância e amplo conhecimento, justificadas e exaradas no processo administrativo;
f) o atraso nos pagamentos devidos pela **CONTRATANTE** decorrentes de serviços ou fornecimentos, ou parcelas destes já recebidos ou executados, salvo em caso de calamidade pública, grave perturbação da ordem interna ou guerra, assegurado ao contratado o direito de optar pela suspensão do cumprimento de suas obrigações até que seja normalizada a situação;
g) a ocorrência de caso fortuito, força maior ou fato do príncipe, regularmente comprovada, impeditiva da execução do Contrato;
h) a aplicação ao contratado de suspensão do direito de licitar e/ou contratar com a **FUNDAÇÃO DO ABC E SUAS UNIDADES GERENCIADAS**;

i) o descumprimento da proibição de trabalho noturno, perigoso ou insalubre a menores de 18 (dezoito) anos e de qualquer trabalho a menores de 16 (dezesseis) anos, salvo na condição de aprendiz, a partir de 14 (quatorze) anos;

j) ter frustrado ou fraudado, mediante ajuste, combinação ou qualquer outro expediente, o caráter competitivo de procedimento licitatório público; ter impedido, perturbado ou fraudado a realização de qualquer ato de procedimento licitatório público; ter afastado ou procurado afastar Proponentes, por meio de fraude ou oferecimento de vantagem de qualquer tipo; ter fraudado licitação pública ou Contrato dela decorrente; ter criado, de modo fraudulento ou irregular, pessoa jurídica para participar de licitação pública ou celebrar Contrato Administrativo; ter obtido vantagem ou benefício indevido, de modo fraudulento, de modificações ou prorrogações de Contratos celebrados com a Administração Pública, sem autorização em lei, no instrumento convocatório da licitação pública ou nos respectivos instrumentos contratuais; ter manipulado ou fraudado o equilíbrio econômico-financeiro dos Contratos celebrados com a Administração Pública; ter dificultado atividade de investigação ou fiscalização de órgãos, entidades ou agentes públicos, ou ter intervindo em sua atuação, inclusive no âmbito das agências reguladoras e dos órgãos de fiscalização do sistema financeiro nacional;

O Contrato poderá ser rescindido unilateralmente, desde que haja conveniência para a **Contratante** mediante autorização escrita e fundamentada da autoridade superior.

DA LEI GERAL DE PROTEÇÃO DE DADOS

A Contratada, por si e por seus administradores, diretores, funcionários e agentes, bem como seus sócios que venham a agir em seu nome, se obriga a conduzir suas práticas comerciais, durante a consecução do presente Contrato, de forma ética e em conformidade com os preceitos legais aplicáveis, incluindo a Lei Anticorrupção Brasileira e o Código de Conduta da Contratante.

Na execução deste Contrato, nem a Contratada, nem qualquer de seus diretores, empregados, agentes ou sócios agindo em seu nome, devem dar, oferecer, pagar, prometer pagar, ou autorizar o pagamento de, direta ou indiretamente, qualquer dinheiro ou qualquer coisa de valor a qualquer autoridade governamental, consultores, representantes, parceiros ou quaisquer terceiros, com a finalidade de influenciar qualquer ato ou decisão do agente ou do governo, ou para assegurar qualquer vantagem indevida, ou direcionar negócios para qualquer pessoa.

PRAZO PARA ASSINATURA DO CONTRATO

A empresa vencedora terá o prazo de até 05 (cinco) dias, contados a partir da convocação, para assinar o contrato.

No ato da contratação, a proponente vencedora, caso não seja sócio, deverá apresentar documento de procuração devidamente reconhecido em cartório, que habilite o seu representante a assinar o contrato em nome da empresa.

DO FORO

Fica eleito o Foro de Santo André – São Paulo, com exclusão de qualquer outro, para dirimir questões decorrentes do cumprimento deste contrato.

_____

José Roberto de Sousa Martins
Gerente de TI

ANEXO II – MODELO DE PROPOSTA

RECURSOS COMPUTACIONAIS						
DESCRIÇÃO	**UNIDADE**	**PREÇO**	**QTD. MÍNIMA**	**QTD. MÁXIMA**	**TOTAL Mín.**	**Total Máx.**
Memória	GB		150	300		
vCPU	vCPU		40	80		
ARMAZENAMENTO						
SSD	GB		9000	9000		
HDD	GB		9000	9000		
OBJECT STORAGE	GB		0	20000		
CONECTIVIDADE						
Link de Internet - VPC	Mbps		100	1000		
Link L2L - 1 Gbps	Gbps		1	3		
IP's válidos	IPS		2	8		
FIREWALL E SEGURANÇA						
Firewall	Instância		1	2		
SOLUÇÃO DE DETECÇÃO E RESPOSTA DE ENDPOINTS						
Solução de Detecção e Resposta de Endpoints	VM		20	50		
BACKUP						
Backup	VM		15	100		
Repositório de Backup	TB		20	100		
RECUPERAÇÃO DE DESASTRES						
Recuperação de Desastre Avançada	VMS		20	50		
SOFTWARES E LICENCIAMENTO						
Windows Server	VM		10	50		
Windows Remote Desktop	Device		0	20		
Red Hat Enterprise Linux	VM		0	10		
SQL Server Standard 2 Lic Core	vCPU		0	2		
SQL Server Enteprise 2 Lic Core	vCPU		0	2		
OUTROS						
Rack Collocation (U)	Rack Unit		0	10		
Operação, Suporte, Analise Avançada e Especialistas	Hora		20	100		

VALOR TOTAL		

ANEXO III - MODELO DE ATESTADO DE CAPACIDADE TÉCNICA

[PAPEL TIMBRADO]
ATESTADO DE CAPACIDADE TÉCNICA

Atestamos, para os devidos fins, que a empresa [nome da empresa prestadora de serviços, em negrito], inscrita no CNPJ sob o nº ____***, estabelecida na Rua _____, nº __, bairro _____, na cidade de _____, Estado de ___, prestou serviços à [nome da empresa contratante, em negrito], CNPJ nº _____, estabelecida na Rua _____, nº __, bairro _____, na cidade de _____, Estado de*** , detém qualificação técnica para [descrever o objeto].

Registramos que a empresa prestou serviços/entregou produtos [descrição dos serviços prestados, especificando o prazo de execução]

Informamos ainda que as prestações dos serviços/entrega dos materiais acima referidos apresentaram bom desempenho operacional, tendo a empresa cumprido fielmente com suas obrigações, nada constando que a desabone técnica e comercialmente, até a presente data.

Cidade, ____ de _____ de _____.

_____

[assinatura e nome do responsável da empresa emitente do atestado]

ANEXO IV
DECLARAÇÃO QUE NÃO EMPREGA MENOR
(papel timbrado da empresa)

AO
CENTRO UNIVERSITÁRIO FMABC
PROCESSO Nº 0544/2023
PREGÃO PRESENCIAL nº 07 / 2023
CONTRATAÇÃO DE COMPUTAÇÃO EM NUVEM, LINK DEDICADO E BACKUP PARA O CENTRO UNIVERSITÁRIO FMABC

Prezados Senhores:

Eu,_____, abaixo qualificado, interessado em participar do processo em epígrafe, do Centro Universitário FMABC, declaro, sob as penas da lei, que, nos termos da Lei Federal nº 9.854 de 27 de outubro de 1999, que encontro em situação regular perante o Ministério do Trabalho e Emprego, no que se refere à observância do disposto no inciso XXXIII do artigo 7º da Constituição Federal e que não emprego menor de dezoito anos em trabalho noturno, perigoso ou insalubre, bem como não emprega menor de dezesseis anos, salvo na condição de aprendiz, a partir de quatorze anos, conforme consta do artigo 403 da CLT (Consolidação das Leis do Trabalho).

[LOCAL] [DATA]

_____

Empresa
Representante Legal

CNPJ:

ANEXO V
DECLARAÇÃO DE MANUTENÇÃO DAS CONDIÇÕES CONTRATUAIS
(papel timbrado da empresa)

AO
CENTRO UNIVERSITÁRIO FMABC
PROCESSO Nº 0544/2023
PREGÃO PRESENCIAL nº 07 / 2023
CONTRATAÇÃO DE COMPUTAÇÃO EM NUVEM, LINK DEDICADO E BACKUP PARA O CENTRO UNIVERSITÁRIO FMABC

Declaramos, sob as penas da lei, que a empresa....., participante do presente Edital realizado pelo Centro Universitário FMABC, possui estrutura disponível e suficiente com pessoal técnico adequado para a execução do serviço, objeto do certame e manterá, durante a vigência contratual, instalações, aparelhamento e pessoal técnico adequado e disponível para a realização do objeto do processo.

[LOCAL] [DATA]

_____

Empresa
Representante Legal

CNPJ:

ANEXO VI
DECLARAÇÃO DE PLENO ATENDIMENTO
(papel timbrado da empresa)

AO
CENTRO UNIVERSITÁRIO FMABC
PROCESSO Nº 0544/2023
PREGÃO PRESENCIAL nº 07 / 2023
CONTRATAÇÃO DE COMPUTAÇÃO EM NUVEM, LINK DEDICADO E BACKUP PARA O CENTRO UNIVERSITÁRIO FMABC

A empresa _____ por intermédio do seu representante ou procurador declara ao Centro Universitário FMABC que atende plenamente os requisitos e todas as condições de habilitação do Processo em epígrafe.

Por ser verdade, o signatário assume responsabilidade civil e criminal por eventual falsidade.

[LOCAL] [DATA]

_____

Empresa
Representante Legal

CNPJ:

ANEXO VII

DECLARAÇÃO DE ENQUADRAMENTO COMO MICROEMPRESA OU EMPRESA DE PEQUENO PORTE
(papel timbrado da empresa)

AO
CENTRO UNIVERSITÁRIO FMABC
PROCESSO Nº 0544/2023
PREGÃO PRESENCIAL nº 07 / 2023
CONTRATAÇÃO DE COMPUTAÇÃO EM NUVEM, LINK DEDICADO E BACKUP PARA O CENTRO UNIVERSITÁRIO FMABC

(Nome da Empresa) _____, inscrita no CNPJ nº _____, por intermédio de seu representante legal, o(a) Sr(a). _____, portador(a) da Carteira de Identidade nº _____ e do CPF nº _____, DECLARA, para fins de comprovação no Edital do Centro Universitário FMABC, sob as sanções administrativas cabíveis e sob as penas da lei, que esta empresa, na presente data, é considerada:

( ) MICROEMPRESA, conforme Inciso I do artigo 3º da Lei Complementar nº 123, de 14/12/2006;

( ) EMPRESA DE PEQUENO PORTE, conforme Inciso II do artigo 3º da Lei Complementar nº 123, de 14/12/2006.

Declara ainda que a empresa está excluída das vedações constantes do parágrafo 4º do artigo 3º da Lei Complementar nº 123, de 14 de dezembro de 2006.

[LOCAL] [DATA]

_____
Empresa
Representante Legal
CNPJ:

ANEXO VIII

DECLARAÇÃO INEXISTÊNCIA DE FATO SUPERVENIENTE IMPEDITIVO
(papel timbrado da empresa)

AO
CENTRO UNIVERSITÁRIO FMABC
PROCESSO Nº 0544/2023
PREGÃO PRESENCIAL nº 07 / 2023
CONTRATAÇÃO DE COMPUTAÇÃO EM NUVEM, LINK DEDICADO E BACKUP PARA O CENTRO UNIVERSITÁRIO FMABC

NOME DA EMPRESA_____ **CNPJ** _____**SEDIADA**_____ **(endereço completo),** declara, sob as penas da lei, que até a presente data inexistem fatos supervenientes impeditivos para sua habilitação no presente processo licitatório, ciente da obrigatoriedade de declarar ocorrências posteriores.

[LOCAL] [DATA]

_____

Empresa
Representante Legal

CNPJ:

ANEXO IX
DECLARAÇÃO DE ELABORAÇÃO INDEPENDENTE DE PROPOSTA E ATUAÇÃO CONFORME AO MARCO LEGAL ANTICORRUPÇÃO
(papel timbrado da empresa)

AO
CENTRO UNIVERSITÁRIO FMABC
PROCESSO Nº 0544/2023
PREGÃO PRESENCIAL nº 07 / 2023
CONTRATAÇÃO DE COMPUTAÇÃO EM NUVEM, LINK DEDICADO E BACKUP PARA O CENTRO UNIVERSITÁRIO FMABC

Prezados Senhores:

Eu, _____, portador do RG nº _____ e do CPF nº _____, representante legal do licitante _____ (nome empresarial), interessado em participar do processo em epígrafe, **DECLARO**, sob as penas da Lei, especialmente o artigo 299 do Código Penal Brasileiro, que:

a) a proposta apresentada foi elaborada de maneira independente e o seu conteúdo não foi, no todo ou em parte, direta ou indiretamente, informado ou discutido com qualquer outro licitante ou interessado, em potencial ou de fato, no presente procedimento licitatório;

b) a intenção de apresentar a proposta não foi informada ou discutida com qualquer outro licitante ou interessado, em potencial ou de fato, no presente procedimento licitatório;

c) o licitante não tentou, por qualquer meio ou por qualquer pessoa, influir na decisão de qualquer outro licitante ou interessado, em potencial ou de fato, no presente procedimento licitatório;

d) o conteúdo da proposta apresentada não será, no todo ou em parte, direta ou indiretamente, comunicado ou discutido com qualquer outro licitante ou interessado, em potencial ou de fato, no presente procedimento licitatório antes da adjudicação do objeto;

e) o conteúdo da proposta apresentada não foi, no todo ou em parte, informado, discutido ou recebido de qualquer integrante relacionado, direta ou indiretamente, ao órgão licitante antes da abertura oficial das propostas; e

f) o representante legal do licitante está plenamente ciente do teor e da extensão desta declaração e que detém plenos poderes e informações para firmá-la.

DECLARO, ainda, que a pessoa jurídica que represento conduz seus negócios de forma a coibir fraudes, corrupção e a prática de quaisquer outros atos lesivos à Administração Pública, nacional ou estrangeira, em atendimento à Lei Federal nº 12.846/ 2013 e ao Decreto Estadual nº 60.106/2014, tais como:
I – prometer, oferecer ou dar, direta ou indiretamente, vantagem indevida a agente público, ou a terceira pessoa a ele relacionada;

II – comprovadamente, financiar, custear, patrocinar ou de qualquer modo subvencionar a prática

dos atos ilícitos previstos em Lei;

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

IV – no tocante a licitações e contratos:

a) frustrar ou fraudar, mediante ajuste, combinação ou qualquer outro expediente, o caráter competitivo de procedimento licitatório público;
b) impedir, perturbar ou fraudar a realização de qualquer ato de procedimento licitatório público;
c) afastar ou procurar afastar licitante, por meio de fraude ou oferecimento de vantagem de qualquer tipo;
d) fraudar licitação pública ou contrato dela decorrente;
e) criar, de modo fraudulento ou irregular, pessoa jurídica para participar de licitação pública ou celebrar contrato administrativo;
f) obter vantagem ou benefício indevido, de modo fraudulento, de modificações ou prorrogações de contratos celebrados com a administração pública, sem autorização em lei, no ato convocatório da licitação pública ou nos respectivos instrumentos contratuais; ou
g) manipular ou fraudar o equilíbrio econômico-financeiro dos contratos celebrados com a administração pública;

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

[LOCAL] [DATA]

_____

Empresa
Representante Legal

CNPJ:

ANEXO X – MINUTA DE CONTRATO

EMENTA: CONTRATAÇÃO DE COMPUTAÇÃO EM NUVEM, LINK DEDICADO E BACKUP PARA O CENTRO UNIVERSITÁRIO FMABC.

Por este instrumento de Contrato de Prestação de Serviços, as partes, de um lado a **FUNDAÇÃO DO ABC – CENTRO UNIVERSITÁRIO FMABC**, com sede na Avenida Lauro Gomes, 2.000, Vila Sacadura Cabral, Santo André, São Paulo/SP, CEP 09060-870, inscrita no CNPJ sob nº 57.571.275/0007-98, neste ato representado pelo seu Reitor Prof. Dr. David Everson Uip, brasileiro, casado, médico, portador do RG/SP sob o número 4.xxx.000, inscrito no CPF/MF número xxx.xxx.xxx-53 e o Vice-Reitor Prof. Dr. Fernando Luiz Affonso Fonseca, brasileiro, solteiro, portador da cédula de identidade RG n° xx.xxx.208, inscrito no CPF/MF n° xxx.xxx.xxx-42, doravante denominada simplesmente "CONTRATANTE", e de outro lado, a empresa _____, com sede à Rua _____, nº _____, Bairro _____, Cidade _____, inscrita no CNPJ sob o n°_____, representada por seu representante legal, **(qualificação completa)**, doravante designada "CONTRATADA", tem por justo e acordado o que segue:

1.0- DO OBJETO

1.1- Contratação de empresa especializada para prestação de serviço de hospedagem, conectividade, segurança de rede e backup (cópia de segurança), incluindo todos os serviços de garantia de funcionamento e suporte técnico, visando atendender às necessidades de infraestrutura do Centro Universitário FMABC, nas condições e especificações constantes do Termo de Referência, tendo em vista o que consta no Processo nº 0544/2023 e em observância às disposições da Lei nº 14.133/2021, na Lei nº 8.078, de 1990 - Código de Defesa do Consumidor, resolvem celebrar o presente Termo de Contrato de Prestação de Serviços, decorrente do Pregão PRESENCIAL nº 07/2023, mediante as cláusulas e condições a seguir enunciadas.

1.2- Constituem parte integrante deste Contrato os seguintes documentos, cujo teor as partes declaram ter pleno conhecimento:,

I – Termo de Referência;
II – Proposta de preços e os documentos de habilitação.
III – Questionário de Due Diligence de Compliance de Fornecedores;
IV – Termo de ciência e notificação.

2.0- VIGÊNCIA

2.1- O prazo de vigência deverá ser pelo período de 12 (doze) meses, contados da assinatura do contrato/contar de xxx, podendo ser prorrogado por iguais períodos a critério da contratante até o período de 60 (sessenta) meses, desde que:

2.2- Esteja formalmente demonstrado que a forma de prestação dos serviços tem natureza continuada;

2.3- Seja juntado relatório que discorra sobre a execução do contrato, com informações de que os serviços tenham sido prestados regularmente;

2.4- Seja apresentado justificativa e motivo, por escrito, de que a Instituição Contratante mantém interesse na realização do serviço;

2.5- Seja comprovado que o valor do contrato permanece economicamente vantajoso para a IES;

2.6- Haja manifestação expressa da Contratada informando o interesse na prorrogação; e

2.7- Seja comprovado que a contratada mantém as condições iniciais de habilitação.

2.8- A prorrogação de contrato deverá ser promovida mediante celebração de termo aditivo.

3.0- PRAZO PARA ASSINATURA DO CONTRATO

3.1- A empresa vencedora terá o prazo de até 05 (cinco) dias, contados a partir da convocação, para assinar o contrato.

3.2- No ato da contratação, a proponente vencedora, caso não seja sócio, deverá apresentar documento de procuração devidamente reconhecido em cartório, que habilite o seu representante a assinar o contrato em nome da empresa.

4.0- DO PRAZO DE INÍCIO DOS SERVIÇOS

4.1- A prestação do serviço terá início em até 15 (quinze) dias após o recebimento da ordem de serviço, a ser expedida por parte da área solicitante.

4.2- Caso, por motivo justo e devidamente justificado, a Contratada solicitar prorrogação do prazo para iniciação dos serviços, este pedido será analisado pela área requisitante sobre sua pertinência, por conveniência e oportunidade do Centro Universitário FMABC.

4.3- Se a Contratada não cumprir o prazo de início, sem justificativa formal aceita pela Contratante, decairá seu do direito de fornecer os serviços adjudicados, sujeitando-se as penalidades previstas neste Termo de Contrato, sendo convocados os proponentes remanescentes em ordem de classificação.

5.0- CARACTERÍSTICAS DA SOLUÇÃO DE CLOUD COMPUTING

5.1 Todos os equipamentos, software, infraestrutura e sustentação, necessários à implementação da solução proposta, são de inteira responsabilidade da Contratada, que deverá realizar de forma continuada tarefas e rotinas que garantam o pleno funcionamento de toda a infraestrutura, de forma integral e ininterrupta, ou seja, "24x7x365" (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias por ano) nas dependências da Contratada, mantendo em pleno funcionamento todo objeto da contratação.

5.2 A Contratada deverá gerenciar, monitorar, sustentar e operar de forma proativa todos os recursos disponibilizados para a CONTRATATANTE, de forma a garantir o correto funcionamento de todas as funcionalidades especificadas neste Termo de Referência, a partir de seu Centro de Operações de Rede (NOC), em regime 24x7 (24 horas por dia, 7 dias por semana).

5.3 A solução de Computação em Nuvem ofertada deve permitir a criação de uma ou mais VPC´s (Virtual Private Cloud), de forma que a CONTRATADA possa provisionar uma seção da nuvem da solução ofertada isolada logicamente, onde é possível executar recursos da solução em uma rede virtual definida pela CONTRATADA, permitindo o controle total sobre seu ambiente de redes virtuais, incluindo a seleção do seu próprio intervalo de endereços IP, a criação de sub redes e a configuração de tabelas de rotas e gateways de rede, para acessar recursos e aplicações com segurança e facilidade. Além disso, a CONTRATANTE poderá criar uma conexão de Hardware Virtual Private Network (VPN) entre seu datacenter corporativo e a VPC e aproveitar a nuvem da solução ofertada como uma extensão do seu datacenter corporativo.

5.4 A solução deverá ser escalável, de forma a permitir aumentar os recursos na infraestrutura de Cloud Computing da CONTRATADA para absorver a demanda complementar oriunda de picos de acesso ou expansão natural dos usuários em ambiente Cloud Computing.

5.5 Os servidores virtuais deverão ser disponibilizados em ambiente de Cloud Computing, em ambiente seguro e separados logicamente de outros clientes, com as seguintes funcionalidades:

5.6 Implementar características de escalabilidade horizontal (novos servidores) e vertical (aumento de recursos do mesmo servidor), flexibilidade de configuração de memória, processador e disco.

5.7 Implementar a movimentação automática de servidores virtuais para redistribuição de carga e recuperação de falhas do ambiente físico.

5.8 É de responsabilidade da Contratada o monitoramento do hardware e seus componentes, bem como a manutenção dos mesmos, identificando necessidades de reposições, adaptações e melhorias, procedendo chamados aos fornecedores, acompanhando, garantindo a devida solução aos problemas que porventura ocorram, observando os tempos definidos no Nível de Serviço Exigido e fornecendo Console de Gestão para monitoramento em tempo real de todos os recursos computacionais.

5.9 O monitoramento deverá ser feito de forma continuada, não sobrecarregando os equipamentos ou consumindo recursos da solução de cloud computing provisionada aos clientes.

6.0- CARACTERÍSTICAS DA INFRAESTRUTURA

6.1 A solução proposta deverá hospedar os dados em datacenter localizado em território nacional;

6.2 Para fins de segurança da informação os dados deverão ser replicados entre datacenters com no mínimo 40km de distância entre eles. Em caso de desastre no datacenter principal o ambiente deverá estar disponível do datacenter réplica.

6.3 Os serviços de Cloud Computing a serem prestados deverão ser baseados em infraestrutura de Datacenter, que deverá manter compatibilidade com padrões internacionais, e deverão manter compatibilidade durante toda vigência do contrato.

6.4 As instalações físicas e recursos de infraestrutura que suportarão o ambiente crítico de serviço atenderão, no mínimo, às características aqui definidas de estrutura física, instalações físicas, energia elétrica, climatização, proteção contra incêndio, segurança física, infraestrutura de acesso à internet do Datacenter e segurança lógica do Datacenter.

6.5 Os datacenters da CONTRATADA deverá possuir um ambiente com alta disponibilidade, atendendo aos seguintes requisitos mínimos:

6.6 Possuir certificação padrão TIER III;

6.7 Garantir a disponibilidade imediata de energia elétrica através do fornecimento de sistemas de nobreaks independentes e redundantes.

6.8 Redundância no fornecimento de link de internet de trânsito (uplink) através da utilização de no mínimo dois links IP's de trânsito diferentes e independentes. A comprovação deste item deverá ser feita através de sites públicos na internet como o https://bgpview.io/ ou https://bgp.he.net.

6.9 Redundância no anúncio de suas rotas através do protocolo BGP através da disponibilização de no mínimo dois roteadores distintos e independentes.

6.10 Redundância no fornecimento de portas de rede de acesso, através da disponibilidade de no mínimo dois switches distintos e independentes com portas Gigabit Ethernet com ao menos duas portas disponíveis em cada switch.

6.11 A fim de se comprovar o atendimento à estes requisitos mínimos, a CONTRATANTE se reserva o direito de realizar uma vistoria técnica presencial no ambiente da CONTRATADA, a qualquer momento durante a vigência deste contrato, mediante agendamento prévio.

6.12 Caso ocorram quaisquer despesas de deslocamento ou viagem para a realização desta vistoria presencial, as despesas serão de responsabilidade da CONTRATADA.

7.0- CONSOLE DE GESTÃO DO AMBIENTE CLOUD COMPUTING

7.1 Permitir o gerenciamento da infraestrutura de Computação em Nuvem de forma independente de softwares de cliente (VNC, Remote Desktop, SSH, etc), por meio de API (Application Programming Interface), acessada via browser, de forma segura (HTTPS), utilizando-se de recursos de autenticação.

7.2 O acesso via interface web browser não poderá permitir a visualização ou edição de qualquer componente persistente a infraestrutura física que compõe a solução.

7.3 Possibilitar o cadastramento dos colaboradores da CONTRATANTE, inclusive, por perfil de acesso para administrar, operar ou consultar o ambiente de produção da solução na infraestrutura de Computação em Nuvem disponibilizada pela Contratada.

7.4 Permitir selecionar modelos preexistentes (templates) de infraestrutura. A visualização dos modelos deve ser gráfica, por meio de diagramas e a sua edição deve ser simplificada.

7.5 Permitir personalizar modelos (templates) que melhor se adaptem às necessidades da CONTRATANTE.

7.6 Permitir modificar os recursos da Infraestrutura de Computação em Nuvem e atualizá-los de uma forma controlada e previsível, aplicando-se, quando necessário, controles de versionamento, devendo ser permitido o rastreamento das alterações históricas efetuadas no ambiente.

7.7 Disponibilizar console via interface gráfica afim de permitir o agendamento, realização de backups e horários de funcionamento por recurso (servidor; banco de dados, fileserver), por ambiente (produção) ou por etiqueta (classificação das soluções/sistemas).

8.0- CONSOLE DE GESTÃO DE DOMÍNIOS E SUBDOMÍNIOS

8.1 Deverá ser disponibilizado um painel de controle (software de gestão para alojamento web) com as opções mínimas de: gerenciamento FTP, gerenciamento de arquivos, gerenciamento de banco de dados, verificação de estatísticas, gerenciamento de domínios;

8.2 Deverá possuir gerenciador de arquivos web;

8.3 Deverá possuir painel de gerenciamento de DNS.

9.0- MONITORAMENTE DE RECURSOS

9.1 A Contratada deverá oferecer Console de Gestão de fácil utilização e que permita criar e gerenciar os recursos e/ou grupo de recursos relacionados ao serviço de Computação em Nuvem por meio de web browsers.

9.2 A solução ofertada deverá permitir o monitoramento das máquinas virtuais, provendo o monitoramento do ambiente de Computação em Nuvem (serviços e recursos), de forma automatizada e abrangendo a gama de aplicações, bancos de dados, servidores, sistemas operacionais e recursos de comunicação, em tempo real (24x7x365), visando detectar problemas (incidentes), no que tange à sustentação operacional e não a aplicação do Contratante.

9.3 Prover o monitoramento constante em amostras com granularidade mínima de 1 hora (24X7X365) dos serviços e recursos, visando detectar os problemas mais frequentes, informando a CONTRATANTE a ocorrência destes.

9.4 Deverá ser realizada pela Contratada a monitoração da qualidade e nível de utilização da infraestrutura de acesso à Internet, disponibilizada pela solução ofertada pela Contratada, bem como as resoluções em caso de problemas.

9.5 Deverá permitir a visualização dos indicadores de desempenho, falhas do ambiente e características e requisitos operacionais dos recursos gerenciados por meio do painel de apresentação (dashboard) Online (tempo real).

9.6 A solução ofertada deverá prover alarmes para a Console de Gestão de eventos, mostrando quais recursos estiveram acima do threshold, permitindo gerar relatório a partir dos eventos observados.

9.7 Para cada servidor virtual, deverá ser possível o acompanhamento e monitoramento dos seguintes recursos: vCPU, RAM, Tráfego de Rede (In/Out) e Disco.

10.0 – PROVISIONAMENTO DO AMBIENTE CLOUD COMPUTING

10.1 A Contratada será responsável por criar os novos servidores no ambiente de Cloud Computing, com as versões do sistema operacional e dos softwares básicos especificados pela CONTRATANTE.

10.2 Será de responsabilidade da equipe técnica da Contratada, com o apoio da equipe técnica da CONTRATANTE, a migração das aplicações para o novo ambiente, sendo que a CONTRATANTE disponibilizará os recursos necessários, tanto de equipamentos quanto humanos, para apoiar a migração das aplicações.

10.3 Será de responsabilidade da equipe técnica da Contratada o acompanhamento e auxilio a instalação dos softwares básicos e a migração das aplicações da CONTRATANTE, durante a migração a CONTRATANTE disponibilizará o conhecimento da estrutura das aplicações e dos softwares básicos necessários (programas, diretórios, arquivos de configuração e demais informações) para a CONTRATADA afim de otimizar os recursos.

10.4 Após a finalização da migração das aplicações para o ambiente Cloud Computing, a CONTRATANTE disponibilizará uma equipe técnica para fazer os testes de homologação das aplicações migradas afim de atestar a conclusão da migração, sendo que os serviços contratados somente serão considerados como entregues aceitos após a conclusão dos testes.

11.0 **RECURSOS COMPUTACIONAIS**

11.1 Todos os servidores virtuais deverão ser disponibilizados em ambiente de Cloud Computing, em ambiente seguro e separados logicamente de outros clientes, com as seguintes funcionalidades:

11.2 Implementar características de escalabilidade vertical (aumento/diminuição de recursos do mesmo servidor), incluindo flexibilidade de configuração de memória, processador e disco;

11.3 Permitir a criação, pela CONTRATANTE, de pelo menos 1 (uma) imagem (snapshot) dos servidores virtuais sem custo adicional;

11.4 Assegurar a comunicação segura e encriptada entre os próprios servidores e os clientes que farão acesso aos mesmos, através de protocolo seguro HTTPS, ou seja, todos os servidores deverão ser disponibilizados com certificados digitais SSL instalados.

11.5 Os recursos computacionais adicionais, poderão ser utilizados para agregação ou distribuição entre os servidores virtualizados existentes ou para a criação de novos servidores virtuais;

11.6 Deverá ser considerado um pool de recursos computacionais para suprir a demanda das máquinas virtuais do ambiente, os recursos computacionais como

memória e vCPU poderão ser utilizados e divididos entre as máquinas virtuais em nuvem conforme necessidade da CONTRATANTE.

11.7 Cada vCPU deverá fornecer uma velocidade de clock com no mínimo 2 GHz.

12.0 ARMAZENAMENTO

12.1 O armazenamento disponível para as máquinas virtuais deverá considerar o armazenamento dos dados de forma persistente.

12.2 Permitir o gerenciamento de discos virtuais pela CONTRANTANTE através do portal WEB, desde sua criação, exclusão, expansão e anexo as máquinas virtuais no ambiente (VPC).
12.3 O(s) volume(s) criado(s) anexado(s) às máquinas virtuais deverão ser reconhecidos(s) pelo sistema operacional como um dispositivo físico local.

12.4 A solução de armazenamento deverá permitir que a CONTRATANTE defina a política de uso dos discos virtuais das máquinas virtuais em seu ambiente (VPC).

12.5 O armazenamento disponível e não alocado deverá permitir as seguintes características.

12.6 Expansão dos discos existentes das máquinas virtuais no ambiente (VPC).

12.7 Inclusão de novos discos nas máquinas virtuais existentes no ambiente (VPC).

12.8 Criação de novas máquinas virtuais no ambiente (VPC).

12.9 O armazenamento disponível deverá permitir que a CONTRATANTE defina através de políticas pré existentes a seguinte carga de uso:
12.9.1 ALTA PERFORMANCE (SSD)
12.9.2 BAIXA PERFORMANCE (HDD)
12.9.3 OBJECT STORAGE
12.9.3.1 Gerenciamento de quotas e permissões de acesso via interface WEB;
12.9.3.2 Compatível com API S3;
12.10 Os dados deverão estar localizados em território nacional;
12.11 O tráfego de dados (Download e Upload) deve ser ilimitado;

12.12 Os dados deverão estar acessíveis imediatamente sem restrições de acesso.

13.0 CONECTIVIDADE

13.1 Link Ponto a Ponto

13.2 A CONTRATADA deverá prover um link de dados ponto a ponto em fibra óptica garantindo a banda dedicada para upload e download entre o site da CONTRATANTE e o datacenter da CONTRATADA onde se encontram os equipamentos que compõem

a solução de datacenter virtual. Este link será utilizado exclusivamente para os serviços de comunicação entre datacenters;

13.3 O volume de tráfego de dados ofertado deve ser ilimitado, tanto no sentido de download como upload, permitindo a transferência, via funcionalidades de backup e restauração, de volume ilimitado de dados.

13.4 IP's públicos.

13.5 A CONTRATADA deverá disponibilizar endereços IP fixos e públicos (válidos) para uso da CONTRATANTE de tal forma que lhe convir para uso em seu ambiente de produção.

13.6 A fim de garantir que o endereçamento IP utilizado pelo serviço de replicação de backup e recuperação de desastres não sofra constantes alterações e consequentes indisponibilidades, a CONTRATADA deverá possuir seu próprio bloco de endereçamento IP atribuído pelo órgão gestor dos serviços de numeração brasileira (NIC.br). A CONTRATADA deve comprovar que possui a devida alocação do bloco ofertado de seu ASN (Autonomous System Number) através de uma declaração do NIC.br.

13.7 Link de Internet VPC.

13.8 A CONTRATADA deverá prover na VPC (Virtual Private Cloud) um link de internet dedicado para uso e comunicação das instâncias virtuais para a internet.

13.9 O volume de tráfego de dados ofertado deve ser ilimitado, tanto no sentido de download como upload, permitindo a transferência, via funcionalidades de backup e restauração, de volume ilimitado de dados.

14.0 FIREWALL E SEGURANÇA

14.1 Deverá ser fornecido uma solução de segurança com as seguintes características mínimas:

14.1.1 A solução deverá suportar throughput (Taxa de Transferência) de, no mínimo, 15 Gbps com a funcionalidade de firewall habilitada, independentemente do tamanho dos pacotes;

14.1.2 A solução deve suportar Throughput (Taxa de Transferência) de, no mínimo,

14.2 Gbps com as seguintes funcionalidades habilitadas simultaneamente:

14.2.1 Firewall, Controle de Aplicação e Prevenção de Ameaças (Anti-Malware, IPS, Application Control URL Filtering). Esta taxa deve referenciar-se a tráfego multiprotocolo em ambiente de produção, tráfego considerado de mundo real ou tráfego misto, ou seja, aquele que não faz referência apenas a um protocolo e/ou um tamanho de pacote para teste em condição ideal;

14.2.2 Suportar throughput (Taxa de Transferência) de, no mínimo, 1 Gbps de VPN IPsec;

14.2.3 Deverá suportar e incluir licenciamento para, no mínimo, 2.000 Túneis VPN Lan-to-Lan (ou Gateway-to-Gateway) com VPN IPSec;

14.2.4 Deverá suportar e incluir licenciamento para, no mínimo, 32.000 usuários remotos (ou client-to-site) com VPN IPSec;

14.2.5 Deverá suportar e incluir licenciamento para, no mínimo, 500 usuários remotos (ou client-to-site) com VPN SSL;
14.2.6 Suporte a, no mínimo, 3.300.000 (três milhões e trezentos mil) conexões TCP simultâneas;
14.2.7 Suporte a, no mínimo, 140.000 (cento e quarenta mil) novas conexões TCP por segundo;

14.3 A solução deve possuir o licenciamento para, no mínimo, 10 sistemas virtuais lógicos (Contextos), independentes entre si e estar licenciado e/ou ter incluído sem custo adicional pelo menos 5 sistemas;
14.4 A solução deve possuir, no mínimo, 2 (duas) interfaces no padrão 10 GbE;
14.5 A solução deve possuir, no mínimo, 8 (oito) interfaces no padrão 1GbE;
14.6 A solução deve possuir console para configuração e gerenciamento por interface de linha de comando (CLI);
14.7 Todas as portas de comunicação e interfaces devem ser capazes de funcionar simultaneamente oferecendo, cada uma, a plenitude de suas capacidades;
14.8 A solução deve apresentar armazenamento interno do tipo SSD (Solid-State Drive), com no mínimo 480GB;
14.9 A solução deve consistir em plataforma para centralização do gerenciamento, dos logs e geração de relatórios dos equipamentos que compõem a solução de segurança rede (NGFW);
14.10 A solução de gerenciamento, logs e relatoria deve ser do mesmo fabricante da solução de segurança de rede (NGFW);
14.11 As funcionalidades de centralização do gerenciamento, dos logs e geração de relatórios que compõe a plataforma, podem funcionar em múltiplos equipamentos desde que obedeçam a todos os requisitos desta especificação;
14.12 Funcionalidades gerais para cluster de equipamentos.
14.13 Funcionalidades gerais para Solução de Segurança de Perímetro (NGFW)
14.14 Funcionalidades Gerais e Recursos mínimos:
14.15 Os dispositivos de proteção de rede devem possuir suporte a 4094 VLAN Tags 802.1q;
14.16 Deve suportar o protocolo padrão da indústria VXLAN;
14.17 Os dispositivos de proteção de rede devem possuir suporte a agregação de links 802.3ad e LACP;
14.18 Os dispositivos de proteção de rede devem possuir suporte a Policy based routing (PBR) ou policy based forwarding (PBF);
14.19 Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
14.20 Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;
14.21 Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;
14.22 Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames;
14.23 Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;
14.24 Deve suportar NAT dinâmico (Many-to-1);
14.25 Deve suportar NAT dinâmico (Many-to-Many);
14.26 Deve suportar NAT estático (1-to-1);
14.27 Deve suportar NAT estático (Many-to-Many);

14.28 Deve suportar NAT estático bidirecional 1-to-1;
14.29 Deve suportar Tradução de porta (PAT);
14.30 Deve suportar NAT de Origem;
14.31 Deve suportar NAT de Destino;
14.32 Deve suportar NAT de Origem e NAT de Destino simultaneamente;
14.33 Deve poder combinar NAT de origem e NAT de destino na mesma politica
14.34 Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
14.35 Deve suportar NAT64 e NAT46;
14.36 Deve implementar Equal-cost Multipath ECMP.
14.37 Deve suportar nativamente ou integração com soluções de SD-WAN;
14.38 Deve permitir monitorar via SNMP falhas de hardware, uso de recursos por número elevado de sessões, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;
14.39 Deve suportar o padrão do protocolo 'syslog' para geração e armazenamento dos logs usando o formato Common Event Format (CEF);
14.40 Deve suportar o armazenamento de logs em tempo real tanto para o ambiente de nuvem quanto o ambiente local (on-premise);
14.41 Enviar log para sistemas de monitoração externos, simultaneamente;
14.42 Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;
14.43 Implementar Proteção anti-spoofing;
14.44 Deve identificar e bloquear comunicação com redes botnets;
14.45 Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos de usuários, permitindo que os mesmos sejam utilizados, ao menos, no acesso administrativo dos equipamentos, autenticação VPN e políticas de firewall, dando assim maior granularidade e controle.
14.46 Deve possuir integração com LDAP para identificação de usuários e grupos de usuários, permitindo que os mesmos sejam utilizados, ao menos, no acesso administrativo dos equipamentos, autenticação VPN e políticas de firewall, dando assim maior granularidade e controle.
14.47 Deve possuir integração com Radius para identificação de usuários e grupos de usuários, permitindo que os mesmos sejam utilizados, ao menos, no acesso administrativo dos equipamentos, autenticação VPN e políticas de firewall, dando assim maior granularidade e controle.
14.48 Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;
14.49 Deve possuir funcionalidade de Single Sign-On. Essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso como, mas não limitado à utilização de sistemas virtuais, segmentos de rede, etc;
14.50 Deve possuir funcionalidade de Captive Portal local para autenticação de usuários que solicitem navegação através de políticas de firewall que façam o controle por usuários/grupos de usuários. Deve permitir também a customização deste Portal.
14.51 Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo

visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

14.52 Deve permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso a internet e gerenciamento da solução;

14.53 Deve prover nativamente, no mínimo, licenciamento de uso de um (1) token, possibilitando autenticação de duplo fator para usuário administrador, acesso VPN e etc;

14.54 Para IPv4, deve suportar roteamento estático e dinâmico (RIP, BGP e OSPF);

14.55 Para IPv6, deve suportar roteamento estático e dinâmico (OSPF e BGP);

14.56 Suportar OSPF graceful restart;

14.57 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);

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

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

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

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

14.62 Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo transparente;

14.63 Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3;

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

14.65 A configuração em alta disponibilidade deve sincronizar: Sessões;

14.66 A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede;

14.67 A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs;

14.68 A configuração em alta disponibilidade deve sincronizar: Tabelas FIB;

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

14.70 Deve possuir suporte a criação de sistemas virtuais lógicos (contexto) no mesmo appliance;

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

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

14.73 Controle, inspeção e decriptografia de SSL para tráfego de entrada (Inbound) e Saída (Outbound), sendo que deve suportar o controle dos certificados

individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);

14.74 Deverá suportar controles por zona de segurança;

14.75 Controles de políticas por porta e protocolo;

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

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

14.78 Firewall deve ser capaz de aplicar a inspeção de camada 7 (Application Control e Webfiltering no mínimo) diretamente às políticas de segurança versus via perfis;

14.79 Além dos endereços e serviços de destino, objetos de serviços de Internet devem poder ser adicionados diretamente às políticas de firewall;

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

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

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

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

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

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

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

14.87 O gerenciamento da solução deve suportar acesso via interface WEB (HTTPS) e interface de linha de comando (SSH), incluindo, mas não limitado à, exportar configuração dos sistemas virtuais lógicos por ambas interfaces;

14.88 Controle de Aplicações.

14.89 Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

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

14.91 Reconhecer pelo menos 1500 aplicações diferentes, incluindo, mas não limitado a: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

14.92 Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos,

ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;

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

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

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

14.96 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;

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

14.98 Identificar o uso de táticas evasivas via comunicações criptografadas;

14.99 Atualizar a base de assinaturas de aplicações automaticamente;

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

14.101 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;

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

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

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

14.105 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;

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

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

14.108 Deve alertar o usuário quando uma aplicação for bloqueada;

14.109 Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;
14.110 Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;
14.111 Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo;
14.112 Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;
14.113 Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);
14.114 Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação;
14.115 Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;
14.116 Prevenção de Ameaças.
14.117 Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;
14.118 Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
14.119 As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;
14.120 Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;
14.121 Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset;
14.122 As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;
14.123 Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
14.124 Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;
14.125 Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
14.126 Deve permitir o bloqueio de vulnerabilidades;
14.127 Deve permitir o bloqueio de exploits conhecidos;
14.128 Deve incluir proteção contra-ataques de negação de serviços;
14.129 Deverá possuir os seguintes mecanismos de inspeção de IPS:
14.130 Análise de padrões de estado de conexões;
14.131 Análise de decodificação de protocolo;

14.132 Análise para detecção de anomalias de protocolo;
14.133 Análise heurística;
14.134 IP Defragmentation;
14.135 Remontagem de pacotes de TCP;
14.136 Bloqueio de pacotes malformados;
14.137 Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood;
14.138 Detectar e bloquear a origem de portscans;
14.139 Bloquear ataques efetuados por worms conhecidos;
14.140 Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
14.141 Possuir assinaturas para bloqueio de ataques de buffer overflow;
14.142 Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica;
14.143 Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;
14.144 Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
14.145 Identificar e bloquear comunicação com botnets;
14.146 Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
14.147 Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;
14.148 Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;
14.149 Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
14.150 Os eventos devem identificar o país de onde partiu a ameaça;
14.151 Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
14.152 Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;
14.153 Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseada em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança;
14.154 Fornecer proteção contra-ataques de dia zero por meio de estreita integração com os componentes Sandbox (on-premise ou nuvem);
14.155 Filtro de URL
14.156 Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

14.157 Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
14.158 Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;
14.159 Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
14.160 Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;
14.161 Possuir pelo menos 50 categorias de URLs;
14.162 Deve possuir a função de exclusão de URLs do bloqueio, por categoria;
14.163 Permitir a customização de página de bloqueio;
14.164 Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site);
14.165 Além do Explicit Web Proxy, suportar proxy Web transparente;
14.166 QoS e Traffic Shaping.
14.167 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 máxima largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;
14.168 Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;
14.169 Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;
14.170 Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo;
14.171 Suportar a criação de políticas de QoS e Traffic Shaping por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube;
14.172 Suportar a criação de políticas de QoS e Traffic Shaping por porta;
14.173 Possibilitar a definição de tráfego com banda garantida;
14.174 Possibilitar a definição de tráfego com banda máxima;
14.175 Possibilitar a definição de fila de prioridade;
14.176 Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;
14.177 Suportar marcação de pacotes Diffserv, inclusive por aplicação;
14.178 Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;
14.179 Deve suportar QOS (traffic-shapping), em interface agregadas ou redundantes;
14.180 VPN
14.181 Suportar VPN Site-to-Site e Cliente-To-Site;
14.182 Suportar IPSec VPN e VPN SSL de forma simultânea;
14.183 A VPN IPSEC deve suportar 3DES;
14.184 A VPN IPSEC deve suportar Autenticação MD5 e SHA-1;
14.185 A VPN IPSEC deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;

14.186 A VPN IPSEC deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
14.187 A VPN IPSEC deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);
14.188 A VPN IPSEC deve suportar Autenticação via certificado IKE PKI;
14.189 Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de throubleshooting;
14.190 A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
14.191 A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
14.192 Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
14.193 Atribuição de DNS nos clientes remotos de VPN;
14.194 Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
14.195 Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;
14.196 Suportar leitura e verificação de CRL (certificate revocation list);
14.197 Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
14.198 Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas:
14.199 Antes do usuário autenticar na estação;
14.200 Após autenticação do usuário na estação;
14.201 Sob demanda do usuário;
14.202 Deverá manter uma conexão segura com o portal durante a sessão;
14.203 O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bits), Windows 8 (32 e 64 bits), Windows 10 (32 e 64 bits) e Mac OS X (v10.10 ou superior).

15.0 SOLUÇÃO DE DETECÇÃO E RESPOSTA DE ENDPOINT

15.1 Requisitos gerais da solução:
15.1 Solução de proteção contra ameaças avançadas, com funcionalidades de detecção, bloqueio, investigação e resposta a incidentes, incluindo console Web ou console gráfica do próprio fabricante para administração da solução e centralização de eventos.
15.2 Fornecimento da console de gerência, incluindo implantação dos agentes, documentação da arquitetura da solução e repasse de conhecimento.
15.3 A Solução de gerência deve ser fornecida pela licitante vencedora e contemplar todos os softwares e respectivas licenças necessárias ou adicionais para a instalação, configuração e funcionamento da solução de proteção.
15.4 A solução de proteção deve ser oferecida na última versão disponibilizada pelo fabricante.

15.5 Na data da proposta, nenhum dos softwares componentes da solução de proteção ofertados poderão estar listados pelo fabricante com data definida para fim de suporte (“end of support”) ou fim de vendas (“end of sale”).

15.6 Requisitos e funcionalidades técnicos da solução:

15.7 A solução de proteção deve ser capaz de detectar e bloquear em tempo real ameaças conhecidas e desconhecidas (zeroday), ataques file-less, ameaças persistentes avançadas (APTs), ransomwares, exploits e outros comportamentos maliciosos, sem depender exclusivamente de base de assinaturas ou heurísticas.

15.8 A solução de proteção deverá possuir funcionalidades especificas para prevenção contra a ação de ransomwares com capacidade de restauração dos arquivos comprometidos.

15.9 A solução de proteção deve ter a funcionalidade específica de impedir as técnicas de manipulação e randomização de memória impossibilitando a exploração de vulnerabilidades em aplicações.

15.10 A solução de proteção deve ter a capacidade de impedir os ataques direcionados mesmo que utilizando as vulnerabilidades de dia zero, mitigando no mínimo os conhecidos comportamentos de exploração de vulnerabilidades.

15.11 Efetuar a análise baseada em técnicas de machine learning, inteligência artificial e threat intelligence, permitindo a proteção contra ataques que explorem vulnerabilidades, mesmo que ainda não existam patches de correção.

15.12 Realizar análise de comportamento com base nas táticas, técnicas e procedimentos (TTPs) listados no framework MITRE ATT&CK.

15.13 A análise dos artefatos deve ocorrer em pré-execução, ou seja, antes de serem executados no sistema operacional, evitando que a máquina seja infectada.

15.14 Detectar e bloquear ameaças que utilizem técnicas de ofuscação e sequestro de DLL.

15.15 Detectar e bloquear técnicas de evasão, incluindo process injection e uso de executáveis legítimos do Windows para rodar scripts e ações maliciosas.

15.16 Reconhecer padrões e bloquear comportamentos potencialmente maliciosos ou o possuir mecanismos automáticos preventivos ou corretivos que sejam capazes de inibir as ações maliciosas resultantes de pelo menos 5(cinco) das ações listadas abaixo:

15.17 Rodar a partir diretórios incomuns (ex: diretório de dados, temp e lixeira);

15.18 Executar elevações de privilégio inesperadas;

15.19 Tentar se passar por processos do Windows;

15.20 Estabelecer conexões de rede suspeitas (call back ou command & control);

15.21 Uso suspeito do PSEXEC;

15.22 Invocação maliciosa através do Rundll;

15.23 Exploração ou modificação do arquivo hosts;

15.24 Tentativa de invocação de Remote Shell.

15.25 Identificar e bloquear alterações suspeitas em chaves de registro e tarefas agendadas na máquina.

15.26 Proteger contra macros maliciosas, bem como scripts e comandos Powershell maliciosos.

15.27 Bloquear exploits e payloads suspeitos do Metasploit.

15.28 As análises poderão ser complementadas utilizando recursos em nuvem da solução, sem custos adicionais, onde será permitido apenas o envio de metadados dos artefatos sob análise, sem submissão do artefato em si ou seu conteúdo à nuvem.

15.29 O agente da solução deve realizar suas análises e bloqueios nas estações mesmo quando estiver sem conectividade com os servidores da solução e sem acesso à Internet.

15.30 O agente da solução deve possuir proteção contra desinstalação e/ou desativação dos seus componentes, serviços e processos de forma não autorizada.

15.31 Deve ser possível realizar a configuração de proxy no agente ou obter as configurações de proxy definidas no próprio sistema operacional.

15.32 Deve ser possível exibir ou inibir alertas ao usuário em caso de detecção de alguma ameaça, conforme definição do administrador.

15.33 Deve ser possível definir as seguintes ações de resposta quando uma ameaça ou comportamento malicioso for detectado:

15.34 Ignorar;

15.35 Registrar em log;

15.36 Alertar;

15.37 Bloquear;

15.38 Remover ou quarentenar;

15.39 Isolar a máquina, de maneira que ela perca a comunicação com a rede ou se comunique apenas com os servidores da solução ou com servidores e serviços definidos na política de isolamento.

I - O agente deve ter a capacidade de fazer o isolamento da máquina por si só, sem precisar de nenhuma integração com outros softwares ou dispositivos de rede para isso.

II - Deve ser possível ao administrador efetuar a liberação da máquina do isolamento via console de gerência ou fornecer uma chave para realizar a liberação.

15.40 A solução deve possuir funcionalidade de EDR e análise forense, provendo uma visão completa do fluxo do ataque e informações detalhadas sobre os comportamentos detectados, de forma a auxiliar e agilizar as ações de remediação.

15.41 A console deve oferecer uma linha do tempo gráfica, contendo toda a sequência de eventos que ocorreram durante a execução do malware, sendo possível ainda expandir os detalhes de cada informação.

15.42 Devem ser coletadas as atividades de todos artefatos analisados, contendo informações sobre interação com outros processos, arquivos e chaves de registro acessadas/modificadas, conexões de rede realizadas, dentre outras. Deve ser possível gerar relatório dessas informações.

15.43 A solução deve correlacionar os eventos de detecção e bloqueio de malwares, permitindo a visualização de relatório com todas as fases do ataque.

15.44 Deve ser possível configurar regras de exclusão (whitelists) determinando quais arquivos, diretórios, processos ou aplicativos não devem ser analisados pela solução.

15.45 A solução deve ser capaz de remover de forma ágil e eficaz outras soluções de antivírus instaladas nos equipamentos do CONTRATANTE ou possuir mecanismos que possibilitem essa remoção.

15.46 A Solução deve ter a capacidade de implementar, no mínimo, cinco das seguintes funcionalidades:

15.46.1.1 Reputação de Arquivos (Com ou sem acesso à internet no endpoint);

15.46.1.2 IPS de Próxima Geração;

15.46.1.3 Proteção de Navegadores;

15.46.1.4 Aprendizado de Máquinas;

15.46.1.5 Análise Comportamental;

15.46.1.6 Mitigação da Exploração de Memória;

15.46.1.7 Controle e isolamento de Aplicações;

15.46.1.8 Controle de Dispositivos;

15.46.1.9 Emulação para Malware;

15.46.1.10 Proteção ao ambiente de Active Directory;

15.46.1.11 Mitigação de Exploração de Vulnerabilidades em aplicações conhecidas.

15.47 Deve ter a capacidade de implementar a funcionalidade de “Machine Learning” utilizando como fonte de aprendizado a rede de inteligência do fabricante, correlacionando no mínimo as seguintes técnicas de proteção com os vetores de ataques, identificando não somente os aspectos maliciosos.

15.48 De forma opcional ou não obrigatória a solução poderá a solução poderá ser capaz de distribuir iscas no ambiente com o objetivo de detectar e interromper tentativas de infiltração, através da implementação de pelo menos:

15.49 Criação de entradas falsas de cache, como Cache de DNS afim de enganar um invasor e identificar ações maliciosas no ambiente;

15.50 Deve possibilitar a criação de arquivos falsos nas máquinas dos usuários;

15.51 Deve possibilitar a criação e distribuição de senhas falsas nos sistemas afim de identificar invasores no ambiente;

15.52 Criação de compartilhamentos de rede falsos em desktops;

15.53 Deve ser capaz de enviar alertas quando as “Iscas” falsas são acionadas e/ou modificadas;

15.54 Deve ter a capacidade de revelar tentativas de ataques dentro da rede interna;

15.55 De forma opcional ou não obrigatória, a solução poderá ter a capacidade de impedir os ataques direcionados mesmo que utilizando as vulnerabilidades de dia zero, mitigando no mínimo um dos conhecidos comportamentos de exploração de vulnerabilidades:

15.55.1.1 SEHOP - Structured Exception Handler Overwrite Protection;

15.55.1.2 Heap Spray (Exploits que iniciam através do HEAP);

15.55.1.3 Java Exploit Protection;

15.56 De forma opcional ou não obrigatória, a solução poderá se capaz de:

15.56.1.1 A solução poderá ter a capacidade de bloquear exploits que trabalham em nível de “shell code”.

15.56.1.2 A solução poderá ter proteção contra técnicas de reconhecimento do domínio, sendo capaz de detectar um invasor que utilize técnicas de movimentação lateral ou roubo de credenciais válidas;

15.56.1.3 A solução poderá proteger contra intrusões por processo, usuário e terminal;

15.56.1.4 A solução poderá ser capaz de identificar vulnerabilidades, erros de configurações e possíveis Backdoors presentes no Active Directory;

15.56.1.5 A solução poderá ser capaz de proteger alterações no Active Directory sem a necessidade de instalação de agentes ou componentes adicionais nas estações de trabalho;

15.56.1.6 A solução poder ser capaz de detectar e proteger roubos de credenciais no ambiente que utilizem a técnica Pass-the-Hash e Pass-the-Ticket;

15.56.2 Instalação dos agentes:

15.56.2.1 A solução deve ser compatível com as versões de Sistema Operacionais:

15.56.2.2 Para computadores de usuários finais (estações: desktop, workstation e notebooks):

I - Microsoft Windows 7 (32-64bit) e superior em todas as suas distribuições (home, starter, professional, ultimate e enterprise).

15.56.2.3 Para servidores de rede físicos ou virtuais

I - Microsoft Windows Server 2012 (64bit) e superior.

II - Ser suportado em sistemas operacionais linux, tais como Ubuntu, CentOS, Debian, Oracle Linux, Red Hat Enterprise, SUSE Linux Enterprise (32-64bit).

III - O agente deve suportar sua instalação em Sistemas Operacionais virtualizados em ambiente Vmware.

15.56.3 O agente não deve impactar a performance das estações e servidores, gerando baixo consumo de CPU, memória, disco e rede.

15.56.4 Deve ser possível a instalação e atualização dos agentes de forma manual ou remota, com suporte à distribuição do agente por ferramentas de terceiros, incluindo o System Center Configuration Manager (SCCM) da Microsoft.

15.56.5 A instalação deve ser feita de forma silenciosa, sem interação com o usuário e sem necessidade de acesso à Internet.

15.56.6 Deve ser possível permitir a desinstalação ou alteração da configuração do agente mediante requisição de senha ou token gerados pela console de gerência.

15.56.7 Deve ser possível impedir alterações na configuração do agente por usuários ou processos não autorizados.

15.56.8 Toda a solução deverá funcionar com agente único na estação de trabalho e servidores físicos e/ou virtuais a fim de diminuir o impacto ao usuário final;

15.56.9 Para equipamentos que não podem se conectar à internet, devido a regras de negócio e/ou restrições impostas pelo próprio equipamento, a solução deve possibilitar a instalação de um componente on-premises, para que tais equipamentos possam ser gerenciados, atualizados e protegidos.

15.56.10 Toda a solução deverá funcionar com agente nas estações de trabalho e servidores físicos e/ou virtuais a fim de diminuir o impacto ao usuário final. Será permitido agentes múltiplos para o atendimento deste requisito.

15.57 Console de Gerência:

15.57.1 A solução deve oferecer console de gerência via protocolo web seguro ou console do próprio fabricante.

15.57.2 Caso a console seja Web, deve ser compatível com pelo menos dois dos seguintes navegadores: Microsoft Edge 41 ou superior; Google Chrome 70 ou superior; Mozilla Firefox 60 ou superior.

15.57.3 A console deve funcionar plenamente sem requerer a instalação de plug-ins, drivers, java e flash player.

15.57.4 Permitir no mínimo 5(cinco) acessos simultâneos.

15.57.5 A console e os agentes da solução devem possuir interface em português ou inglês.

15.57.6 Toda comunicação da solução deve ocorrer de forma criptografada usando protocolo seguro conforme padrão aceito pela indústria.

15.57.7 Permitir a configuração de perfis com permissões agrupadas que possam ser vinculados às contas de acesso à solução, para possibilitar a segregação de funções.

15.57.8 Suporte à criação de usuários, permitindo senhas de no mínimo 8 caracteres de 3 ou mais tipos, como: letras maiúsculas, letras minúsculas, dígitos numéricos e caracteres especiais.

15.57.9 A solução de console de gerência, deve ser possível configurar autenticação em múltiplos fatores.

15.57.10 Permitir ao administrador criar diferentes políticas de segurança e aplicá-las a diferentes grupos de máquinas de acordo com seus atributos.

15.57.11 Registro em log de todas as ações de detecção e bloqueio de malware e comportamento malicioso.

15.57.12 Deve ser possível efetuar busca no log pelo IP de Origem, IP de destino, nome da máquina, nome do processo, arquivo e chave de registro.

15.57.13 Deve ser possível efetuar o “drill down” das consultas realizadas a fim de avaliação mais detalhada das ocorrências.

15.57.14 A partir dos eventos exibidos na console, deve ser possível tomar ações como quarentenar a máquina, adicionar o artefato a blacklist ou lista de exclusão (whitelist), dentre outras.

15.57.15 Permitir a geração de relatórios, consulta em log ou dashboard para visualizar no mínimo as informações abaixo:

15.57.15.1 Eventos de ameaças;

15.57.15.2 Eventos de comportamentos suspeitos;

15.57.15.3 Malwares detectados e bloqueados;

15.57.15.4 Computadores infectados.

15.57.16 Deve ser possível exportar os relatórios para o formato CSV ou PDF.

15.57.17 Permitir a configuração de alertas em tempo real de ameaças com envio de e-mail a usuários pré-definidos.

15.57.18 A solução deve manter log de auditoria com registro das configurações realizadas por qualquer usuário ou administrador do sistema.

15.57.19 Permitir a visualização do inventário das máquinas que possuem o agente instalado, contendo no mínimo as seguintes informações:

15.57.19.1 Nome da máquina;

15.57.19.2 Endereço IP;

15.57.19.3 Versão do sistema operacional (incluindo a versão do Service Pack);
15.57.19.4 Versão do agente;
15.57.19.5 Política aplicada.
15.57.20 A partir do console de gerenciamento da solução, deve ser possível identificar o equipamento que está sofrendo ataques e comandar o agente de endpoint para que aquele determinado equipamento seja movido para uma área de quarentena.
15.58 Monitoramento Assistido:
15.58.1 Este serviço tem por objetivo operacionalizar as atividades de monitoração, detecção e resposta a incidentes de segurança, tratando os incidentes de forma coordenada, organizada e eficaz conforme necessidade do CONTRATANTE.
15.58.2 Deverá ser realizado de forma remota, externamente à CONTRATANTE, em dependências sob responsabilidade da CONTRATADA;
15.58.3 Deverá atuar na resposta à incidentes e ser realizado em língua portuguesa com monitoração em regime 12x5 (doze horas e cinco dias por semana);
15.58.4 Este serviço deverá ser prestado por equipe própria da CONTRATADA ou pela fabricante da solução;
15.58.5 Este serviço deverá interagir com o CONTRATANTE via sistema de gestão e orquestração de incidentes de segurança da informação, sistemas disponibilizados pelo CONTRATANTE, ligação telefônica e correio eletrônico;
15.58.6 As solicitações e respostas de informações adicionais sobre os incidentes, como logs e evidências, devem ser anexadas ao tíquete registrado na ferramenta;
15.58.7 A CONTRATADA deverá garantir a prestação de serviço com disponibilidade mensal de 97% no regime de monitoração 12x5(doze horas e cinco dias por semana). Em casos de indisponibilidade, esta não deverá atingir períodos superiores a 4 horas consecutivas;
15.58.8 A CONTRATADA deverá apresentar plano de continuidade para a prestação deste serviço; será considerado incidente de segurança qualquer ação que vise comprometer a integridade, a confidencialidade das informações ou a disponibilidade dos serviços de tecnologia da informação do CONTRATANTE;
15.58.9 O serviço deverá atender os seguintes requisitos:
15.58.9.1 Monitorar ferramentas de segurança;
15.58.9.2 Monitorar o armazenamento dos logs de eventos e e incidentes de segurança;
15.58.9.3 Monitorar sistema de gestão, orquestração e automação de incidentes de segurança da informação, controlando eventos, alertas, painéis e incidentes;
15.58.9.4 Iniciar tratamento de incidentes em até 10 min;
15.58.9.5 Realizar triagem, classificação e categorização de eventos de segurança da informação;
15.58.9.6 Realizar triagem, classificação e categorização de incidentes de segurança da informação, também identificando casos de falso positivo;

15.58.9.7 Identificar incidentes de segurança da informação; Registrar, escalar e notificar incidentes de segurança da informação;

15.58.9.8 Registrar, escalar e notificar incidentes de segurança da informação;

15.58.9.9 Realizar coleta de dados, informações e evidências para inclusão no registro do evento ou incidente;

15.58.9.10 Executar ações de mitigação, contenção, diagnóstico, resolução e outros procedimentos necessários para tratamento de incidentes de segurança da informação, solicitados pelo CONTRATANTE;

15.58.9.11 Interagir com a ETIR e demais equipes da CONTRATANTE, podendo realizar ações em conjunto;

15.58.9.12 Registrar e documentar ações e procedimentos realizados;

15.58.9.13 Emitir relatório semanal estatístico das operações realizadas;

15.58.9.14 Emitir relatórios conforme necessidade, periodicidade e padrões estabelecidos pela CONTRATANTE;

15.58.9.15 Apoiar na definição, documentação e manutenção de Política de Gerenciamento de Eventos, contendo diretrizes para geração, coleta, retenção e classificação de eventos e monitoramento de logs;

15.58.9.16 Apoiar na definição, documentação e manutenção de estratégia de visibilidade de ameaças, devendo abordar: rotinas, periodicidade, métodos para identificação de novos casos de uso, utilização de fontes de visibilidade e inteligência de ameaças;

15.58.9.17 Apoiar na definição, documentação e manutenção da normas, diretrizes e Política de Segurança da Informação e Comunicação da CONTRATANTE , visando refletir as definições instituídas por esses serviços de monitoramento;

15.58.9.18 Apoiar na Análise de Requisitos Regulatórios, Contratuais e Legais que se referem à segurança da informação e aplicáveis a CONTRATANTE;

15.58.9.19 Apoiar na avaliação de Helth Check das soluções de segurança do CONTRATANTE, validando o mesmo e apresentando recomendações;

15.58.9.20 Apoiar na definição de ajustes e configuração de ferramentas de Segurança, apresentando recomendações a serem realizadas pela equipe técnica da CONTRATANTE.

15.58.9.21 Apoiar na realização de Avaliação da Utilização de ferramentas de Segurança, observando: regras, alertas, painéis, fontes de dados, automatizações, integrações, relatórios e dimensionamento; apresentar recomendações e indicações de melhores práticas no que se refere à monitoração, análises, casos de uso de forma eficiente; e participar da implementação das recomendações quando necessário;

15.58.9.22 Realizar Avaliação de Performance, com base nas métricas e indicadores definidos;

15.58.9.23 Gerar subsídios e recomendações para elaboração de conteúdo para divulgação de definições e orientações de segurança da informação e cibernética, a serem utilizados em ações de cultura e conscientização;

15.58.9.24 Apoiar na definição, documentação e manutenção de linha base (baseline) de comportamento para monitoração do ambiente de TI da CONTRATANTE, ajustando métricas e limiares de detecção, com o objetivo de reduzir o número de falsos positivos e aumentar a precisão da detecção;

15.58.9.25 Interagir com o sistema do CONTRATANTE para o processo de Gestão de Mudanças, Gestão de Incidentes de TI Gestão de requisições.

15.59 Instalação da solução e repasse de conhecimento.

15.59.1 A disponibilização da solução de gerência e a instalação e configuração dos agentes da solução deverá ser realizada pela Contratada ou pelo fabricante da solução presencialmente na Sede do CONTRATANTE, em dias úteis, no período de 8h00 às 12h00 e de 14h00 às 18h00.

15.59.2 A disponibilização da solução de gerência e a instalação e configuração dos agentes da solução deve ser executada por pessoal especializado, qualificado e com certificação na solução.

15.59.3 A disponibilização da solução de gerência e a instalação e configuração dos agentes da solução deverá ser concluída em 30 (trinta) dias corridos para a sede do CONTRATANTE e em até 60 (sessenta) dias corridos para as unidades nas demais localidades, contados a partir da assinatura da Ordem de Serviço

15.59.4 A instalação compreenderá:

15.59.4.1 Implantação de todos os componentes em sua última versão estável.

15.59.4.2 Configuração completa da solução, incluindo o apoio na definição de políticas e melhores práticas de segurança.

15.59.4.3 Configuração de dashboards, relatórios e alertas, de maneira coordenada com o CONTRATANTE.

15.59.4.4 Customização dos pacotes de instalação dos agentes e distribuição a todas as estações do CONTRATANTE, inclusive nas unidades descentralizadas nos estados da federação.

15.59.4.5 Instrução da equipe técnica do CONTRATANTE para a integração da a solução com ferramenta SIEM ou envio para servidor de registro de logs (Syslog).

15.59.4.6 Documentação da topologia da solução, relatório das atividades e configurações realizadas.

15.59.4.7 Apresentação da solução configurada e implantada.

15.59.4.8 Deverá ser realizado repasse de conhecimento da solução de gerência para 1 grupo de até 4 pessoas, oferecido por técnico certificado na solução.

15.59.4.9 No repasse de conhecimento deve ser utilizado material em português.

15.59.4.10 Não é necessário que o repasse seja feito para um grupo fechado do CONTRATANTE e o mesmo pode ser realizado de forma remota.

15.59.4.11 O repasse de conhecimento deve conter parte teórica e prática, incluindo tópicos sobre a instalação, uso, configuração, resolução de problemas da solução, análise de relatórios, respostas a incidentes, introdução ao Framework MITRE ATT&CK e outros.

15.59.4.12 As datas dos repasses de conhecimento devem ser previamente combinadas com o CONTRATANTE.

15.59.4.13 Todas as despesas do repasse de conhecimento devem correr por conta da Contratada.

15.59.4.14 Caso o repasse de conhecimento seja ministrado presencialmente e fora de São Paulo, deverão estar incluídas as despesas com passagens aéreas, hospedagem e traslado entre aeroporto, hotel e local de treinamento.

15.59.4.15 O CONTRATANTE se reserva o direito de solicitar novo repasse caso aquele oferecido venha a ser questionado com relação à qualidade ou à carga horária. Neste caso, eventuais despesas de locomoção e estadia serão ressarcidas ao CONTRATANTE pela Contratada.

15.59.4.16 Deverá ser disponibilizado formulário de avaliação (online ou impresso) e a média das notas deverá ser superior a 80%. Caso a média das notas seja inferior a 80% a contratada deverá ministrar novo repasse.

15.59.4.17 A fornecedora e/ou fabricante da solução poderá, a qualquer tempo, durante a vigência do contrato, sem ônus extra para o CONTRATANTE, oferecer participação em seminários, conferências, visitas técnicas, eventos educacionais e treinamentos não previstos nesta especificação técnica, desde que relacionados ao objeto contratado.

16.0 BACKUP

16.1 A Contratada deverá disponibilizar serviços que permitam realizar backup e restore rápidos dos servidores virtuais com retenção em storage. As políticas de backup deverão ser configuradas conforme necessidades de tempo de retenção e periodicidade que o cliente desejar.

16.2 A fim de manter a integridade das informações e dos dados armazenados, a solução de Cloud Computing deverá garantir o backup das instâncias baseado nas características técnicas mínimas de uma solução de Backup conforme listadas abaixo:

16.3 Os Backups poderão ser completos do tipo imagem dos volumes, sendo executados de forma automática (agendada) ou através de comandos manuais. Os backups das bases de dados de aplicações de execução contínua deverão ser realizados sem interrupção dos serviços (backup on line), e deverá ser utilizada uma rede de alta velocidade evitando que o tráfego de backup afete a operação normal dos sistemas.

16.4 Para realização da funcionalidade Backup e Restore, a Contratada deverá disponibilizar solução completa, com todos os recursos necessários para executar as rotinas da CONTRATANTE, sendo que a solução de Backup deverá estar preparada para geração automática de imagens das máquinas virtuais /Snapshots, gravados em ambiente de armazenamento em nuvem da Contratada, que devem ser acessíveis aos recursos de Computação em Nuvem disponibilizados para a CONTRATANTE.

16.5 As políticas de backup poderão ser ajustadas para uma maior quantidade de backups diários e/ou retenção no repositório de armazenamento a ser disponibilizado para as cópias de segurança das instâncias contratadas respeitando a capacidade contratada sem considerar eventuais ganhos com compressão e deduplicação.

16.6 Não serão permitidas soluções de backup de dados baseados em cópias realizadas de forma manual, nem baseadas em scripts automatizados, devendo ser utilizado um software de uso específico e dedicado para backup.

16.7 Não serão permitidas soluções de backup de dados baseados em sistemas operacionais gratuitos ou de código aberto.

16.8 A solução proposta deverá dispor de software profissional para gerência e execução de backup e restauração de dados em nuvem, com garantia de atualizações e expansões durante o período do contrato sem ônus financeiro para a CONTRATANTE.

16.9 Deverá ter a capacidade de testar a consistência do backup e replicação (Sistema Operacional, aplicação, máquina virtual), emitindo relatório de auditoria para garantir a capacidade de recuperação, sempre que solicitado.

16.10 Deverá incluir ferramentas de recuperação, mediante as quais os administradores dos servidores de serviços de diretório Microsoft Active Directory, possam recuperar objetos individuais como usuários, grupos, contas, Objetos de Política de Grupo (GPOs), registros do Microsoft DNS integrados ao Active Directory, sem a necessidade de recuperar os arquivos das máquinas virtuais como um todo ou reiniciar a mesma.

16.11 Deverá incluir ferramentas de recuperação, mediante as quais os administradores dos servidores de banco de dados Microsoft SQL Server, possam recuperar objetos individuais, tais como bases, tabelas, registros, entre outros, sem a necessidade de recuperar os arquivos das máquinas virtuais como um todo ou reiniciar a mesma.

16.12 Deverá ter a capacidade de realizar proteção (backup) incremental e replicação diferencial, aproveitando a tecnologia de “rastreio de blocos modificados” (CBT – changed block tracking), reduzindo ao mínimo necessário, o tempo de backup e possibilitando proteção (backup e replicação).

16.13 Deverá oferecer a possibilidade de armazenar backups de forma criptografada, bem como garantir o trânsito de informações sob esse esquema a partir do arquivo de backup, sem exigir criptografia do sistema de armazenamento.

16.14 Deverá prover acesso ao conteúdo das máquinas virtuais, para recuperação de arquivos, pastas ou anexos, diretamente do ambiente protegido (repositório de backup) ou replicados, sem a necessidade de recuperar completamente o backup e inicializar.

16.15 Deverá assegurar a consistência de aplicações transacionais de forma automática por meio da integração com Microsoft VSS, dentro de sistemas operacionais Windows.

16.16 Deverá permitir criar uma cópia da máquina virtual de produção para criação de ambiente de homologação, testes ou desenvolvimento, em qualquer estado anterior, para a resolução de problemas, provas de procedimentos ou capacitação.

16.17 Deverá permitir a recuperação de mais de uma máquina virtual e pontos de restauração simultâneo, permitindo assim, ter múltiplos pontos de tempo de uma ou mais máquinas virtuais.

16.18 O software deverá possuir painel de gerenciamento de ambiente de backup (dashboard) com suporte a visualização de todas as rotinas de backup, com opção de gerar relatórios online e enviar estes relatórios aos endereços designados pela CONTRATATANTE.

16.19 O software deverá permitir a execução de backup de arquivos abertos em Windows, mesmo que estejam sendo alterados durante a operação e backup, sem necessidade de suspender a utilização de aplicações pelos usuários nem a conexão

da rede. A cópia do arquivo salvo deverá ser idêntica ao arquivo residente em disco, quando do início da operação de backup.

16.20 A replicação dos dados deve ter funcionalidade nativa do software de backup, não podendo usar sistemas externos (appliances).

16.21 O sistema deve prover quantidade ilimitada de restaurações, conforme as solicitações da CONTRATANTE, durante a vigência deste Contrato.

16.22 O console central de administração dos backups deve ser via WEB e acessível via navegador utilizando protocolos HTTPS integrado a solução de Console de gestão do ambiente Cloud Computing (ITEM 7).

17.0 RECUPERAÇÃO DE DESASTRES

17.1 Deverá fornecer solução de recuperação de desastres, baseado em replicação automatizada entre os datacenters da CONTRATADA.

17.2 A solução deverá ser integrada a mesma solução de gerenciamento do ambiente de máquinas virtuais, não sendo permitido utilização de software externos.

17.3 Garantir a proteção e replicação automatizada de máquinas virtuais.

17.4 Permitir a criação de planos de recuperação personalizáveis.

17.5 Deverá possuir funcionalidade de testes de plano de recuperação sem impacto.

17.6 Permitir a recuperação orquestrada quando necessário.

17.7 Permitir a replicação e recuperação para outro ambiente de Cloud Computing.

17.8 Permitir a utilização do ambiente em nuvem como datacenter secundário ou como um ambiente de recuperação.

17.9 Fornecer o monitoramento e envio de alertas do estado de suas instâncias protegidas.

17.10 A solução deverá permitir a reconfiguração das interfaces de rede destino.

17.11 Solução de Desastre Avançada.

17.12 A solução de desastre avançada deverá ser licenciada por máquina virtual.

17.13 A solução de desastre avançada deverá ser entregue com uma política de replicação para no mínimo 15 minutos de RPO (Recovery Point Object).

17.14 A solução de desastre avançada deverá ser entregue com a funcionalidade de retenção para os pontos no tempo, provendo no mínimo 7 dias de retenção.

18.0 SOFTWARES E LICENCIAMENTO

18.1 Todos os licenciamentos necessários para a prestação dos serviços de Cloud Computing, conforme descrito no Termo de Referência, serão responsabilidade da contratada.

18.2 Durante a vigência do contrato, a Contratada deverá fornecer os seguintes softwares licenciados:

18.3 Windows Server na sua versão mais recente;

18.4 Red Hat Enterprise Linux na sua versão mais recente;

18.5 Windows Remote Desktop na sua versão mais recente;

18.6 Microsoft SQL Server Standard;

18.7 Caso haja a requisição de uso do licenciamento SQL Server Standard, deverá ser considerado o consumo mensal para no mínimo 4 vCPUs.

18.8 Microsoft SQL Server Enterprise;

18.9 Caso haja a requisição de uso do licenciamento SQL Server Entreprise, deverá ser considerado o consumo mensal para no mínimo 4 vCPUs.

18.10 Os softwares poderão ser atualizados pela contratada durante toda a vigência do contrato.

18.11 A solução deve permitir licenciamentos atuais de posse desta Administração, conforme os parâmetros de licenças determinados, não se limitando a estes.

19.1 **OPERAÇÃO, SUPORTE E GERENCIAMENTO**

19.2 A CONTRATADA deverá prover todo o suporte e gestão da solução ofertada.

19.2 É responsabilidade da CONTRATADA monitorar a solução 24 x 7 x 365 (vinte e quatro horas, sete dias por semana, 365 dias por ano) para garantia da disponibilidade da mesma.

19.3 A CONTRATADA será responsável por operar e gerenciar as tarefas de backup de acordo com as solicitações realizadas pelo time da CONTRATANTE, devendo adicionar, alterar ou remover tarefas e rotinas de backup, de acordo com as solicitações.

19.4 A CONTRATADA será responsável em verificar a execução das rotinas e tarefas de backup.

19.5 Em casos de falha, a CONTRATADA deverá notificar prontamente o time da CONTRATANTE, verificar a causa raiz da falha, e sendo possível a correção, corrigir e executar novamente a tarefa.

19.6 A CONTRATANTE terá direito a um número ilimitado de alterações mensais nas políticas e rotinas vigentes em seu cenário de backup sem qualquer custo adicional.

19.7 A CONTRATADA deverá enviar mensalmente relatório estatístico das rotinas de backup.

19.8 A CONTRATADA deverá fornecer suporte técnico na modalidade 8 x 5 (8 horas por dia e 5 dias por semana) em língua portuguesa, para sanar dúvidas quanto da solução, sua configuração ou quaisquer outros assuntos relacionados à solução, através de suporte telefônico, por e-mail e através de um sistema online de chamados.

19.9 Em casos de acionamento de desastre, restaurações de bancos ou que seja necessária a restauração baremetal de um ou mais servidores, a CONTRATADA deve disponibilizar time técnico devidamente qualificado e de forma presencial nas dependências da CONTRATADA para a realização ou acompanhamento das tarefas.

19.10 A equipe técnica deverá estar alocada em até no máximo 4 horas na CONTRATANTE, após a constatação efetiva do desastre.

19.11 Durante a execução deste serviço a CONTRATADA se obriga a manter profissional(ais) com todas as qualificações.

19.12 SUPORTE A AMBIENTE MICROSOFT

19.12.1 Alguns serviços a serem executados incluem, mas não se limitam a:

19.12.1.1 Auxílio na migração de servidores Windows 2008 para Windows 2019;

19.12.1.2 Auxílio na migração de servidores Windows 2012 para Windows 2019;

19.12.1.3 Auxílio na atualização da estrutura de domínio para ambiente Windows 2019;
19.12.1.4 Auxílio no troubleshooting de problemas de operação;
19.12.1.5 Auxílio no planejamento de Life-cycle de servidores;
19.12.1.6 Auxílio na implantação de novos serviços e rotinas pertinentes ao domínio.

19.13 SUPORTE A AMBIENTE RED HAT

19.13.1 Alguns serviços a serem executados incluem, mas não se limitam a:
19.13.1.1 Auxílio na migração de servidores;
19.13.1.2 Auxílio na atualização da estrutura;
19.13.1.3 Auxílio no troubleshooting de problemas de operação;
19.13.1.4 Auxílio no planejamento de Life-cycle de servidores;
19.13.1.5 Auxílio na implantação de novos serviços e rotinas pertinentes ao ambiente.

19.14 SUPORTE A BANCO DE DADOS

19.14.1 Alguns serviços a serem executados incluem, mas não se limitam a:
19.14.1.1 Auxílio no monitoramento
19.14.1.2 Auxílio no troubleshooting de problemas de operação;
19.14.1.3 Auxílio na implantação de novos serviços e rotinas pertinentes ao banco de dados.

19.15 SUPORTE A AMBIENTE DE FIREWALL

19.15.1 O serviço deve ser prestado por profissional certificado pela solução NSE4, SNSA, JNCIP, PCNSA ou equivalentes (certificação ativa ou desativa) ou especialista em solução de segurança baseada em firewall.
19.15.2 Alguns serviços a serem executados incluem, mas não se limitam a:
19.15.2.1 Auxílio na migração das regras do firewall existente para o firewall em nuvem;
19.15.2.2 Auxílio no troubleshooting de problemas de operação;
19.15.2.3 Auxílio na implantação de novos serviços e rotinas pertinentes ao ambiente.

20.0 DA PRIVACIDADE E DISPONIBILIDADE

20.1 O prazo para disponibilização dos serviços para a CONTRATANTE deverá ser de até 60 dias após a assinatura do contrato.

20.2 A qualquer momento durante a execução deste contrato, todos os dados e informações da CONTRATADA poderão ser solicitados pela CONTRATADA para a CONTRATANTE e deverão ser disponibilizados em até 48 horas após esta solicitação. Os dados deverão ser disponibilizados em formato de padrão de mercado, sem qualquer tipo de criptografia ou formato proprietário da CONTRATADA, de forma que permita serem lidos, acessados e modificados pela CONTRATANTE.

20.3 Após o término do contrato, todos os dados e informações da CONTRATADA devem ser disponibilizados em formato de padrão de mercado, sem qualquer tipo de criptografia ou formato proprietário da CONTRATADA, de forma que permita serem lidos, acessados ou modificados pela CONTRATANTE. Os dados deverão ser disponibilizados em um local a ser disponibilizado pela CONTRATANTE em um prazo de até 48 horas após a solicitação formal.

21.0 IMPLANTAÇÃO E INTEGRAÇÃO

21.1 Deve compreender a instalação física e lógica da solução (desde a montagem dos equipamentos, configuração, testes, até que o a solução esteja ativa e em pleno funcionamento), além de ligações de energia elétrica. A solução deverá ser instalada e configurada em seu local de funcionamento, ligados à alimentação elétrica dos nobreaks indicados pela equipe técnica;

21.2 Caso a ligação elétrica existente não seja suficiente para ligação ou mesmo haja necessidade de complemento de material, a contratada deverá realizar o provimento desta instalação através do fornecimento e a passagem da infraestrutura e cabeamento elétrico do quadro até o rack, inclusive com o fornecimento dos plugues ou o que for necessário para a correta instalação do equipamento, conforme a recomendação do fabricante.

21.3 A Solução deverá vir com todos os acessórios, réguas e tomadas para se interligar às atuais existentes.

21.4 Realizar a instalação física e configuração lógica dos switches.

21.5 Realizar serviço de migração dos dados, servidores (limitado a 300 servidores) e serviços atuais armazenados nos storage atuais para a nova solução. Acompanhar e desenvolver solução conjunta para os problemas que houver durante a migração.

21.6 Todo cabeamento (fibras, patch cords, cabos elétricos) necessários para que o datacenter da CONTRATADA deverão ser previstas para atender suas capacidades plenas e integrado à infraestrutura da CONTRATANTE deverá ser fornecido pela CONTRATADA;

21.7 Os componentes dos equipamentos deverão ser homologados pelo fabricante. Não será aceita a adição ou subtração de qualquer componente não original de fábrica para adequação do equipamento;

21.8 Os horários de instalação, serão executados em hora e dia previstos pela equipe técnica responsável da CONTRATANTE, podendo ser requisitados fora do horário normal de expediente, estes combinados com antecedência;

21.9 Deverá ser elaborado cronograma contemplando as etapas de instalação e configurações;

21.10 Análise de ambiente, ligações de cabos, apresentação lógica e ativação da solução.

21.11 Depois de concluída a instalação e configuração dos novos equipamentos, a Contratada deverá fornecer documentação detalhada de todo o processo de instalação e configuração dos equipamentos ativos da solução;

21.12 Realização de testes da solução;

21.13 Preparação e detalhamento do ambiente a ser implantado.

21.14 Todos os equipamentos deverão ser fornecidos com manuais técnicos do usuário e de referência contendo todas as informações sobre os produtos com as instruções para instalação, configuração, operação e administração.

22.0 OUTROS

22.1 Quando o Licitante não for o próprio fabricante dos equipamentos ofertados, deverá apresentar declaração do Fabricante específica para o edital, autorizando a empresa licitante a comercializar os equipamentos ofertados;

22.2 Os componentes do equipamento deverão ser homologados pelo fabricante. Não será aceita a adição ou subtração de qualquer componente não original de fábrica para adequação do equipamento;

22.3 Apresentação de no mínimo um atestado emitido por pessoa jurídica de direito público ou privado, comprovando que a proponente fornece/forneceu bens compatíveis com os objetos da licitação emitidos em papel timbrado, com assinatura, identificação e telefone do emitente.

23.0 TREINAMENTO

23.1 A contratada deverá fornecer treinamento via web ou presencial para a equipe técnica da CONTRATANTE, habilitando-a a realizar Diagnóstico e Manutenção dos equipamentos fornecidos;

23.2 O treinamento capacitará equipe técnica a realizar diagnósticos, abrir chamados diretamente em ferramenta do fabricante, solicitar peça e se necessário realizar a troca do componente;

23.3 Esse escopo será tratado como um recurso opcional e/ou complementar, ao nível de suporte dos equipamentos visando incrementar o atendimento referente ao suporte técnico do fabricante. Tal certificação/habilitação não torna a CONTRATANTE responsável técnica pelos atendimentos dos referidos equipamentos. Esta responsabilidade permanece do fabricante;

23.4 O treinamento deve propiciar aos técnicos da CONTRATANTE a autorização de abertura dos equipamentos para diagnóstico e acréscimo de periféricos / dispositivos

homologados sem perda da garantia, bem como solicitação de peças para reposição e abertura de chamados com o fabricante.

23.5 1 visita mensal presencial durante a vigência do contrato para manutenção preventiva, corretiva e atualização das máquinas virtuais.

24.0 ENTREGA

24.1 O prazo máximo de entrega deverá ser de até 30 dias a partir do recebimento do empenho, ou no caso de haver contrato formal, a partir da data de assinatura;

24.2 A entrega deverá ser realizada na sede da CONTRATANTE, observando o horário de funcionamento da Instituição.

25.0 LOCAL DE ENTREGA

25.1 A entrega do serviço deverá ser realizada no Centro Universitário FMABC, localizado na Av. Lauro Gomes, 2000 – Vila Sacadura Cabral – Santo André – SP – CEP: 09060-650 (Portaria 1), devendo ser previamente agendada utilizando como forma de comunicação oficial o e-mail ti@fmabc.br e telefone (11)4993-7271.

26.0 PRAZO DE ENTREGA

26.1 A Contratada iniciará a prestação dos serviços no prazo de 15 (quinze) dias após a emissão da ordem de serviço.

27.0 OBRIGAÇÕES DA CONTRATADA

27.1 A Contratada além do fornecimento dos produtos, obriga-se a:

27.2 Fornecer dentro do prazo acordado os respectivos produtos relacionados no Termo de Referência, nos horários estabelecidos pela Contratante.

27.3 Responsabilizar-se integralmente pela qualidade dos produtos fornecidos, cumprindo as disposições legais que interfiram em sua comercialização.

27.4 Designar por escrito, no ato do recebimento da Autorização de Fornecimento, preposto (s) que tenha (m) poder (es) para resolução de possíveis ocorrências durante o fornecimento dos itens contratados.

27.5 Responsabilizar-se pelos danos causados diretamente à Contratante ou a terceiros, decorrentes de sua culpa ou dolo, não excluindo ou reduzindo essa responsabilidade à fiscalização do Contratante.

27.6 Manter todas as condições que culminaram em sua habilitação desde a entrega o início da vigência contratual, durante a entrega do serviço, até o término de sua vigência com a atestação dos produtos contratados.

27.7 Comunicar, por escrito, imediatamente, a impossibilidade atendimento à qualquer obrigação contratual, para adoção das providências cabíveis.

27.8 Reparar, corrigir, remover, refazer ou substituir, às suas expensas, imediatamente, os equipamentos em que se verificarem vícios, defeitos ou incorreções.

27.9 Permitir e facilitar a supervisão dos seus serviços pela fiscalização.

27.10 Substituir, por sua conta e responsabilidade, os equipamentos recusados pela fiscalização, em prazo a ser estabelecido pelo Contratante de acordo com cada caso.

28.0 OBRIGAÇÕES DA CONTRATANTE

28.1 O Centro Universitário fiscalizará a entrega do serviço através de funcionário designado para esse fim, com a incumbência de relatar as falhas ou irregularidades que verificar, as quais, se não forem sanadas, estarão passíveis de aplicação das sanções estabelecidas por lei, bem como as constantes no Termo de Referência.

28.2 Indicar, formalmente, o gestor e ou fiscal para acompanhamento da entrega do serviço, objeto no Termo de Referência.

28.3 Efetuar os pagamentos nas condições e preços pactuados no contrato.

28.4 Rejeitar no todo ou em parte, os equipamentos em desacordo com as exigências no Termo de Referência e do contrato, atestando seu recebimento, após verificação das especificações.

28.5 Expedir Autorização de Fornecimento no prazo máximo de 15 (quinze) dias após a divulgação do vencedor.

28.6 A Contratante elegerá como responsável pela fiscalização e acompanhamento da entrega do objeto do presente contrato, **o Sr. José Roberto de Sousa Martins,** o qual poderá ser contactado em horário comercial, através dos canais abaixo descritos:

E-mail: roberto.martins@fmabc.br

Telefone: (011) 4993-5420

28.7 Aplicar as penalidades previstas para o caso do não cumprimento de cláusulas contratuais, ou aceitar as justificativas apresentadas pela empresa

29.1 DO REPRESENTANTE DA CONTRATADA

29.1 Designar, por escrito, no ato da assinatura do contrato, 01 (um) ou mais representantes, devidamente qualificados, conhecedores dos serviços prestados pela Contratada, para realizar visitas à Contratante, para, juntamente com profissionais

responsáveis designados pela Contratante, tratar de não conformidades nos serviços prestados, quinzenalmente, em dia e horário a ser estipulado entre as partes.

30.1 CONTROLE DA EXECUÇÃO DO SERVIÇO

30.1 A fiscalização e acompanhamento da execução do objeto será por meio da área requisitante, observando que:

30.1.1 O Fiscal designado anotará em registro próprio todas as ocorrências relacionadas com a execução do objeto, determinando o que for necessário à regularização das faltas ou defeitos observados.

30.1.2 As decisões e providências que ultrapassarem a competência do fiscal deverá ser solicitada a seus superiores em tempo hábil para a adoção das medidas convenientes.

30.1.3 A fiscalização por parte da Contratante não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por qualquer irregularidade de seus agentes e prepostos, ressaltando-se, ainda, que mesmo atestado o serviço adquirido, subsistirá a responsabilidade da Contratada pela solidez, qualidade e segurança deste último.

30.1.4 A fiscalização dos serviços pela Contratante não exime, nem diminui a completa responsabilidade da Contratada, por qualquer inobservância ou omissão às cláusulas Contratuais.

30.1.5 O acompanhamento quanto ao cumprimento do objeto ocorrerá por conta da Contratada, e cabe a fiscalização por conta da Contratante, que deverá designar o colaborador responsável, ao qual compete o acompanhamento, controle e avaliação da execução contratual.

30.1.6 A Fiscalização poderá exigir o afastamento de qualquer funcionário ou do preposto da empresa Contratada que venha causar embaraço à fiscalização, que adotem procedimentos incompatíveis com o exercício das funções que lhe forem atribuídas ou, ainda, por incompetência, falta de conhecimento, indisciplina ou que perturbe o bom andamento dos trabalhos. Esta avaliação cabe a Fiscalização de execução do contrato por parte da Contratante.

30.1.7 A Contratada ficará sujeita a mais ampla e irrestrita fiscalização, obrigando-se a prestar todos os esclarecimentos porventura requeridos pela Contratante.

30.1.8 A Fiscalização se reserva o direito de impugnar os trabalhos que não forem feitos a contento, ficando a Contratada na obrigação de refazê-los, sem ônus para a Contratante.

31.0 DO PREÇO E DAS CONDIÇÕES DE PAGAMENTOS

31.1 O Centro Universitário FMABC compromete-se a pagar o preço constante da proposta da Contratada, observadas as seguintes condições:

31.1.1 O pagamento será efetuado à Contratada em 12 (doze) parcelas iguais, sendo:

- A **Primeira parcela** – 30 (trinta) dias após o início dos serviços e aceite da respectiva nota fiscal pelo Contratante;

31.2 Caso seja detectado algum problema na documentação entregue anexada à nota fiscal, será concedido, pela Contratante, prazo para regularização. Após o decurso deste, em permanecendo a inércia da Contratada, o contrato será rescindido com aplicação de multa prevista em capítulo próprio.

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

31.4 Em caso de eventuais atrasos, os valores serão atualizados de acordo com a legislação vigente.

31.5 A Contratada deverá indicar, com a documentação fiscal, o número da conta corrente e a agência do Banco Santander S/A, a fim de agilizar o pagamento.

31.6 A Contratada deverá enviar a nota fiscal para os e-mails: compras@fmabc.br e ti@fmabc.br, na nota deverá constar o número do processo ao qual corresponde.

31.7 As notas fiscais deverão ser entregues em tempo considerável (até o quinto dia útil do mês subsequente), para que a Contratante possa proceder com as análises devidas e o subsequente pagamento dos valores.

32.0 DO REAJUSTE

32.1 Em havendo prorrogação do presente contrato de prestação de serviços, e após decorrido 12 (doze) meses, poderá haver reajustamento de preços, em havendo solicitação expressa da Contratada e anuência da Contratante, conforme descrito abaixo:

32.2 Fica instituído o IPCA - Índice de Preços ao Consumidor Amplo, para reajustamento de preços após decorridos 12 meses de contrato com anuência da Contratante.

32.3 Eleição do Índice:
a)Dois meses de retroação da data base (mês da proposta);
b)Dois meses de retroação da Indecência.

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

32.5 Na Incidência:
a) A variação verificada no período de 12(doze) meses, apurada na forma citada nas cláusulas anteriores, será aplicada sobre o preço inicial (proposta).

32.6 O Centro Universitário FMABC não assumirá responsabilidade alguma por pagamento de impostos e encargos que competirem a Contratada, nem estará

obrigado a restituir-lhe valores, principais e acessórios, que porventura despender com pagamento dessa natureza.

33.0 VALOR

33.1 Dá-se ao presente contrato o valor total de R$ xxx.xxx.xx (xxxxxxxxxxxxxxxxx).

34.0 DAS COMUNICAÇÕES

34.1 As comunicações entre as partes contratantes, relacionadas com o acompanhamento e controle do presente contrato, serão feitas sempre por escrito.

35.0 DAS PENALIDADES

35.1 A Contratante poderá, garantida a prévia defesa, aplicar à Contratada as seguintes sanções:

I) advertência;

II) multa, a ser recolhida no prazo máximo de 15 (quinze) dias corridos, a contar da comunicação oficial, nas seguintes hipóteses:

a) 0,3% (zero vírgula três por cento) por dia de atraso injustificado e por descumprimento das obrigações estabelecidas em contrato, até o máximo de 10% (dez por cento) sobre o valor total do contrato;

b) 10% (dez por cento) sobre o valor total do contrato, no caso de inexecução total ou 5% (cinco por cento) do valor total do objeto contratado, no caso de inexecução parcial;

III) impedimento de licitar e contratar;

IV) declaração de inidoneidade para licitar ou contratar, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação perante a própria autoridade que aplicou a penalidade.

35.2 As sanções previstas nos incisos I, III, e IV do caput poderão ser aplicadas juntamente com as do inciso II.

35.3 Da aplicação das penalidades previstas nos incisos I, II e III do caput, poderão ser interpostos recursos no prazo máximo de 5 (cinco) dias úteis, a contar da intimação do ato ou da lavratura da ata.

35.4 No caso da penalidade prevista no inciso IV do caput, caberá pedido de reconsideração, no prazo de 10 (dez) dias úteis, a contar da intimação do ato, podendo a reabilitação ser requerida após 2 (dois) anos de sua aplicação.

36.0 DA RESCISÃO

36.1 A inexecução total do Contrato ensejará a sua rescisão, enquanto a inexecução parcial poderá ensejar a sua rescisão, com as consequências cabíveis, conforme penalidades do artigo anterior.

36.2 As práticas passíveis de rescisão, tratadas no inciso anterior, podem ser definidas, dentre outras, como:

36.3 corrupta: oferecer, dar, receber ou solicitar, direta ou indiretamente, qualquer vantagem com o objetivo de influenciar a ação do empregado da Contratante no processo administrativo ou na execução do Contrato;

36.4 fraudulenta: falsificar ou omitir fatos, com o objetivo de influenciar o processo administrativo ou de execução do Contrato;

36.5 colusiva: esquematizar ou estabelecer um acordo entre dois ou mais interessados, com ou sem conhecimento de representantes da Companhia, visando estabelecer preços em níveis artificiais e não competitivos;

36.6 coercitiva: causar dano ou ameaçar, direta ou indiretamente, as pessoas físicas ou jurídicas, visando influenciar sua participação em processo administrativo ou afetar a execução do Contrato;

36.7 obstrutiva: destruir, falsificar, alterar ou ocultar provas ou fazer declarações falsas, com objetivo de impedir materialmente a apuração de práticas ilícitas.

36.8 As práticas acima exemplificadas, além de acarretarem responsabilização administrativa e judicial da pessoa física e/ou jurídica, implicarão na responsabilidade individual dos dirigentes da Contratada e dos administradores ou gestores, enquanto autores, coautores ou partícipes do ato ilícito, nos termos da lei.

36.9 São considerados motivos para a rescisão:

36.10 a inexecução parcial ou total das obrigações e prazos constantes nos Instrumentos Convocatórios e Contratuais;

36.11 a dissolução da sociedade ou o falecimento do contratado;

36.12 a decretação de falência ou a insolvência civil do contratado;

36.13 a alteração social ou a modificação da finalidade ou da estrutura da Contratada, desde que prejudique a execução do Contrato;

36.14 razões de interesse público, de alta relevância e amplo conhecimento, justificadas e exaradas no processo administrativo;

36.15 o atraso nos pagamentos devidos pela Contratante decorrentes de serviços ou fornecimentos, ou parcelas destes já recebidos ou executados, salvo em caso de calamidade pública, grave perturbação da ordem interna ou guerra, assegurado ao contratado o direito de optar pela suspensão do cumprimento de suas obrigações até que seja normalizada a situação;

36.16 a ocorrência de caso fortuito, força maior ou fato do príncipe, regularmente comprovada, impeditiva da execução do Contrato;

36.17 a aplicação ao contratado de suspensão do direito de licitar e/ou contratar com a FUNDAÇÃO DO ABC E SUAS UNIDADES GERENCIADAS;

36.18 o descumprimento da proibição de trabalho noturno, perigoso ou insalubre a menores de 18 (dezoito) anos e de qualquer trabalho a menores de 16 (dezesseis) anos, salvo na condição de aprendiz, a partir de 14 (quatorze) anos;

36.19 ter frustrado ou fraudado, mediante ajuste, combinação ou qualquer outro expediente, o caráter competitivo de procedimento administrativo regulamentar e licitatório público;

36.20 ter impedido, perturbado ou fraudado a realização de qualquer ato de procedimento administrativo regulamentar e/ou licitatório público; ter afastado ou procurado afastar Proponentes, por meio de fraude ou oferecimento de vantagem de qualquer tipo;

36.21 ter fraudado procedimento administrativo regulamentar e/ou licitação pública ou Contrato dela decorrente;

36.22 ter criado, de modo fraudulento ou irregular, pessoa jurídica para participar de licitação pública ou celebrar Contrato Administrativo;

36.23 ter obtido vantagem ou benefício indevido, de modo fraudulento, de modificações ou prorrogações de Contratos celebrados com a Administração Pública e demais entes licitantes, sem autorização em lei, no instrumento convocatório da licitação pública ou nos respectivos instrumentos contratuais;

36.24 ter manipulado ou fraudado o equilíbrio econômico-financeiro dos Contratos celebrados com a Administração Pública;

36.25 ter dificultado atividade de investigação ou fiscalização de órgãos, entidades ou agentes públicos, ou ter intervindo em sua atuação, inclusive no âmbito das agências reguladoras e dos órgãos de fiscalização do sistema financeiro nacional;

36.26 O Contrato poderá ser rescindido unilateralmente, desde que haja conveniência para a Contratante mediante autorização escrita e fundamentada da autoridade superior, de acordo com o artigo 44, do Regulamento de Compras da FUABC.

37.0 DA CESSÃO E TRANSFERÊNCIA

37.1 É vedada a cessão ou transferência total ou parcial dos direitos e/ou obrigações inerentes a este contrato, por quaisquer das partes, sem prévia e expressa autorização da outra.

38.0 DAS VEDAÇÕES

38.1 É vedado à CONTRATADA:

18.1.1- Caucionar ou utilizar este Termo de Contrato para qualquer operação financeira;

18.1.2- Interromper a execução contratual sob alegação de inadimplemento por parte da CONTRATANTE, salvo nos casos previstos em lei.

39.0 A ALTERAÇÃO DO OBJETO DO CONTRATO

39.1 Este contrato poderá ser modificado no todo ou em parte, por acordo entre as partes, somente através de Termo Aditivo de acordo com a previsão contida no Regulamento de Compras em seu artigo 44 do Capítulo II.

40.0 DISPOSIÇÕES FINAIS

40.1 Este contrato, bem como os direitos e obrigações dele decorrentes, não poderá ser subcontratado, cedido ou transferido, total ou parcialmente, nem ser executado em associação da Contratada com terceiros, sem autorização prévia da Contratante, por escrito, sob pena de aplicação de sanção, inclusive rescisão contratual.

40.2 Este contrato não poderá ser utilizado, sem prévia e expressa autorização da Contratante, em operações financeiras ou como caução/ garantia em contrato ou outro tipo de obrigação, sob pena de sanção, inclusive rescisão contratual.

40.3 A Contratante reserva para si o direito de não aceitar ou receber qualquer produto em desacordo com o previsto neste contrato ou em desconformidade com as normas legais ou técnicas pertinentes ao seu objeto, podendo rescindi-lo sem prejuízo das sanções previstas neste instrumento.

40.4 A inobservância dos prazos estipulados neste contrato ocasionará a aplicação das penalidades previstas neste mesmo instrumento.

41.0 DA LEI GERAL DE PROTEÇÃO DE DADOS E DAS NORMAS DE COMPLIANCE

41.1 A Contratada, por si e por seus administradores, diretores, funcionários e agentes, bem como seus sócios que venham a agir em seu nome, se obriga a conduzir suas práticas comerciais, durante a consecução do presente Contrato, de forma ética e em conformidade com os preceitos legais aplicáveis, incluindo a Lei Anticorrupção Brasileira e o Código de Conduta da Contratante.

41.2 Na execução deste Contrato, nem a Contratada, nem qualquer de seus diretores, empregados, agentes ou sócios agindo em seu nome, devem dar, oferecer, pagar, prometer pagar, ou autorizar o pagamento de, direta ou indiretamente, qualquer dinheiro ou qualquer coisa de valor a qualquer autoridade governamental, consultores, representantes, parceiros, ou quaisquer terceiros, com a finalidade de influenciar qualquer ato ou decisão do agente ou do governo, ou para assegurar qualquer vantagem indevida, ou direcionar negócios para qualquer pessoa.

42.0 DO FORO

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

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

Santo André, ____ de _____ de _____

_____
Centro Universitário FMABC

_____
CONTRATADA

Testemunhas:

_____
CPF:

_____
CPF:

ANEXO XI – CONTRATO DE PRESTAÇÃO DE SERVIÇO
PROCESSO Nº 0544/2023
DA PROTEÇÃO DE DADOS

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

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

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

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

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

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

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

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

Todos os demais termos não definidos neste Contrato que possuem definição na Lei Geral de Proteção de Dados (Lei Federal nº 13.709/2018) serão compreendidos como ali descritos.

1.2. As Partes, neste ato, se comprometem a cumprir toda a legislação aplicável sobre a segurança da informação, privacidade e proteção de dados, inclusive (sempre e quando aplicáveis) a Constituição Federal, o Código de Defesa do Consumidor, o Código Civil, o Marco Civil da Internet (Lei Federal nº

12.965/2014), seu decreto regulamentar (Decreto 8.771/2016), a Lei Geral de Proteção de Dados (Lei Federal nº 13.709/2018) (LGPD), e as demais normas setoriais ou gerais sobre o tema, se comprometendo a tratar os dados pessoais e sensíveis ("Dados") de acordo com as melhores práticas de proteção de dados utilizadas no mercado, se comprometendo a:

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

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

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

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

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

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

(vii) Manter registro dos Tratamentos realizados e

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

1.3. As Partes declaram que têm compromisso com a privacidade de seus clientes, parceiros e empregados, sendo sua atuação guiada pelos seguintes princípios: (a) limitação de uso de dados pessoais ao extremamente necessário para atender aos propósitos empresariais; (b) acesso aos dados pessoais apenas por pessoas imprescindíveis e eliminação de dados quando não mais necessários; (c) cuidado adicional no tratamento de dados pessoais sensíveis; (d) transparência com clientes, parceiros e empregados; (e) segurança dos dados pessoais.

1.4. A parte prejudicada terá o direito de ser reembolsada pela parte infratora por quaisquer perdas, danos, multas, custos ou despesas (incluindo despesas e desembolsos legais) incorridos pela parte prejudicadas e que resultem de uma Violação de Dados Pessoais, falha na adoção de medidas de segurança exigidas pelo artigo 46 da LGPD ou da violação de algum item desta cláusula

em relação a quaisquer dados pessoais tratados em conexão com o Contrato, e que tais valores serão considerados perdas diretas e serão devidos pela arte infratora à parte prejudicada, mediante comprovação.

Santo André, _____ de _____ de 2023.

_____

(CONTRATANTE)

Nome:
CPF:

_____

(CONTRATADA)

Nome:
CPF: