SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

PREGÃO ELETRÔNICO Nº 007/2022
PROCESSO ADMINISTRATIVO - V-0050/2020

Torna-se público, para conhecimento dos interessados, que o **Conselho Regional de Engenharia e Agronomia do Estado de São Paulo – CREA-SP**, por meio da Unidade de Licitações – UL, sediada à Avenida Brigadeiro Faria Lima, 1059 – 8º andar, Pinheiros – São Paulo – SP, CEP – 01452-920, realizará licitação na modalidade **PREGÃO**, na forma **ELETRÔNICA**, do Tipo **MENOR PREÇO GLOBAL**, nos termos da Lei nº 10.520, de 17 de julho de 2002, do Decreto nº 10.024, de 20 de setembro de 2019, do Decreto nº 7.746, de 05 de junho de 2012, da Instrução Normativa SEGES/MP nº 05, de 26 de maio de 2017, da Instrução Normativa SLTI/MP nº 01, de 19 de janeiro de 2010, da Instrução Normativa SEGES/MP nº 03, de 26 de abril, de 2018, da Lei Complementar n° 123, de 14 de dezembro de 2006, do Decreto n° 8.538, de 06 de outubro de 2015, aplicando-se, subsidiariamente, a Lei nº 8.666, de 21 de junho de 1993, e as exigências estabelecidas neste Edital.

DATA DA SESSÃO: **1º/06/2022;**
UASG: **389423**;
Horário da Realização do Pregão: 10 horas.
Local: Portal de Compras do Governo Federal – www.comprasgovernamentais.gov.br.

1. DO OBJETO

1.1. O objeto desta licitação é a contratação de empresa para prestação de serviços de hospedagem de sistemas de software e arquivos, com seus respectivos sistemas operacionais, aplicações e bancos de dados, composto por seus equipamentos (hardware), softwares, licenciamento, planejamento, instalação, migração de dados e aplicações, manutenção, comunicação de dados, suporte, operação, treinamento e gerenciamento da solução de hospedagem, conforme condições, quantidades, exigências e especificações estabelecidas neste Edital e seus anexos.

Nota: Em caso de discordância existente entre as especificações deste objeto descritas no sistema Comprasnet e as especificações constantes deste Edital, prevalecerão as últimas.

1.2. A licitação será realizada em único grupo, formado por 06 (seis) itens, conforme tabela constante no Termo de Referência, devendo o licitante oferecer proposta para todos os itens que a compõem.

1.3. O critério de julgamento adotado será o menor preço do grupo único sob a forma de execução indireta, no regime de empreitada por preço global do grupo único, observadas as exigências contidas neste Edital e seus anexos quanto às especificações do objeto.

2. DA DOTAÇÃO ORÇAMENTÁRIA

2.1. A despesa para atender a esta licitação está programada em dotação orçamentária própria da Equipe de Infraestrutura e Segurança da Informação - EISI da Gerência de Desenvolvimento e Execução de Projetos - GDEP da Superintendência de Tecnologia e Inovação - SUPTEC, prevista no orçamento do CREA-SP no exercício de financeiro de 2022, oriundo da conta no 6.2.2.1.1.01.04.09.005 – Serviços de Informática - PJ.

2.2 A despesa com a execução dos serviços de que trata o objeto desta licitação é estimada no período de 36 (trinta e seis) meses.

3 DO CREDENCIAMENTO

3.1 O Credenciamento é o nível básico do registro cadastral no Sistema de Cadastramento Unificado de Fornecedores - SICAF, que permite a participação dos interessados na modalidade licitatória Pregão, em sua forma eletrônica.

3.2 O cadastro no SICAF deverá ser feito no Portal de Compras do Governo Federal, no sítio www.comprasgovernamentais.gov.br, por meio de certificado digital conferido pela Infraestrutura de Chaves Públicas Brasileira – ICP - Brasil.

3.3 O credenciamento junto ao provedor do sistema implica a responsabilidade do licitante ou de seu representante legal e a presunção de sua capacidade técnica para realização das transações inerentes a este Pregão.

3.4 O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assumir como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou do órgão ou entidade promotora da licitação por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.

3.5 É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais no SICAF e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

3.5.1 A não observância do disposto no subitem anterior poderá ensejar desclassificação no momento da habilitação.

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

4 DA PARTICIPAÇÃO NO PREGÃO

4.1 Poderão participar deste Pregão interessados cujo ramo de atividade seja compatível com o objeto desta licitação, e que estejam com Credenciamento Regular no Sistema de Cadastramento Unificado de Fornecedores – SICAF, conforme disposto no art. 9º da IN SEGES/MP nº 3, de 2018.

4.2 Os licitantes deverão utilizar o certificado digital para acesso ao Sistema.

4.3 **Não poderão participar desta licitação os interessados:**

4.3.1 Proibidos de participar de licitações e celebrar contratos administrativos, na forma da legislação vigente;

4.3.2 Que não atendam às condições deste Edital e seus anexos;

4.3.3 Estrangeiros que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativa ou judicialmente;

4.3.4 Que se enquadrem nas vedações previstas no artigo 9º da Lei nº 8.666, de 1993;

4.3.5 Que estejam sob falência, concurso de credores, concordata ou insolvência, em processo de dissolução ou liquidação;

4.3.6 Entidades empresariais que estejam reunidas em consórcio;

4.3.7. Sociedades cooperativas, considerando a vedação contida no art. 10 da Instrução Normativa SEGES/MP nº 5, de 2017.

4.3.8. Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição (Acórdão nº 746/2014-TCU-Plenário);

4.4 Nos termos do art. 5º do Decreto nº 9.507, de 2018, é vedada a contratação de pessoa jurídica na qual haja administrador ou sócio com poder de direção, familiar de:

a) detentor de cargo em comissão ou função de confiança que atue na área responsável pela demanda ou contratação; ou

b) de autoridade hierarquicamente superior no âmbito do órgão contratante.

4.4.1 Para os fins do disposto neste item, considera-se familiar o cônjuge, o companheiro ou o parente em linha reta ou colateral, por consanguinidade ou afinidade, até o terceiro grau (Súmula Vinculante/STF nº 13, art. 5º, inciso V, da Lei nº 12.813, de 16 de maio de 2013 e art. 2º, inciso III, do Decreto nº 7.203, de 04 de junho de 2010).

4.5 Nos termos do art. 7° do Decreto n° 7.203, de 2010, é vedada, ainda, a utilização, na execução dos serviços contratados, de empregado da futura Contratada que seja familiar de agente público ocupante de cargo em comissão ou função de confiança neste órgão contratante.

4.6 Como condição para participação no Pregão, o licitante assinalará “sim” ou “não” em campo próprio do sistema eletrônico, relativo às **seguintes declarações**:Que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123, de 2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49.

4.6.1.1 Nos itens exclusivos para participação de microempresas e empresas de pequeno porte, a assinalação do campo “não” impedirá o prosseguimento no certame;

4.6.1.2 Nos itens em que a participação não for exclusiva para microempresas e empresas de pequeno porte, a assinalação do campo “não” apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto na Lei Complementar nº 123, de 2006, mesmo que microempresa, empresa de pequeno porte.

4.6.2 Que está ciente e concorda com as condições contidas no Edital e seus anexos;

4.6.3 Que cumpre os requisitos de habilitação definidos no Edital e que a proposta apresentada está em conformidade com as exigências editalícias;

4.6.4 Que inexistem fatos impeditivos para sua habilitação no certame, ciente da obrigatoriedade de declarar ocorrências posteriores;

4.6.5 Que não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7°, XXXIII, da Constituição;

4.6.6 Que a proposta foi elaborada de forma independente, nos termos da Instrução Normativa SLTI/MP nº 2, de 16 de setembro de 2009.

4.6.7 Que não possui, em sua cadeia produtiva, empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;

4.6.8 Que os serviços são prestados por empresas que comprovem cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação, conforme disposto no art. 93 da Lei nº 8.213, de 24 de julho de 1991.

4.7 A declaração falsa relativa ao cumprimento de qualquer condição sujeitará o licitante às sanções previstas em lei e neste Edital.

5 DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

5.1 Os licitantes encaminharão, exclusivamente por meio do sistema, concomitantemente com os documentos de habilitação exigidos no Edital, a proposta de preços, devidamente preenchida com todos os dados, inclusive assinada pelo representante legal, até a data e o horário estabelecidos para a abertura da sessão pública, quando, então, encerrar-se-á automaticamente a etapa de envio dessa documentação.

5.2 O envio da proposta, acompanhada dos documentos de habilitação exigidos neste Edital, ocorrerá por meio de chave de acesso e senha.

5.3 Os licitantes poderão deixar de apresentar os documentos de habilitação que constem do SICAF, assegurado aos demais licitantes o direito de acesso aos dados constantes dos sistemas.

5.4 As Microempresas e Empresas de Pequeno Porte deverão encaminhar a documentação de habilitação, ainda que haja alguma restrição de regularidade fiscal e trabalhista, nos termos do art. 43, §1º, da LC nº 123, de 2006.

5.5 Incumbirá ao licitante acompanhar as operações no sistema eletrônico durante a sessão pública do Pregão, ficando responsável pelo ônus decorrente da perda de negócios, diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

5.6 Até a abertura da sessão pública, os licitantes poderão retirar ou substituir a proposta e os documentos de habilitação anteriormente inseridos no sistema;

5.7 Não será estabelecida, nessa etapa do certame, ordem de classificação entre as propostas apresentadas, o que somente ocorrerá após a realização dos procedimentos de negociação e julgamento da proposta.

5.8 Os documentos que compõem a proposta e a habilitação do licitante melhor classificado somente serão disponibilizados para avaliação do Pregoeiro e para acesso público após o encerramento do envio de lances.

6. DO PREENCHIMENTO DA PROPOSTA

6.1. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos:

6.1.1. Valor Total Geral do Grupo 1 – Único – considerando o descrito no Termo de Referência – Anexo I, deste Edital;

6.1.2. Descrição do objeto, contendo as informações similares à especificação do Termo de Referência.

6.2. Todas as especificações do objeto contidas na proposta vinculam a Contratada.

6.3. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na prestação dos serviços, apurados mediante o preenchimento do modelo de proposta de preços, conforme anexo deste Edital.

6.4. A empresa é a única responsável pela cotação correta dos encargos tributários.

6.5. A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o que dispõe o Termo de Referência, assumindo o proponente o compromisso de executar os serviços nos seus termos, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.

6.6. Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.

6.7. O prazo de validade da proposta não será inferior a 60 (sessenta) dias**,** a contar da data de sua apresentação.

6.8. Os licitantes devem respeitar os preços máximos estabelecidos nas normas de regência de contratações públicas federais, quando participarem de licitações públicas.

6.8.1. O descumprimento das regras supramencionadas pela Administração por parte dos contratados pode ensejar a responsabilização pelo Tribunal de Contas da União e, após o devido processo legal, gerar as seguintes consequências: assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do art. 71, inciso IX, da Constituição; ou condenação dos agentes públicos responsáveis e da empresa contratada ao pagamento dos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

7. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES

7.1. A abertura da presente licitação dar-se-á em sessão pública, por meio de sistema eletrônico, na data, horário e local indicados neste Edital.

7.2. O Pregoeiro verificará as propostas apresentadas, desclassificando desde logo aquelas que não estejam em conformidade com os requisitos estabelecidos neste Edital, contenham vícios insanáveis, ilegalidades, ou não apresentem as especificações exigidas no Termo de Referência.

7.2.1. Também será desclassificada a proposta que identifique o licitante - (que se identificar quando do preenchimento no sistema da descrição detalhada do objeto ofertado, de livre acesso a todos os licitantes que servirá de análise prévia antes do início da etapa de lances).

7.2.2. A desclassificação da proposta será sempre fundamentada e registrada no sistema, com acompanhamento em tempo real por todos os participantes.

7.2.3. A não desclassificação da proposta não impede o seu julgamento definitivo em sentido contrário, levado a efeito na fase de aceitação.

7.3. O sistema ordenará automaticamente as propostas classificadas, sendo que somente estas participarão da fase de lances.

7.4. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os licitantes.

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

7.5. Iniciada a etapa competitiva, os licitantes deverão encaminhar lances exclusivamente por meio de sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

7.5.1. O lance deverá ser ofertado pelo Valor Total do Grupo 1 – Único.

7.6. Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no Edital.

7.7. O licitante somente poderá oferecer lance de valor inferior ao último por ele ofertado e registrado pelo sistema.

7.8. O intervalo mínimo de diferença de valores entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de R$ 1.000,00 (hum mil reais).

7.9. Será adotado para o envio de lances no pregão eletrônico o modo de disputa "**ABERTO**", em que os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

7.10. A etapa de lances da sessão pública terá duração de 10 (dez) minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos 2 (dois) minutos do período de duração da sessão pública.

7.11. A prorrogação automática da etapa de lances, de que trata o item anterior, será de 2 (dois) minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

7.12. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente.

7.13. Encerrada a fase competitiva sem que haja a prorrogação automática pelo sistema, poderá o Pregoeiro, assessorado pela equipe de apoio, justificadamente, admitir o reinício da sessão pública de lances, em prol da consecução do melhor preço.

7.14. Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.

7.15. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.

7.16. No caso de desconexão do sistema eletrônico com o Pregoeiro, no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.

7.17. Quando a desconexão do sistema eletrônico para o pregoeiro persistir por tempo superior a 10 (dez) minutos, a sessão pública será suspensa e reiniciada somente após decorridas 24 (vinte e quatro) horas da comunicação do fato pelo Pregoeiro aos participantes, no sítio eletrônico utilizado para divulgação.

7.18. O critério de julgamento adotado será o menor preço do grupo 1 - Único, conforme definido neste Edital e seus anexos.

7.19. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta e na hipótese de desistência de apresentar outros lances, valerá o último lance por ele ofertado, para efeito de ordenação das propostas.

7.20. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da LC nº 123, de 2006, regulamentada pelo Decreto nº 8.538, de 2015.

7.21. Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima da melhor proposta ou melhor lance serão consideradas empatadas com a primeira colocada.

7.22. A melhor classificada nos termos do item anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 05 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.

7.23. Caso a microempresa ou a empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresa e empresa de pequeno porte que se encontrem naquele intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.

7.24. No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem nos intervalos estabelecidos nos subitens anteriores, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.

7.25. Só poderá haver empate entre propostas iguais (não seguidas de lances).

7.26. Havendo eventual empate entre propostas, o critério de desempate será aquele previsto no art. 3º, § 2º, da Lei nº 8.666, de 1993, assegurando-se a preferência, sucessivamente, ao objeto executado:

7.26.1. por empresas brasileiras;

7.26.2. por empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

7.26.3. por empresas que comprovem cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação.

7.27. Persistindo o empate, a proposta vencedora será sorteada pelo sistema eletrônico dentre as propostas ou os lances empatados.

7.28. Encerrada a etapa de envio de lances da sessão pública, o pregoeiro deverá encaminhar, pelo sistema eletrônico, contraproposta ao licitante que tenha apresentado o melhor preço, para que seja obtida melhor proposta, vedada a negociação em condições diferentes das previstas neste Edital.

7.28.1. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

7.28.2. O Pregoeiro solicitará ao licitante melhor classificado que, no prazo de 2 (duas) horas, envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

7.28.2.1. É facultado ao Pregoeiro prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante, antes de findo o prazo.

7.29. Após a negociação do preço, o Pregoeiro iniciará a fase de aceitação e julgamento da proposta.

8. DA ACEITABILIDADE DA PROPOSTA VENCEDORA

8.1. Encerrada a etapa de negociação, o Pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos, observado o disposto no parágrafo único do art. 7º e no § 9º do art. 26 do Decreto nº 10.024/2019.

8.2. A análise da exequibilidade da proposta de preços deverá ser realizada com o auxílio da proposta de formação de preços, a ser preenchida pelo licitante em relação à sua proposta final, conforme anexo deste Edital.

8.3. A inexequibilidade dos valores referentes a itens isolados da proposta de preços não caracteriza motivo suficiente para a desclassificação da proposta, desde que não contrariem exigências legais.

8.4. Será desclassificada a proposta, nos termos do item 9.1 do Anexo VII-A da IN SEGES/MP nº 5/2017, que:

8.4.1. Não estiver em conformidade com os requisitos estabelecidos neste edital;

8.4.2. Contenha vício insanável ou ilegalidade;

8.4.3. Não apresente as especificações técnicas exigidas pelo Termo de Referência;

8.4.4. Apresentar preço final superior ao preço máximo fixado (Acórdão nº 1455/2018 -TCU - Plenário), ou que apresentar preço manifestamente inexequível.

8.5. Quando o licitante não conseguir comprovar que possui ou possuirá recursos suficientes para executar a contento o objeto, será considerada inexequível a proposta de preços ou menor lance que:

8.5.1. For insuficiente para a cobertura dos custos da contratação, apresente preços global ou unitários simbólicos, irrisórios ou de valor zero, incompatíveis com os preços dos insumos e salários de mercado, acrescidos dos respectivos encargos, ainda que o ato convocatório da licitação não tenha

estabelecido limites mínimos, exceto quando se referirem a materiais e instalações de propriedade do próprio licitante, para os quais ele renuncie a parcela ou à totalidade da remuneração.

8.6. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, na forma do § 3° do artigo 43 da Lei n° 8.666, de 1993 e a exemplo das enumeradas no item 9.4 do Anexo VII-A da IN SEGES/MP N. 5, de 2017, para que a empresa comprove a exequibilidade da proposta.

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

8.8. Qualquer interessado poderá requerer que se realizem diligências para aferir a exequibilidade e a legalidade das propostas, devendo apresentar as provas ou os indícios que fundamentam a suspeita.

8.8.1. Na hipótese de necessidade de suspensão da sessão pública para a realização de diligências, com vistas ao saneamento das propostas, a sessão pública somente poderá ser reiniciada mediante aviso prévio no sistema com, no mínimo, 24 (vinte e quatro) horas de antecedência, e a ocorrência será registrada em ata.

8.9. O Pregoeiro poderá convocar o licitante para enviar documento digital complementar, por meio de funcionalidade disponível no sistema, no prazo de **2 (duas) horas**, sob pena de não aceitação da proposta.

8.9.1. É facultado ao Pregoeiro prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante, antes de findo o prazo.

8.10. Erros no preenchimento da proposta não constituem motivo para a desclassificação da proposta. A proposta poderá ser ajustada pelo licitante, no prazo indicado pelo Pregoeiro, desde que não haja majoração do preço proposto.

8.10.1. O ajuste de que trata este dispositivo se limita a sanar erros ou falhas que não alterem a substância das propostas.

8.11. Para fins de análise da proposta quanto ao cumprimento das especificações do objeto, poderá ser colhida a manifestação escrita do setor requisitante do serviço ou da área especializada no objeto.

8.12. Se a proposta for desclassificada, o Pregoeiro examinará a proposta subsequente, e, assim sucessivamente, na ordem de classificação.

8.13. Havendo necessidade, o Pregoeiro suspenderá a sessão, informando no “chat” a nova data e horário para a sua continuidade.

8.14. Nos itens não exclusivos para a participação de microempresas e empresas de pequeno porte, sempre que a proposta não for aceita, e antes de o Pregoeiro passar à subsequente, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida, se for o caso.

8.15. Encerrada a análise quanto à aceitação da proposta, o Pregoeiro verificará a habilitação do licitante, observado o disposto neste Edital.

9. DA HABILITAÇÃO

9.1. Como condição prévia ao exame da documentação de habilitação do licitante detentor da proposta classificada em primeiro lugar, o Pregoeiro verificará o eventual descumprimento das condições de participação, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

NOTA: - Visando melhor organização processual, solicitamos aos licitantes que, quando forem inserir no sistema do Comprasnet os documentos relativos a este item (habilitação), observem a ordem crescente dos subitens conforme se apresentam.

a) www.comprasgovernamentais.gov.br/ - SICAF;

b) Lista de Inidôneos e o Cadastro Integrado de Condenações por Ilícitos Administrativos - CADICON, mantidos pelo Tribunal de Contas da União – TCU - https://contas.tcu.gov.br/ords/f?p=INABILITADO:INIDONEOS

c) Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa, mantido pelo Conselho Nacional de Justiça www.cnj.jus.br/improbidade_adm/consultar_requerido.php

d) Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União - http://www.portaltransparencia.gov.br/sancoes/ceis?ordenarPor=nome&direcao=asc

e) Cadastro Nacional de Empresas Punidas – CNEP - http://www.portaltransparencia.gov.br/sancoes/cnep?ordenarPor=nome&direcao=asc.

d) Para a consulta de licitantes pessoa jurídica poderá haver a substituição das consultas das alíneas “b”, “c”, “d” e “e” acima pela Consulta Consolidada de Pessoa Jurídica do TCU - https://certidoes-apf.apps.tcu.gov.br/.

9.1.1. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força do artigo 12 da Lei n° 8.429, de 1992, que prevê, dentre as sanções impostas ao responsável pela prática de ato de improbidade administrativa, a proibição de contratar com o Poder Público, inclusive por intermédio de pessoa jurídica da qual seja sócio majoritário.

9.1.1.1. Caso conste na Consulta de Situação do Fornecedor a existência de Ocorrências Impeditivas Indiretas, o gestor diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.

9.1.1.2. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros.

9.1.1.3. O licitante será convocado para manifestação previamente à sua desclassificação.

9.1.2. Constatada a existência de sanção, o Pregoeiro reputará o licitante inabilitado, por falta de condição de participação.

9.1.3. No caso de inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos arts. 44 e 45 da Lei Complementar nº 123, de 2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente.

9.2. Caso atendidas as condições de participação, a habilitação do licitante será verificada por meio do SICAF, nos documentos por ele abrangidos, em relação à habilitação jurídica, à regularidade fiscal, à qualificação econômica financeira e habilitação técnica, conforme o disposto na Instrução Normativa SEGES/MP nº 03, de 2018.

9.2.1. O interessado, para efeitos de habilitação prevista na Instrução Normativa SEGES/MP nº 03, de 2018 mediante utilização do sistema, deverá atender às condições exigidas no cadastramento no SICAF até o terceiro dia útil anterior à data prevista para recebimento das propostas;

9.2.2. É dever do licitante atualizar previamente as comprovações constantes do SICAF para que estejam vigentes na data da abertura da sessão pública, ou encaminhar, em conjunto com a apresentação da proposta, a respectiva documentação atualizada.

9.2.3. O descumprimento do subitem acima implicará a inabilitação do licitante, exceto se a consulta aos sítios eletrônicos oficiais emissores de certidões feita pelo Pregoeiro lograr êxito em encontrar a(s) certidão(ões) válida(s), conforme art. 43, §3º, do Decreto nº 10.024, de 2019.

9.3. Havendo a necessidade de envio de documentos de habilitação complementares, necessários à confirmação daqueles exigidos neste Edital e já apresentados, o licitante será convocado a encaminhá-los, em formato digital, via sistema, no prazo de **2 (duas) horas**, sob pena de inabilitação.

9.4. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital.

9.5. Não serão aceitos documentos de habilitação com indicação de CNPJ/CPF diferentes, salvo aqueles legalmente permitidos.

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

9.6.1. Serão aceitos registros de CNPJ de licitante matriz e filial com diferenças de números de documentos pertinentes ao CND e ao CRF/FGTS, quando for comprovada a centralização do recolhimento dessas contribuições.

9.7. Ressalvado o disposto no item **"5.3"**, os licitantes deverão encaminhar, nos termos deste Edital, a documentação relacionada nos itens a seguir, para fins de habilitação.

9.8. **HABILITAÇÃO JURÍDICA**

9.8.1. No caso de sociedade empresária ou empresa individual de responsabilidade limitada - EIRELI: ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial da respectiva sede, acompanhado de documento comprobatório de seus administradores;

9.8.2. Inscrição no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz, no caso de ser a participante sucursal, filial ou agência;

9.8.3. No caso de sociedade simples: inscrição do ato constitutivo no Registro Civil das Pessoas Jurídicas do local de sua sede, acompanhada de prova da indicação dos seus administradores;

9.8.4. Decreto de autorização, em se tratando de sociedade empresária estrangeira em funcionamento no País;

9.8.5. Os documentos acima deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

9.9. **REGULARIDADE FISCAL E TRABALHISTA**

9.9.1. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas - CNPJ;

9.9.2. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02/10/2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

9.9.3. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

9.9.4. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

9.9.5. Prova de inscrição no cadastro de contribuintes municipal, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

9.9.6. Prova de regularidade com a Fazenda Municipal do domicílio ou sede do licitante, relativa à atividade em cujo exercício contrata ou concorre;

9.9.7. Prova de inscrição no cadastro de contribuintes estadual, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

9.9.8. Prova de regularidade com a Fazenda Estadual do domicílio ou sede do licitante, relativa à atividade em cujo exercício contrata ou concorre.

9.9.9. **Caso o licitante seja considerado isento dos tributos municipais ou estaduais relacionados ao objeto licitatório, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda Municipal ou Fazenda Estadual do seu domicílio ou sede, ou outra equivalente, na forma da lei.**

9.10. **QUALIFICAÇÃO ECONÔMICO-FINANCEIRA**

9.10.1. **Certidão negativa de falência** expedida pelo distribuidor da sede do licitante;

9.10.2. **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 encerrado há mais de 3 (três) meses da data de apresentação da proposta;

9.10.2.1. No caso de empresa constituída no exercício social vigente, admite-se a apresentação de balanço patrimonial e demonstrações contábeis referentes ao período de existência da sociedade;

9.10.2.2. É admissível o balanço intermediário, se decorrer de lei ou contrato/estatuto social.

9.10.3. **Comprovação da boa situação financeira** da empresa mediante obtenção de índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um), obtidos pela aplicação das seguintes fórmulas:

LG =	Ativo Circulante + Realizável a Longo Prazo
	Passivo Circulante + Passivo Não Circulante
SG =	Ativo Total
	Passivo Circulante + Passivo Não Circulante
LC =	Ativo Circulante
	Passivo Circulante

9.10.4. As empresas, cadastradas ou não no SICAF, que apresentarem resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), deverão comprovar patrimônio líquido mínimo de 10% (dez por cento) do valor estimado da contratação.

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

9.11. **QUALIFICAÇÃO TÉCNICA**

9.11.1. **Comprovação de aptidão para o fornecimentos de licenças, produtos, manutenção, atualização e suporte dos mesmos, serviços de implantação e migração com a devida transferência de conhecimento** em características, quantidades e prazos compatíveis com o objeto desta licitação, mediante a apresentação de atestado(s) fornecido(s) por pessoas jurídicas de direito público ou privado.

9.11.1.1. O(s) atestado(s) deverão ser apresentados em papel timbrado do emitente, conter identificação do signatário, nome, endereço, telefone e se for o caso, correio eletrônico para contato, a fim de possibilitar possíveis diligências.

9.11.2. Poderá ser admitida, para fins de comprovação de quantitativo mínimo do serviço, a apresentação de diferentes atestados de serviços executados no período de 12 (doze) meses, pois essa situação se equivale, para fins de comprovação de capacidade técnico-operacional, a uma única contratação, nos termos do item 10.9 do Anexo VII-A da IN SEGES/MP nº 5/2017.

9.11.3. Os atestados deverão referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente.

9.11.4. Somente serão aceitos atestados expedidos após a conclusão do contrato ou se decorrido, pelo menos, um ano do início de sua execução, exceto se firmado para ser executado em prazo inferior, conforme item 10.8 do Anexo VII-A da IN SEGES/MP nº 5, de 2017.

9.11.5. O licitante disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados apresentados, se for solicitado pelo Pregoeiro, apresentando, dentre outros documentos, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foram prestados os serviços, consoante o disposto no item 10.10 do Anexo VII-A da IN SEGES/MP nº 5/2017.

9.11.6. A critério da Administração, o CREA-SP poderá diligenciar a pessoa jurídica indicada no Atestado de Capacidade Técnica, visando obter informações sobre o serviço prestado.

9.12. **DAS DISPOSIÇÕES GERAIS DA HABILITAÇÃO**

9.12.1. A existência de restrição relativamente à regularidade fiscal e trabalhista não impede que a licitante qualificada como microempresa ou empresa de pequeno porte seja declarada vencedora, uma vez que atenda a todas as demais exigências do Edital.

9.12.2. A declaração do vencedor acontecerá no momento imediatamente posterior à fase de habilitação.

9.12.3. Caso a proposta mais vantajosa seja ofertada por microempresa, empresa de pequeno porte ou sociedade cooperativa equiparada, e uma vez constatada a existência de alguma restrição no que tange à regularidade fiscal e trabalhista, a mesma será convocada para, no prazo de 5 (cinco) dias úteis, após a declaração do vencedor, comprovar a regularização. O prazo poderá ser prorrogado por igual período, a critério da administração pública, quando requerida pelo licitante, mediante apresentação de justificativa.

9.12.4. A não regularização fiscal e trabalhista no prazo previsto no subitem anterior acarretará a inabilitação do licitante, sem prejuízo das sanções previstas neste Edital, sendo facultada a convocação dos licitantes remanescentes, na ordem de classificação. Se, na ordem de classificação, seguir-se outra microempresa, empresa de pequeno porte ou sociedade cooperativa com alguma restrição na documentação fiscal e trabalhista, será concedido o mesmo prazo para regularização.

9.12.5. Havendo necessidade de analisar minuciosamente os documentos exigidos, o Pregoeiro suspenderá a sessão, informando no “chat” a nova data e horário para a continuidade da mesma.

9.12.6. Será inabilitado o licitante que não comprovar sua habilitação, seja por não apresentar quaisquer dos documentos exigidos, ou apresentá-los em desacordo com o estabelecido neste Edital.

9.12.7. Nos itens não exclusivos a microempresas e empresas de pequeno porte, em havendo inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente.

9.12.8. Constatado o atendimento às exigências de habilitação fixadas no Edital, o licitante será declarado vencedor.

10. DO ENCAMINHAMENTO DA PROPOSTA VENCEDORA

10.1. A proposta final do licitante declarado vencedor deverá ser encaminhada no prazo de até 2 (duas) horas, a contar da solicitação do Pregoeiro no sistema eletrônico e deverá:

10.1.1. Ser redigida em papel timbrado do licitante, em língua portuguesa, datilografada ou digitada, em uma via, sem emendas, rasuras, entrelinhas ou ressalvas, devendo a última folha ser assinada e as demais rubricadas pelo licitante ou seu representante legal.

10.1.2. Apresentar a proposta de preços, devidamente ajustada ao lance vencedor, em conformidade com o modelo anexo a este instrumento convocatório.

10.1.3. Conter a indicação do banco, número da conta e agência do licitante vencedor, para fins de pagamento.

10.1.4 Inserir prazo de validade da proposta que, não será inferior a 60 (sessenta) dias, a contar da data de sua apresentação.

10.1.5 **Para fins de assinatura do futura Contrato,** informar:

a) Razão Social;

b) CNPJ, Inscrição Estadual e Municipal;

c) Endereço completo da empresa, inclusive CEP;

d) Telefone e *e-mail* do **Representante Legal, Preposto e Testemunha**;

e) Nome, número do CPF, número do RG e cargo do **Representante Legal** da empresa com poderes para assinatura do contrato;

f) Nome, número do CPF, número do RG do responsável (**Preposto**), que deverá ser mantido, aceito pelo **CREA-SP**, para representá-la na execução do contrato.

g) Nome, número do CPF e do RG do responsável **(Testemunha)**, que deverá ser mantido, aceito pelo **CREA-SP**, para representá-la na execução do contrato.

10.2. A proposta final deverá ser documentada nos autos e será levada em consideração no decorrer da execução do contrato e aplicação de eventual sanção à Contratada, se for o caso.

10.2.1. Todas as especificações do objeto contidas na proposta vinculam a Contratada.

10.3. Os preços deverão ser expressos em moeda corrente nacional, o valor unitário em algarismos e o valor global em algarismos e por extenso (art. 5º da Lei nº 8.666/93).

10.3.1. Ocorrendo divergência entre os preços unitários e o preço global, prevalecerão os primeiros; no caso de divergência entre os valores numéricos e os valores expressos por extenso, prevalecerão estes últimos.

10.4. A oferta deverá ser firme e precisa, limitada, rigorosamente, ao objeto deste Edital, sem conter alternativas de preço ou de qualquer outra condição que induza o julgamento a mais de um resultado, sob pena de desclassificação.

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

10.6. As propostas que contenham a descrição do objeto, o valor e os documentos complementares estarão disponíveis na internet, após a homologação.

11. DOS RECURSOS

11.1. Declarado o vencedor e decorrida a fase de regularização fiscal e trabalhista do licitante qualificado como microempresa ou empresa de pequeno porte, se for o caso, será concedido o prazo de no mínimo 30 (trinta) minutos, para que qualquer licitante manifeste a intenção de recorrer, de forma motivada, isto é, indicando contra qual(is) decisão(ões) pretende recorrer e por quais motivos, em campo próprio do sistema.

11.2. Havendo quem se manifeste, caberá ao Pregoeiro verificar a tempestividade e a existência de motivação da intenção de recorrer, para decidir se admite ou não o recurso, fundamentadamente.

11.2.1. Nesse momento o Pregoeiro não adentrará no mérito recursal, mas apenas verificará as condições de admissibilidade do recurso.

11.2.2. A ausência de manifestação motivada do licitante quanto à intenção de recorrer, nos termos do disposto no item “11.1”, importará na decadência desse direito, e o Pregoeiro estará autorizado a adjudicar o objeto ao licitante declarado vencedor.

11.2.3. Uma vez admitido o recurso, o recorrente terá, a partir de então, o prazo de 3 (três) dias para apresentar as razões, pelo sistema eletrônico, ficando os demais licitantes, desde logo, intimados para, querendo, apresentarem contrarrazões também pelo sistema eletrônico, em outros 3 (três) dias, que começarão a contar do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos elementos indispensáveis à defesa de seus interesses.

11.2.4. O recurso será dirigido à autoridade superior, por intermédio da que praticou o ato recorrido, a qual poderá reconsiderar sua decisão, no prazo de 05 (cinco) dias úteis, ou no mesmo prazo fazê-lo subir, devidamente informados para decisão.

11.3. O acolhimento do recurso invalida tão somente os atos insuscetíveis de aproveitamento.

11.4. Os autos do processo permanecerão com vista franqueada aos interessados, no endereço constante neste Edital.

12. DA REABERTURA DA SESSÃO PÚBLICA

12.1. A sessão pública poderá ser reaberta:

12.1.1. Nas hipóteses de provimento de recurso que leve à anulação de atos anteriores à realização da sessão pública precedente ou em que seja anulada a própria sessão pública, situação em que serão repetidos os atos anulados e os que dele dependam.

12.1.2. Quando houver erro na aceitação do preço melhor classificado ou quando o licitante declarado vencedor não assinar o contrato, não retirar o instrumento equivalente ou não comprovar a regularização fiscal e trabalhista, nos termos do art. 43, §1º da LC nº 123/2006, serão adotados os procedimentos imediatamente posteriores ao encerramento da etapa de lances.

12.2. Todos os licitantes remanescentes deverão ser convocados para acompanhar a sessão reaberta.

12.2.1. A convocação se dará por meio do sistema eletrônico (“chat”) ou e-mail de acordo com a fase do procedimento licitatório.

12.2.2. A convocação feita por e-mail dar-se-á de acordo com os dados contidos no SICAF, sendo responsabilidade do licitante manter seus dados cadastrais atualizados.

13. DA ADJUDICAÇÃO E HOMOLOGAÇÃO

13.1. O objeto da licitação será adjudicado ao licitante declarado vencedor, por ato do Pregoeiro, caso não haja interposição de recurso, ou pela autoridade competente, após a regular decisão dos recursos apresentados.

13.2. Após a fase recursal, constatada a regularidade dos atos praticados, a autoridade competente homologará o procedimento licitatório.

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

14. DA GARANTIA DE EXECUÇÃO

14.1. Não será exigida a prestação de garantia de execução para celebrar a contratação, decorrente deste certame licitatório.

15. DO TERMO DE CONTRATO OU INSTRUMENTO EQUIVALENTE

15.1. Após a homologação da licitação, em sendo realizada a contratação, será firmado Termo de Contrato ou emitido instrumento equivalente.

15.2. O adjudicatário terá o prazo de 05 (cinco) dias úteis, contados a partir da data de sua convocação, para assinar o Termo de Contrato ou aceitar instrumento equivalente, conforme o caso (Nota de Empenho/Carta Contrato/Autorização), sob pena de decair do direito à contratação, sem prejuízo das sanções previstas neste Edital.

15.2.1. Alternativamente à convocação para comparecer perante o órgão para a assinatura do Termo de Contrato ou aceite/retirada do instrumento equivalente, a Administração poderá encaminhá-lo para assinatura ou aceite, mediante correspondência postal com aviso de recebimento (AR) ou meio eletrônico, para que seja assinado e devolvido no prazo de 5 (cinco) dias, a contar da data de seu recebimento ou da disponibilização do acesso ao sistema de processo eletrônico.

15.2.2. O prazo previsto no subitem anterior poderá ser prorrogado, por igual período, por solicitação justificada do adjudicatário e aceita pela Administração.

15.3. O Aceite da Nota de Empenho ou do instrumento equivalente, emitida à empresa adjudicada, implica no reconhecimento de que:

15.3.1. Referida Nota está substituindo o contrato, aplicando-se à relação de negócios ali estabelecida as disposições da Lei nº 8.666, de 1993;

15.3.2. A Contratada se vincula à sua proposta e às previsões contidas no Edital e seus anexos;

15.3.3. A Contratada reconhece que as hipóteses de rescisão são aquelas previstas nos artigos 77 e 78 da Lei nº 8.666/93 e reconhece os direitos da Administração previstos nos artigos 79 e 80 da mesma Lei.

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

15.4. O prazo de vigência da contratação é de 36 (trinta e seis) meses, a contar da data de assinatura do Contrato, podendo ter sua duração prorrogada, limitada a 60 (sessenta) meses, em conformidade com o disposto no inciso II do Art. 57 da Lei nº 8.666/93.

15.5. Previamente à contratação a Administração realizará consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018, e nos casos do art. 6º, III, da Lei nº 10.522, de 19 de julho de 2002, consulta prévia ao CADIN.

15.5.1. Nos casos em que houver necessidade de assinatura do instrumento de contrato, e o fornecedor não estiver inscrito no SICAF, este deverá proceder ao seu cadastramento, sem ônus, antes da contratação.

15.5.2. Na hipótese de irregularidade do registro no SICAF, o contratado deverá regularizar a sua situação perante o cadastro no prazo de até 05 (cinco) dias úteis, sob pena de aplicação das penalidades previstas no Edital e anexos.

15.6. Na assinatura do contrato, será exigida a comprovação das condições de habilitação consignadas no Edital, que deverão ser mantidas pelo licitante durante a vigência do contrato.

15.7. **Deverá ainda, apresentar obrigatoriamente, na assinatura do contrato:**

15.7.1. **Comprovação de que o datacenter fornecido possuir a certificação mínima Tier III;**

15.7.2 **Comprovação de que o datacenter fornecido possui as certificações de Segurança Mínimas – ISO 27017 e 27018.**

15.8. Na hipótese de o vencedor da licitação não comprovar as condições de habilitação consignadas no Edital ou se recusar a assinar o contrato, a Administração, sem prejuízo da aplicação das sanções das demais cominações legais cabíveis a esse licitante, poderá convocar outro licitante, respeitada a ordem de classificação, para, após a comprovação dos requisitos para habilitação, analisada a proposta e eventuais documentos complementares e, feita a negociação, assinar o contrato.

16. DA SUBCONTRATAÇÃO

16.1. Os parâmetros para a subcontratação encontram-se definidos no item “15.2.2 - subcontratação” do Termo de Referência - Anexo I, deste Edital.

17. DO REAJUSTE

17.1. As regras acerca do reajuste do valor contratual estão estabelecidas no item “7.4.4 – reajuste” do Termo de Referência – Anexo I, deste Edital.

18. DO MODELO DE EXECUÇÃO DO CONTRATO E DO PROCEDIMENTO DE FISCALIZAÇÃO DA EXECUÇÃO CONTRATUAL

18.1. O modelo de execução do contrato e dos critérios do procedimento de fiscalização da execução contratual estão estabelecidos nos itens “7.1.1 – da reunião inicial do contrato” ao “7.3 – mecanismos formais de comunicação entre a contratada e a administração” e item “9 – procedimentos de fiscalização da execução contratual” do Termo de Referência – Anexo I, deste Edital.

19. DOS DEVERES E RESPONSABILIDADES DA CONTRATANTE

19.1. Os deveres e responsabilidades da Contratante são as estabelecidas no item “5 – deveres e responsabilidades da contratante” do Termo de Referência – Anexo I, deste Edital.

20. DOS DEVERES E RESPONSABILIDADES DA CONTRATADA

20.1. Os deveres e responsabilidades da Contratada são as estabelecidas no item “6 – deveres e responsabilidades da contratada” do Termo de Referência – Anexo I, deste Edital.

21. DA FORMA DE PAGAMENTO EM FUNÇÃO DOS RESULTADOS

21.1. As regras acerca do pagamento são as estabelecidas no item “7.4 – forma de pagamento em função dos resultados do item 7.4.1 até o item 7.4.3 – cronograma físico financeiro” do Termo de Referência – Anexo I, deste Edital.

21.1.1. É admitida a cessão de crédito decorrente da contratação de que trata este instrumento convocatório, nos termos do previsto na minuta contratual anexa a este Edital.

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

22. DAS SANÇÕES ADMINISTRATIVAS

22.1. Comete infração administrativa, nos termos da Lei nº 10.520, de 2002, o licitante/adjudicatário que:

22.1.1. Não assinar o termo de contrato ou aceitar/retirar o instrumento equivalente, quando convocado dentro do prazo de validade da proposta;

22.1.2. Apresentar documentação falsa;

22.1.3. Deixar de entregar os documentos exigidos no certame;

22.1.4. Ensejar o retardamento da execução do objeto;

22.1.5. Não mantiver a proposta;

22.1.6. Cometer fraude fiscal;

22.1.7. Comportar-se de modo inidôneo;

22.2. Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os licitantes, em qualquer momento da licitação, mesmo após o encerramento da fase de lances.

22.3. O licitante/adjudicatário que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

22.3.1. **Advertência por faltas leves**, assim entendidas como aquelas que não acarretarem prejuízos significativos ao objeto da contratação;

22.3.2. **Multa** de 10% (dez por cento) sobre o valor estimado do item prejudicado pela conduta do licitante;

22.3.3. **Suspensão de licitar** e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até 2 (dois) anos;

22.3.4. **Impedimento de licitar** e de contratar com a União e descredenciamento no SICAF, pelo prazo de até 5 (cinco) anos;

22.3.4.1. A Sanção de impedimento de licitar e contratar prevista neste subitem também é aplicável em quaisquer das hipóteses previstas como infração administrativa no subitem “22.1” deste Edital.

22.4. A penalidade de multa pode ser aplicada cumulativamente com as demais sanções.

22.5. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao licitante/adjudicatário, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente na Lei nº 9.784, de 1999.

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

22.7. As penalidades serão obrigatoriamente registradas no SICAF.

22.8. As sanções por atos praticados no decorrer da contratação estão previstas na Cláusula Décima Quinta da Minuta do Termo de Contrato – Anexo II, deste Edital.

23. DA VIGÊNCIA DA CONTRATAÇÃO

23.1. Será firmado contrato com cláusula de vigência de 36 (trinta e seis) meses, a contar da data de assinatura do Contrato, podendo ter sua duração prorrogada, limitada a 60 (sessenta) meses, em conformidade com o disposto no inciso II do Art. 57 da Lei nº 8.666/93.

23.2. O contrato poderá ser rescindindo nos termos e hipóteses dos arts. 77 a 80 da Lei nº 8.666/93, e suas atualizações.

24. DA IMPUGNAÇÃO AO EDITAL

24.1. Qualquer pessoa poderá impugnar os termos do Edital do pregão, por meio eletrônico, na forma prevista no Edital, até 3 (três) dias úteis anteriores à data fixada para abertura da sessão pública, conforme Decreto n° 10.024/2019.

24.2. A impugnação não possui efeito suspensivo e caberá ao Pregoeiro, auxiliado pelos responsáveis pela elaboração do Edital e dos anexos, decidir sobre a impugnação no prazo de 2 (dois) dias úteis, contado da data de recebimento da impugnação.

24.3. Acolhida a impugnação contra o Edital, será definida e publicada nova data para a realização do certame.

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

24.4. A impugnação poderá ser realizada por forma eletrônica, pelo *e-mail* compras.licitacao@creasp.org.br, ou, por petição dirigida ou protocolada no seguinte endereço: Avenida Brigadeiro Faria Lima, 1059 – 8º andar – Pinheiros – São Paulo, SP – CEP – 01452-920, na Unidade de Licitações – UL, nos dias úteis, no horário das 8h30min às 16h30min.

25. DOS PEDIDOS DE ESCLARECIMENTOS

25.1. Os pedidos de esclarecimentos referentes ao processo licitatório deverão ser enviados ao Pregoeiro, até 3 (três) dias úteis anteriores à data fixada para abertura da sessão pública, por meio eletrônico, pelo *e-mail* compras.licitacao@creasp.org.br.

25.1.1. O Pregoeiro responderá aos pedidos de esclarecimentos no prazo de 2 (dois) dias úteis, contados da data de recebimento do pedido, podendo requisitar subsídios formais aos responsáveis pela elaboração do Edital e dos anexos.

25.1.2. As respostas aos pedidos de esclarecimentos prestados pelo Pregoeiro serão entranhados nos autos do processo licitatório e estarão disponíveis para consulta por qualquer interessado, bem como serão disponibilizadas nos seguintes sistemas eletrônicos www.comprasgovernamentais.gov.br e www.creasp.org.br – Link – Institucional - Licitação e, vincularão os participantes e o CREA-SP.

26. DAS DISPOSIÇÕES GERAIS

26.1. Da sessão pública do Pregão divulgar-se-á Ata no sistema eletrônico.

26.2. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário, pelo Pregoeiro.

26.3. Todas as referências de tempo no Edital, no aviso e durante a sessão pública observarão o horário de Brasília – DF.

26.4. O licitante será responsável por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras suas propostas e lances.

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

26.5. Incumbirá o licitante acompanhar as operações no sistema eletrônico durante a sessão pública do Pregão, ficando responsável pelo ônus decorrente da perda de negócios, diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

26.6. No julgamento das propostas e da habilitação, o Pregoeiro poderá sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante despacho fundamentado, registrado em ata e acessível a todos, atribuindo-lhes validade e eficácia para fins de habilitação e classificação.

26.7. A homologação do resultado desta licitação não implicará direito à contratação.

26.8. As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.

26.9. Os licitantes assumem todos os custos de preparação e apresentação de suas propostas e a Administração não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

26.10. Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente na Administração.

26.11. O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público.

26.12. Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital.

26.13. O Edital está disponibilizado, na íntegra, no endereço eletrônico: www.comprasgovernamentais.gov.br e www.creasp.org.br no link – Institucional - Licitação, e também poderão ser lidos e/ou obtidos no endereço Avenida Brigadeiro Faria Lima, 1059 – 8° andar, Pinheiros, São Paulo, SP – CEP – 01452-920, nos dias úteis de segunda a sexta-feira, no horário das 8h30min às 16h30min, mesmo endereço e período no qual os autos do processo administrativo permanecerão com vista franqueada aos interessados.

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

26.12. Integram este Edital, para todos os fins e efeitos, os seguintes anexos:

26.12.1. ANEXO - I - Termo de Referência;

26.12.2. ANEXO - II - Modelo de Proposta de Preços;

26.12.2. ANEXO III - Minuta do Termo de Contrato.

26.12.1.2. ANEXO – III-A - Termo de Compromisso de Manutenção e Sigilo;

26.12.1.3. ANEXO – III-B - Termo de Ciência;

São Paulo, 18 de maio de 2022.

Original assinado eletronicamente
Alessandro Baumgartner
Superintendente Administrativo Financeiro
Portaria nº 15/2022

ANEXO I - TERMO DE REFERÊNCIA

INTRODUÇÃO

O presente Projeto Básico tem por objetivo descrever os elementos necessários e suficientes, com nível de precisão adequado,para subsidiar o processo licitatório, demonstrando sua viabilidade e conveniência. Seu conteúdo dependerá da natureza da solução a ser licitada, sendo mais complexo e minucioso na medida em que a contratação assim exigir. Ele será elaborado combase nas informações constantes do Estudo Técnico preliminar.

1 - OBJETO DA CONTRATAÇÃO

1.1 Contratação de serviços de hospedagem de sistemas de software e arquivos, com seus respetivos sistemas operacionais, aplicações e bancos de dados, composto por seus equipamentos (hardware), softwares, licenciamento, planejamento,instalação, migração de dados e aplicações, manutenção, comunicação de dados, suporte, operação, treinamento e gerenciamento da solução de Hospedagem.

2 - JUSTIFICATIVA E FUNDAMENTAÇÃO DA CONTRATAÇÃO

2.1 **1** Responsável pela fiscalização de atividades profissionais nas várias modalidades da Engenharia e Agronomia, o CREA-SP realiza a fiscalização, o controle , a orientação e o aprimoramento do exercício e das atividades profissionais das diversas Engenharias (Civil, Ambiental, Sanitarista, de Infraestrutura Aeronáutica, Hídrica, Elétrica, de Computação, de Telecomunicações, de Controle e Automação, Eletrônica e Eletrotécnica, Mecânica, Industrial, de Produção, de Operação, Metalúrgica, Aeronáutica, Naval, Química, de Alimentos, de Materiais, Têxtil, de Minas, de Geologia, de Agrimensura, Cartográfica, Agronômica, Florestal, Agrícola, de Pesca, de Aquicultura e de Segurança do Trabalho), além das atividades de Geologia, Geografia, Meteorologia e dos Tecnólogos de áreas correlatas.

2 Além dos profissionais do sistema registrados, como pessoas físicas, o CREA-SP também registra empresas, pessoas jurídicas, das áreas de atuação do Conselho.

3 Com atuação em todo o estado de São Paulo, o CREA-SP é composto por 4 sedes na capital e 187 unidades distribuídas por todo o estado, congregando 705 profissionais **(Funcionários, Estagiários e Aprendiz)**.

4 O CREA-SP conta com uma equipe de Agentes Fiscais, lotados em doze Regiões Administrativas de São Paulo, querealizam pesquisas, internas e externas, além das diligências que englobam obras, empresas de áreas correlatas e órgãos públicos, objetivando a verificação da regularidade de responsabilidades técnicas, da adequação às normas (técnicas e legais), melhores práticas e recomendações de fabricantes, além dos aspectos de segurança operacional. Para essas diligências, o Órgão faz uso de frota contratada de veículos, equipados com tecnologia de monitoramento eprocessamento de dados de última geração.

5 Quando da identificação de alguma irregularidade, o Conselho realiza a lavratura da Notificação e, quando necessário, o Auto de Infração, que pode dar origem a um processo administrativo, conforme a tipificação pertinente à atividade e/ou irregularidade encontrada, devendo acompanhar e manter atualizado cada um desses casos até a sua extinção definitiva, quando o caso deverá ser arquivado e mantido disponível para consulta pelo prazo legal.

6 Para o correto cumprimento de todas as suas atribuições, o CREA-SP conta com uma equipe, de funcionários e colaboradores terceirizados, com 705 profissionais (Funcionários) distribuídos na seguinte estrutura:

6.1 Estrutura Básica: responsável pela criação de condições para o desempenho integrado e sistemático das finalidades do Conselho Regional, sendo composta por órgãos de caráter decisório ou executivo, compreendendo: Plenário, Câmaras Especializadas, Presidência, Diretoria e Inspetorias;

6.2 Estrutura de Suporte: responsável pelo apoio aos órgãos da Estrutura Básica nos limites de sua competência específica, sendo composta por órgãos de caráter permanente, especial ou temporário, compreendendo: Comissões Permanentes, Comissões Especiais, Grupos de Trabalho e Órgãos Consultivos; e

6.3 Estrutura auxiliar: responsável pelos serviços administrativos, financeiros, jurídicos e técnicos, tem por finalidade prover apoio para o funcionamento da Estrutura Básica e da Estrutura de Suporte, para a fiscalização do exercício profissional e para a gestão do Conselho Regional. A Estrutura Auxiliar é coordenada, orientada e supervisionada pelas Secretarias e pelo Gabinete da Presidência, e seus serviços são executados pelas Superintendências, responsáveis pela gestão das respectivas áreas de atuação.

7 Na execução de suas atividades o CREA-SP gera e mantém um enorme volume de informações, se tornando inviável o tratamento manual deste vasto acervo informacional. Portanto, se faz necessária a utilização de infraestrutura, processos e serviços de Tecnologia da Informação e Comunicação (TIC).

8 Além disso, para suportar o seu negócio, tanto em suas atividades finalísticas, quanto em suas atividades de apoio ao negócio, é necessária a utilização de diversos sistemas de informação, que demandam gerenciamento e controle por parte de uma equipe especializada de TIC.

9 Diante do anteriormente descrito, fica evidente a dependência do Conselho em relação ao seu ambiente de TIC para o seu funcionamento e cumprimento de suas responsabilidades institucionais. Desta forma, a indisponibilidade ou queda de desempenho em qualquer dos componentes deste ambiente de TIC irá impactar no funcionamento do Órgão, com reflexo direto sobre seus tomadores de serviços e sobre a sociedade em geral.

10 Assim, objetivando minimizar impactos sobre o CREA-SP, se faz obrigatório garantir o

adequado gerenciamento doseu ambiente de TIC.

11 Como consequência natural dos elevados volumes de informação e dos também elevados volumes de transaçõesexecutadas sobre estas informações, o ambiente de TIC (por "ambiente de TIC", entende-se o conjunto formado pela infraestrutura, pelos processos e pelos serviços de TIC) do CREA-SP apresenta-se grande e complexo, exigindo uma grande quantidade de equipamentos, servidores, switches, roteadores, softwares gerenciadores de bancos de dados, aplicativos, servidores de arquivos e links de comunicação.

12 Como consequência natural dessa complexidade, existe a necessidade de um grande aparato tecnológico de infraestrutura, que hoje está distribuída, sendo uma parte atendida por serviços em Nuvem, na modalidade IaaS, e outraparte sendo atendida por infraestrutura administrada pelo próprio CREA-SP.

13 Da necessidade de aumentar o Escopo da Contratação atual

13.1 De acordo com o Estudo Técnico preliminar realizado pela equipe de planejamento, foi detectada anecessidade de aumentar o escopo da contratação anterior.

13.2 O dimensionamento realizado para atendimento das demandas do CREA-SP inclui, portanto:

13.2.1 Os serviços que já estavam sendo hospedados em Datacenter externo;

13.2.2 Os serviços que estavam sendo hospedados em servidores do próprio CREA-SP;

13.2.3 Os novos serviços planejados;

14 CONCLUSÃO

15 Levando em Consideração:

15.1 Que a contratação atual C-0049/2015, gerado pelo processo L-045/2015 será encerrado em novembro de2021, sem possibilidade jurídica de prorrogação;

15.2 Que há necessidade de adequação da infraestrutura de hospedagem do CREA-SP.

16 A conclusão que chegamos é que há necessidade de um novo ambiente de hospedagem, com serviços que garantam uma melhor operação, e gestão do ambiente de TIC do CREA-SP, sem o qual coloca-se em risco toda aoperação do Conselho.

17 Esses serviços são fundamentais para garantir a continuidade do Serviço Prestado pelo CREA-SP à Sociedade.

3 - DESCRIÇÃO DA SOLUÇÃO

3.1 DESCRIÇÃO GERAL DA SOLUÇÃO

Composição da solução

1. A Solução será composta pelos serviços conforme listados na tabela a seguir:

Tabela de Periodicidade e unidade de Mensuração

Item	Descrição	Unidade de Mensuração	Periodicidade da Execução
1	Serviço de Hospedagem em Datacenter; Composto dos Preços da Tabela A - Serviços de hospedagem.	Período	Mensal
2	Serviço de interligação conforme Tabela B - Serviços de Interligação.	Período	Mensal
3	Serviços de Gestão conforme descrito Tabela C - Serviços de Gestão.	Período	Mensal
4	Serviços de Administração e Operação conforme Tabela D - Serviços de Administração.	Período	Mensal
5	Serviço de Planejamento e instalação conforme Tabela E - Serviçosde Planejamento e Instalação.	Serviço Executado	Único
6	Serviço de Área de Armazenamento (Storage)	Período	Mensal

2. A CONTRATADA deverá atender aos requisitos técnicos especificados neste Documento.

3. A aferição da qualidade dos serviços, tanto para os continuados quanto para os projetizados, será realizada pelo CONTRATANTE, por meio da análise do cumprimento dos padrões, prazos e disponibilidade estabelecidos no Nível Mínimo de Serviço exigido.

> *Súmula 269 TCU*
>
> *Nas contratações para a prestação de serviços de tecnologia da informação, a remuneração deve estar vinculada a resultados ou ao atendimento de níveis de serviço, admitindo-se o pagamento por hora trabalhada ou por postode serviço somente quando as características do objeto não o permitirem, hipótese em que a excepcionalidade deve estar prévia e adequadamente justificada nos respectivos processos administrativos.*

4. A proposta dos serviços a serem contratados, combinada com o modelo de remuneração proposto de contratação por resultado, corroborado pelas premissas defendidas, por exemplo, pela biblioteca de melhores práticas de Gestão de Serviçosde TI, ITIL®, proporcionam a possibilidade de remuneração por resultado.

5. De forma geral, a contratação de serviços operacionais especializados em TIC vem sendo fortalecida no âmbito da Administração Pública em decorrência das normas legais, de orientações do TCU e do seu comprovado sucesso.

6. Para execução dos serviços, será implementado o método de trabalho baseado no conceito de delegação de responsabilidade. Esse conceito define o CONTRATANTE como responsável pela gestão e fiscalização do contrato, e pela atestação da aderência aos padrões de qualidade exigidos dos serviços entregues à CONTRATADA, responsável pela execução dos serviços e gestão dos profissionais a seu cargo.

7. Todos os serviços deverão ser prestados de acordo com as boas práticas de mercado e baseados na biblioteca InformationTechnology Infrastructure Library – ITIL®, no framework de governança COBIT® 5, no padrão ISO/IEC 20.000, nas práticas ágeis (Scrum, Lean, Kanban, etc.), e nas melhores práticas de gerenciamento de projetos reunidas no PMBok, incluindo práticas ágeis adotadas em sua mais recente edição.

8. A CONTRATADA deve possuir capacitação técnica mínima para atender em plenitude a execução dos serviços demandados, sendo sua atribuição o dimensionamento da equipe responsável pela prestação das atividades a serem desempenhadas, considerando a volumetria de recursos computacionais de TIC e dos serviços executados.

3.2 DESCRIÇÃO GERAL DOS SERVIÇOS

3.2.1 SERVIÇOS DE HOSPEDAGEM

1 Compreende todos os serviços e produtos necessários para hospedar os servidores do CREA-SP, com seus bancosde dados, Aplicações, Programas e Sistemas Operacionais no Datacenter da Empresa Contratada, conforme especificados e quantificados descritos na Tabela A - Serviços de hospedagem.

3.2.2 SERVIÇOS DE PLANEJAMENTO

1 Compreende todos os serviços necessários para planejar, e migrar o ambiente atual do CREA-SP para o ambienteda Empresa CONTRATADA, conforme quantificados e especificados na Tabela E - Serviços de Planejamento e Instalação.

3.2.3 SERVIÇOS DE INTERLIGAÇÃO

1 Compreende todos os serviços, softwares e produtos necessários para interligar o Datacenter de Hospedagem àRede do CREA-SP, conforme especificados e quantificados na Tabela B - Serviços de Interligação.

3.2.4 SERVIÇOS DE ADMINISTRAÇÃO e OPERAÇÃO

1 Compreende todos os serviços necessários para administrar e operar o ambiente proposto, conforme especificado equantificado na Tabela D - Serviços de Administração e Operação.

3.2.5 SERVIÇOS DE GESTÃO

1 Compreende todos os serviços necessários para fornecer informações de Gestão ao CREA-SP, sobre o andamento dos demais serviços e soluções que fornecidos pela CONTRATADA, conforme especificados e quantificados na TabelaC - Serviços de Gestão.

3.2.6 SERVIÇOS DE ÁREA DE ARMAZENAMENTO (STORAGE)

1 Área de Armazenamento e storage incluindo:

1.1 Storage produção

1.2 Storage de Backup

1.3 Storage DB2

2 Conforme descritos e quantificados no item Requisitos de Armazenamento.

4 - ESPECIFICAÇÃO TÉCNICA

4.1 REQUISITOS DE HOSPEDAGEM

1. A CONTRATADA deverá disponibilizar, em modalidade *Hosting*, devidamente acondicionados conforme descrição,equipamentos com as seguintes características mínimas.

Tabela A - Serviços de hospedagem:

Item	**Descrição**	**Qtd**	**Unidade deMedida**
1	Hosting com Serviço de Virtualização com sistema de gerenciamento gráfico via web, com as devidas licenças Calculadas pela CONTRATADA, de acordo com o hardware fornecido para atender o ambiente vCloud, item8 desta tabela.	1	Licenciamento
2	Licenciamento do SO Windows Server Data Center, fornecido por Core, sem a necessidade de cobrança doshosts virtuais instalados no ambiente virtual. Calculado de acordo com os servidores utilizados para oserviço de Hosting.	1	Licenciamento
3	Licenciamento Banco de Dados IBM DB2;	1	Licenciamento
4	Licenciamento Banco de Dados MS SQL ServerEnterprise;	4	licença para 02Cores
5	Licenciamento Banco de Dados MS SQL ServerStandard;	8	licença para 02Cores
6	Certificado Wildcard	1	Certificado Digital para 3 anos
7	Hosting para sistema Operacional IBM AIX;	1	Servidor Físico
8	Ambiente de VCloud composto pelos servidores físicos,de acordo com os Requisitos de Sistema de Virtualização	1	Ambiente
9	Serviços de segurança; (Firewall, IPS/IDS, WAF, Gerenciamento de vulnerabilidades e ameaças, Cofre deSenhas para 10 usuários), conforme descrito no itens REQUISITOS GERAIS DE SEGURANÇA	1	Serviço
10	SIEM (Sistema de informações e eventos de segurança).conforme descrito no item REQUISITOS DE GERENCIAMENTO DE DE EVENTOS DE SEGURANÇADA INFORMAÇÃO (SIEM)	150 GB/dia	Serviço

11	Load Balancer, conforme descrito no item Requisitos de Balanceamento de Carga Local	1	Serviço
12	Serviço de Backup e Restauração	1	Serviço
13	Rede de Comunicação TCP/IP, conforme descrito no itemrequisitos de comunicação	1	Rede

4.2 REQUISITOS DE INTERLIGAÇÃO

Tabela B - Serviços de Interligação

Item	Descrição	Largura de banda	Qtde
1	Link de Fibra óptica Redundante (Sistema Ativo/Ativo com balanceamento de Carga)	10 Gbps, dedicado, full duplex	1
2	Banda IP (fornecida através de um link redundante comcapacidade de 200Mbps);	200 Mbps, dedicado, full duplex	1

1 A CONTRATADA deverá fornecer os seguintes links de comunicação:

1.1 Link de Acesso à internet redundante partindo do centro de processamento da CONTRATADA.

1.1.1 A capacidade inicial do link será de 200 Mbps.

1.2 Links de Fibra dedicado entre a sede da CONTRATANTE (São Paulo) e CONTRATADA.

2 Planejamento e Instalação

2.1 A CONTRATADA deve planejar e acompanhar a instalação e provisionamento dos links de comunicação,conforme especificado no item REQUISITOS DE PLANEJAMENTO

3 Operação

3.1 A CONTRATADA deve realizar a operação dos Links de comunicação conforme descrito no item REQUISITOSDE OPERAÇÃO

4 Suporte e Gestão de Incidentes

4.1 A CONTRATADA deve realizar o suporte e gestão de incidentes dos links de comunicação conforme descritono item REQUISITOS DE SUPORTE E GESTÃO DE INCIDENTES

5 Manutenção

5.1 A Contratada deve realizar a manutenção preventiva e corretiva dos links de comunicação conforme descritono item RREQUISITOS DE MANUTENÇÃO

6 Disponibilidade dos Links

6.1 Os Links de interligação devem ser fornecido no Site do CREA à Avenida Brigadeiro Faria Lima, 1059.

6.2 O link de internet deve ser fornecido no Local do Datacenter remoto, da CONTRATADA.

6.3 A disponibilidade Geral Mensal de ambos e cada um dos Links individuais deve ser de 99,99%.

6.4 Ambos os links fornecidos devem ser redundantes.

6.5 Características do Link de interligação entre o Datacenter e o CREA-SP

6.5.1 O link deve ser de Fibra óptica, composto por dois enlaces, sendo um redundante do outro.

6.5.2 Cada um dos enlaces deve seguir um encaminhamento diferente entre as duas localidades (O CREA e oDatacenter da CONTRATADA).

6.5.3 No Site do CREA, cada um dos enlaces deve entrar por entradas diferentes. O link principal entrando pelaRua Teodoro Sampaio e o Link Redundante pela Av. Brigadeiro Faria Lima.

6.6 A CONTRATADA deve se gerenciar a disponibilidade dos links de comunicação conforme descrito no itemREQUSITOS DE NIVEL DE SERVIÇO

6.7 A CONTRATADA deve fornecer relatório de disponibilidade mensal, conforme especificado no itemREQUISITOS DE RELATÓRIOS

7 Gerenciamento dos Links

7.1 A CONTRATADA deve realizar o gerenciamento de operação dos links, sendo responsável por:

7.2 Monitoramento, detecção e recuperação de falhas conforme especificado no item REQUISITOS DEGERENCIAMENTO

4.3 REQUISITOS DO SERVIÇO DE GESTÃO

Tabela C - Serviços de Gestão

Item	Descrição	Qtde	Unidade	Periodicidade
1	Serviço de Supervisão da Solução	1	Serviço	Apuração mensal
2	Serviço de Relatórios de Gestão	1	Serviço	Apuração Mensal

1 A Gestão da solução compreende dois sub Serviços, a supervisão da solução de a emissão de todos os relatóriosgerenciais necessários.

2 A CONTRATADA deverá fornecer, no mínimo os seguintes entregáveis e atividades:

2.1 Relatórios mensais de Gestão, conforme especificado no item REQUISITOS DO SERVIÇO DE RELATÓRIOSDE GESTÃO.

2.2 Atividades de planejamento para atender a novas necessidades.

2.3 Atividades de planejamento de mudanças.

2.4 Atividades de planejamento de atualizações dos sistemas.

4.3.1 REQUISITOS DO SERVIÇO DE SUPERVISÃO DA SOLUÇÃO

1 A Contratada deverá fornecer no mínimo um profissional devidamente qualificado para prestar aos serviços deSupervisão do Ambiente CONTRATADO.

2 O profissional deverá trabalhar em conjunto com a administração do CREA-SP no atendimento das demandasrelacionadas à administração, operação do ambiente contratado.

3 Responsabilidades mínimas do Profissional Supervisor de Gestão:

0.1 Coordenar os trabalhos dos demais profissionais da contratada responsáveis pela Administração e operaçãodos Serviços CONTRATADOS.

0.2 Fazer a conexão entre os profissionais do CREA e os profissionais da CONTRATADA.

0.3 Monitorar e Gerenciar todas as demandas do CREA, garantindo que sejam atendidas dentro dos Níveis deserviço previamente contratados.

0.4 Elaborar e entregar os Relatórios de Gestão conforme especificados.

0.5 Coordenar os trabalhos de Gestão de Mudanças

0.6 Coordenar os trabalhos de Gestão de atualizações dos sistemas

4 Capacitação mínima do Profissional Supervisor de Gestão

0.1 O profissional designado pela empresa CONTRATADA para realizar tal função deverá possui certificação emitida pelo Project Management Institute com validade adequada para acompanhar toda a vigência contratual.

0.2 O profissional designado pela empresa CONTRATADA para realizar tal função deverá possuir vínculo empregatício com a mesma, comprovado em Carteira de Trabalho e Previdência Social, com registro vigente em função adequada para realizar a supervisão.

0.3 O profissional designado pela empresa CONTRATADA para realizar tal função deverá

possuir experiência em funções relacionadas a infraestrutura de Data Centers e já deve ter participado de pelo menos um projeto de porte semelhante.

0.4 A qualquer momento durante a vigência do Contrato a empresa CONTRATADA deverá apresentar os documentos comprobatórios dos requisitos 0.1, 02.e 03. acima, se requisitado pela CONTRATANTE.

4.3.2 REQUISITOS DO SERVIÇO DE RELATÓRIOS DE GESTÃO

1 Todos os Relatórios solicitados devem possuir os itens mínimos requeridos. Caso não haja informação útilpara um determinado item, a CONTRATADA deve informar que aquele item não tem informações relevantes.

Exemplo:

2 O Relatório de Segurança requer que haja uma análise conclusiva do sistema de ameaças. No entanto, num determinado mês, não foi detectada nenhuma ameaça. Nesta situação a CONTRATADA, ao invés de suprimir o Item Conclusão, do relatório, deve informar nesta conclusão, que naquele mês não há dados para serem analisados.

3 É responsabilidade da CONTRATADA levantar e compilar todas as informações necessárias para execução dosrelatórios.

4 Todos os relatórios devem ser entregues no formato .pdf e/ou docx. Não serão aceitos em hipótese nenhuma,relatórios em sistemas web, ou qualquer outro formato.

5 A CONTRATADA deve apresentar mensalmente um book (pode ser no formato digital) contendo no mínimo osSeguintes Relatórios:

6 Relatórios de Gestão de Incidentes

6.0.1 A empresa CONTRATADA deverá apresentar mensalmente relatório contendo todos os chamados abertos pelo CREA-SP, os tempos de reação, tempos de atendimento, assertividade, no formato da TABELAde NMS de OPERAÇÃO.

6.0.2 O Relatório deverá conte a lista dos problemas que ainda não possuem solução.

6.0.3 O relatório deverá apresentar um plano de ação para solucionar os problemas recorrentes ou semsolução por mais de um mês.

6.0.4 O CREA-SP resguarda-se o direito de elaborar seus próprios relatórios para fins de auditoria efiscalização dos fornecidos pela contratada.

7 Relatórios de Manutenção

7.0.1 A Contratada deverá apresentar um relatório mensal contendo as datas e atividades de manutençãopreventiva e/ou corretiva que foram realizados no Ambiente contratado, tanto no Serviço de Hospedagem, quanto no Serviço de Redundância.

7.0.2 O Relatório deve apresentar uma conclusão apontando ações necessárias para corrigir possíveisproblemas encontrados durante as manutenções programadas

8 Relatórios de Gestão

8.1 A Contratada deve apresentar um relatório mensal com a relação de todos os serviços de Gestão realizados,sua descrição, os problemas solucionados, os problemas não solucionados

8.2 O Relatório deve conter o consumo dos recursos (storage, disco, memória, cpu, rede) utilizados nos serviçosde hospedagem

8.3 O Relatório apresentado deve ser conclusivo (com conclusão), apresentando possíveis ações para corrigirproblemas encontrados.

9 Relatório de Segurança

9.0.1 A CONTRATADA deverá apresentar relatório de segurança do sistema contratado.

9.0.2 O relatório de segurança deverá conter o relatório de vulnerabilidades e ameaças do sistema contratado,incluindo os servidores virtuais do CREA-SP.

9.0.3 Qualquer plano de ação apresentado deve discriminarem diferentes classes quais ações são de Responsabilidade do CREA-SP e quais ações são de responsabilidade de CONTRATADA, bem como classificar as ações em solução remediadora, ou solução definitiva.

9.0.4 O Relatório deve conter, no mínimo, mas não se limitando os seguintes itens:

9.0.4.1 a) Análise Conclusiva da situação de segurança do sistema de hospedagem.

9.0.4.2 b) Plano de Ações que devem ser realizadas para corrigir e/ou melhorar a situação de segurança.

9.0.4.3 c) Análise Conclusiva da situação de disponibilidade do sistema.

9.0.4.4 d) Plano de Ações que devem ser realizadas para corrigir e/ou melhorar a situação de disponibilidade

9.0.4.5 e) Informações detalhadas sobre as ameaças encontradas pelo sistema de IDS (Intrusion Detection System), IPS (Intrusion Prevent System) e gerenciamento de Vulnerabilidades.

9.0.4.6 f) Análise conclusiva das ameaças que foram detectadas pelos sistemas de IDS, IPS e Gerenciamento do Vulnerabilidades, com informações necessárias para identificar se alguma das ameaçasapresenta risco eminente para o sistema

9.0.4.7 g) Plano de Ações que devem ser realizadas para corrigir/remediar/mitigar possíveis riscos

9.0.4.8 h) Informações detalhadas sobre possíveis vulnerabilidades, com classificação das

mesmas em CRÍTICA, ALTA, MÉDIA e BAIXA

9.0.4.9 i) Análise conclusiva das Vulnerabilidades do sistema, informado quais delas representam riscoreal a segurança.

9.0.4.10 j) Plano de ações para corrigir/remediar/mitigar as vulnerabilidades que representam risco real àsegurança.

10 Relatórios de Operação

10.0.1 A CONTRATADA deverá apresentar relatório técnico conclusivo de todas as GMUDS realizadasdurante o período de execução vigente;

11 Relatórios de Instalação

11.0.1 A CONTRATADA deverá apresentar Relatório técnico conclusivo de todas as ordens de serviçoexecutadas;

11.0.2 Os relatórios de instalação deverão conter no mínimo as seguintes informações:

11.0.3 a) As Built contendo:

11.0.4 Desenhos de topologia lógica e física.

11.0.5 Diagramas esquemáticos e comprovações através de fotos.

11.0.6 Senhas e usuários utilizados na instalação.

11.0.7 Endereços IP, MAC, etc. utilizados.

11.0.8 Detalhes de interligação física e lógica.

11.0.9 Pendências, contendo no mínimo

11.0.9.1 Descrição da pendência, contendo o motivo dela existir e quais fatores foram responsáveis pelanão conclusão das atividades que deram origem à referida pendência.

11.0.9.2 Responsável pela resolução da pendência

11.0.9.3 Prazo

11.0.9.4 Plano de ação contendo as atividades que serão realizadas com seus respectivos prazos eresponsáveis.

12 Relatório de Disponibilidade dos Links de Comunicação

12.1 A CONTRATADA deverá apresentar o Relatório Mensal de Interrupções (RMI)

12.2 A CONTRATADA deverá prover relatório estatístico demonstrando a utilização dos links de comunicaçãocom a Internet;

12.3 A CONTRATADA deverá prover relatório estatístico demonstrando a utilização dos links de interligaçãoentre o Datacenter e o CREA-SP;

13 Relatório de consumo de banda

13.1 A CONTRATADA deverá apresentar o relatório mensal de consumo de banda dos links contratados.

13.2 O Relatório deve apresentar graficamente o consumo diário entrante e sainte do período de execuçãovigente.

14 Caso julgue NECESSÁRIO, a CONTRATADA pode adicionar itens e relatórios ao book mensal, sempredescrevendo detalhadamente qual a função e benefício do relatório apresentado

15 A Liberação do Pagamento Mensal ficará atrelada ao Recebimento dos Relatórios Mensais pelo CREA-SP.

16 O Fiscal do Contrato, no CREA-SP será o responsável por receber os Relatórios e liberar os pagamentos.

4.4 REQUISITOS GERAIS

1 A CONTRATADA deverá disponibilizar, em modalidade Hosting, devidamente acondicionados conforme descrição,equipamentos com as seguintes características mínimas:

1.1 A CONTRATADA deverá fornecer servidores e sistemas de armazenamento, com conectividade redundante entre eles, para instalar os aplicativos e bases de dados do CREA-SP. A CONTRATADA deverá possuir servidores distintos desses, dedicados aos serviços internos do Datacenter.

1.2 Todos os servidores deverão ter seus relógios sincronizados por uma solução de hardware e software quereflita a hora oficial do Brasil.

1.3 Os servidores deverão ser otimizados para rack, escaláveis e de alta disponibilidade para execução dos respectivos sistemas operacionais e aplicativos. Deverão ter administração remota, redundância em seus itensprincipais, tais como: comunicação com a rede e com o sistema de armazenamento, fontes e ventiladores.

1.4 Os hardwares propostos deverão consolidar os ambientes operacionais existentes no CREA-SP e suportar as versões mais recentes disponíveis no mercado, manter a compatibilidade binária dos aplicativos e ser homologadospelos fabricantes e desenvolvedores dos respectivos sistemas operacionais.

1.5 Sistema de fitoteca robotizado, tape library, com drives de gravação e leitura compatíveis com os comercializados atualmente no mercado de informática, com agentes de software para os sistemas operacionais ebanco de dados.

1.6 Não será aceita entrega de servidores não auditados pelo SPEC – Standard

Performance EvaluationCorporation no índice SPECint_rate_base2006.

4.4.1 REQUISITOS GERAIS DA INFRAESTRUTURA DO DATA CENTER

1 Para atender às necessidades do CREA-SP, são exigidas determinadas características mínimas quanto à Infraestrutura de Data Center da CONTRATADA. Portanto, segue a descrição da infraestrutura e característicasrequeridas do Data Center, que o classificam como sendo de Classe Mundial.

2 O Data Center deverá possuir infraestrutura que atenda, no mínimo, aos requisitos especificados abaixo para fins devistoria e homologação pela equipe técnica do CREA-SP.

3 A CONTRATADA deverá disponibilizar e ser responsável pela supervisão do ambiente físico da infraestrutura de Data Center, com monitoramento remoto via TCP/IP, garantindo que atenda às especificações de rede local, suprimento de energia, climatização, proteção contra incêndio e segurança física em regime de tempo integral, 24 x7, entre outros.

4 Para fins de alto desempenho da conectividade, a distância geodésica entre a sede do CREA-SP e do Data Center não poderá ser superior a 150 Km, permitindo, dessa forma o acompanhamento e supervisão das atividades técnicas por parte dos especialistas em TI do CREA-SP.

0.1 A Empresa contratada deverá permitir a visita às dependências do Datacenter contratado sempre que solicitada dos Analistas de T.I. do CREA-SP previamente cadastrados para fins de acompanhamento técnico das atividades, fiscalizações, auditorias e outras atividades técnicas durante toda a vigência do contrato e principalmente durante o processo de migração das soluções, no qual esse acompanhamento deve constar do plano de implantação.

4.4.1.1 REQUISITOS GERAIS DE INSTALAÇÃO FÍSICA DO DATACENTER DA CONTRATADA

1 O Data Center deverá ter estrutura física adequada aos serviços de hosting, de modo a garantir um ambiente seguro e controlado.

2 Ter instalado piso elevado e sistema de cabeamento estruturado em níveis distintos para cabos elétricos e dedados.

3 Possuir sistema de segurança, climatização, quadros de distribuição elétrica, suprimento ininterrupto de energiaelétrica, proteção contra descargas atmosféricas, indução eletromagnética e aterramento.

4 Possuir ambientes definidos para computadores, sistemas de armazenamento, rede, administração predial,NOC, SOC e sala para clientes.

5 Fornecer cofre para fitoteca com controle de acesso 24 horas por dia, para armazenamento das fitas de backup,com proteção para riscos de incêndio, calor, água, gases corrosivos, tóxicos e magnetismos.

6 Caso o armazenamento das fitas seja em instalações prediais distintas da sala destinada à produção, tais instalações deverão respeitar as mesmas características descritas neste documento.

4.4.1.2 REQUISITOS DE SEGURANÇA FÍSICA

1 Possuir metodologia para classificação e controle de ativos e de acessos ao ambiente do Data Center.

2 Acondicionar equipamentos e mídias geradas no ambiente do Data Center, livres de riscos físicos.

3 Manter sempre disponíveis pessoas dedicadas, treinadas e responsáveis pela vigilância dos ambientes internose externo, segurança de acesso ao prédio e controle de entrada e saída de veículos.

4 Possuir rígido controle de acessos aos equipamentos do Data Center.

5 Disponibilizar mecanismos efetivos de controle de entrada e saída de pessoas, que acessam ou façam uso doData Center, com leitores biométricos, cartões magnéticos e senhas individuais, bem como manter registros passíveis de posterior pesquisa.

6 Possuir travas eletrônicas que, de acordo com a política de segurança estabelecida para o Data Center, o separe em regiões com níveis de restrição diferenciados.

7 Eventuais tentativas de acesso indevido devem ser monitoradas, verificadas e registradas para posteriorpesquisa.

8 Utilizar Sistema de Gerenciamento de CFTV, que viabilizem o rastreamento de pessoas dentro do Data Center ecujas imagens possam ser recuperadas.

9 Disponibilizar relatórios das visitas ao Data Center por representantes do CREA-SP.

4.4.1.3 REQUISITOS DE ENERGIA ELÉTRICA

1 Possuir sistema de energia totalmente gerenciado, com circuitos e quadros redundantes, com sistema deproteção e aterramento de acordo com a norma ANSI TIA J-STD-607_A.

2 Garantir total independência no suprimento de energia elétrica para a eventualidade de falta prolongada na rededa concessionária local.

3 Possuir sistema redundante de UPSs para garantir a transição entre o fornecimento normal de energia e o grupogerador.

4 Possuir solução de grupo motor gerador (GMG), redundante e independente, com acionamento automático na eventualidade de interrupção no fornecimento de energia. O grupo gerador deverá possuir combustível suficiente para, pelo menos, 48 (quarenta e oito) horas de operação assumindo todo o ambiente necessário à prestação dosserviços.

5 Garantir alimentação elétrica independente para os setores de computadores e áreas administrativas.

6 Possuir os componentes necessários que garantam autonomia plena de energia elétrica para o Data Center emregime de tempo integral.

7 Deverá possuir réguas de alimentação do tipo PDU (power distribution unit) redundantes por rack.

4.4.1.4 REQUISITOS DE CLIMATIZAÇÃO

1 Possuir sistema de climatização e renovação de ar de modo a garantir o correto condicionamento térmico dosequipamentos.

2 Manter a temperatura e a umidade relativa do ar controlada dinamicamente dentro dos níveis recomendados.

3 Ter sistema redundante com disponibilidade de equipamentos igual a, pelo menos, N + 1.

4 O sistema deve possuir filtros de poeira e abafador de ruído.

5 Fornecer os componentes necessários que garantam o controle da temperatura de todo o ambiente deprodução ideal e constante.

4.4.1.5 REQUISTOS DE PROTEÇÃO CONTRA INCENDIO

1 O sistema de detecção e combate a incêndios deve abranger todo o Data Center, incluindo as seguintes áreasfísicas:

1.1 Sala de Produção;

1.2 Almoxarifados e locais de carga e descarga de mercadorias;

1.3 Administrativas;

1.4 Hardwares de rede e computação;

1.5 Abaixo do piso elevado;

1.6 Produção e distribuição de energia elétrica;

1.7 Depósito de combustíveis e

1.8 Ar condicionado.

2 Possuir dispositivos de detecção precoce de incêndio pela análise do superaquecimento de cabos ou hardwaresque sejam de maior sensibilidade que os tradicionais detectores de fumaça.

3 Possuir sistema de detecção de incêndio por sensores termovelocimétricos para os ambientes de servidores ede armazenamento de dados.

4 Possuir dispositivos tradicionais de prevenção e combate a incêndio, tais como: extintores manuais e detectoresde fumaça.

5 Possuir brigada de incêndio especializada em prevenção e combate a incêndio em regime 24x7.

6 Disponibilizar mecanismos automáticos de extinção de fogo por agentes gasosos não poluentes – como o FE227com ação baseada na quebra de moléculas de oxigênio – que não danifiquem os equipamentos eletroeletrônicos e sejam inertes e não tóxicos aos seres humanos.

7 Possuir os componentes de segurança necessários para garantir a preservação dos dados em casos de incêndioe execução de plano de recuperação de catástrofes.

4.4.2 REQUISITOS GERAIS DE NÍVEL DE SERVIÇO MÍNIMO (NMS)

1 Para cada tipo de serviço deve haver um NMS correspondente, cujo não atendimento pode ser penalizado aCONTRATADA com multas e descontos nos pagamentos mensais.

2 Há duas formas de abertura de chamados:

2.1 Os chamados automáticos

2.1.1 O sistema de Monitoramento/proatividade deve ao detectar uma falha, imediatamente abrir um chamadona contratada dentro dos tempos mínimos especificados.

2.1.2 A severidade/criticidade dos chamados automáticos será negociada e ajustada entre a CONTRATADA ea CONTRATANTE baseado nos tipos de problema e na tabela de níveis mínimos de serviço.

2.2 Os chamados abertos pelos colaboradores do CREA-SP ou da CONTRATADA.

3 Tempo de Proatividade refere-se ao tempo decorrente entre a detecção da falha/solicitação de abertura e aefetivação da abertura do chamado.

4 Tempo de resposta refere-se ao tempo decorrente entre a abertura do chamado e o contato telefônico (não é contabilizado contato por e-mail, SMS ou outro meio de mão única) entre a contratada e o analista do CREA-SP.

5 Tempo de solução é o tempo decorrido da abertura do chamado até a solução de contorno ou definitiva;

6 Solução de contorno entende se por uma solução temporária que restaure a funcionalidade perdida de forma queos efeitos do problema não sejam mais percebidos pelos usuários.

7 Solução definitiva entende-se pela solução que sanará a causa do problema.

8 Nas situações em que for detectado e/ou comprovado um problema de firmware (bug) na solução ofertada, o prazo de atendimento será fornecido diretamente pela engenharia do fabricante da solução ofertada.

9 Assertividade é a medida da quantidade de chamados atendidos dentro do NMS;

10 Em caso de a assertividade não ser cumprida o CREA-SP solicitará desconto no pagamento mensal idêntico à porcentagem de descumprimento do NMS. Por Exemplo: se a assertividade for 80% em algum item o CREA descontará 10% no pagamento da mensalidade, que corresponde a diferença entre a assertividade contratada e a fornecida.

11 NMS de Gestão

11.1 Os Relatórios devem ser entregues até o quinto dia útil de cada mês.

11.2 A CONTRATADA deverá entregar, no mínimo, todos os relatórios solicitados no termo de referência.

4.4.2.1 1 NMS de Operação

1.1 O NMS de operação cobre os serviços de Gestão de incidentes, tickets, ou chamados abertos pelaCONTRATANTE na central de Atendimento da CONTRATADA.

1.2 Para o NMS de atendimento aos Incidentes, os tempos de início de atendimento e resposta,deverão estar dentro dos padrões estabelecidos no quadro abaixo:

TABELA de NMS de OPERAÇÃO

Severidade	Definição	Início do Atendimento/Tempo de Proatividade	Tempo de Resposta	Tempo de Solução	Assertividade
Emergencial	Solicitações oriundas do CREA-SP, com nível de severidade independente da criticidade do problema. A severidade é definida pela administração do CREA como Emergencial.	Até 05 minutos	Até 30 Minutos	Até 04 horas	95%
Crítica	Queda total, parcial ou degradação do serviço que comprometa a continuidade das operações e não exista alternativas para restabelecer o serviço.	Imediato	Até 10 minutos	Até 04 horas	95%

Alta	Queda parcial ou degradação do serviço que não afete em sua totalidade a capacidade de continuar as operações e não exista alternativas para restabelecer o serviço.	Até 30 minutos	Até 15 minutos	Até 06 horas	95%
Média	Queda parcial ou degradação do serviço quenão afete as operações ou provoque falhas de gravidade Crítica ou Alta. Existe meio alternativo para restabelecer o serviço.	Até 1 hora	Até 1 horas	Até 12 horas	95%
Baixa	Não existe impacto negativo na operação.	Até 2 horas	Até 2 horas	Até 24 horas	95%
Programado	Atividades Programadas GMUDS	n/a	Até 06 horas	Até 24 horas	99%

4.4.2.2 NMS ESPECÍFICOS

Tabela de NMS específicos

Nome	Descrição	Valor	Frequência	Assertividade(%)
Disponibilidadedos Servidores	A porcentagem de tempo que os servidor está disponível para operações normais de negócios.	Servidor Disponível	Mensal, Medido por servidor / nível de sistema	99.90
Gerenciamentode patches de segurança	A quantidade de tempoque a CONTRATADA deve levar para corrigir os servidores para fins de segurança.	Patches concluídos em 24 horas após a aprovação do CREA-SP;	Mensal	99.0
Ocorrência -Backup de dados	Porcentagem de tempoque os backups são executados no prazo e sem erros e omissões.	Backups concluídos com sucesso dentro da janela de backup identificada	Mensal	99,50
Ocorrência —Data Restore	Duração para iniciar a restauração de dados	Dentro de 4 horas após a mídia estar no local e restauração 100% bem- sucedida	Mensal	95,0
Provisionamentode servidor	Tempo necessário para provisionar os requisitos de servidor necessários, conforme solicitado pela organização.	Servidores concluídos dentro do período de tempo de 4 horas.	Mensal	95,00

Provisionamentode armazenamento	Tempo necessário para provisionar os requisitos de servidor necessários, conforme solicitado pela organização.	Provisionamento concluídos dentro do período de tempo de 4horas.	Mensal	95,00
Provisionamentode DNS	Tempo necessário para provisionar alterações no DNS	Provisionamento concluídos dentro do período de tempo de 4horas.	Mensal	95,00
Provisionamentode Regra de Firewall	Tempo necessário para provisionar alterações na configuração do Firewall	Provisionamento concluídos dentro do período de tempo de 4horas.	Mensal	95,00

4.4.2.3 NMS DE REDE

1 Considera-se WAN os links com a Internet e os links de interligação entre o Datacenter da CONTRATADA e oCREA-SP, os demais enlaces são considerados como LAN para termos de medição.

2 Operações e manutenções programadas pela CONTRATADA entram na conta como indisponibilidade.

3 A disponibilidade mensal dos links deve ser apresentada no RMI (Relatório Mensal de Interrupções).

4 Entende-se como primeira milha o seguinte site: https://www.speedtest.net/ ou outro que deve ser acordadoentre as partes, na sua ausência.

Tabela de NMS de Rede

Nome	Descrição	Valor	Frequência	Assertividade(%)
DisponibilidadeWAN	Porcentagem de tempo que a WAN está disponível para uso	Link disponível	Mensal Medido no nível de link;	99,99 (link redundante) 99,9 (Link principal)
DisponibilidadeLAN	Porcentagem de tempo que a LAN está disponível para uso	equipamento disponível	Mensal Medido a nível de equipamento (switch, roteador, etc.)	99,99

Desempenho de rede / WAN	Métricas relacionadas à latência, perda de pacotes e velocidade	Entrega de pacotes	Mensal, medido na primeira milha para links de internet e entreo Switch Core do CREA-SP para o link de interligação entre o Datacenter da CONTRATADA e o CREA-SP	99 a 99,99
		latência máxima entre 50 e 70 ms	Mensal. Medido na primeira milha para links de internet.	99,99
		latência máxima entre 10 e 20 ms	Mensal. Medido entre o switch dos servidores o Switch Core do CREA-SP para o link de interligação entre o Datacenter da CONTRATADA e o CREA-SP	99,99
		velocidade do link dentro de 5% de variância da velocidade contratada	Mensal, medido na primeira milha para links de internet	99
			Mensal, para o link de interligação entre o Datacenter da CONTRATADA e o CREA-SP.	99

4.4.2.4 NMS DE SEGURANÇA

1 1. Para mais detalhes dobre o sistema de segurança verifique o ITEM **REQUISITOS GERAIS DE SEGURANÇA.**

2 Níveis de gravidade para problemas de segurança:

Severidade	Definição

Crítica	Vulnerabilidades com pontuação na faixa crítica geralmente têm amaioria das seguintes características: -A exploração da vulnerabilidade provavelmente resulta no comprometimento de nível root/admin de servidores ou dispositivos deinfraestrutura. -A exploração é geralmente direta, no sentido de que o invasor nãoprecisa de nenhuma credencial de autenticação especial ou conhecimento sobre vítimas individuais, e não precisa persuadir um usuário alvo, por exemplo, por meio de engenharia social, a realizar nenhuma função especial.
Alta	Vulnerabilidades com pontuação alta geralmente têm algumas dasseguintes características: -A vulnerabilidade é difícil de explorar. -A exploração pode resultar em privilégios elevados. -A exploração pode resultar em perda significativa de dados ou tempo de inatividade.
Média	Vulnerabilidades com pontuação média geralmente têm algumas dasseguintes características: -Vulnerabilidades que exigem que o invasor manipule vítimas individuaispor meio de táticas de engenharia social. -Vulnerabilidades de negação de serviço que são difíceis de configurar. -Explorações que exigem que um invasor resida na mesma rede local davítima. -Vulnerabilidades onde a exploração fornece acesso muito limitado. -Vulnerabilidades que requerem privilégios de usuário para umaexploração bem-sucedida.
Baixa	Vulnerabilidades na faixa baixa geralmente têm muito pouco impacto nos negócios de uma organização. A exploração de tais vulnerabilidades geralmente requer acesso ao sistema local ou físico.

Tabela de NMS de Segurança

Nome	Descrição	Valor	Frequência	Assertividade (%)
Disponibilidade de componentes de segurança	Porcentagem de tempo disponível planejado para componentes de segurança	equipamento disponível	Mensal, observação - medido no componente individual	99,99
Taxa de atualização de caso de uso de SIEM	Porcentagem de casos de uso de SIEM atualizados a cada mês. O objetivo é que o fornecedor crie novos casos deuso e / ou analise / atualize os casos de uso existentes dentrodo SIEM para garantir a vigência	número total de casos de uso no SIEM atualizado a cada mês	Mensal	acima de 10,0
Notificações de Ameaça	Porcentagem de ameaças suspeitas críticas / altas comunicadas dentro do período de tempo identificado	dentro de 30 minutos (crítico); 1 hora (alta)	Mensal	95.0
Resposta aincidente de segurança de severidade Crítica	Porcentagem de incidentes de segurança de Severidade Crítica respondidos dentro do prazo identificado (incluindo notificação do CREA-SP)	15 minutos	Mensal	95,0

contenção de incidentes de segurança de Severidade Crítica	Porcentagem de incidentes de segurança de Severidade Crítica contidos dentro do tempo identificado	-1 hora para publicação do plano de contenção - 4 horas para contenção	Mensal	95,0
Resposta aincidente de segurança de severidade Alta	Porcentagem de incidentes de segurança de Severidade Alta respondidos dentro do prazo identificado (incluindo notificação do CREA-SP)	30 minutos	Mensal	95,0
contenção de incidentes de segurança de Severidade Alta	Porcentagem de incidentes de segurança de Severidade Alta contidos dentro do tempo identificado	-4 horas para publicação do plano de contenção - 8 horas para contenção	Mensal	95.0

4.4.3 REQUISITOS GERAIS DO SISTEMA DE VIRTUALIZAÇÃO

1 A CONTRATADA deverá disponibilizar todos os *hardwares*, ativos e passivos, necessários à plena execução dosserviços e aplicativos do CREA-SP. Deverá também atender aos seguintes termos:

1.1 Data Center com o espaço físico e infraestrutura planejada, dimensionamento e distribuição de *hardware.*

1.2 *Switches* para SAN, para *Ethernet* e cabeamento, totalmente gerenciáveis.

1.3 Dispositivos de segurança física, equipamentos de energia elétrica e climatização com avançada combinaçãode características técnicas e funcionais.

1.4 Todo o *hardware* disponibilizado pela CONTRATADA deverá ser dedicado ao CREA-SP, novos e cobertos porcontratos de garantia e suporte no regime 24x7x365.

4.4.3.1 HARDWARE PARA VIRTUALIZAÇÃO

1 A CONTRATADA deverá disponibilizar pelo menos 06 (seis) servidores (hardware) iguais entre si, para a modalidade de consolidação por virtualização. Deverão possuir tecnologia de virtualização; estar dispostos em

Cluster com funcionalidades de DRS (Distributed Resource Scheduler) e HA (High Availability), para instalação deaplicativos e com as seguintes características mínimas:

4.4.3.1.1 SOLUÇÃO INTEGRADA

1 A solução integrada deverá ser composta por todos os equipamentos e softwares especificados, incluindo licenciamento de software necessário para o completo atendimento da especificação técnica;

2 O hardware deverá ser projetado, desenvolvido, testado e homologado para o software

proposto, desde que osuporte e garantia sejam prestados por um único fornecedor;

3 Não serão aceitos produtos meramente baseados em armazenamento definido por software e hardwaregenéricos de forma acoplada, sendo o objetivo deste edital apenas soluções integradas;

4 A solução proposta, hardware e software, deverão existir como produto único antes da publicação desse edital, caracterizando assim uma tecnologia integrada de armazenamento e processamento;

5 Para esse edital a denominação servidor será sinônimo de nó, *"appliance"* ou lâmina;

6 Deve permitir e ser compatível na hospedagem de serviços de Tecnologia da Informação, instalados em máquinas virtuais Linux, CentOS, Ubuntu, Microsoft Windows Server sejam eles Sistema de Gerenciamento de Banco de Dados Oracle, MySQL ou PostgreSQL e servidores de arquivos compartilhados, serviços de diretórios, virtualização de desktops, gerenciamento de e-mail e colaboração e containers, exemplo Docker. O mesmo poderá ser comprovado através de boletins de suporte do respectivo fabricante ou por documentos de parcerias tecnológicas;

7 Deverá prover uma infraestrutura integrada de alta disponibilidade em configuração de cluster para ambientesvirtualizados, de forma que na falha de um servidor os demais 5 possam assumir imediatamente e a plena carga todos os serviços/maquinas/servidores hospedados. Não serão aceitas soluções ou funcionalidades implementadas via software ainda em fase de desenvolvimento, ou seja, àquelas que ainda não foram homologadas para ambientes de produção.

8 Deverá suportar um dos seguintes hipervisores *"bare metal"* e suas versões:

8.1 Vmware ESXi 7, ou superiores;

8.2 Baseado Linux KVM, desde que suportado e mantido pelo fabricante da solução integrada possuindo todas as características descritas no item e subitens que compõem as propriedades do hipervisor.

8.3 Deverá ser completamente compatível com o hypervisor fornecido pela contratada para a solução de virtualização.

9 Deverá suportar servidores com diferentes especificações de hardware no mesmo cluster ou futuros, servidorcom configurações distintas de processadores, memória RAM, discos rígidos e SSDs, conforme Tabela de Modelos abaixo:

Especificações de hardware	Quantidade Mínima	Quantidade bruta total mínima de núcleos. Por Servidor	Volumetria bruta total mínima de memória RAM (GB) Por Servidor	Volumetria bruta total mínima (TB) dos discos HDD Por Servidor	Volumetria total bruta mínima (TB) dos discos SSD por Servidor
Servidor Tipo 1 Hospedagem	6	32	512	2	2

4.4.3.1.2 CARACTERÍSTICAS MÍNIMAS DE CADA SERVIDOR DO TIPO 1

1 Cada servidor do Tipo 01 deverá atender as seguintes especificações mínimas:

2 Poderão ser instalados em um chassi modular ou unidade única com no máximo 02 (duas) unidades de rackde altura (2U).

3 Cada chassi deverá conter 02 (duas) fontes de alimentação redundantes do tipo hot-swap, sendo que, naocorrência de falha de uma delas, o sistema deverá permanecer funcionando em plena capacidade. A fonte dealimentação deverá ter a seguinte especificação:

4 2.0 kW de saída em 200-240v no máximo;

5 Certificação 80 Plus de eficiência ou similar.

6 BIOS do mesmo fabricante do servidor, podendo ser atualizável pela rede;

7 32 slots para DIMM DDR4 com capacidade máxima expansível de até 2 TB RDIMM com velocidades de até3200 MT/s;

8 Possuir barramento de virtualização distinto dos demais;

9 Possuir software de gerência do mesmo fabricante do hardware que ofereça as funções de console remota, com as mesmas funcionalidades de uma console local, possibilidade de ligar e desligar o servidor, receber alertasde pré-falhas e defeitos dos componentes, emitir alertas sempre que os principais componentes atinjam valores preestabelecidos, com a possibilidade de emissão de inventário de hardware.

10 Deve possuir a refrigeração adequada, ar/liquida de para garantir temperatura operacional adequada.

11 Os servidores deverão suportar os sistemas operacionais MS Windows 2008/2012 e superiores e software devirtualização tecnicamente compatível.

12 Deve ser compatível com os seguintes protocolos de segurança

12.0.1 Cryptographically signed firmware

12.0.2 Secure Boot

12.0.3 Secure Erase

12.0.4 Silicon Root of Trust

12.0.5 System Lockdown (requires iDRAC9 Enterprise or Datacenter)

12.0.6 TPM 1.2/2.0 FIPS, CC-TCG certified, TPM 2.0 China NationZ

13 Se instalado em um chassi modular deverá ser do tipo hot-pluggable;

14 Possuir 2 (dois) processadores físicos padrão x86, no mínimo, *Intel Xeon Gold 6226R*. Cada processador deve possuir capacidade de, no mínimo, *16 (dezesseis)* cores físicos, *32 (trinta e duas)* threads, *22 MB (vinte edois megabytes)* de cache, suportar conjunto de instrução de 64-bits (sessenta e quatro bits), frequência baseada em processador de *2.9GHz (dois virgula nove gigahertz)* e frequência turbo máxima de *3.90 GHz (três virgulanove gigahertz)*. Especificação dos processadores conforme tabela de modelos;

15 Suportar até *1536 (Um mil, quinhentos e trinta e seis)* de memória RAM DDR4 ECC. A quantidade de memória RAM fornecida deverá ser conforme tabela de modelos;

16 Possuir discos de estado sólido (SSD) padrão de 6.0 Gb/s, ou superior, e hot-swap. Volumetria bruta conforme tabela de modelos;

17 Possuir no mínimo 2 (dois) discos de estado sólido (SSD) padrão SATA de 6.0 Gb/s e hot-swap. Volumetriados discos SSD conforme tabela de modelos;

18 Possuir no mínimo 10 (dez) discos padrão SATA de 6 Gb/s e hot-swap. Volumetria dos discos rígidos conforme tabela de modelos;

19 Prover interfaces de comunicação sendo:

19.0.1 06 (seis) interfaces de rede a 100/1.000/10.000 Mbps auto-sense, com conector de Fibra óptica,com gerenciamento SNMP e leds de monitoramento e diagnóstico;

19.0.2 02 interface 10/100/1000 Mbps auto sense, com conector RJ-45, com gerenciamento SNMP e ledsde monitoramento e diagnóstico.

19.0.3 Todas as interfaces de Rede devem ter capacidade mínima de 10 VLans (redes virtuais).

19.0.4 Possuir duas portas Gigabit Ethernet padrão 1000Base-T dedicada ao módulo de gerenciamento IPMI ou similar, uma das portas 10Gb (dez gigabits) Ethernet para comunicação com a rede externa, deverá funcionar como redundância da porta IPMI dedicada ou similar, permitindo o acesso aos recursosIPMI em caso de falhas na comunicação com a porta IPMI dedicada.

20 Possuir uma porta VGA;

21 Possuir duas portas USB 3.0;

22 No painel frontal do chassi, as seguintes funcionalidades e/ou luzes indicativos deverão estar presentes:

23 Botão de energia com sinalizador integrado para cada um dos servidores;

24 Botão identificação frontal e traseiro para identificação, por servidor;

25 Para determinar atividade ou falha dos discos SSD e discos rígidos;

26 Para determinar atividade das interfaces Gigabit Ethernet LAN1 ou LAN2;

27 Para indicar de alertas como: superaquecimento do equipamento, falhas nas ventoinhas e fonte de alimentação.

28 O equipamento deverá ser fornecido com todos os acessórios necessários para sua instalação, incluindo, mas não se limitando a, trilhos para montagem em rack, cabos de alimentação elétrica e cabos para pelo menos duas conexões de rede 10 GbE (Dez Gigabit Ethernet) por servidor, respeitando as seguintes especificações mínimas:

4.4.3.2 SOFTWARE PARA VIRTUALIZAÇÃO

1 Licenciamento necessário a suportar todo o ambiente de virtualização permitido para todos os servidores físicos fornecidos pela CONTRATADA conforme por ela dimensionados.

2 Software Hypervisor bare metal que execute diretamente no próprio hardware do servidor SMP, mapeie as definições do hardware virtual para o hardware real e tenha independência dos sistemas operacionais.

3 Capacidade de receber, no mínimo, todas as máquinas virtuais do CREA-SP possui hoje, conforme lista abaixo:

HOSTNAME	SISTEMA OPERACIONAL
HOST 1	Microsoft Windows 7 (32-bit)
HOST 2	Linux CentOS 8 (64-bit)
HOST 3	Microsoft Windows Server 2016 (64-bit)
HOST 4	Kali Linux 2020 (64-bit)
HOST 5	Microsoft Windows Server 2016 (64-bit)
HOST 6	Microsoft Windows Server 2008 R2 (64-bit)
HOST 7	Microsoft Windows Server 2008 R2 (64-bit)

HOST 8	Microsoft Windows Server 2008 R2 (64-bit)
HOST 9	Microsoft Windows Server 2008 R2 (64-bit)
HOST 10	Microsoft Windows Server 2016 (64-bit)
HOST 11	Microsoft Windows Server 2016 (64-bit)
HOST 12	Microsoft Windows Server 2016 (64-bit)
HOST 13	Microsoft Windows Server 2016 (64-bit)
HOST 14	Microsoft Windows Server 2016 (64-bit)
HOST 15	Microsoft Windows Server 2016 (64-bit)
HOST 16	Microsoft Windows Server 2016 (64-bit)
HOST 17	Microsoft Windows Server 2016 (64-bit)
HOST 18	Blockbit GSM 1.2 - Linux (64-bit)
HOST 19	Blockbit GSM 2.0 - Linux (64-bit)
HOST 20	Microsoft Windows Server 2016 (64-bit)
HOST 21	Microsoft Windows Server 2016 (64-bit)
HOST 22	Microsoft Windows Server 2016 (64-bit)
HOST 23	CentOS 8 (64-bit)
HOST 24	Microsoft Windows Server 2016 (64-bit)
HOST 25	Microsoft Windows Server 2016 (64-bit)
HOST 26	Microsoft Windows Server 2016 (64-bit)
HOST 27	Microsoft Windows Server 2016 (64-bit)
HOST 28	Microsoft Windows Server 2012 (64-bit)
HOST 29	Microsoft Windows Server 2012 (64-bit)
HOST 30	Microsoft Windows Server 2012 (64-bit)
HOST 31	Microsoft Windows Server 2012 (64-bit)
HOST 32	Microsoft Windows Server 2012 (64-bit)
HOST 33	Microsoft Windows Server 2012 (64-bit)
HOST 34	Microsoft Windows Server 2012 (64-bit)
HOST 35	Microsoft Windows Server 2012 (64-bit)
HOST 36	Microsoft Windows Server 2016 (64-bit)
HOST 37	Microsoft Windows Server 2016 (64-bit)
HOST 38	Microsoft Windows Server 2016 (64-bit)
HOST 39	Microsoft Windows Server 2012 (64-bit)
HOST 40	Microsoft Windows Server 2012 (64-bit)
HOST 41	Microsoft Windows Server 2003 Standard (32-bit)
HOST 42	CentOS 6 (64-bit)
HOST 43	Microsoft Windows Server 2016 (64-bit)
HOST 44	CentOS 6 (64-bit)
HOST 45	CentOS 6 (64-bit)

HOST 46	CentOS 6 (64-bit)
HOST 47	CentOS 6 (64-bit)
HOST 48	CentOS 6 (64-bit)
HOST 49	Microsoft Windows Server 2016 (64-bit)
HOST 50	Microsoft Windows Server 2016 (64-bit)
HOST 51	Microsoft Windows Server 2016 (64-bit)
HOST 52	Microsoft Windows Server 2016 (64-bit)
HOST 53	Microsoft Windows Server 2016 (64-bit)
HOST 54	Microsoft Windows Server 2016 (64-bit)
HOST 55	Microsoft Windows Server 2016 (64-bit)
HOST 56	Linux CentOS 5.11 (64-bit)
HOST 57	Linux CentOS 7.4 (64-bit)
HOST 58	Microsoft Windows Server 2019 (64-bit)
HOST 59	CentOS 7 (64-bit)
HOST 60	Microsoft Windows Server 2016 (64-bit)
HOST 61	Microsoft Windows Server 2008 R2 (64-bit)
HOST 62	Microsoft Windows Server 2008 R2 (64-bit)
HOST 63	Microsoft Windows Server 2008 R2 (64-bit)
HOST 64	Microsoft Windows Server 2019 (64-bit)
HOST 65	CentOS 6 (64-bit)
HOST 66	Microsoft Windows Server 2016 (64-bit)
HOST 67	Microsoft Windows Server 2016 (64-bit)
HOST 68	Ubuntu Linux 16.4 (64-bit)
HOST 69	Microsoft Windows Server 2016 (64-bit)
HOST 70	Microsoft Windows Server 2016 (64-bit)
HOST 71	Microsoft Windows 10 (32-bit)
HOST 72	Ubuntu Linux 10 (64-bit)
HOST 73	Ubuntu Linux 9 (64-bit)
HOST 74	Debian GNU/Linux 6 (64-bit)
HOST 75	Debian GNU/Linux 8 (64-bit)
HOST 76	Microsoft Windows Server 2016 (64-bit)
HOST 77	Ubuntu Linux 9 (64-bit)
HOST 78	Microsoft Windows Server 2012 (64-bit)
HOST 79	Ubuntu Linux 9 (64-bit)
HOST 80	Microsoft Windows Server 2008 (64-bit)
HOST 81	Microsoft Windows Server 2016 (64-bit)
HOST 82	Microsoft Windows Server 2008 (64-bit)
HOST 83	Microsoft Windows Server 2008 R2 (64-bit)
HOST 84	Microsoft Windows 10 (64-bit)
HOST 85	CentOS 6 (64-bit)
HOST 86	Microsoft Windows Server 2016 (64-bit)
HOST 87	CentOS 8 (64-bit)

HOST 88	Microsoft Windows Server 2019 (64-bit)
HOST 89	Ubuntu Server 20.04
HOST 90	Microsoft Windows Server 2019 (64-bit)
HOST 91	Microsoft Windows Server 2019 (64-bit)
HOST 92	Microsoft Windows Server 2019 (64-bit)
HOST 93	Microsoft Windows Server 2019 (64-bit)
HOST 94	Microsoft Windows 10 (64-bit)
HOST 95	Microsoft Windows Server 2016 (64-bit)
HOST 96	Microsoft Windows Server 2016 (64-bit)
HOST 97	
HOST 98	Microsoft Windows Server 2016 (64-bit)
HOST 99	Microsoft Windows Server 2016 (64-bit)
HOST 100	Microsoft Windows Server 2012 (64-bit)
HOST 101	Microsoft Windows Server 2008 R2 (64-bit)
HOST 102	Microsoft Windows Server 2008 R2 (64-bit)
HOST 103	Red Hat Enterprise Linux 5 (64-bit)
HOST 104	Microsoft Windows Server 2019 (64-bit)
HOST 105	Microsoft Windows Server 2008 R2 (64-bit)
HOST 106	Microsoft Windows Server 2016 (64-bit)
HOST 107	Microsoft Windows Server 2016 (64-bit)
HOST 108	Microsoft Windows Server 2008 R2 (64-bit)
HOST 109	Microsoft Windows Server 2008 R2 (64-bit)
HOST 110	Microsoft Windows Server 2008 R2 (64-bit)
HOST 111	Microsoft Windows Server 2008 R2 (64-bit)
HOST 112	Microsoft Windows Server 2008 R2 (64-bit)
HOST 113	Microsoft Windows Server 2016 (64-bit)
HOST 114	Microsoft Windows Server 2019 (64-bit)
HOST 115	CentOS 7 (64-bit)
HOST 116	Microsoft Windows Server 2008 R2 (64-bit)
HOST 117	CentOS 7 (64-bit)
HOST 118	Microsoft Windows Server 2019 (64-bit)
HOST 119	Microsoft Windows Server 2016 (64-bit)
HOST 120	Microsoft Windows Server 2016 (64-bit)
HOST 121	Microsoft Windows Server 2016 (64-bit)
HOST 122	Ubuntu Linux (64-bit)
HOST 123	Ubuntu Linux (64-bit)
HOST 124	Microsoft Windows Server 2016 (64-bit)
HOST 125	Microsoft Windows Server 2019 (64-bit)
HOST 126	Microsoft Windows Server 2019 (64-bit)

HOST 127	Microsoft Windows Server 2012 (64-bit)
HOST 128	Microsoft Windows Server 2008 (64-bit)
HOST 129	Microsoft Windows Server 2008 R2 (64-bit)
HOST 130	Microsoft Windows Server 2016 (64-bit)
HOST 131	Linux Ubuntu Server 20.04 LTS
HOST 132	Linux Ubuntu Server 20.04 LTS
HOST 133	Linux Ubuntu Server 20.04 LTS
HOST 134	Linux Ubuntu Server 20.04 LTS
HOST 135	Debian GNU/Linux 8 (64-bit)
HOST 136	Microsoft Windows Server 2016 (64-bit)
HOST 137	Microsoft Windows Server 2016 (64-bit)
HOST 138	Microsoft Windows Server 2008 (64-bit)
HOST 139	VMware Photon OS (64-bit)
HOST 140	Ubuntu Linux (64-bit)
HOST 141	Microsoft Windows Server 2016 (64-bit)
HOST 142	Microsoft Windows Server 2016 (64-bit)

4 É responsabilidade da CONTRATADA garantir que o seu sistema suporte todas as máquinas listadas acima, com seus respectivos sistemas operacionais, e encontrar soluções para possíveis incompatibilidades sem requerer que o CREA-SP atualize o sistema operacional de suas máquinas.

5 Esta lista é dinâmica, e não significa que na época da contratação serão exatamente esses os servidores que o CREA-SP possuirá.

4.4.3.2.1 CARACTERÍSTICAS GERAIS MÍNIMAS DO HYPERVISOR

1 Gerenciamento centralizado do parque virtualizado com interface gráfica de usuário (GUI).

2 Capacidade de agendamento de tarefas e geração de alertas.

3 Segurança de acesso integrada com o Microsoft Active Directory, possibilitando a delegação de autoridade emníveis de responsabilidade.

4 Capacidade de gerenciamento de recursos de disponibilidade do ambiente virtualizado, tais como asfuncionalidades de:

4.1 Migração de servidor virtual de um servidor físico para outro;

4.2 Migração de servidor virtual de um agrupamento de armazenamento físico para outro;

4.3 Movimentação automática dos servidores virtuais de um servidor físico para outro em uma eventual falhade um servidor físico;

4.4 Atualização automática por intermédio de mecanismos de regra de conformidade;

4.5 Distribuição da carga de processamento entre os servidores físicos de forma otimizada para economia deenergia.

5 Suporte a migrações de máquinas virtuais entre servidores físicos distintos sem perda de informação e seminterrupção do processamento ao usuário final.

6 Capacidade de detectar servidores virtuais que não estão consumindo recursos e colocá-los em modo deespera sem prejudicar o ANS (Acordo de Nível de Serviço).

7 Capacidade de automatizar processos de administração do ambiente.

8 Capacidade de ligar e desligar máquinas virtuais.

9 Banco de dados que armazene informações de configurações e desempenho dos servidores.

10 Interface Web que possibilite o acesso remoto via Web Browser.

11 Controle da utilização de recursos do hardware: CPU, memória, disco e rede, por múltiplos sistemasoperacionais.

12 Suporte a multiprocessamento simétrico, ou seja, utilizando mais de um processador.

13 Capacidade de expansão e redução das partições com balanceamento de carga entre os servidores.

14 Independência de hardware, funcionando em servidor físico distinto dos que hospedam os servidores virtuais.

15 Suporte ao Microsoft® Clustering.

16 Possibilidade de otimização de recursos de hardware conforme a real necessidade de cada servidor virtual.

17 Capacidade de clonagem das máquinas virtuais, ou seja, capacidade de criar máquinas virtuais idênticas.

18 Manutenção através de console remota de qualquer servidor virtual.

19 Suporte a função de gerenciamento ao controle de acesso de usuários com níveis de permissões distintospara administradores e operadores.

20 Permitir o compartilhamento de sistemas de armazenamento em discos através de uma rede de armazenamento SAN iSCSI provendo maior facilidade de gerenciamento, flexibilidade e disponibilidade.

21 Suporte a função de gerenciamento de permitir implantação de soluções de alta disponibilidade.

22 Permitir integração com o software de backup adotado pelo CREA-SP – Backup Exec.

23 Suporte a backup centralizado sem a necessidade de agentes nos servidores virtuais.

24 Capacidade de aperfeiçoar e reduzir o uso de memória física compartilhando páginas idênticas em memóriaacessadas por máquinas virtuais independentes que executam o mesmo tipo de aplicação ou serviço.

25 Disponibilizar políticas de segurança na camada 2 de rede.

26 Compatibilidade com Hyper-Threading.

27 Suporte a hardware com configuração descrita nos itens e requisitos de Hardware deste documento.

28 Suporte a failover, ou seja, tolerância de falhas em placas de rede, fibra e UTP.

29 Permitir a implantação de soluções com balanceamento de carga, link aggregation ou teaming de placas derede.

30 Permitir a criação de máquinas virtuais que possibilitem alteração pelo usuário, mas que retornem ao estadooriginal sem nenhuma alteração.

31 Possuir a funcionalidade de controle de I/O de storage possibilitando a configuração de prioridades porservidor virtual.

32 Possuir a funcionalidade de controle de I/O de rede possibilitando a configuração de regras de prioridade deacesso em função da necessidade da CONTRATADA.

33 Contrato de suporte e atualização de patches, hot fixes e services packs por todo o período contratual.

34 Possuir integração com a solução proposta;

35 Não serão aceitos hipervisores em fase de desenvolvimento ou homologação;

36 Permitir a criação de máquinas virtuais 32 ou 64 bits;

37 Permitir a criação de máquinas virtuais com, no mínimo, os seguintes sistemas operacionais:

37.1 Microsoft Windows Server 2012 ou superiores;

37.2 Microsoft Windows 7 ou superiores;

37.3 Red Hat Enterprise Linux 4.8 ou superiores;

37.4 Linux CentOS 5.11 ou superiores;

37.5 Linux Ubuntu Server e Desktop, 12.04.x ou superiores;

37.6 FreeBSD 9.3 ou superiores;

37.7 SUSE Linux Enterprise Server 11 ou superiores;

37.8 Oracle Linux 6.1 ou superiores;

37.9 Debian 8.5 ou superiores;

37.10 Sistemas Legados:

37.10.1 Windows Server 2003, 2008 e 2008 R2 e superiores;

38 Permitir a criação de novas máquinas virtuais através de interface gráfica.

39 Possibilitar que seja feita alterações de configurações (CPU, memória, disco e rede) de máquinas virtuaisexistentes através de interface gráfica.

40 Possibilitar adição dinâmica de CPU e memória de máquinas virtuais existentes, conforme a compatibilidadedo sistema operacional;

41 Possuir interface gráfica de gerenciamento de recursos como CPU, Memória e I/O para as máquinas virtuais.

42 Possuir configuração distribuída de redes virtuais em todos os servidores do cluster.

43 Permitir que as máquinas virtuais possam utilizar diferentes redes virtuais em um mesmo servidor.

44 Capacidade de monitorar, gerenciar e alterar continuamente a utilização dos recursos de processamento representado pelo conjunto de servidores físicos, alocando inteligentemente e redistribuindo dinamicamente as máquinas virtuais entre os servidores baseado em regras pré-definidas que reflitam as necessidades e mudançasde prioridades de cada máquina virtual.

45 Permitir a criação de ambiente de alta disponibilidade, na perspectiva do hipervisor, um cluster entre os servidores físicos, e na indisponibilidade de um dos servidores, efetuar inteligentemente a redistribuição dasmáquinas virtuais entre os demais servidores, sem requerer intervenção manual.

46 Possuir recurso de virtualização de uma ou mais placas de rede, cada uma com seu próprio endereço IP eMAC address.

47 Possibilitar a criação de novas máquinas virtuais através de modelos já criados e prontos para sereminstalados em qualquer cluster sobre o virtualizador de qualquer servidor físico que componha a solução integrada.

48 Monitorar a utilização individual de cada máquina virtual criada.

49 Possibilitar parar, iniciar, suspender e resetar máquinas virtuais.

50 Permitir criação de regras de afinidade entre máquinas virtuais e servidores do cluster, ou seja, com base em políticas pré-definidas determinadas máquinas virtuais deverão ser hospedadas somente em um conjunto determinado de servidores.

51 Permitir a criação de regras de anti-afinidade entre máquinas virtuais, ou seja, com base em políticas pré-definidas determinadas máquinas virtuais não poderão ser hospedadas no mesmo servidor do cluster.

52 Permitir a configuração de acesso não uniforme à memória RAM (vNUMA) oriundo das máquinas virtuais.

53 Permitir a entrega de placas de aceleração gráfica de modo direto (dedicado) ou partes (virtual).

54 Possuir de forma gráfica toda visibilidade física e lógica do ambiente de rede de dados do cluster.

4.4.3.2.2 REQUISITOS GERAIS DE GERENCIAMENTO DO SISTEMA DE VIRTUALIZAÇÃO

1 Deverá possuir console de administração WEB (em alta disponibilidade);

2 A interface de administração WEB e SSH deve ser acessível a partir de qualquer dos endereços IPs configurados nas máquinas virtuais controladoras ou hipervisores integrados, configuradas no cluster. A funcionalidade de alta disponibilidade também deve estar disponível para a interface de administração, garantindoque mesmo em caso de falhas, a interface de administração continue disponível.

3 A console Web deve suportar o acesso via HTTPS utilizando certificados digitais. Estes certificados digitais poderão ser gerados e auto assinados automaticamente pela solução ou importados através de uma opção disponível no console Web.

4 A solução deve disponibilizar acesso ao sistema operacional da solução através do protocolo padrão SSH(Secure Shell) ou similar;

5 A console WEB deve ser acessível por browsers que suportam a tecnologia HTML5.

6 A console WEB deve permitir integração com Active Directory da Microsoft para autenticação, ou então,utilizar autenticação local.

7 Com a finalidade de automatizar os processos de implementação, manutenção e gerenciamento do cluster, osistema operacional em execução na solução integrada deverá oferecer REST APIs.

8 A solução deverá implementar uma interface de linha de comando completa para administração emonitoramento de os componentes do cluster, tais como:

8.1 Informar saúde dos componentes do cluster;

8.2 Criar, alterar ou deletar um novo container;

8.3 Habilitar ou desabilitar desduplicação em um disco virtual;

8.4 Parâmetros avançados do Erasure Coding*;*

9 A solução integrada deverá suportar autenticação de 02 (dois) níveis, permitindo a autenticação e controle deacesso através da combinação de dispositivos de segurança física e senhas de acesso;

10 Com o objetivo de proporcionar maior segurança, o sistema operacional deve oferecer uma funcionalidade deimpedir o acesso ao terminal de linha de comando.

11 Quando necessário, a solução deverá permitir acesso externo aos dados armazenados no cluster*,* através de uma funcionalidade liberação a partir de um dado segmento de rede configurado pelo administrador.

12 A console WEB deve fornecer acesso à, no mínimo, as seguintes opções:

12.1 Painel principal;

12.2 Painel da saúde do Sistema (cluster);

12.3 Painel das Máquinas Virtuais;

12.4 Painel do Storage;

12.5 Painel do Hardware;

12.6 Painel de Recuperação de Desastres;

12.7 Painel de Análise de Performance;

12.8 Painel de Alertas e Eventos.

13 Deve suportar envio de alertas e eventos via SNMP.

14 Permitir a visualização de informações dos switches topo de rack na console Web de administração docluster.

15 A solução deverá oferecer a opção de adicionar os switches de rede, obtendo as informações através do protocolo SNMPv2c, SNMPv3 ou através de CDP. Ao menos as seguintes informações deverão estar disponíveis:

15.1 Situação dos switches;

15.2 Quantidade de portas;

15.3 Velocidade das portas.

16 Com o objetivo de facilitar o monitoramento e visualização das informações do cluster, ao menos asseguintes informações deverão estar disponíveis no cluster:

16.1 Sumário do hipervisor;

16.2 Sumário do hardware;

16.3 IOPS do *cluster*;

16.4 Utilização de banda do *cluster*;

16.5 Latência do cluster;

16.6 Situação da resiliência dos dados;

16.7 Alertas e eventos.

17 Deverão estar disponíveis os seguintes tipos de usuários e suas respectivas funções:

17.1 Visualização - Não permitindo nenhuma alteração na configuração;

17.2 Administração do cluster - Pode realizar todas as operações disponíveis, exceto criar ou modificar osusuários;

17.3 Usuário administrativo - Pode realizar todas as operações disponíveis.

18 Quando empregado 02 (dois) ou mais clusters distintos, uma ferramenta de gerência unificada deverá ser disponibilizada, facilitando a tarefa de administração diária dos clusters localizados distantes geograficamente. Aferramenta deverá apresentar as seguintes informações consolidadas de todos os clusters registrados:

18.1 Saúde dos Sistema clusters;

18.2 Máquinas Virtuais;

18.3 Armazenamento;

18.4 Situação do Hardware;

18.5 Painel de Análise de Performance;

18.6 Painel de Alertas e Eventos;

18.7 Gerenciamento de capacidade baseado em cenário, previsão de crescimento e otimização deconsumo;

18.8 Gerenciamento de capacidade baseado nas métricas de cenário;

18.9 Atualização centralizada de todos os cluster gerenciados;

18.10 Alertas dinâmicos baseados em anomalias de comportamento e com geração automática demétricas;

18.10.1 Sobre o provisionamento das máquinas virtuais, que evidencie se elas estão "corretamente"e/ou superdimensionamento na perspectiva de consumo de recursos (RAM, CPU, etc), inatividade ou

Impacto de desempenho entre máquinas virtuais no mesmo nó;

19 Geração de relatórios sobre o provisionamento seja por inatividade ou ociosidade, para futura captura ouredistribuição de recursos (RAM, CPU, etc);

20 Agendamento de relatórios para envio por e-mail;

21 A interface IPMI ou similar presente em cada um dos servidores deverá ser baseada em Web, acessívelatravés de um endereço IP. No mínimo as seguintes opções deverão estar disponíveis na interface Web:

22 Configuração remota do BIOS;

23 Console remoto gráfico;

24 Ligar, desligar e reiniciar o servidor remotamente;

25 Monitoramento do Hardware;

26 Atualização do software IPMI ou similar através da interface Web.

27 O gerenciador do cluster deverá enviar periodicamente informações e estatísticas automaticamente para o suporte do fabricante, funcionalidade conhecida como call-home. Este recurso tem por objetivo aplicar análisesavançadas para otimizar a implementação da solução ou atuar pro ativamente na identificação de problemas. Deverá ser permitido desabilitar este recurso a qualquer momento através da interface WEB.

28 A console de administração gráfica deverá disponibilizar, quando necessário, o acesso remoto do time de suporte do fabricante. Essa funcionalidade deverá estabelecer um túnel SSH reverso ou similar aos servidores dofabricante com o objetivo de permitir ao suporte, executar manutenções no software dos controladores de armazenamento virtuais. O administrador do sistema poderá habilitar ou desabilitar o acesso a qualquer momento.

29 A solução deverá possuir ferramenta de checagem interna integrada a console de gerenciamento, buscandopor problemas de saúde no cluster pro ativamente.

4.4.3.3 AMBIENTE DE NUVEM

1 A CONTRATADA deverá disponibilizar em seu ambiente de virtualização Cloud (Nuvem)

a capacidade paraatender a seguinte demanda inicial:

1.1 Quantidade mínima inicial de 874 vCPU's.

1.2 Quantidade inicial mínima de 1.700 GB de Memória Virtual.

2 O ambiente de computação cloud da CONTRATADA deverá atender as especificações abaixo:

2.1 Virtual vCPU, com frequência não inferior a 2 GHZ.

2.2 Quantidade de vCPU igualmente distribuída entre os Servidores Físicos.

2.3 Memória RAM DDR4 ou superior, com frequência de mínima de 2 GHZ.

3 Deve manter compatibilidade com os seguintes sistemas operacionais e bancos de dados:

3.1 Windows Server 2008 R2 e superiores.

3.2 MS SQL Server Standard/Enterprise 2008 e superiores.

3.3 MS SQL Server Standard/Enterprise 2012 e superiores.

4 Deve permitir comunicação com os demais ambientes da CONTRATADA no ambiente do data center.

5 Deve permitir alocação de 1 (um) a 8 (oito) vcpu's por máquina virtual no mínimo;

6 Deve permitir alocação máxima de no mínimo até 32 (trinta e dois) gigabytes de memória RAM virtual pormáquina virtual hospedada no cloud.

4.4.4 REQUISITOS GERAIS DE COMUNICAÇÃO

1 A comunicação de Rede no Datacenter de Hospedagem, quanto no Datacenter Redundante devem possuir osseguintes Requisitos:

4.4.4.1 REQUISITOS GERAIS DE COMUNICAÇÃO DE REDE

1 Deverá ser disponibilizada uma rede local logicamente isolada e dedicada para o CREA-SP dentro do DataCenter. Esta disponibilização deverá ser feita através de VLANs configuradas sobre switches redundantes, permitindo a construção de múltiplos segmentos lógicos de rede para acomodar as tecnologias necessárias paraaplicativos, backup de dados, monitoramento, gestão remota de aplicações, dentre outras.

2 Possuir switches L3 Ethernet 10/1000/10000 Mbps, aderente aos padrões IEEE 802, com segurança e gerenciamento SNMP e RMON, suporte a protocolos TCP/IP, operações de port trunking e mirroring, supressão depacotes de broadcast e multicast, conectividade em LAN e WAN, fontes e ventiladores redundantes.

3 Possuir um gerenciamento dinâmico e otimizado dos múltiplos canais de comunicação, assegurandodesempenho e disponibilidade no acesso.

4 Possuir conexões redundantes, responsáveis pelo tráfego interno do Data Center, facilitando o monitoramento eadministração em diferentes pontos.

5 Possuir sistema de cabeamento estruturado categoria 6, gerenciado, construído sob piso elevado e em sistemade calhas aramadas.

6 A interligação entre os Servidores e os Storages deve Ser em Link de fibra Óptica co capacidade de 10 Gbps

7 A interligação entre os Servidores IBM e os seus respectivos Storages deve ser através de canais Fiber Chanel

8 A Interligação entre os Servidores e os Equipamentos de Backup deve ser através de Links de Fibra Óptica comcapacidade de 10 Gbps

9 A interligação entre os servidores e os equipamentos de interligação entre o Data Center principal e CREA-SP (Faria Lima) deverá ser através de enlaces de Fibra óptica com capacidade mínima de 10 Gbps

10 Cada Servidor deve ser interligado aos Switches por, no mínio 4 interfaces de rede de 10Gbps, conformediagrama TOPOLOGIA FÍSICA.

4.4.4.2 REQUISITOS GERAIS DOS EQUIPAMENTOS DE REDE

4.4.4.2.1 **1** Os equipamentos devem possuir dimensões apropriadas para montagem em rack de 19'' (dezenove polegadas), devendo vir acompanhado dos acessórios necessários;

2 Os equipamentos ofertados devem ter pelo menos 48 (quarenta e oito) portas híbridas 1/10 Gbps que podemoperar a 01 Gbps e 10 Gbps de acordo com a velocidade dos transceivers utilizados. Essas portas devem ser compatíveis com transceivers SFP e SFP+ que utilizam conectores do tipo LC;

3 Os equipamentos ofertados devem ter pelo menos 48 portas 10Gbps habilitadas para uso;

4 Os equipamentos ofertados devem ser compatíveis com transceivers 1000BASE-SX e 1000BASE-LX;

5 Os equipamentos ofertados devem ser compatíveis com transceivers 1Gbps com conectores RJ-45.

6 Os equipamentos ofertados devem ser compatíveis com transceivers 10GBASE-SR e 10GBASE-LR;

7 Os equipamentos ofertados devem ser compatíveis com cabos 10Gbps "Direct

Attached”/“Twinax” de pelomenos 5m de comprimento;

8 Os equipamentos ofertados devem suportar a instalação de 4 (quatro) portas 40 Gbps Ethernet. A instalaçãodessas portas pode ser realizada através da instalação física de um módulo de interface ou habilitação de

Interfaces através de licença de software. Essas portas devem ser compatíveis com transceivers QSFP+ queutilizam conectores do tipo LC ou MPO;

9 Os equipamentos ofertados deverão ter pelo menos 4 portas 40 Gbps habilitadas para uso;

10 Os equipamentos ofertados devem suportar a instalação pelo menos 16 (dezesseis) portas 16 Gbps FC. A instalação dessas portas pode ser realizada através da instalação física de um módulo de interface ou habilitaçãode interfaces através de licença de software. Essas portas podem operar em modo Universal Port ou Flex Port, onde a mesma porta pode operar como 1/10 Gbps Ethernet e como 16 Gbps FC;

11 Os equipamentos devem possuir ao menos uma interface 10 Gbps de longa distância até 10 Km licenciada ehabilitada, pronto para uso, homologada e certificada pelo fabricante;

12 Os equipamentos ofertados devem suportar em sua configuração pelo menos 52 portas ativas simultaneamente, sendo pelo menos 48 (quarenta e oito) portas 1/10Gbps Ethernet para transceivers SFP+ e 4(quatro) portas 40Gbps Ethernet para transceivers QSFP;

13 A capacidade de comutação dos equipamentos ofertados devem ser de pelo menos 1.2 Tbps;

14 Todas as portas dos equipamentos ofertados devem operar em modo wire-speed e non-blocking;

15 Os equipamentos ofertados devem possuir fonte de alimentação interna, do tipo “hot swappable”, comchaveamento automático entre 127/220V AC;

16 Os equipamentos ofertados devem possuir fonte de alimentação redundante interna, do tipo “hot swappable”,com características idênticas à fonte principal;

17 Os equipamentos ofertados devem possuir latência inferior a 1 µs;

18 Os equipamentos ofertados devem possuir pelo menos 24 MB de buffer;

19 A proposta comercial deve descriminar o fabricante e o modelo dos equipamentos ofertados bem como seusrespectivos Part Numbers para tornar mais fácil e clara a identificação do produto ofertado;

20 Os equipamentos ofertados devem ser novo e em plena fabricação. Não serão aceitos equipamentos com avisos de “End of Life”, ou seja, aviso de que o produto está fora de linha de fabricação emitida pelo fabricante;

21 Os equipamentos ofertados devem possuir garantia e suporte de 36 meses com direito a atualização de firmware, troca de peças no próximo dia útil em horário comercial e abertura de chamados no fabricante. Tal procedimento se justifica pelo fato de que, de forma geral a contratação, de serviços de manutenção para ativosfora de garantia, usualmente é mais onerosa para a Administração do que quando o bem é adquirido com garantia para toda sua vida útil;

22 Os equipamentos ofertados devem possuir homologação junto a ANATEL conforme a resolução nº 242, de 30 de novembro de 2000. A exigência de certificação de Produtos de Telecomunicação classificáveis nas Categorias I, II e III do art. 4o da Resolução Anatel 242/2000 é pré-requisito obrigatório para fins de comercialização e utilização no país, para atendimento ao disposto no parágrafo único do art. 20 da Resolução 242 da

Anatel. Todas as certificações necessárias devem estar disponíveis publicamente no sítio eletrônico da agenciareguladora conforme endereço eletrônico http://sistemas.anatel.gov.br/sgch/.

4.4.4.2.2 VIRTUALIZAÇÃO E ESCALABILIDADE

1 Os equipamentos ofertados devem permitir escabilidade utilizando protocolo de fabric baseado em TRILL ousimilar;

2 O fabric deve permitir escalabilidade de pelo menos 48 (quarenta e oito) equipamentos;

3 O fabric deve permitir as topologias de interconexão do tipo estrela, anel e full-mesh;

4 O fabric deve permitir a adição dos equipamentos de Chassis;

5 O fabric deve implementar mecanismo para mobilidade de máquinas virtuais (VMs). Esse mecanismo devepermitir a migração de uma VM de qualquer porta de qualquer equipamento do fabric para qualquer porta de qualquer equipamento do fabric, de forma que todas as características e configurações necessárias para operação da VM na nova porta física estejam disponíveis automaticamente (VLAN utilizada, ACLs e características de QoS), sem necessidade de configuração manual dos equipamentos;

6 O mecanismo de mobilidade de máquinas virtuais deverá ser implementado nativamente nOs equipamentos físico ou via software de mesmo fabricante, em todos os casos a capacidade mínima deverá ser de 8000 (oito mil) máquinas virtuais. Todas as licenças adicionais para a implementação dessa funcionalidade devem ser fornecidas;

7 Caso o mecanismo de mobilidade de máquinas virtuais possua restrições quanto a capacidade de processamento das máquinas físicas, o mecanismo em questão deverá ser licenciado de forma a permitir a conexão simultânea de uma máquina física com 4 processadores em cada uma das portas 48 portas 10Gbpssolicitadas;

8 A solução ofertada deve permitir seu gerenciamento através de um endereço IP único atribuído ao fabric;

9 Caso a solução de Fabric ofertada necessite de elementos adicionais para seu pleno

funcionamento, todosesses elementos devem ser fornecidos de forma redundante para garantir a alta disponibilidade do ambiente;

10 Os equipamentos ofertados devem permitir a atribuição de um perfil com VLAN, QoS e ACLs aos dispositivos conectados. O controle desta atribuição deve ser realizado através do endereço MAC de cada dispositivo;

11 Os equipamentos ofertados devem implementar funcionalidades que permitam a integração com pelo menosum fabricante de software de virtualização de mercado. Este mecanismo deve realizar a importação de informações do software de virtualização como Nome de VM, Endereço MAC, PortGroup e VLAN correspondente das VMs importadas, criar VLANs automaticamente no ambiente de fabric e atribuir um perfil com as características pertinentes de cada VM ao seu tráfego de dados de forma automática, independente da porta do fabric que essa VM está conectada;

4.4.4.2.3 FUNÇÕES DE CAMADA 2

1 Os equipamentos ofertados devem suportar Jumbo Frames de pelo menos 9000 bytes em todas as suas portas;

2 Os equipamentos ofertados devem implementar o padrão LACP IEEE 802.3ad para criação de grupos de portasagregadas;

3 Os equipamentos ofertados devem permitir a criação de grupos de LACP utilizando portas próprias e portas deoutros equipamentos do mesmo fabric dentro do mesmo grupo de portas agregadas;

4 Os equipamentos ofertados devem permitir a criação de pelo menos 64 (sessenta e quatro) grupos de portasagregadas;

5 Os equipamentos ofertados devem permitir a criação de grupos de LACP contendo pelo menos 16 (dezesseis)portas dentro do mesmo grupo;

6 Os equipamentos ofertados devem suportar tabela MAC com capacidade de pelo menos 120.000 (cento e vintemil) endereços;

7 Os equipamentos ofertados devem implementar o padrão IEEE 802.3x (Flow Control);

8 Os equipamentos ofertados devem implementar o padrão IEEE 802.1Q;

9 Os equipamentos ofertados devem implementar private VLANs;

10 Os equipamentos ofertados devem implementar VXLAN Gateway;

11 Os equipamentos ofertados devem permitir a utilização simultânea de pelo menos 3500 (três mil e quinhentas)VLANs IDs;

12 Os equipamentos ofertados devem implementar IGMP snooping para v1 e v2;

4.4.4.2.4 FUNÇÕES DE CAMADA 3

1 Os equipamentos ofertados devem permitir a configuração de pelo menos 1000 (mil) rotas estáticas IPv4;

2 Os equipamentos ofertados devem suportar 4.000 (quatro mil) rotas IPv4 em hardware;

3 Os equipamentos ofertados devem permitir a configuração de pelo menos 256 (duzentos e cinquenta e seis)interfaces virtuais (SVI) para o roteamento entre VLANs;

4 Os equipamentos ofertados devem implementar rotas estáticas;

5 Os equipamentos ofertados devem implementar roteamento baseado em políticas (PBR) para IPv4 e IPv6;

6 Os equipamentos ofertados devem implementar IPv4/IPv6 dual stack;

7 Os equipamentos ofertados devem implementar OSPFv2 e v3;

8 Deve permitir a configuração de pelo menos 32 (trinta e dois) caminhos de ECMP (Equal Cost Multipath);

9 Os equipamentos ofertados devem implementar PIM-SM;

10 Os equipamentos ofertados devem implementar VRRPv2 e v3;

11 Os equipamentos ofertados devem implementar BGP/BGP4+;

12 Os equipamentos ofertados devem implementar pelo menos 32 (trinta e duas) instâncias de VRF ou VRF-Lite;

4.4.4.2.5 CONVERGÊNCIA

1 Os equipamentos ofertados devem suportar o padrão DCB (Data Center Bridging) incluindo as seguintescaracterísticas:

1.1 IEEE 802.1Qaz;

1.2 IEEE 802.1Qbb;

1.3 DCBX;

2 Deve suportar a priorização do tráfego FCoE através de TLVs;

3 Os equipamentos ofertados devem suportar funcionalidades de FCoE incluindo os seguintes padrões ecaracterísticas:

4 T11 Fibre Channel Forwarder (FCF) usando FC-BB-5;

5 FCoE Initialization Protocol (FIP);

6 Deve suportar FCoE multi-hop;

7 Deve suportar a conexão direta de FCoE Initiators e FCoE Targets;

8 Os equipamentos devem suportar a conexão de dispositivos FC operando a 2, 4, 8 e 16 Gbps;

4.4.4.2.6 QUALIDADE DE SERVIÇO

1 Os equipamentos ofertados devem implementar a classificação e priorização de pacotes de acordo com osseguintes critérios:

1.1 Campo PCP Priority Code Point (IEEE 802.1p);

1.2 DSCP;

1.3 Interface física;

1.4 Baseada em parâmetros de camada 02;

2 Os equipamentos ofertados devem possuir pelo menos 08 (oito) filas por porta;

3 Os equipamentos ofertados devem permitir o uso das filas de hardware nos modos prioridade estrita,ponderada e ambas combinadas;

4 Os equipamentos ofertados devem implementar Deficit Weighted Round-Robin (DWRR);

4.4.4.2.7 GERENCIAMENTO E SEGURANÇA

1 Os equipamentos ofertados devem permitir o gerenciamento via IPv4 e IPv6;

2 Os equipamentos ofertados devem implementar atualização de software em serviço (ISSU). Este recurso deveser habilitado em hardware;

3 Os equipamentos ofertados devem implementar controle de acesso baseado em regra;

4 Os equipamentos ofertados devem possuir uma porta ethernet com conector RJ-45 por módulo de gerência parao gerenciamento “out-of-band”;

5 Os equipamentos ofertados devem possuir uma interface para gerenciamento de console serial por módulo degerência;

6 Os equipamentos ofertados devem implementar o protocolo SNTP (Simple Network Time Protocol) ou NTP(Network Time Protocol);

7 Os equipamentos ofertados devem implementar o padrão IEEE 802.1ab (LLDP);

8 Os equipamentos ofertados devem permitir a captura de pacotes CDP para a integração

com ferramentas devirtualização que utilizem esse protocolo;

9 Os equipamentos ofertados devem permitir gerenciamento in-band usando TELNET e SSHv2;

10 Os equipamentos ofertados devem suportar a configuração utilizando Netconf;

11 Os equipamentos ofertados devem suportar o protocolo FTP ou TFTP para de transferência de arquivos deconfiguração e imagens de software;

12 Os equipamentos ofertados devem suportar o protocolo SFTP ou SCP para de transferência de arquivos deconfiguração e imagens de software de forma segura;

13 Os equipamentos ofertados devem possuir serviço local para autenticação de usuários, permitindo vários níveisde acesso;

14 Os equipamentos ofertados devem permitir autenticação e autorização de acesso usando servidores RADIUSexternos;

15 Os equipamentos devem implementar Port security;

16 Os equipamentos ofertados devem implementar 802.1x controle de acesso a rede baseado em porta;

17 Os equipamentos ofertados devem permitir gerência via SNMPv1, v2 e v3;

18 Os equipamentos ofertados devem implementar ao menos 02 grupos de RMON;

19 Os equipamentos ofertados devem gerar de mensagens de syslog para eventos relevantes do sistema;

20 Os equipamentos ofertados devem permitir a configuração de pelo menos 4 (quatro) servidores de syslog;

21 Os equipamentos ofertados devem implementar ACLs para a filtragem de tráfego baseado nas informações deendereço MAC de origem e destino, endereço IP de origem e destino, portas TCP e UDP de origem e destino e valor DSCP;

22 Os equipamentos ofertados devem permitir a criação de 10.000 (dez mil) regras de ACL;

23 Os equipamentos ofertados devem implementar espelhamento de tráfego;

24 Os equipamentos ofertados devem implementar espelhamento de tráfego remoto RSPAN;

4.4.4.2.8 MONITORAMENTO DE TRÁFEGO

1 Os equipamentos ofertados deve implementar sFlow ou NetFlow e ter a capacidade de enviar os

dados tráfego coletados para os monitores instalados na rede interna do CREA-SP.

4.4.4.3 REQUISITOS DE REDES VIRTUAIS (VLANS) e COMUNICAÇÃO TCP/IP

1 A rede de comunicação deve ser segmentada, disponibilizando os seguintes segmentos:

2 Rede de Operação

3 Rede DMZ

4 Rede de Backup

5 Rede de Banco de Dados

6 Descrição dos Segmentos de Rede:

6.1 Rede de Operação

6.1.1 Rede de comunicação dos servidores com acesso interno exclusivo para os colaboradores do CREA-SP

6.2 Rede DMZ

6.2.1 Rede de Comunicação para servidores com acesso externo, da internet

6.3 Rede de Backup

6.3.1 Rede de comunicação exclusiva para realização de Backup dos Servidores e seus dados e arquivos

6.4 Rede de Banco de dados

6.4.1 Rede de comunicação entre os servidores de aplicação e os servidores de Banco de Dados. Não temconectividade com a Internet e a conectividade com a rede externa de utilizadores e programadores é limitada apenas para os serviços de administração dos Banco de Dados.

4.4.5 REQUISITOS GERAIS DE SEGURANÇA

1 A CONTRATADA deverá fornecer no mínimo os seguintes dispositivos de segurança:

1.1 Sistemas WAF (Web Application Firewall), para bloquear e proteger os servidores contra-ataques vindosda Internet.

1.2 Appliances de Segurança (Firewalls) com IPS (Intrusion Prevention System) e IDS (Intrusion DetectionSystem)

1.3 Cofre de Senhas

1.4 Security information and event management (SIEM)

1.5 SOC (Security Operations Center) com gestão de vulnerabilidades.

2 A CONTRATADA deverá fornecer usuários de leitura (read only) para as interfaces gráficas e terminal (caso disponível) de todos os sistemas de segurança disponibilizados, de forma a permitir aos analistas do CREA-SP acompanhar sua configuração, verificação de seus logs e informações pertinentes a todo o sistema de segurança.

3 A CONTRATADA deverá implementar e seguir uma Política de Gestão de Segurança da Informação, baseada na Norma ABNT NBR ISO/IEC 27002, com a devida descrição dos controles que foram estabelecidos e implementados, os quais devem ser periodicamente monitorados, analisados e melhorados com o objetivo de identificar riscos, falhas, vulnerabilidades e descumprimentos das medidas de segurança da informação.

4.4.5.1 CARACTERISTICAS DOS APPLIANCES DE SEGURANÇA

4.4.5.1.1 CARACTERÍSTICAS GERAIS

1 As interfaces devem ser capazes de se comunicar, no mínimo nas seguintes velocidades: 10/100/1000 Base-T;

2 Deve ser interligado ao ambiente de virtualização (Servidores) e ao CREA-SP através do serviço deinterligação, com a velocidade de 10Gbps SFP+, no mínimo;

3 Deve possuir interfaces para gerência out-of-band 10/100/1000 e interfaces dedicadas para altadisponibilidade 10/100/1000;

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

4.1 Suporte a proteção de firewall de, no mínimo, 35Gbps medidos em simulação com tráfego enterprise mixou que simule ambiente com tráfego real;

4.2 Suporte a, no mínimo, 1 milhão de sessões protegidas;

4.3 Suporte a, no mínimo, 45 mil novas sessões por segundo;

4.4 Suporte a 4094 VLAN Tags 802.1q;

4.5 Agregação de links 802.3ad e LACP;

4.6 Policy based routing ou policy based forwarding;

4.7 Roteamento multicast (PIM-SM);

4.8 DHCP Relay;

4.9 DHCP Server;

4.10 Suporte à criação de objetos de rede que possam ser u lizados como endereço IP de

interfaces L3;

4.11 Suportar sub-interfaces ethernet logicas.

4.12 O firewall deve ter a capacidade de testar o funcionamento de rotas estáticas e rota default com a definição de um endereço IP de destino que deve estar comunicável através de uma rota. Caso haja falha nacomunicação o firewall deve ter a capacidade de usar rota alternativa para estabelecer a comunicação;

4.13 Deve suportar os seguintes tipos de NAT:

4.14 Nat dinâmico (Many-to-1);

4.15 Nat dynamic (Many-to-Many);

4.16 Nat estático (1-to-1);

4.17 NAT static (Many-to-Many);

4.18 Nat estático bidirecional 1-to-1;

4.19 Tradução de porta (PAT);

4.20 NAT de Origem;

4.21 NAT de Des no;

4.22 Suportar NAT de Origem e NAT de Des no simultaneamente;

4.23 Deve implementar Network Prefix Transla on (NPTv6), prevenindo problemas de roteamento assimétrico;

4.24 Deve implementar o protocolo ECMP;

4.25 Deve implementar balanceamento de link por hash do IP de origem;

4.26 Deve implementar balanceamento de link por hash do IP de origem e destino;

4.27 Deve implementar balanceamento de link através do método round-robin;

4.28 Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentualde tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, quarto links;

4.29 Deve implementar balanceamento de link através de políticas por usuário e grupos de usuários doLDAP/AD;

4.30 Deve implementar balanceamento de link através de políticas por aplicação e porta de destino;

4.31 Deve implementar o protocolo Link Layer Dicovery (LLDP), permitindo que o appliance e outros ativos darede se comuniquem para identificação da topologia da rede em que estão conectados e a função dos mesmos facilitando o processo de troubleshooting. As informações aprendidas e armazenadas pelo appliance devem ser acessíveis via SNMP;

4.32 Enviar log para sistemas de monitoração externos, simultaneamente;

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

4.34 Deve permitir configurar certificado caso necessário para autenticação no sistema de monitoraçãoexterno de logs; 13.1.18. Proteção contra anti-spoofing;

4.35 Deve permitir bloquear sessões TCP que usarem variações do 3-way hand-shake, como 4 way e 5 waysplit hand-shake, prevenindo desta forma possíveis tráfegos maliciosos;

4.36 Dever permitir bloquear conexões que contenham dados no payload de pacotes TCP-SYN e SYN-ACKdurante o three-way handshake;

4.37 Deve exibir nos logs de tráfego o motivo para o término da sessão no firewall, incluindo sessõesfinalizadas onde houver de-criptografia de SSL e SSH;

4.38 Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

4.39 Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

4.40 Suportar a OSPF graceful restart;

4.41 Deve suportar o protocolo MP-BGP (Mul protocol BGP) permitindo que o firewall possa anunciar rotasmulticast para IPv4 e rotas unicast para IPv6;

4.42 Suportar no mínimo as seguintes funcionalidades em IPv6: SLAAC (address auto configuration), NAT64,Identificação de usuários a par r do LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Regras de proteção contra DoS (Denial of Service), De-criptografia SSL e SSH, PBF (Policy Based Forwarding), QoS,

4.43 DHCPv6 Relay, IPSEc, VPN SSL, Ativo/Ativo, Ativo/Passivo, SNMP, NTP, SYSLOG, DNS, NeighborDiscovery (ND), Recursive DNS Server (RDNSS), DNS Search List

4.44 (DNSSL) e controle de aplicação;

4.45 Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma únicainstância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (l2) e camada 3 (l3);

4.46 Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

4.47 Modo Camada 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do

tráfego em nívelde aplicação;

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

4.49 Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;

4.50 Suporte à configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo:

4.51 Em modo transparente;

4.52 Em layer 3;

4.53 A configuração em alta disponibilidade deve sincronizar:

4.54 Sessões;

4.55 Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de rede;

4.56 Certificados de-criptografados;

4.57 Associações de Segurança das VPNs;

4.58 Tabelas FIB;

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

4.60 As funcionalidades de controle de aplicações, VPN IPSec e SSL, QOS, SSL e SSH Decryp on e protocolos de roteamento dinâmico devem operar em caráter permanente, podendo ser u lizadas por tempoindeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.

4.61 Deverá suportar controles por zona de segurança.

4.62 Controles de políticas por porta e protocolo.

4.63 Controle de políticas por aplicações grupos está cos de aplicações, grupos dinâmicos de aplicações(baseados em características e comportamento das aplicações) e categorias de aplicações.

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

4.65 Deve suportar a consulta a fontes externas de endereços IP, domínios e URLs podendo ser adicionadosnas políticas de firewall para bloqueio ou permissão do tráfego;

4.66 Deve permitir autenticação segura através de certificado nas fontes externas de endereços IP, domíniose URLs;

4.67 Deve permitir consultar e criar exceção para objetos das listas externas a par r da interface de gerênciado próprio firewall;

4.68 Controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS).

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

4.70 Deve descriptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2;

4.71 Deve descriptografar sites e aplicações que u lizam certificados ECC, incluindo Elliptical Curve DigitalSignature Algorithm (ECDSA);

4.72 Controle de inspeção e de-criptografia de SSH por política;

4.73 A de-criptografia de SSH deve possibilitar a identificação e bloqueio de tráfego caso o protocolo estejasendo usado para tunelar aplicações como técnica evasiva para burlar os controles de segurança;

4.74 Bloqueios dos seguintes pos de arquivos: bat, cab, dll, exe, pif, e reg

4.75 Traffic shaping QoS baseado em Políticas (Prioridade, Garan a e Máximo)

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

4.77 Suporte a objetos e regras IPV6.

4.78 Suporte a objetos e regras multicast.

4.79 Deve suportar no mínimo três tipos de negação de tráfego nas políticas de firewall: Drop sem notificação do bloqueio ao usuário, Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão;

4.80 Suportar a atribuição de agendamento as políticas com o objetivo de habilitar e desabilitar políticas emhorários pré-definidos automaticamente.

4.4.5.1.2 - **CARACTERISTICAS DO CONTROLE DE APLICAÇÕES**

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

2 Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas eprotocolos.

3 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;

4 Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix,logmein, teamviewer, ms-rdp, vnc, gmail, youtube, h p-proxy, h p-tunnel, facebook chat, gmail chat, whatsapp,

4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp,p, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs, etc;

5 Deve inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo. A checagem de assinaturas também deve determinar se uma aplicação está u lizando a porta default ou não, incluindo, mas nãolimitado a RDP na porta 80 ao invés de 389;

6 Deve aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado,incluindo, mas não limitado a Encrypted Bittorrent e aplicações VOIP que u lizam criptografia proprietária;

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

8 Para tráfego criptografado SSL, deve descriptografar pacotes a fim de possibilitar a leitura de payload parachecagem de assinaturas de aplicações conhecidas pelo fabricante;

9 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 funcionalidadesespecificas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas;

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

11 Identificar o uso de táticas evasivas via comunicações criptografadas;

12 Atualizar a base de assinaturas de aplicações automaticamente;

13 Reconhecer aplicações em IPv6;

14 Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuáriose grupos do LDAP/AD;

15 Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsot Active Directory, sem a necessidade de instalação de agente no Domain Controller, nemnas estações dos usuários;

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

17 Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagemde assinaturas, decodificação de protocolos e análise heurística;

18 Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e nãosomente sobre aplicações conhecidas;

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

20 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 seguintesprotocolos:

21 HTTP, FTP, SMB, SMT P, Telnet, SSH, MS-SQL, IMAP, IMAP, MS-RPC, RTSP e File body.

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

23 Deve alertar o usuário quando uma aplicação for bloqueada;

24 Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;

25 Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, neonet, etc.) possuindogranularidade de controle/políticas para os mesmos;

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

27 Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Gtalk chat ebloquear a transferência de arquivos;

28 Deve possibilitar a diferenciação de aplicações Proxies (ghostsurf, freegate, etc.) possuindo granularidade decontrole/políticas para os mesmos; 13.2.28. Deve ser possível a criação de grupos está cos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:

29 Tecnologia u lizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc).

30 Nível de risco da aplicação.

31 Categoria e subcategoria de aplicações.

32 Aplicações que usem técnicas evasivas, u lizadas por malwares, como transferência de arquivos e/ou usoexcessivo de banda, etc.

4.4.5.1.3 CARACTERISTICAS DA PREVENÇÃO DE AMEAÇAS

1 Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS,

Antivírus e AntiSpyware integrados no próprio appliance de Firewall ou entregue através de composição comoutro equipamento ou fabricante.

2 A prevenção de ameaças deve suportar proteção de, no mínimo, 20Gbps com suporte à camada 7, IPS, anti-vírus e anti-spyware habilitados simultaneamente e mensurado em simulação de tráfego enterprise mix ou que simule ambiente com trafego real;

3 Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus eAntiSpyware);

4 As funcionalidades de IPS, Antivírus e AntiSpyware devem operar em caráter permanente, podendo ser u lizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.

5 Deve sincronizar as assinaturas de IPS, Antivírus, AntiSpyware quando implementado em alta disponibilidadeativo/ativo e ativo/passivo;

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

7 As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo demonitoração;

8 Exceções por IP de origem ou de destino devem ser possíveis nas regras, de forma geral e assinatura aassinatura;

9 Deve suportar granularidade nas políticas de IPS Antivírus e AntiSpyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação detodos esses itens.

10 Deve permitir o bloqueio de vulnerabilidades.

11 Deve permitir o bloqueio de exploits conhecidos.

12 Deve incluir proteção contra-ataques de negação de serviços.

13 Deve suportar a inspeção e criação de regras de proteção de DOS e QOS para o conteúdo de tráfegotunelados pelos protocolos GRE e IPSEC não criptografado;

14 Deverá possuir os seguintes mecanismos de inspeção de IPS:

15 Análise de padrões de estado de conexões;

16 Análise de decodificação de protocolo;

17 Análise para detecção de anomalias de protocolo;

18 Análise heurística;

19 IP Defragmentation;

20 Remontagem de pacotes de TCP;

21 Bloqueio de pacotes malformados.

22 Ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPfloof, etc;

23 Detectar e bloquear a origem de portscans com possibilidade de criar exceções para endereços IPs deferramentas de monitoramento da organização;

24 Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;

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

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

27 Possuir assinaturas para bloqueio de ataques de buffer overflow;

28 Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

29 Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS e AntiSpyware,permitindo a criação de exceções com granularidade nas configurações;

30 Permitir o bloqueio de vírus e spyware em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMT P ePOP3;

31 É permitir do uso de appliance externo (Antivírus de rede), para o bloqueio de vírus e

spyware em protocoloSMB de forma a conter malwares se espalhando horizontalmente pela rede;

32 Suportar bloqueio de arquivos por tipo;

33 Identificar e bloquear comunicação com botnets;

34 Deve suportar várias técnicas de prevenção, incluindo Drop e tcp-rst (Cliente, Servidor e ambos);

35 Deve suportar referência cruzada com CVE;

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

37 O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da açãotomada pelo dispositivo;

38 Deve suportar a captura de pacotes (PCAP), por assinatura de IPS e AntiSpyware;

39 Deve permitir que na captura de pacotes por assinaturas de IPS e AntiSpyware seja definido o número de pacotes a serem capturados. Esta captura deve permitir selecionar, no mínimo, 50 pacotes;

40 Deve possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos sejam resolvidas pelo Firewall com endereços (IPv4 e IPv6), previamente definidos;

41 Permitir o bloqueio de vírus, pelo menos, nos seguintes protocolos: HTTP, FTP, SMB, SMT P e POP3;

42 Os eventos devem identificar o país de onde par u a ameaça;

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

44 Proteção contra downloads involuntários usando HTTP de arquivos executáveis Maliciosos.

45 Rastreamento de vírus em Pdf.

46 Deve permitir a inspeção em arquivos comprimidos que u lizam o algoritmo deflate (zip, gzip, etc.)

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

4.4.5.1.4 ANÁLISE DE MALWARES MODERNOS

1 Devido aos Malwares hoje em dia serem muito dinâmicos e um antivírus comum reativo não ser capaz de detectar os mesmos com a mesma velocidade que suas variações são criadas, a solução ofertada dever possuirfuncionalidades para análise de Malwares não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante;

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

3 Selecionar através de políticas granulares quais tipos de arquivos sofrerão esta análise incluindo, mas não limitado a: endereço IP de origem/destino, usuário/grupo do AD/LDAP, aplicação, porta, URL/categoria de URL dedestino, tipo de arquivo e todas estas opções simultaneamente;

4 Deve possuir a capacidade de diferenciar arquivos analisados em pelo menos três categorias: malicioso, não malicioso e arquivos não maliciosos, mas com características indesejáveis como softwares que deixa o sistema operacional lento, que alteram parâmetros do sistema, etc.;

5 Suportar a análise com pelo menos 100 (cem) tipos de comportamentos maliciosos para a análise da ameaça não conhecida;

6 Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacionalWindows XP, Windows 7 (32 bits) e

7 Windows 7 (64 bits);

8 Deve suportar a monitoração de arquivos trafegados na internet (HTTPs, FTP, HTTP, SMT P) como tambémarquivos trafegados internamente entre servidores de arquivos usando SMB em todos os modos de implementação: sniffer, transparente e L3;

9 A solução deve possuir a capacidade de analisar em Sandbox links (h p e h ps) presentes no corpo de e-mails trafegados em SMT P e POP3. Deve ser gerado um relatório caso a abertura do link pela Sandbox o identifique como site hospedeiro de exploits;

10 A análise de links em Sandbox deve ser capaz de classificar sites falsos na categoria de phishing e atualizar abase de filtro de URL da solução;

11 Para ameaças trafegadas em protocolo SMT P e POP3, a solução deve ter a capacidade de mostrar nosrelatórios o remetente, destinatário e assunto dos e-mails permitindo identificação ágil do usuário vítima do ataque;

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

13 O sistema automático de análise "In Cloud" ou local deve emitir relatório com identificação de quais soluções de Antivírus existentes no mercado possuem assinaturas para bloquear o malware;

14 Deve permitir exportar o resultado das análises de malwares de dia Zero em PDF e CSV a par r da própriainterface de gerência;

15 Deve permitir o download dos malwares identificados a par r da própria interface de gerência;

16 Deve permitir visualizar os resultados das análises de malwares de dia zero nos diferentes sistemasoperacionais suportados;

17 Deve permitir informar ao fabricante quanto a suspeita de ocorrências de falso-positivo e falso-negativo naanálise de malwares de dia zero a par r da própria interface de gerência.

18 Caso a solução seja fornecida em appliance local, deve possuir, no mínimo, 28 ambientes controlados (sand-box) independentes para execução simultânea de arquivos suspeitos;

19 Caso seja necessárias licenças de sistemas operacional e softwares para execução de arquivos no ambientecontrolado (sand-box), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante;

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

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

22 Deve atualizar a base com assinaturas para bloqueio dos malwares identificados em sand-box comfrequência de, pelo menos, 5 minutos;

23 Permitir o envio de arquivos e links para análise no ambiente controlado de forma automática via API. 13.4.23. Deve permitir o envio para análise em sand-box de malwares bloqueados pelo Antivírus da solução;

4.4.5.1.5 FILTRO DE URL

1 A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

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

3 Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, Ips, Redes e Zonas de segurança.

4 Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está u lizandoquais URLs através da integração com serviços de diretório, autenticação via

ldap, Active Directory, E-directory e base de dados local.

5 Permite popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;

6 Suporta a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

7 Deve bloquear o acesso a sites de busca (Google, Bing e Yahoo), caso a opção Safe Search esteja desabilitada. Deve ainda exibir página de bloqueio fornecendo instruções ao usuário de como habilitar a função;

8 Suporta base ou cache de URLs local no appliance, evitando delay de comunicação/validação das URLs;

9 Possui pelo menos 60 categorias de URLs;

10 A categorização de URL deve analisar toda a URL e não somente até o nível de diretório;

11 Suporta a criação categorias de URLs customizadas;

12 Suporta a exclusão de URLs do bloqueio, por categoria;

13 Permite a customização de página de bloqueio;

14 Deve proteger contra o roubo de credenciais, usuários e senhas identificadas através da integração com Active Directory submetidos em sites não corporativos. Deve ainda permitir criação de regra onde usuários do Active Directory só possam enviar informações de login para sites autorizados na solução;

15 Deve permitir bloquear o acesso do usuário caso o mesmo tente fazer o envio de suas credencias em sitesclassificados como phishing pelo filtro de URL da solução;

16 Permite 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 ousuário continuar acessando o site);

17 Suporta a inclusão nos logs do produto de informações das atividades dos usuários;

18 Deve salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs:UserAgent, Referer, e X-Forwarded For;

4.4.5.1.6 IDENTIFICAÇÃO DE USUÁRIOS

1 Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está u lizandoquais aplicações através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local;

2 Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindogranularidade de controle/políticas baseadas em usuários e grupos de usuários;

3 Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade decontrole/políticas baseadas em usuários e grupos de usuários;

4 Deve implementar a criação de políticas de segurança baseada em atributos específicos do Radius, incluindo, mas não limitado a: baseado no sistema operacional do usuário remoto exigir autenticação padrão Windows e on-me password (OTP) para usuários Android;

5 Deve possuir integração com Ldap para identificação de usuários e grupos permitindo granularidade decontrole/políticas baseadas em Usuários e Grupos de usuários;

6 Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x esoluções NAC via syslog, para a identificação de endereços IP e usuários;

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

8 Suporte a autenticação Kerberos;

9 Deve suportar autenticação via Kerberos para administradores da plataforma de segurança, captive portal eusuário de VPN SSL;

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

11 Deve identificar usuários através de leitura do campo x-fowarded-for, populando nos logs do firewall oendereço IP, bem como o usuário de rede responsável pelo acesso;

12 Deve permitir a criação de políticas de segurança baseadas em usuários de rede com reconhecimento dosmesmos através de leitura do campo xfowarded-for;

13 O firewall deve operar/suportar Security Asser on Markup Language (SAML) 2.0, com single sign-on e singlelogout para as funcionalidades de Captive Portal e VPN SSL (client to server), permitindo login único e interativo para fornecer acesso automático a serviços autenticados, internos e externos a organização;

14 Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos doLDAP/AD;

15 Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP emservidores acessados remotamente, mesmo que não sejam servidores Windows.

4.4.5.1.7 QOS

1 Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como YouTube, upstream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de bandaquando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming.

2 Suportar a criação de políticas de QoS por:

3 Endereço de origem

4 Endereço de destino

5 Por usuário e grupo do LDAP/AD.

6 Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus; 13.7.2.5. Por porta;

7 O QoS deve possibilitar a definição de classes por:

8 Banda Garantida

9 Banda Máxima

10 Fila de Prioridade.

11 Suportar priorização RealTime de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicaçõescomo Skype.

12 Suportar marcação de pacotes Diffserv, inclusive por aplicação;

13 Deve implementar QOS (traffic-shapping), para pacotes marcados por outros a vos na rede (DSCP). Apriorização e limitação do tráfego deve ser efetuada nos dois sentidos da conexão (inboud e outbound);

14 Disponibilizar estatísticas RealTime para classes de QoS.

15 Deve suportar QOS (traffic-shapping), em interface agregadas;

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

4.4.5.1.8 FILTRO DE DADOS

1 Permite a criação de filtros para arquivos e dados pré-definidos;

2 Os arquivos devem ser identificados por extensão e assinaturas;

3 Permite identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc)identificados sobre aplicações (P2P, Instant Messaging, SMB, etc);

4 Suportar identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses tipos dearquivos;

5 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;

6 Permitir listar o número de aplicações suportadas para controle de dados;

7 Permitir listar o número de tipos de arquivos suportados para controle de dados;

4.4.5.1.9 GEO-LOCALIZAÇÃO

1 Suportar a criação de políticas por Geo Localização, permitindo o tráfego de determinado País/Países sejambloqueados.

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

3 Deve permitir visualizar nos logs e criar políticas para liberar e bloquear tráfego de países por tipo de arquivo,aplicação e categoria de URL;

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

5 VPN

6 Deve possuir suporte a 18 Gbps de tráfego VPN;

7 Suportar VPN Site-to-Site e Cliente-To-Site;

8 Suportar IPSec VPN;

9 Suportar SSL VPN;

10 A VPN IPSEc deve suportar:

11 DES e 3DES;

12 Autenticação MD5 e SHA-1;

13 Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;

14 Algoritmo Internet Key Exchange (IKEv1 e v2); 13.10.5.5. AES 128, 192 e 256 (Advanced EncryptionStandard)

15 Autenticação via certificado IKE PKI.

16 Deve possuir interoperabilidade com os seguintes fabricantes:

16.1 Cisco;

16.2 Checkpoint;

16.3 Juniper;

16.4 Palo Alto Networks;

16.5 Fortinet;

16.6 Sonic Wall;

17 Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEc a par r dainterface gráfica da solução, facilitando o processo de troubleshooting;

18 A VPN SSL deve suportar:

19 O usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou pormeio de interface WEB;

20 A funcionalidades de VPN SSL devem ser atendidas com e sem o uso de agente;

21 Atribuição de endereço IP nos clientes remotos de VPN SSL;

22 Deve permitir a atribuição de IPs fixos nos usuários remotos de VPN SSL;

23 Deve permitir a criação de rotas de acesso e faixas de endereços IP atribuídas a clientes remotos de VPN deforma customizada por usuário

24 AD/LDAP e grupo de usuário AD/LDAP;

25 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;

26 Atribuição de DNS nos clientes remotos de VPN;

27 Deve permitir que seja definido métodos de autenticação distintos por sistema operacional do dispositivoremoto de VPN (Android, IOS, Mac

28 Windows e Chrome OS);

29 A solução de VPN deve verificar se o cliente que está conectando é o mesmo para o qual o certificado foiemitido inicialmente. O acesso deve ser bloqueado caso o dispositivo não seja o correto;

30 Deve possuir lista de bloqueio para dispositivos que forem reportados com roubado ou perdido pelo usuário;

31 Deve haver a opção de ocultar o agente de VPN instalado no cliente remoto, tornando

o mesmo invisível paraо usuário;

32 Deve exibir mensagens de notificação customizada toda vez que um usuário remoto se conectar a VPN. Devepermitir que o usuário desabilite a exibição da mensagem nas conexões seguintes;

33 Deve avisar ao usuário remoto de VPN quanto a proximidade da expiração de senha LDAP. Deve permitirtambém a customização da mensagem com informações relevantes para o usuário;

34 Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, AntiSpyware e filtro de URL paratráfego dos clientes remotos conectados na VPN SSL;

35 A VPN SSL deve suportar proxy arp e uso de interfaces PPPOE;

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

37 Deve permitir a distribuição de certificado para o usuário de remoto através do portal de VPN de formaautomatizada;

38 Deve possuir lista de bloqueio para dispositivos em casos quando, por exemplo, o usuário reportar que odispositivo foi perdido ou roubado;

39 Permite estabelecer um túnel VPN client-to-site do cliente a plataforma de segurança, fornecendo umasolução de single-sign-on aos usuários, integrando-se com as ferramentas de Windows-logon;

40 Suporta leitura e verificação de CRL (certificate revoca on list);

41 Permite a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneisSSL;

42 O agente de VPN a ser instalado nos equipamentos desktop e laptops, dever ser capaz de ser distribuído demaneira automática via Microsoft SMS, Active Directory e ser descarregado diretamente desde o seu próprio portal, o qual residirá no centralizador de VPN;

43 O agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário,

44 Deve permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas:

45 Antes do usuário autenticar na estação;

46 Após autenticação do usuário na estação;

47 Sob demanda do usuário;

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

49 O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows XP, Vista Windows 7,Windows 8, Mac OSx e Chrome OS;

50 O portal de VPN deve enviar ao cliente remoto, a lista de gateways de VPN a vos para estabelecimento daconexão, os quais devem poder ser administrados centralmente;

51 Deve haver a opção de o cliente remoto escolher manualmente o gateway de VPN e de forma automáticaatravés da melhor rota entre os gateways disponíveis com base no tempo de resposta mais rápido;

52 Deve possuir a capacidade de identificar se a origem da conexão de VPN é externa ou interna;

4.4.5.1.10 CONSOLE DE GERÊNCIA E MONITORAÇÃO

1 Centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento;

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

3 Deve permitir substituir o certificado de fábrica no acesso HTTPS a gerência do firewall como possibilidade deuso de certificado criado localmente na própria solução ou importado de fonte externa;

4 Caso haja a necessidade de instalação de cliente para administração da solução o mesmo deve ser compatívelcom sistemas operacionais

5 Windows e Linux;

6 O gerenciamento deve permitir/possuir:

7 Criação e administração de políticas de firewall e controle de aplicação;

8 Criação e administração de políticas de IPS, Antivírus e AntiSpyware;

9 Criação e administração de políticas de Filtro de URL;

10 Monitoração de logs;

11 Ferramentas de investigação de logs;

12 Debugging;

13 Captura de pacotes.

14 Acesso concorrente de administradores;

15 Deve permitir que administradores concorrentes façam modificações, valide configurações e reverta configurações do firewall simultaneamente e que cada administrador consiga aplicar apenas as suas alteraçõesde forma independente das realizadas por outro administrador;

16 Deve mostrar ao administrador do firewall a hora e data do último login e tentativas de login com falha paraacessos a par r da interface gráfica e CLI.

17 Deve possuir mecanismo busca global na solução onde possa se consultar por uma string tais como: nomede objetos, ID ou nome de ameaças, nome de aplicações, nome de políticas, endereços IPs, permitindo a localização e uso dos mesmos na configuração do dispositivo;

18 Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização decomandos;

19 Deve permitir usar palavras chaves e cores para facilitar identificação de regras;

20 Deve permitir monitorar via SNMP falhas de hardware, inserção ou remoção de fontes, discos e coolers, uso de recursos por número elevado de sessões, número de túneis estabelecidos na VPN cliente-to-site, porcentagem de utilização em referência ao número total suportado/licenciado e número de sessões estabelecidas, estatísticas/taxa de logs, uso de disco, período de retenção dos logs e status do envio de logs parasoluções externas;

21 Deve suportar também o monitoramento dos seguintes recursos via SNMP: IP fragmenta on, TCP state edropped packets;

22 Bloqueio de alterações, no caso acesso simultâneo de dois ou mais administradores;

23 Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso deleitura, criação de usuários, alteração de configurações;

24 Autenticação integrada ao Microsoft Active Directory e servidor Radius;

25 Localização de em quais regras um endereço IP, IP Range, subnet ou objetos estão sendo u lizados;

26 Deve atribuir sequencialmente um número a cada regra de firewall, NAT, QOS e regras de DOS;

27 Criação de regras que fiquem ativas em horário definido;

28 Criação de regras com data de expiração;

29 Backup das configurações e rollback de configuração para a última configuração salva;

30 Suportar Rollback de Sistema Operacional para a última versão local;

31 Habilidade de upgrade via SCP, TFTP e interface de gerenciamento;

32 Deve possuir mecanismo de análise de impacto na política de segurança antes de atualizar a base com novasaplicações disponibilizadas pelo fabricante;

33 Validação de regras antes da aplicação;

34 Deve implementar mecanismo de validação de configurações antes da aplicação das mesmas permitindoidentificar erros, tais como: rota de destino inválida, regras em shadowing etc.

35 É permitido o uso de appliance externo para permitir a validação de regras antes da aplicação.

36 Validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);

37 É permitido o uso de appliance externo para permitir a validação de políticas, avisando quando houver regrasque, ofusquem ou conflitem com outras (shadowing);

38 Deve possibilitar a visualização e comparação de configurações Atuais, configuração anterior e configuraçõesantigas.

39 Deve possibilitar a integração com outras soluções de SIEM de mercado (third-party SIEM vendors)

40 Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizoue o horário da alteração;

41 Deverá ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização deaplicações na rede no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado;

42 Geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens edestinos do tráfego gerado na instituição;

43 Deve prover relatórios com visão correlacionada de aplicações, ameaças (IPS, Antivírus e Anti-Spware),URLs e filtro de arquivos, para melhor diagnóstico e resposta a incidentes;

44 Deve permitir a criação de Dash-Boards customizados para visibilidades do tráfego de aplica vos, usuários, categorias de URL, ameaças identificadas pelo IPS, Antivírus, AntiSpyware, malwares "Zero Day" detectados emsand-box e tráfego bloqueado;

45 O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelosdispositivos de segurança;

46 Dever permitir a visualização dos logs de malwares modernos, tráfego (IP de origem, destino, usuário eporta), aplicação, IPS, Antivírus, AntiSpyware, Filtro de URL e filtro de arquivos em uma única tela.

47 Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-Spware), etc;

48 Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus e AntiSpyware), eURLs que passaram pela solução;

49 Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em RealTime;

50 Nas opções de "Drill-Down", ser possível identificar o usuário que fez determinado acesso;

51 Deve possuir relatório de visibilidade e uso sobre aplica vos (SaaS). O relatório também deve mostrar osriscos para a segurança do ambiente, tais como a entrega de malwares através de aplica vos SaaS com a informação do usuário responsável pelo acesso;

52 Os relatórios de visibilidade e uso sobre aplica vos (SaaS) devem poder ser extraídos por grupo de usuáriosapresentando o uso e consumo de aplicações por grupo de usuário;

53 Deve ser possível exportar os logs em CSV;

54 Deverá ser possível acessar o equipamento a aplicar configurações durante momentos onde o trafego é muitoalto e a CPU e memória do equipamento es ver totalmente u lizada.

55 Rotação do log;

56 Deve permitir que os logs e relatórios sejam rotacionados automaticamente baseado no tempo em que estãoarmazenados na solução, assim como no espaço em disco usado;

57 Deve permitir fazer o envio de logs para soluções externas de forma granular podendo selecionar quaiscampos dos logs serão enviados incluindo, mas não limitado a: tipo de ameaça, usuário, aplicação, etc;

58 Exibição das seguintes informações, de forma histórica e em tempo real (atualizado de forma automática econtinua a cada 1 minuto):

59 Situação do dispositivo e do cluster;

60 Principais aplicações;

61 Principais aplicações por risco;

62 Administradores autenticados na gerência da plataforma de segurança;

63 Número de sessões simultâneas;

64 Status das interfaces;

65 Uso de CPU;

66 Geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:

67 Resumo gráfico de aplicações u lizadas;

68 Principais aplicações por utilização de largura de banda de entrada e saída;

69 Principais aplicações por taxa de transferência de bytes;

70 Principais hosts por número de ameaças identificadas;

71 Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e AntiSpyware), de rede vinculadas a estetráfego;

72 Deve permitir a criação de relatórios personalizados;

Em cada critério de pesquisa do log deve ser possível incluir múltiplas entradas (ex. 10 redes e IP's distintos;serviços HTTP, HTTPS e SMTP), exceto no campo horário, onde deve ser possível definir um faixa de tempo como critério de pesquisa;

73 Gerar alertas automáticos via:

74 Email;

75 SNMP;

76 Syslog;

4.4.5.1.11 REQUISITOS MÍNIMOS DO(s) WAF (WEB APPLICATIONS FIREWALL)

1 A solução de WAF deve, minimamente:

2 Ter capacidade de proteger um domínio Master (*.creasp.org.br)

3 Ter capacidade de proteger no mínio 50 aplicações hospedadas nos servidores do CREA-SP

4 Ter capacidade para atender o tráfego total dos enlaces de rede disponibilizados pela CONTRATADA para o CREA-SP. (não há informações de utilização de banda disponíveis para o cálculo da capacidade, portanto a CONTRATADA deverá estimar a capacidade com os dados fornecidos neste documento).

5 Possuir regras de detecção e bloqueio pré-definidas, baseadas em assinaturas;

6 As regras pré-definidas devem ser atualizadas periodicamente de forma automática pelo fabricante;

7 Permitir a criação de novas regras, com parâmetros e expressões regulares definidos pelo administrador;

8 Permitir que novas assinaturas provenientes de atualizações passem por um período de

simulação, em que nenhuma requisição que viole a assinatura seja bloqueada, e sim apenas registrada em log.

9 Permitir a detecção e bloqueio de ataques a aplicações Web dos tipos abaixo:

10 SQL, Cookie e Command Injection;

11 Cross-Site Scripting (XSS);

12 Cross-Site Request Forgery;

13 Violações do protocolo HTTP;

14 Web Parameter Tampering;

15 Cookie Tampering;

16 Code Injection;

17 Permitir a detecção e bloqueio de crawlers e/ou scanners de vulnerabilidade Web;

18 Permitir a detecção e bloqueio da resposta de determinada aplicação Web nos casos abaixo:

19 Ausência de tratamento de erros pela aplicação;

20 Vazamento de dados.

21 Proteger contra de ataques de força bruta em páginas de login;

22 Permitir o bloqueio de métodos HTTP a critério do usuário;

23 Permitir o bloqueio de ataques no modo blacklisting (bloqueio de ataques conhecidos por assinatura) e whitelisting (permitir apenas requisições e respostas conhecidas);

24 Possuir funcionalidade de aprendizagem automática do funcionamento de uma aplicação Web, suas URLs,parâmetros, campos de formulário, cookies, dentre outras, para a configuração do bloqueio por blacklisting;

25 Permitir a customização, pelo administrador, dos parâmetros aprendidos, de forma a criar regras baseadas notamanho do parâmetro, tipo de conteúdo, e expressões regulares.

26 Permitir o mapeamento de diversas aplicações em um mesmo IP virtual, enviando informações paraconjuntos de servidores diferentes de acordo com a URL requisitada;

27 Permitir o mapeamento em um mesmo IP virtual, de acordo com a URL requisitada, que exija certificadodigital de cliente para algumas aplicações e não exija para outras.

28 Permitir a criação de regras por diretório que liberem apenas determinados tipos de

arquivo;

29 Permitir a aplicação de novas regras sem interromper as conexões já abertas;

30 Permitir o bloqueio, automático ou manual, de IPs de origem que realizarem muitas conexões;

31 Permitir a inclusão do IP do cliente no campo X-Forwarded-For;

32 Funcionar como proxy reverso de aplicações;

33 Permitir a inclusão de parâmetros customizados nos cabeçalhos (headers) HTTP, além da alteração dosexistentes, para envio à aplicação de destino;

34 Recursos proativos de segurança de aplicativos

35 Cross Site Scripting (XSS)

36 Permitir a criação de regras personalizadas em padrões XSS específicos;

37 Excluir cargas úteis de XSS suspeitas;

38 Validação de entrada gerada pelo usuário;

39 Detectar tentativas de execução de código malicioso em um banco de dados ou script;

40 Aplicar criptografia para dados em trânsito;

41 Filtrar tráfego de saída para vazamento de dados;

42 Mascarar dados sensíveis;

43 Mascarar dados confidenciais, como SSN, informações de cartão de crédito;

44 Proteger os dados do usuário e da sessão contra a exposição por meio de links fracos, como cookies desessão e tokens.

45 Implementar controles sobre tempos limite e limites de sessão do usuário;

46 Alterar cookies de sessão fraca para gerenciamento de sessão segura;

47 Certificar que as sessões de usuário comecem em pontos de entrada aprovados;

48 Identificar vulnerabilidades e ataques conhecidos por lista negra e/ou expressões regulares;

49 Aplicar URLs qualificadas para proteger contra redirecionamentos indesejados;

50 Falhas de injeção por meio de vetores como SQL, LDAP ou Shell;

51 As regras personalizadas podem ser definidas para procurar padrões específicos do aplicativo;

52 Gestão Segura de Sessão;

53 Proteção de linha de base;

54 Permitir a atualização de políticas através do Proteção de Linha de Base;

55 Protege contra validação fraca de critérios de redirecionamento;

56 Defina os alvos de redirecionamento preferidos para interceptar os ataques;

57 Permitir relatórios de:

58 Versão do conjunto de regras de detecção;

59 Versão do conjunto de regras de proteção;

60 Lista de administradores de aplicativos;

61 Lista das definições de conjunto de regras;

62 Lista dos hosts dos aplicativos;

63 Lista das licenças de instalação;

64 Análise consolidada do arquivo de log para cada host do aplicativo, listando:

65 solicitações negadas por IP, solicitações negadas por URI

66 Solicitações por nome do manipulador, solicitações por IP

4.4.5.2 REQUISITOS DE GERENCIAMENTO DE EVENTOS DE SEGURANÇA DA INFORMAÇÃO (SIEM)

1 A CONTRATADA deve fornecer um SIEM, para o qual, através de sensores, os ativos de rede, servidores esistemas de segurança monitorados devem enviar eventos;

2 Os dados coletados devem ser processados e correlacionados usando boas práticas de segurança e IA(Inteligência Artificial).

3 Através de integração com o ITSM, os eventos devem gerar alarmes, que devem ser analisados e tratados peloSOC.

4 O sistema SIEM deve ser exclusivo para tratamento das informações do CREA-SP.

5 A Contratada deve fornecer usuários e senhas com permissão de leitura à interface gráfica WEB do SIEM paraos analistas da equipe de Infraestrutura do CREA-SP.

6 O Sistema de SIEM, com gerenciamentos dos logs pertencentes ao negócio e infraestrutura, deve cobrir os itensrelacionados à segurança deverão abranger a integralidade da solução apresentada, tratando-a de maneira integrada e unificada;

7 A CONTRATADA deverá fornecer uma capacidade de 150 GB por dia de tratamento de Logs para tratamento, nomínimo, dos seguintes dispositivos;

7.1 O SIEM deverá coletar logs de todos os servidores da infraestrutura do CREA-SP hospedados naCONTRATADA

7.2 O SIEM deverá coletar logs de todos os bancos de dados do CREA-SP hospedados na CONTRATADA (inicialmente entre (inicialmente entre 80 a 100 bancos de dados SQL Server/MySQL/PostGreSQL/DB2)

7.3 O SIEM deverá coletar logs de todos os dispositivos de redes (switches, roteadores, hosts, storages,. etc) esegurança (AWF, Firewall, Load Balancer, .etc) contratados (dispositivos fornecidos pela CONTRATADA)

7.4 O SIEM deverá coletar logs de todos os servidores WEB do CREA-SP (inicialmente entre 20 e 30)

7.5 O SIEM deverá coletar logs das aplicações de missão crítica do CREA-SP hospedadas na CONTRATADA.(Inicialmente entre 1500 a 2000 aplicações)

7.6 No advento do CREA-SP contratar um serviço de segurança (SOC + SIEM) para os equipamentos da suainfraestrutura interna e maquinas virtuais:

7.6.1 A CONTRATADA deverá compartilhar os logs e dados do SIEM fornecido com o SIEM da novaempresa contratada do CREA-SP.

4.4.5.3 REQUISITOS DO COFRE DE SENHAS

1 A Contratada deverá fornecer um cofre de senhas para 10 usuários com as seguintes características mínimas:

1.1 Função Auditoria, que analisa a força das senhas e identifica as que precisam ser mudadas ou que estãorepetidas;

1.2 Função que avisa quando uma senha vazar;

1.3 Autenticação de dois fatores;

1.4 Criptografia AES de 256 bits.

1.5 Senhas ilimitadas

1.6 Criptografia ponta a ponta

4.4.5.4 REQUISITOS GERAIS DO SISTEMA DE SOC COM GESTÃO DE VULNERABILIDADES

1 Escopo:

1.1 Todo o Hardware de servidores (com seus sistemas operacionais: vmware, windows, etc) e equipamentos(switches, roteadores, firewalls, etc) fornecidos pela CONTRATADA no escopo da contratação atual.

1.2 Não inclui os servidores virtuais do CREA-SP

4.4.5.5 REQUISITOS DA LEI GERAL DE PROTEÇÃO DE DADOS

1 Os requisitos legais da LGPD, nos termos da lei Nº 13.709/2018, que a contratada deverá seguir estão no anexo: Clausulas_de_protecao_de_dados_LEI_N_13.709_2018_-_DATA_CENTER

4.4.6 REQUISITOS GERAIS DE BALANCEAMENTO DE CARGA LOCAL

1 Visando alta disponibilidade dos serviços pertencentes ao CREA-SP e a distribuição dos acessos as aplicações, faz- se necessária a inclusão da camada de Load Balance (Balanceador de Carga), de modo a balancear o tráfego das requisições de serviço, através de um grupo de dispositivos, respondendo simultaneamente aos elementos pertencentes à rede do CREA- SP. Os equipamentos deverão ser dedicados ao CREA-SP, físicos ou virtuais, configurados em Alta Disponibilidade.

4.4.6.1 CARACTERÍSTICAS GERAIS

1 Deve ser ofertado em modelo de appliance virtual (tratado neste termo simplesmente como “appliance”) e ser instalável em plataforma de virtualização Vmware vSphere 5.0 ou superior, KVM, OracleVM, Microsoft Hyper-V 2012 e 2012R2 e XenServer 6.1 ou superior. Também deve suportar instalação no modelo “bare metal” de arquitetura x86;

2 Licenças de software devem ser perpétuas e ser licenciada de modo que não tenha restrição de uso de qualquer funcionalidade ou recurso de software, ou seja, isso significa que a solução deve vir com todas as licençasdisponíveis para o modelo;

3 Deve ser ofertado licenciamento que permita a portabilidade da solução para emprego em ambientes virtuais, cloud e bare metal;

4 A solução deve ser licenciada por appliance virtual, não importando o número de processadores, interfaces derede ou servidores back-end a serem balanceados;

5 A solução deve ser licenciada pelo agregado de banda e não limitada e vinculada ao processamento do hardware do servidor. Caso a solução ofertada possua licenciamento vinculado ao processador do hardware, estedeve ser entregue licenciado para suportar a solução completa de servidores scale-out deste processo;

6 A solução deve ser capaz de realizar, no mínimo, os seguintes números de

desempenho (desde que seja atribuído recursos computacionais suficientes para o virtual appliance):

7 40 Gbps de throughput por apliance virtual;

8 Não deve haver limitação via software de transações SSL/TLS.

9 A solução deve ser licenciada para, no mínimo, 40Gbps por virtual appliance;

10 A comprovação de capacidade deverá seguir os seguintes critérios obrigatórios:

11 Medição em sentido único. Caso a solução apresente valores para ambas as direções, será considerado apenas 50% do valor apresentado;

12 Tráfego de saída para o cliente ou tráfego de entrada;

13 Capacidade após aplicado manipulação de Camada 7, ou seja, após a compressão; após aplicado caching. Não será considerado a apresentação de valores aplicados antes de manipulação de Camada 7;

14 Tráfego enviado a partir do servidor de balanceamento de carga para o cliente. Caso a solução apresente valores para ambas as solicitações de cliente mais as respostas do servidor, será considerado apenas 50% do valor apresentado;

15 Não será contabilizado os valores apresentados para a passagem pelo tráfego do tipo encaminhado ou “routedtraffic”;

16 Deve funcionar em conjunto com 1 (um) ou mais instâncias/virtual appliances de balanceadores/controladores, formando cluster ativo/ativo sem a necessidade de elementos externos;

17 O cluster de balanceadores deve comportar qualquer número entre 2 e 32 appliances virtuais, todos operandoativamente;

18 A solução deve implementar segurança de acesso;

19 No caso de falha de um dos appliances do cluster ativo/ativo, o seu par deverá assumir automaticamente as funções do balanceador falho (failover). Logo após restabelecido o serviço do balanceador falho, o appliances deverão voltar automaticamente a funcionar como um cluster ativo/ativo (failback);

20 Deve agrupar servidores back-end que entregam o mesmo serviço em um “pool” ou grupo;

21 Deve ser possível gerenciar a solução via interface de gerência, interface de front-end e interface back-end. Também deve ser possível bloquear acesso a gerência da solução através das interfaces citadas para que a implementação esteja de acordo com as normas de segurança da contratante;

22 Interface de gerenciamento WEB, que permita a configuração e o gerenciamento dos serviços de maneira simples e rápida;

23 Possibilitar a criação de uma ou mais interfaces de front-end que possuem um ou mais IPs acessíveis para tráfego front-end. Estas interfaces de front-end devem balancear o tráfego entre os servidores configurados no respectivo pool;

24 Ser apto e licenciado para usar toda a capacidade de acordo com o hardware disponível para efetuar suas operações - tais como caching, SSL e XML offload, compressão de conteúdo, controle de banda e rate shaping;

25 Suportar qualquer tipo de aplicação baseada em web (HTTP, HTTPS), e-mail (POP3, POP3S, SMTP, IMAPS,IMAPv2, IMAPv3, IMAPv4), FTP, Telnet, SSH, SIP (TCP e UDP), RTSP, bancos de dados SQL, SharePoint, IBM WebSphere Application Server, JBoss, GlassFish, entre outros;

26 A solução deve possuir mecanismo de otimização e aceleração de conteúdo de páginas web;

27 Realizar balanceamento de carga baseado nas camadas 4 a 7 entre servidores back-end que entregam um determinado serviço;

28 A solução deve implementar Route Health Injection;

29 Deve suportar mecanismo de segurança em camada 7;

30 A solução deve possuir firewall para aplicação Web e deve permitir gerenciamento transparente de sessão segura;

31 A solução de firewall para aplicação Web deve permitir criptografia de URL;

32 Deve ser possível customizar o balanceamento de acordo com scripts e criar regras condicionais para realizar obalanceamento;

33 Os scripts e regras condicionais devem ser capazes de:

34 Inspecionar tráfego em ambas direções (inbound e outbound);

35 De alterar o conteúdo do cabeçalho do pacote, URL de destino e/ou payload;

36 Redirecionar links inexistentes;

37 Direcionar conteúdo de web sites diferentes de acordo as regras de requisição;

38 Aplicar regras com critérios baseados em endereço IP;

39 Utilizar diferentes pools de servidores;

40 Mascarar informações acordo com uma expressão regular;

41 Permitir comparação de parâmetros com operadores: igual, diferente, contém, está vazio, não está vazio, expressão regular, termina com, começa com, entre outros.

42 Verificar Cookie, método HTTP, URL Path, porta TCP/UDP, Query SQL, SIP Version, SIP Method, RTSPVersion, RTSP Method;

43 Realizar as seguintes ações em caso de hit nas regras: gerar log de erros, warning e informação, definir throughput, drop de conexão, alterar pool de servidores, entre outras;

44 A funcionalidade de script não poderá ser limitada por licenciamento;

45 O balanceamento de carga deve ser feito nas camadas 4 a 7 da rede e diferentes algoritmos de balanceamentodevem estar disponíveis para cada serviço, dentre eles:

46 Round robin – Direciona as requisições alternadamente entre os servidores retaguarda;

47 Round-robin com peso - Direciona as requisições alternadamente entre os servidores back-end de forma proporcional aos seus pesos;

48 Menos conexões – Direciona as requisições para o servidor back-end com o menor número de conexões;

49 Menor tempo de resposta – Direciona as requisições para o servidor back-end com o menor tempo de resposta;

50 Menos conexões com peso - Direciona as requisições para o servidor back-end com base no seu número de conexões concorrentes e no seu peso;

51 Perceptivo ou preditivo - Monitora a carga e tempo de resposta dos servidores de back-end e direciona de acordo com algoritmo de otimização para que não haja sobrecarga em um servidor.

52 Deve possuir capacidade de monitorar qualidade da entrega (tempo de resposta) de serviços/aplicações de acordo com limites de tolerância customizáveis e gerar alertas de warning e críticos;

53 Deve possuir a capacidade de monitorar a status dos servidores de aplicação e gerar alertas baseados, no mínimo, nos seguintes parâmetros: ping, conexões TCP, HTTP e HTTPS. Deve ser possível customizar os thresholds.

54 Deve ser possível verificar visualmente através de sinalizações coloridas se foi detectado alguma tentativa deataque;

55 Realizar automaticamente a retirada de operação de um servidor back-end que apresente falha na aplicação e/ou na rede (failover). Em caso de falha, a conexão não deve ser terminada, mas sim, balanceada para outro(s) servidor(es) disponível(is).

56 Logo após restabelecido o ambiente operacional anterior à ocorrência da falha, o

servidor back-end deverá serautomaticamente recolocado em operação no cluster de servidores (failback) se, e somente se, apresentar comportamento adequado de acordo com os parâmetros de monitoramento de saúde.

57 Fazer draining (drenagem) de servidores back-end;

58 A drenagem permite que um determinado servidor back-end seja retirado de operação de maneira programada, para manutenção e upgrades, sem desconectar os usuários abruptamente;

59 Deve ser possível redirecionar tráfego para um pool de contingência em caso de falha no pool primário;

60 Deve ser possível configurar quantos servidores de back-end podem falhar no pool primário antes que o poolde contingência seja acionado;

61 Cada grupo de servidores (pool) deve permitir a aplicação de configurações específicas, tal como o algoritmode balanceamento e métodos de monitoramento;

62 Fazer caching HTTP armazenando o conteúdo HTTP em memória RAM de modo a desafogar os servidores back-end.

63 O recurso de caching HTTP poderá ser configurado de forma independente por serviço/aplicação e por tipo deobjeto.

64 O tempo de vida em cache deve ser customizável, assim como o tempo de refresh do conteúdo.

65 Fazer compressão de conteúdo dos pacotes.

66 Deve possuir recurso que otimize tráfego e possuir os requisitos abaixo:

67 Realizar otimização de conteúdo do protocolo HTTP, com suporte a HTTP/1.1 e HTTP/2;

68 Recurso que versione imagens de background;

69 Recurso que realize a compressão de arquivos JavaScript;

70 Compressão de conteúdo dos pacotes;

71 No caso do protocolo HTTP/2, deve realizar divisão de conexões, multiplexação de requisições de páginas eotimizar conteúdo web.

72 Realizar Offload SSL, ou seja, receber requisições HTTPS e encaminhá-las aos servidores back-end usandoHTTP, desonerando-os de fazer transações SSL.

73 Realizar Offloaf TLS para livrar carga de processamento dos servidores de back-end;

74 Realizar parsing de dados XML com Xpath e suportar Offload e aceleração entre a translação entre versões deXML com XSLT;

75 Realizar otimização TCP, ou seja, o appliance deverá funcionar como um proxy recebendo um conjunto sessões TCP iniciadas no lado do cliente e multiplexá-las numa única sessão com o servidor back-end;

76 Dispor de um mecanismo de aceleração das aplicações, gerenciando e otimizando as requisições aos servidores back-end, bem como as respostas destes. Também deve dispor de mecanismo de aceleração/otimização automático, isto é, sem a necessidade de configuração;

77 Permitir monitorar o nível de serviço entregue por cada servidor back-end, emitindo alertas em caso de falha oudeterioração da qualidade do serviço. Em caso de problemas no nível de serviço, deve ser possível configurar ações de remediação, tais como: priorização de requisições e/ou banda para o serviço afetado, chaveamento para outro pool de servidores e balanceamento entre pools de acordo com o que o usuário está acessando;

78 Deve ser capaz de bloquear tráfego de IPs ou range de IPs baseados na ocorrência de alertas e/ou eventosde segurança;

79 Registrar em log toda a atividade ocorrida cluster, tanto nos appliances virtuais quanto eventos perceptíveis pela solução nos servidores back-end, desde os acessos normais, eventos de auditoria, conexões falhas, serviçosde balanceamento global, problemas de licença, erros de scripts e problemas críticos;

80 Deve ser capaz de monitorar tentativas de ataques às aplicações, gerar logs e impedir os ataques assim comodeve ser passivo, isto é, monitorar tentativas de ataques às aplicações, gerar logs e não interferir no tráfego.

81 Prover em tela gráficos variados que demonstrem o nível de utilização dos serviços entregues pelo balanceador/cluster, tais como banda, banda por pool, content cache, conexões, nós drenados, tempo mínimo deresposta, tempo máximo de resposta, tempo médio de resposta, quantidade de vezes que sessões ASP, SSL e J2EE são encontradas em cache e transito de pacotes nas interfaces de rede. Os gráficos devem ser criados em tempo real ou com dados históricos;

82 Possuir visualização gráfica de estatísticas de requisições aceitas ou negadas pelas regras de segurança;

83 Deve ser capaz de exibir:

83.1 Quantidade de ataques;

83.2 Servidores atacados;

83.3 Tipo de ataque;

83.4 Severidade;

83.5 Fonte do ataque (endereço IP);

84 Deve ser possível agendar o envio relatórios de segurança via e-mail;

85 Prover API de controle baseado em SOAP para integração com outros aplicativos de rede, por exemplo quandosoluções de segurança detectarem ameaças, via API, o balanceador recebe as informações/instruções sobre tráfego malicioso e dropa suas conexões;

86 Deve possuir suporte ao protocolo SNMP;

87 Quando dois ou mais Balanceadores virtuais formarem um cluster, deve ser possível configurar o cluster de uma única interface, sem a necessidade de replicar manualmente as configurações realizadas;

88 Oferecer proteção contra-ataques do tipo DoS (Denial of Service), através de ferramenta modelagem de requisições (request rate shaping);

89 Proteger contra outros tipos de ataques, como: worms e vírus e URLs malformadas;

90 Realizar modelagem de tráfego (rate shaping) por meio da limitação do número de conexões e/ou restrição dosIPs que podem acessar os serviços;

91 Realizar priorização de banda por aplicação considerando aspectos como IP de origem, URL, versão de HTTP,cabeçalho HTTP, Cookie e horário de acesso;

92 Realizar redirecionamento de tráfego com base na inspeção de conteúdo da camada 7;

93 Implantar mecanismos de persistência de sessão, de modo que um usuário conectado a uma aplicação em um servidor back-end tenha suas requisições sempre processadas pelo mesmo servidor.

94 A persistência de sessão deve utilizar como parâmetro endereço IP, ID da sessão SSL ou sessão J2EE comopossível chave para atrelar um usuário final a um servidor back-end;

95 Fazer gerenciamento de banda por serviço e/ou usuário;

96 Deve possuir capacidade de realizar global load balance para redirecionamento de tráfego em caso de recuperação de desastres;

97 Deve possuir arquitetura escalável horizontalmente e verticalmente;

98 Deve possuir mecanismo de aceleração para aplicações HTML;

99 A quantidade de sessões que o balanceador suporta não deve ser limitado via software, isto é, a capacidade que o balanceador apresenta é baseado nos recursos de hardware entregues pela plataforma de virtualização.

100 Deve haver mecanismo que envie o tráfego outbound pelo mesmo caminho que o tráfego inbound. Esta funcionalidade é necessária quando se utiliza NAT ou firewall stateful para acesso dos usuários;

101 Deve suportar gerenciamento de cluster de Balanceadores distribuídos geograficamente;

102 Deve ser possível desativar regras de segurança para uma aplicação temporariamente sem a necessidade deexclusão de configuração;

103 Deve ser possível identificar ataques: Cross-site Scripting (XSS), Injeção de Código, Injeção de SQL, Path Traversal, Injeção de comandos via Shell e outros;

104 A solução deve ser capaz de integrar com soluções de SIEM (Security Incident and Event Management) deoutros fabricantes afim de evitar vendor lock-in;

4.4.7 REQUISITOS GERAIS DE SOFTWARE

Todos os Softwares disponibilizados devem ser fornecidos com os seguintes requisitos mínimos:

Contrato de suporte e atualização de *patches*, *hot fixes* e *services packs* por todo o período contratual.

1 A CONTRATADA deverá fornecer, dar garantia e suporte técnico aos softwares de gerenciamento, segurança,backup e sistemas operacionais para o ambiente de Hosting. Deverão ser utilizados equipamentos próprios da CONTRATADA, não envolvendo o parque computacional dedicado ao CREA-SP, para implantar as soluções abaixo:

1.1 Solução para monitoramento do ambiente de TI destinado ao CREA-SP.

1.2 Solução para gerenciamento de serviços, inclusive Service Desk.

1.3 Solução de segurança para o ambiente de TI do CREA-SP, envolvendo firewall, IPS, Webfilter, Antivírus,AntiSpam e VPN (Ipsec).

1.4 Solução para backup/restore do ambiente de TI do CREA-SP.

1.5 Solução antivírus em edição empresarial, filtro HTTP para todos os servidores.

2 Será de responsabilidade da CONTRATADA o licenciamento dos softwares listados abaixo, em quantidadesuficiente para operar nos elementos de hardware do presente projeto:

2.1 Licenciamento do sistema operacional Microsoft Windows Server para os servidores de aplicação instaladosnos dois datacenters (Principal e Redundante) secundário previstos compatíveis com a quantidade de núcleos fornecidos no Hardware de Virtualização.

2.2 Licenciamento de certificados SSL wildcard para os servidores de aplicação e demais serviços do CREA-SP.

2.3 Licenciamento do sistema operacional AIX para o servidor RISC do banco de dados DB2 compatível com osHardwares ofertados.

2.4 Licenciamento do sistema gerenciador de banco de dados IBM DB2 Enterprise Server Edition com quantidade de PVUs (Processor Value Unit) compatível com a quantidade de núcleos dos processadores doservidor RISC.

2.5 Licenciamento do banco de dados Microsoft SQL Server para os servidores de banco de dados da plataforma Documentum, conforme requisitados nas Tabelas A e B.

2.6 Licenciamento do software de virtualização e seu respectivo sistema de gerenciamento compatíveis aquantidade de núcleos fornecidos no Hardware de Virtualização.

4.4.7.1 SOFTWARE PARA VIRTUALIZAÇÃO

1 VER OS REQUISITOS GERAIS DE VIRTUALIZAÇÃO-SOFTWARE PARA VIRTUALIZAÇÃO

4.4.7.2 SISTEMA OPERACIONAL PARA BANCO DE DADOS DB2

1 O sistema operacional AIX para o DB2 deve ser o mais atual no momento da contratação, não podendo serinferior ao:

2 Sistema Operacional IBM AIX Standard Edition Versão 7.2.2TL3SP3

3 A Contratada deve prover atualização da versão do sistema operacional sempre que solicitada, durante o período da vigência contratual, além de aplicar os patches de segurança e correção necessários.

4.4.7.3 SOFTWARE DO SISTEMA DE ARMAZENAMENTO

O Software dos equipamentos de Armazenamento devem ser compatíveis com os Sistemas operacionais de Virtualização,Windows e AIX/DB2 fornecidos pela contratada.

4.4.7.3.1 CARACTERÍSTICAS GERAIS

1 Deverá replicar automaticamente todas as gravações para um ou mais servidores do cluster, utilizando as interfaces de maior velocidade (throughput) presentes em cada um dos servidores, as quais deverão ser de nomínimo 10Gbps com redundância;

2 Deverá garantir que os dados estejam sempre gravados em mais de um servidor ao mesmo tempo. Se houver mais de um chassi ou servidor os dados deverão ser gravados preferencialmente nos equipamentos adjacentes, permitindo o pleno funcionamento do ambiente mesmo com a total indisponibilidade de um dos dois servidores, dependendo da configuração;

3 Permitir a escolha de 02 (duas) ou 03 (três) réplicas de dados, dependendo da configuração e dadisponibilidade desejada;

4 Caso a solução for baseada em RAID tradicional, deverá fornecer 30% a mais de capacidade devido aosoverheads desta tecnologia;

5 A solução deverá permitir criptografia, à nível de software, do tipo Data-At-Rest

6 Deverá ser baseada no padrão de criptografia AES-256;

7 Deverá possuir gerenciador de chaves nativo e suportar servidor de gerenciamento de chaves externo, deterceiros;

8 A solução deverá suportar a falha de 01 (um) servidor por cluster;

9 Permitir escalabilidade horizontal, isso é, a adição de novos chassis ou novos servidores ao cluster através deuma console gráfica, sem a parada do ambiente de produção, aumentando como um todo a capacidade de armazenamento, processamento e memória disponibilizados ao hipervisor, além de crescer de forma linear o desempenho do cluster;

10 Deverá possuir um mecanismo para mover os dados não acessados para os discos rígidos pertencentes aocluster, deixando os discos SSD de cache para dados acessados com frequência. Caso o dado volte a ser requisitado, o mesmo deverá ser migrado para o cache unificado;

11 Durante o processo de gravação de dados no cluster distribuído a solução deverá ser capaz de fazer o cálculode integridade com degradação mínima de desempenho e armazená-lo;

12 Deverá trabalhar com o conceito de pool armazenamento, formado pelo conjunto de todos os discos presentes no cluster. O pool de armazenamento poderá ser expandido com novos discos à medida que novosservidores são adicionados ao cluster;

13 Deverá permitir a criação de um subconjunto do espaço disponibilizado pelo cluster lógico integrado denominado volume de dados. O volume de dados é a unidade de armazenamento compartilhada apresentadaao hipervisor, onde serão armazenados os discos virtuais, aos quais poderão possuir o tamanho total do clusterlógico de armazenamento ou reserva de espaço conforme política configurável pela interface gráfica;

14 Deverá permitir a criação de no mínimo 03 (três) volumes de dados (datastore) com diferentes característicase propriedades de otimização de espaço e desempenho habilitados ou desabilitados;

15 Os volumes de dados presentes no *cluster* integrado, deverá suportar o tamanho máximo de disco virtualsuportado por cada hipervisor;

16 O sistema distribuído de arquivos empregado pela solução deverá prover os seguintes protocolos: NFS (Network Files System), iSCSI (Internet Small Computer System Interface)**,** SMB 3.0 (Server Message Block) ouvSAN.

17 Prover em cada um dos servidores, atualizações do tipo “menor esforço”, possibilitando a atualização detodos os servidores do *cluster* de forma simples e automatizada, eliminando a intervenção manual do administrador e necessidade de parada completa do ambiente. Essa funcionalidade deverá atualizar os seguintescomponentes:

18 Sistema operacional do controlador de armazenamento virtual;

19 Hipervisor;

20 Micro-códigos de discos rígidos e flash;

21 BMC/IPMI (ou similar) e BIOS;

22 Ferramenta de monitoramento do cluster.

23 Deverá suportar o inventário e o gerenciamento do ciclo de vida dos principais componentes do Cluster, ouseja, versões das camadas de software e micro-códigos do hardware.

24 Prover, via software, compressão inline (durante o processo de gravação);

25 Prover, via software, desduplicação de dados inline (durante o processo de leitura);

26 Caso a solução de armazenamento ofertada for híbrida (discos SSD e HDD) prover compressão pós- processada, sendo que após uma operação de escrita, exista um atraso em minutos para iniciar o processo decompressão. O atraso deverá ser configurável pelo administrador do sistema. A compressão deverá se utilizar de técnicas de processamento paralelo distribuído, distribuindo o custo computacional da compressão entre diversosservidores pertencentes ao cluster;

27 Deverá prover desduplicação pós-processado, que diferentemente da inline, deverá atuar nos discos rígidos utilizados na solução. A desduplicação deverá ocorrer em um processo posterior a gravação e utilizar de técnicasde processamento paralelo distribuído, otimizando a capacidade de armazenamento;

28 Prover um melhor aproveitamento dos recursos de armazenamento do cluster, implementando método de proteção de dados Erasure Coding, no qual os dados são divididos em fragmentos, estendidos e codificados com pedaços de dados redundantes e armazenados em diferentes servidores. Esse método deverá utilizar técnicas deprocessamento paralelo distribuído no cluster para calcular a paridade dos blocos;

29 Prover capacidade de alocar e fixar determinadas máquinas virtuais nos discos SSD, garantindo melhorperformance possível, em soluções híbridas.

30 Prover snapshots por máquina virtual nativamente independente do hipervisor, armazenando esses snapshotsno cluster para proteção local. O snapshot criado deve ser do tipo consistência de erros, ou seja, o snapshot poderá ser feito com o ambiente em produção e deverá garantir a proteção dos dados que estão gravados em disco e a integridade do sistema operacional da VM;

31 Prover acesso a armazenamento via protocolo iSCSI, em nível de blocos a uma ou mais máquinas virtuais oufísicas externas ao ambiente integrado, visando atender aplicações em alta disponibilidade.

32 Prover snapshots de consistência de aplicação em sistemas operacionais:

33 Windows 2012 R2 ou superiores;

34 Linux Ubuntu 14.04 ou superiores;

35 CentOs 6.5 ou superiores;

36 Red Hat Enterprise Linux 6.5 ou superiores.

37 Permitir, a réplica de dados de duplicados e comprimidos.

38 Em relação ao portal de infraestrutura como serviço, a solução deve possibilitar o provisionamento derecursos computacionais e possuir as seguintes características:

39 Definir repositórios externo de autenticação para usuários - Active Directory da Microsoft;

40 Gerenciar catálogos de objetos (ISO ou Discos);

41 Criar grupos de trabalho;

42 Alocar recursos de CPU, memória e armazenamento por grupos de trabalho;

43 Definir permissões de acesso por grupo de trabalho;

44 Criar máquinas virtuais por grupo de trabalho;

45 Interagir com as máquinas virtuais conforme o grupo de trabalho;

46 Segregar grupos de trabalho.

4.4.7.3.2 CARACTERÍSTICAS DE REPLICAÇÃO SOFTWARE INTEGRADO

1 Permitir a criação de grupos de consistência para a replicação, permitindo que, no momento da restauração oudo desastre, todas as máquinas virtuais contidas nesse grupo voltem ao mesmo ponto no tempo.

2 A replicação poderá ser realizada para um cluster, com base nas mesmas tecnologias propostas, nasdependências da CONTRATANTE ou baseado em nuvem pública suportada;

3 A solução deverá possuir ferramenta para orquestração de recuperação de desastre para um cluster, com basenas mesmas tecnologias propostas, nas dependências da CONTRATANTE ou em um baseado em nuvem pública suportada, que permita a organização da inicialização de máquinas virtuais e testes de recuperação de desastre sem impactar a produção;

4 Deverá suportar nativamente, ou seja, sem integração com produtos de terceiros, replicação síncrona eassíncrona, entre dois sites.

5 A replicação assíncrona deverá prover um RPO (objetivo do ponto de recuperação) mínimo de 15 (quinze)minutos e a replicação síncrona deverá prover um RPO (objetivo do ponto de recuperação) 0 (zero) para distâncias de até 100 KM (cem quilômetros) com menos de 5 (cinco) milissegundos (RTT);

6 A funcionalidade de replicação nativa da solução deverá trabalhar com snapshots das máquinas virtuais e suportar as seguintes topologias de interconexão entre clusters em diferentes localidades: um para um, um paravários, vários para um e vários para vários.

7 As soluções de replicação e orquestração de recuperação de desastre;

4.4.7.4 SOFTWARE BANCO DE DADOS DB2

1 O Banco de Dados DB2 deve ser a última versão de mercado disponível na época da contratação, não podendoser inferior à:

1.1 Bancos de Dados IBM DB2 9.5

1.2 Deve ser disponibilizada a versão Enterprise do DB2.

2 A contratada deverá providenciar a migração completa da versão atual (Db2 9.5) para a versão mais recente, bem como atualizar para a versão Enterprise

3 A Contratada deverá atualizar a versão do banco de dados sempre que solicitada, durante a vigência contratual, bem como aplicar os patches de segurança e correção necessários.

4.4.8 REQUISITOS GERAIS DE HARDWARE

1 A CONTRATADA deverá disponibilizar todos os hardwares, ativos e passivos, necessários à plena execução dosserviços e aplicativos do CREA-SP. Deverá também atender aos seguintes termos:

2 Data Center com o espaço físico e infraestrutura planejada, dimensionamento e distribuição de hardware.

3 Switches para SAN, para Ethernet e cabeamento, totalmente gerenciáveis.

4 Dispositivos de segurança física, equipamentos de energia elétrica e climatização com avançada combinação decaracterísticas técnicas e funcionais.

5 O Data Center deverá prover tempo médio de reparação de qualquer nível de hardware disponibilizado ao CREA-SP inferior a 02 (duas) horas.

6 Todo o hardware para atender os serviços requisitados nesta especificação deverá ser exclusivo e dedicado aoCREA-SP, novo e coberto por contratos de garantia e suporte no regime 24x7x365 durante todo o período de vigência e execução contratual.

4.4.8.1 HARDWARE PARA O SISTEMA DE BANCO DE DADOS DB2

1 A CONTRATADA deverá fornecer no Data Center no mínimo 01 (um) servidor para banco de dados DB2 para o ambiente de produção e 01 servidor para o ambiente de redundância física e lógica do Banco de Dados, com as seguintes características mínimas:

2 02 (um) processador Power 8 de no mínimo 8 (oito) núcleos cada com velocidade mínima de 3.7Ghz.

3 128 (cento e vinte e oito) GB de memória RAM DDR3, com capacidade de expansão para até 512 GB de memória no mínimo.

4 02 (dois) discos SAS, com capacidade mínima de 300 GB e 15.000 rpm.

5 01 (uma) unidade de DVD-RAM SATA.

6 02 (duas) interfaces 8GB PCI Express Dual Port Fiber Channel/ ou tecnologia com capacidade superior para interligação com o Storage.

7 02 (duas) interfaces PCIe2 quatro portas 1Gbps.

8 02 interface com portas 10Gbps

9 02 (duas) fontes redundantes de 1400W

10 Contrato de suporte e atualização de patches, hot fixes e services packs por todo o período contratual.

4.4.8.2 HARDWARE PARA O SISTEMA DE VIRTUALIZAÇÃO

1 Ver o item REQUISITOS GERAIS DO SISTEMA DE VIRTUALIZAÇÃO - HARDWARE DO SISTEMA DEVIRTUALIZAÇÃO

4.4.9 REQUISITOS GERAIS DE ARMAZENAMENTO

1. A CONTRATADA deverá disponibilizar um ou mais sistemas de armazenamento de dados em seu centro de processamento, com capacidade equivalente ao especificado na tabela abaixo para todos os ambientes operacionaiscontratados que se relacionem, inicialmente, ao escopo.

TABELA F - Serviço de Armazenamento

Item	Descrição	Qtde Inicial Mínima (TB)	Qtde Máxima (TB)
1	Área em storage Comum (Servidores Windows e Linux);	170	340
2	Área de Storage DB2, conectada ao Servidor AIX	53	106
Total		223	446

2. O Sistema de Armazenamento será contratado por Quantidade com a previsão mínima de 223 e máxima de 440 duranteos 3 anos de contrato.

3. Os equipamentos fornecidos devem atender exclusivamente ao CREA-SP e serem novos, sem nenhuma utilização anterior.

4. O incremento mínimo que a CONTRATANTE Poderá Solicitar a será de 10TB, com prazo de 30 dias para implementação.

4.4.9.1 REQUISITOS TÉCNICOS:

1 Os sistemas de armazenamento deverão ter, pelo menos, a seguinte configuração mínima:

2 02 controladoras em ativo/ativo.

3 Desempenho mínimo de 30.000 IOPS (*Input/Output per Second)*.

4 Capacidade inicial útil mínima de acordo com o especificado nas tabelas A e B, configurados em RAID-5.

5 Função Dynamic Sparing:

5.1 A solução deverá contemplar discos SPARE. A quantidade deverá ser dimensionada de acordo com asmelhores práticas de cada fabricante.

5.2 Os discos de hot-spare deverão obedecer às características e tamanhos especificados neste edital, bem como serem suficientes para, sem a necessidade de intervenção manual, substituir qualquer disco do equipamento que venha a falhar.

5.3 A solução deve permitir a troca de disco avariado, pertencente a um Array Disk, sem interrupção daaplicação que está acessando o Array.

5.4 Os equipamentos de processamento de dados que fazem uso do Subsistema de Armazenamento de Dados podem ser: Partições lógicas de servidores particionáveis ou servidores físicos de rede corporativa.

6 Controladoras:

6.1 Cada subsistema deverá possuir, no mínimo, 02 (duas) controladoras ativas, sendo que na falha de umacontroladora, a outra deverá assumir o tráfego total de forma automática, sem intervenção manual.

6.2 As controladoras deverão trabalhar de modo Ativo-Ativo Simétrico, ou seja, ambas deverão estar habilitadas a trabalhar ao mesmo tempo com balanceamento de carga no acesso aos discos automático, sem anecessidade de intervenção do usuário.

7 Portas para conexão com os servidores compatível com a quantidade de servidores solicitada nestaespecificação.

8 Cada conexão da Solução ofertada deverá possuir, de forma nativa, a capacidade de

autodeterminar avelocidade de transmissão dos dados, para o caso de conectar-se a dispositivos que operem em outras velocidades.

9 Deverão ser fornecidos todos os cabos necessários e componentes (ex: Mini Gbic) para a plena utilização dasolução com todas as suas funcionalidades, conforme as normas técnicas de fabricação e especificações dofabricante.

10 A CONTRATADA deverá fornecer todo hardware e software necessários para operação e configuração do equipamento, bem como o gerenciamento de seus recursos. O software também deverá gerenciar o desempenhodos seguintes componentes: discos, canais e cache, inclusive com dados históricos.

11 O equipamento deve possuir monitoramento proativo que permita a detecção e isolamento de falhas antes mesmo que elas ocorram. Tal função abrangerá a monitoração e geração de log de erros, detecção de erros de memória, detecção e isolamento de erros no disco.

12 Possibilidade de substituição para manutenção e atualização dos componentes sem interrupção dofuncionamento do equipamento Storage:

12.1 Controladoras;

12.2 Discos;

12.3 Ventiladores;

12.4 Fontes.

13 Balanceamento dinâmico de carga entre discos e controladoras.

14 Software de gerenciamento de armazenamento centralizado, para controle da organização dos dados e dodesempenho, diagnóstico remoto, proteção, recuperação de dados e notificação de eventos.

15 Os table spaces e logs transacionais dos bancos de dados DB2 e MS SQL Server deverão ser armazenadas nostorage.

4.4.9.2 ARMAZENAMENTO PARA O SISTEMA DE VIRTUALIZAÇÃO E BACKUP

1 O Sistema de Armazenamento deve manter compatibilidade mínima com os seguintes ambientes de software:

1.1 Windows 2008 / 2008R2 e superiores.

1.2 Software de virtualização, conforme especificado nas Tabelas a e B nas versões fornecidas pelaCONTRATADA.

1.3 Bancos de Dados SQL Server 2008, 2008 R2 e versão superior.

1.4 Banco de Dados IBM DB2 conforme a versão fornecida pela contratada.

1.5 IBM AIX conforme a versão fornecida pela contratada.

4.4.9.3 ARMAZENAMENTO PARA O SISTEMA AIX/DB2

1 A CONTRATADA deverá fornecer no mínimo uma solução que forneça a seguinte configuração:

1.1 Este ambiente deverá, necessariamente, ser conectado a uma Storage SAN de solução unificada de mesmo fabricante com conectividade FC (Fiber Channel) ou outra tecnologia de com capacidade de transmissão superior ao FC.

1.2 Conexões Front End - FC (FibreChannel) ou da tecnologia fornecida:

1.3 A quantidade de portas deverá ser dimensionada para a capacidade e funcionalidades solicitadas neste documento, mas considerando, um mínimo de 24 (vinte e quatro) portas de no mínio 8Gbps (oito gigabites por segundo) para conexão aos servidores.

1.3.1 A quantidade de fibras deve ser, no mínimo, igual ao número de portas ofertado.

1.3.2 Todos os cabos deverão ser resistentes à tração.

2 Matriz de Compatibilidade do Subsistema de armazenamento e Virtualização:

2.1 Manter compatibilidade com os seguintes ambientes de software:

2.1.1 AIX 7.1 e versão superior (Deve ser compatível com a versão oferecida pela CONTRATADA).

2.1.2 Bancos de Dados IBM DB2 9.5 e superior (deve ser compatível com a versão oferecida pelaCONTRATADA).

3 Será aceita uma configuração que comprovadamente possua uma performance melhor que a oferecida pelaconfiguração requerida acima.

4 Será dever da contratada fornecer os estudos comparativos de performance que justifiquem uma outraarquitetura de conexão e comunicação entre o sistema de storage e o Banco de dados IBM DB2.

4.4.10 REQUISITOS GERAIS DE ARQUITETURA TECNOLÓGICA

1 **Segurança da Informação -** A CONTRATADA deverá submeter-se às políticas de segurança do CREA-SP e assumir todos os possíveis danos físicos e/ou materiais causados ao CREA-SP ou a terceiros, advindos de imperícia,negligência, imprudência ou desrespeito às normas de segurança, quando da execução dos serviços, sempre atentando aos princípios de:

2 **Disponibilidade** – garantir aos usuários, autorizados pelo gestor do contrato, acesso às informações e aos locaisde instalação dos ativos de rede, quando necessário, disponibilizando, ainda,

todas as informações solicitadas pelo gestor ou fiscais quanto aos serviços executados e as condições atuais da estrutura da rede (fragilidade, oportunidades de implementações e melhorias, etc).

3 **Integridade** -guardar a exatidão e inteireza das informações e, ainda, documentar as atividades realizadas, objetivando manter a consistência das informações contidas nos arquivos com as condições reais das instalações.

4 **Confidencialidade** - garantir que as informações sejam acessíveis somente ao pessoal autorizado, não fornecendo arquivos digitalizados ou mesmo impresso a pessoas que não foram autorizadas pelo gestor do contrato.Além disto, não permitir o uso da estação de trabalho por seus empregados para atividades diferentes das previstas no contrato e não permitir a entrada de pessoas não autorizadas no ambiente disponibilizado pela contratante para uso da CONTRATADA nas instalações do CREA-SP.

5 **Autenticidade** -todas as comunicações entre a contratada e a contratante deverão ser formalizadas e todos os documentos devidamente identificados com os dados pessoais dos responsáveis, garantindo a autenticidade dos documentos e a possibilidade de auditoria das atuações das partes envolvidas. A CONTRATADA deve comunicarformal e imediatamente ao representante do CREA-SP qualquer ponto de fragilidade percebido que exponha aconfidencialidade, integridade ou disponibilidade das informações e do serviço. A CONTRATADA deverá assinar termo de sigilo que estabeleça sua ampla responsabilidade pelas informações processadas ou armazenadas.

4.4.11 REQUISITOS GERAIS DO SERVIÇO DE BACKUP

1 A Comunicação com os servidores deverá ser de no mínimo 10 Gbps.

2 O sistema deverá possibilitar o Backup e Restore de todos os dados, arquivos, servidores do ambiente do CREA-SP;

3 O sistema deverá permitir o restore de arquivos independentes.

4 Deverá permitir o backup e restore de arquivos abertos, garantindo a integridade do backup.

5 Deverá possuir mecanismo de verificação e checagem de consistência da base de dados no intuito de garantir aintegridade dos dados.

6 Possuir capacidade de estabelecer níveis de acesso diferenciados e configuráveis para atividades deadministração e operação do software de backup;

7 Deverá possuir catálogo ou banco de dados centralizado contendo as informações sobre todos os dados e mídiasonde os backups foram armazenados.

8 A CONTRATADA deverá fornecer usuários de leitura e pesquisa do sistema de Backup e seu catálogo quepermitam aos analistas do CREA-SP, através de interface gráfica, pesquisar os arquivos, servidores e dados armazenados no mínimo por nome, data de criação, data de

arquivamento.

9 Permitir restaurar o backup de recuperação de desastres para hardware diferente do original para ambienteWindows.

10 Deverá suportar backup do Microsoft Active Directory, com possibilidade de restore granular, ou seja, restauraçãode todo um diretório, de objetos selecionados e até de atributos individuais.

11 Possuir Interface única para gerenciamento de todos os servidores independente do S.O que hospeda esseserviço (Windows, Linux).

12 Deverá permitir a integração com a funcionalidade de cópias instantâneas (snapshot) de subsistemas dearmazenamento em disco (storage).

4.4.12 REQUISITOS GERAIS DE ENDEREÇAMENTO IP e DNS (Domain Name System)

4.4.12.1 IP'S VÁLIDOS NA INTERNET

1 A CONTRATADA deverá fornecer até 128 endereçamentos IP's Válido na internet para aplicações que o CREA-SP publique.

2 A CONTRATADA Deverá realizar toda a configuração interna (servidores, equipamentos de rede, etc.) e externa(na Internet, em servidores de DNS, registro BR, etc.) e migração dos endereços IP's atuais para os fornecidos por ela.

4.4.12.2 REQUISITOS DE DNS

1 A CONTRATADA deverá realizar a ADMINISTRAÇÃO dos servidores de DNS do domínio creasp.org.br, realizando todas as inserções, alterações, deleções de registros necessárias.

2 A CONTRATADA deverá disponibilizar usuário de leitura (read-only) para o sistema de DNS que permita aosanalistas do CREA-SP em tempo real verificar as configurações e nomes publicados na internet.

3 A CONTRATADA deverá realizar TODA a migração e configuração dos serviços de DNS atualmente contratadospara o fornecido através desta contratação.

4.5 REQUISITOS DE PLANEJAMENTO, INSTALAÇÃO E MIGRAÇÃO

1 Quando especificamos Serviços de planejamento, estamos incluindo todo e qualquer projeto e planejamento necessário para viabilizar a funcionalidade dos serviços contratados. Dentro dos serviços de planejamento estãoincluídos a instalação da solução e a migração dos dados e aplicações do Datacenter atual para o Datacenter CONTRATADO.

2 Os serviços de PLANEJAMENTO Serão pagos mediante sua execução, com apuração e pagamento único.

Tabela E - Serviços de Planejamento e Instalação

Item	Descrição	**Qtde**	**Unidade**	**Periodicidade**
1	Serviços de Planejamento	1	Serviço	Apuração Única.
2	Serviço de Instalação	1	Serviço	Apuração Única
3	Serviço de Migração / Replicação	1	Serviço	Apuração Única

4.5.1 SERVIÇO DE PLANEJAMENTO

1 A CONTRATADA deverá realizar o planejamento da Prestação dos Serviços CONTRATADOS, o Planejamentodeverá incluir, mas não se limitar aos seguintes itens:

1.1 Planejamento de provisionamento dos links de comunicação

1.2 Planejamento de BayFace dos Racks

1.3 Planejamento de Endereçamento IP

1.4 Planejamento de Comunicação de Dados

1.5 Planejamento de implantação do sistema SIEM

1.6 Planejamento de implantação do WAF

1.7 Planejamento de implantação do Cofre de Senhas

1.8 Planejamento de implantação dos Appliances de segurança (Firewalls)

1.9 Planejamento de implantação do sistema de monitoramento

1.10 Planejamento de Migração de dados e aplicativos

1.11 Planejamento de Migração de endereçamento IP e DNS

1.12 Planejamento de migração de versões de bancos de dados e servidores

4.5.2 SERVIÇOS DE MIGRAÇÃO

1 A Contratada Deverá Realizar TODA a migração do ambiente atual para o seu ambiente de hospedagem.

2 A CONTRATADA deverá se arcar com todos os custos durante o processo de Migração,

incluindo, mas não selimitando à:

2.1 Custos de transporte, transferência e armazenamento de dados;

2.2 Custos de manutenção do sistema de hospedagem atual;

3 Estes serviços devem incluir, mas não se limitar aos itens descritos abaixo:

3.1 Migrar os Servidores (Windows, Linux, AIX, etc.) Virtuais e Físicos, Banco de Dados (SQL Server, DB2, MySQL, Postgres, etc) que estão no Ambiente da sala de Equipamentos do CREA-SP, (Sede Faria Lima) para oAmbiente da Hospedagem.

3.2 Migrar os Servidores (Windows, Linux, AIX, etc.) Virtuais e Físicos, Banco de Dados (SQL Seerver, DB2, MySQL, Postgres, etc) que estão atualmente no Datacenter Atual, para o Ambiente do Datacenter da CONTRATADA, Principal e Redundante;

3.3 Atualizar a Versão do Sistema operacional AIX e do Banco de Dados DB2 para a Versão mais atualdisponível no momento da CONTRATAÇÃO.

3.4 Migrar os Dados do Banco de Dados DB2 que está hospedado no Datacenter atual, para os ambientes daCONTRATADA, (ou para a versão atual, item 3.3).

3.5 Migrar os Dados do Banco de Dados DB2 que está hospedado na sala de equipamentos do CREA (sedeFaria Lima), para os ambientes da CONTRATADA.

3.6 Configurar o Banco de Dados DB2 para realizar a replicação de dados entre os ambientes principal eredundante.

3.7 Realizar todos os testes de redundância necessários para garantir que os dados replicados serãoefetivamente utilizados no momento de um incidente.

3.8 Migrar os endereços IP Válidos e não válidos, inclusive o DNS

4.6 REQUISITOS DE ADMINISTRAÇÃO E OPERAÇÃO

1 A Operação da Solução compreende os serviços de administração dos recursos de Infraestrutura hospedados.

2 A Administração inclui, mas não se limita, aos serviços de Operação, Manutenção Preventiva e Corretiva, Suporte eGestão de incidentes

Tabela D - Serviços de Administração

Item	**Descrição**	**Qtde**	**Unidade**	Forma de Pagamento
1	Serviços de OPERAÇÃO, compostos pela administração das Maquinas, virtuais,	1	Serviço	Pagamento Mensal

	Bancos de Dados, Redes, Segurança, etc.			
2	Serviços de Manutenção e Monitoramento	1	Serviço	
3	Serviço de Suporte e Gestão de incidentes	1	Serviço	

4.6.1 REQUISITOS DE SUPORTE E GESTÃO DE INCIDENTES

1 A CONTRATADA deverá possuir um Centro de Operações totalmente funcional, que permita o atendimento ao CREA-SP com todas as funcionalidades contratadas neste edital, 24 x 7 x 365 - 4 (vinte e quatro) horas por dia e 7(sete) dias da semana, 365 (trezentos e sessenta e cinco) dias por ano.

2 A CONTRATADA deverá disponibilizar uma equipe de solução de problemas que atue em regime 24 x 7 x 365, na solução de qualquer problema de severidades Alta e/ou Crítica e/ou emergencial.

4.6.1.1 CENTRO DE OPERAÇÕES

1 A CONTRATADA deverá garantir a redundância de toda infraestrutura necessária para a operação do Centro de Operações, de modo que a indisponibilidade de uma localidade, ou sistema, não afete nenhum aspecto dos serviços prestados.

2 Os ativos necessários para a execução dos serviços do "Centro de Operações" devem estar hospedados em Data-Center com certificação Padrão Tier III, no mínimo, e com redundância de alimentação, energia e conexões de WAN (entre do Data Center e o Centro de Operações);

3 O "Centro de Operações" deve Possuir estrutura central para visualização dos painéis dos sistemas de suporte técnico, monitoramento, administração e gerenciamento, que permita a todos os profissionais visualizarem eventos relevantes simultaneamente.

4 A CONTRATADA deve manter registros de acesso aos dados da contratante, os quais permitam identificar quais pessoas acessaram e/ou modificaram, e quando o fizeram.

4.6.1.2 CENTRO DE ATENDIMENTO

1 A CONTRATADA deverá disponibilizar uma Central de Atendimento para que a equipe técnica do CREA-SP faça registros de ocorrências e solicitações de reparo, bem como o acompanhamento da solução dos problemas. A Central de Atendimento deverá ser acessada por um número único nacional não tarifado (0800) exclusivo para o CREA-SP ou corporativo.

2 Será responsabilidade da CONTRATADA redirecionar e encaminhar os chamados internamente, encontrando o profissional/equipe correto (os) para dar a solução ao problema referido, não importando de qual área se trata o mesmo. Ex. Se o problema for

encaminhado para a equipe de Redes, mas for constatado que o mesmo é da equipe de servidores, é responsabilidade da equipe de redes da Contratada entrar em contato com a equipe de servidores e encaminhar a solução do problema, sem pedir que a CONTRATANTE abra outro chamado para a outra equipe.

4.6.1.3 DISPONIBILIDADE DO SERVIÇO DE ATENDIMENTO E CONTROLE DE CHAMADAS

1 O serviço de registro de chamadas deverá estar disponível nas 24 (vinte e quatro) horas do dia e nos 7 (sete) dias da semana.

2 A Empresa contratada deverá disponibilizar um número telefônico para receber as chamadas técnicas do CREA- SP. E realizar a comunicação entre o CREA-SP e a central de Atendimento da Contratada.

3 A Central de Atendimento deverá gerar um identificador de registro de chamadas que deverá ser informado aoCREA-SP no momento da abertura do chamado, e que terá por finalidade identificar a qualquer momento o problema específico, possibilitando o controle de chamados.

4 O CREA-SP poderá também realizar a abertura de chamados técnicos e solicitações de serviços para todos ositens desta especificação técnica diretamente no sistema de atendimento da CONTRATADA através de um Portalde Atendimento com acessos web, para abertura de chamados técnicos e solicitações de serviços e acompanhamento dos mesmos.

5 As informações relativas aos chamados deverão ser atualizadas automaticamente sempre que houver algumaalteração em sua situação. O acompanhamento on-line da resolução de chamados pelo CREA-SP poderá ser feitotambém através do sistema de atendimento.

6 Os chamados abertos no sistema de atendimento ou na Central de Atendimento serão referentes a todas as atividades de responsabilidade da CONTRATADA, englobando, mas não se limitando, à instalação, configuração, recuperação, alteração e remoção de equipamentos, à configuração de roteadores, ao roteamento, endereçamentoIP, SNMP, organização e atualização da gerência, considerando-se todos os serviços contratados (serviços de hospedagem, rede IP, etc.), de maneira a assegurar a integridade dos meios de comunicação fim-a-fim e a qualidade e desempenho dos serviços dentro dos limites estabelecidos.

7 Os registros dos chamados deverão conter todas as informações relativas ao chamado aberto, como tempo de início e fim de atendimento, identificação do elemento (equipamento, enlace ou serviço) afetado, nome, fone e e-mail do contato no CREA-SP que foi posicionado acerca do reparo e restabelecimento do serviço, descrição detalhada da resolução do chamado com um código associado e responsabilidades.

8 Na ocorrência de um problema que afete um conjunto de enlaces ou equipamentos de uma ou mais Unidades,deverão ser gerados registros para cada um dos elementos afetados.

9 A contratada deverá atender chamados abertos por usuário, não técnicos, previamente cadastrados daCONTRATANTE.

4.6.2 REQUISITOS DE MANUTENÇÃO E MONITORAMENTO

1 Faz Parte do sistema de manutenção o sistema de monitoramento e as atividades de manutenção preventiva dosambientes (refrigeração, Energia Elétrica)

2 Manutenção Preventiva dos Links de Comunicação, verificando mensalmente, no mínimo, mas não se limitando,os seguintes itens.

2.1 Deve verificar se os links estão corretamente identificados

2.2 Deve verificar se os links estão apresentando alarmes de ocupação de CPU, Memória e Disco superiores a70%

2.3 Deve verificar se os equipamentos apresentaram alarme de temperatura excessiva

3 A CONTRATADA deve fornecer relatório de manutenção preventiva dos links de comunicação, conformeespecificado no item REQUISITOS DE RELATÓRIOS

4.6.2.1 REQUISITOS DE MONITORAMENTO

1 Responsabilidades quanto ao monitoramento

1.1 Será de responsabilidade da CONTRATADA, gerenciar, monitorar, através de software específico para talfuncionalidade, os servidores, aplicações, trafego de rede, banco de dados, enlaces de comunicação, equipamentos e qualquer ativo que faça parte da solução;

1.2 O Monitoramento da solução deverá estar operacional e disponível 24 x 7 x 365.

1.3 A CONTRATADA deverá disponibilizar o acesso de leitura ao console e gerenciador da ferramenta de monitoramento aos profissionais de T.I. definidos pelo CREA-SP.

1.4 Qualquer recurso monitorado deverá emitir alertas de mal funcionamento e/ou parada. Os alertas deverãoser filtrados pelos profissionais da CONTRATADA que operam a solução;

1.5 A CONTRATADA deverá gerar/criar chamados, com a severidade adequada, ao identificar qualquer problema através do monitoramento. Os chamados devem ser enviados diretamente aos analistas que farão aanálise e atuarão na solução dos problemas.

1.6 Será responsabilidade da contratada, entrar em contato, supervisionar os serviços da operadora dos linkssempre que detectar que algum deles falhou, ou está inoperante, podendo abrir chamados no "*call center*" da operadora e acompanhar sua resolução, mas sempre se reportando ao CREA-SP;

4.6.2.1.1 MONITORAMENTO POR PARTE DA CONTRATADA

1 A contratada deverá prover um sistema de Monitoramento em Tempo Real, disponível 24 horas por dia e 7 dias por semana, para o controle da disponibilidade de desempenho do sistema contratado, o sistema deverá entre outras funções prover o envio de alarmes e notificações via

SMS, WhatsApp e/ou Telegram, e-mail e ainda por meio de alarmes sonoros, além das seguintes informações complementares referentes ao sistema contratado:

1.1 Informações mínimas de Performance e Resiliência;

1.2 Consumo de Memória;

1.3 Números de conexões abertas;

1.4 Consumo da CPU;

1.5 Consumo de Disco;

1.6 Latência;

1.7 *Up/DownTime;*

2 A solução deverá ser composta de Hardware e Software e deverá ter como objetivo único o monitoramento de todo e quaisquer dos enlaces de comunicação fornecidos pela CONTRATADA através deste contrato, incluindo os equipamentos fornecidos juntamente com a solução, por exemplo, servidores físicos, servidores virtuais, storages, firewalls, switches, roteadores, hubs, etc.

3 Dispositivos adicionados ou retirados durante a vigência do contrato devem ser adicionados ou retirados do monitoramento sem gerar nenhum ônus ao CREA-SP.

4 A tecnologia deverá possuir as seguintes características técnicas gerais:

5 Todas as informações devem ser centralizadas e acessadas através de um front-end web, permitindo a visualização, configuração e auditoria de praticamente todas as funcionalidades, tanto em ambiente internoquanto externo;

6 A interface web deverá ser compatível com qualquer navegador recente, para desktops, tablets esmartphones;

7 Todos os parâmetros monitorados deverão ser armazenados em soluções com tecnologias que são preparadas para grandes volumes de dados e informações tipo Big Data e/ou banco de dados relacional;

8 Todos os dados coletados devem ser armazenados e ficar disponíveis para consulta durante todo o período de vigência contratual.

9 A solução deverá possuir funções de relatórios e visualização de dados baseados nas informações coletadas,com períodos longos para análise estatística;

10 A solução deverá possuir sistema de notificação e deverá funcionar através de avisos visuais, sonoros, e-maile sms;

11 A solução não deverá possuir restrição de quantidade de usuários e cadastrados para envio de alertas;

12 Deverá efetuar o registro de logs e eventos;

13 Permitir a criação, edição e visualização de mapas, telas e slide shows;

14 Configuração deverá ser armazenada em banco de dados;

15 Permitir a criação, edição e visualização de gráficos em diversos formatos e com Zoom;

16 A infraestrutura lógica, tais como: arquivos de atualização, nome de usuário e senha de comunidades SNMP (Simple Network Management Protocol), devem ser compartilhados para leitura (acesso completo), com o objetivo de se realizar o gerenciamento e análise dos circuitos nas localidades central e remotas por parte do CREA-SP ou a quem ele designar;

17 A CONTRATADA deverá disponibilizar ao CREA-SP, consultas, emissão e visualização de relatórios na própria internet, por intermédio de navegador web e protocolo HTTPS com certificação digital, com informações referentes aos estados dos equipamentos (up/down), falhas na rede, tráfego no circuito, disponibilidade no período, alarmes e eventos, tendências e desvios de comportamentos, todos referentes a rede da CONTRATADA, com atraso máximo de 30 minutos para a atualização. Esses dados deverão ficar disponíveis para acesso por um período nunca inferior a 90 (noventa) dias;

18 A Solução de Gerência da Rede da CONTRATADA deverá atuar de forma proativa, antecipando-se aos problemas na rede e garantindo a qualidade do serviço estabelecida no Acordo de Nível de Serviço (ANS), realizando abertura, acompanhamento e fechamento de chamados técnicos relacionados com indisponibilidade e desempenho nos serviços de rede, gerenciamento da rede e segurança;

19 A Solução deverá permitir a geração e emissão de relatórios gerenciais que possibilitem o acompanhamento da qualidade dos serviços, dos níveis de serviços contratados (ANS) para a validação das faturas;

20 O CREA-SP exercerá a fiscalização dos serviços e gerenciamento da sua execução, através do gestor do contrato especialmente designado para esse fim o qual fará gestões através do (s) preposto (s) designado (s) pela CONTRATADA visando à exclusiva execução do objeto contratual, sem prejuízo, redução ou exclusão da responsabilidade da CONTRATADA, inclusive perante terceiros da CONTRATADA se houver;

21 A indisponibilidade dos dados de gerência (coleta não realizada, dados não acessíveis) será contabilizada como indisponibilidade do serviço, no período em que os dados não forem coletados ou ficarem inacessíveis, caso isto implique em perda de dados de gerenciamento.

4.6.2.1.2 MONITORAMENTO POR PARTE DA CONTRATANTE

1 A CONTRATADA Deverá disponibilizar na sede do CREA-SP, um sistema de

monitoramento da solução.

2 O sistema de monitoramento deve ser composto de no mínimo 4 Monitores de 50 polegadas.

3 A CONTRATADA deverá disponibilizar usuário de leitura para o sistema de monitoramento, com acesos atodas as telas, configurações, triggers, etc;

3.1 Todos os acessos aos sistemas da CONTRATADA fornecidos pela CONTRATADA ao CREA-SP devem ser individuais, por usuário da CONTRATANTE.

3.2 Todos os acessos fornecidos devem possuir senha individual de conhecimento apenas do próprio usuárioda CONTRATANTE.

4 Os monitores deverão disponibilizar vários Dashboards com as informações que a CONTRATADA achar pertinente, no momento de planejamento.

5 A CONTRATADA deve fornecer a CONTRATANTE acesso através de portal WEB ao ambiente Cloud daCONTRATADA, com as seguintes funcionalidades mínimas:

5.1 Criação de templates de máquinas virtuais, pré-configurados, para provisionamento, de acordo comcatálogo de máquinas virtuais solicitado pela contratante.

5.2 Ligar, desligar e reiniciar máquinas virtuais.

5.3 Criar snapShots de máquinas virtuais.

6 A CONTRATADA deve fornecer à CONTRATANTE acesso de console, através do protocolo SSH, no modo somente leitura a todos os equipamentos de rede, segurança, firewall, NLB, servidores físicos, etc. que fazem parte da solução contratada*, podendo visualizar as configurações e as informações de "status" das interfaces eenlaces de comunicação.*

7 A CONTRATADA deve fornecer a CONTRATANTE acesso através de portal WEB, no modo read only, ao console e sistema monitor de todos os equipamentos de rede, segurança, firewall, NLB, WAF, SIEM, servidores físicos, servidores virtuais, sistema devirtualização, etc. que fazem parte da solução contratada;

8 A CONTRATADA deve fornecer acesso SNMP somente leitura dos *sistemas de monitoramento do CREA-SP* atodos os equipamentos da de rede, segurança, servidores físicos, NLB, WAF, firewalls, etc. que fazem parte da solução contratada;

4.6.2.1.3 REQUISITOS ESPECÍFICOS DE MONITORAMENTO DE TRÁFEGO

1 A CONTRATADA Deverá implementar o monitoramento do tráfego de internet dos links dedicados do CREA-SP 24x7x365 dias através de gráficos de utilização de banda tanto de entrada, quanto de saída em tempo real.

2 Os dados devem ser armazenados e estar disponíveis para consulta durante todo o

período de vigência contratual, no mínimo.

3 A CONTRATADA deverá implementar o monitoramento do tráfego entre o Datacenter e o CREA-SP 24x7x365dias/ano através de gráficos de utilização de banda tanto de entrada, quanto de saída.

4 A CONTRATADA deverá disponibilizar usuários de leitura para a interface gráfica do monitor de tráfego, demodo a possibilitar a consulta pelos analistas do CREA-SP.

5 A CONTRATADA deverá configurar os equipamentos de rede para enviar dados no protocolo sFlow para omonitor de tráfego do CREA-SP.

5.1 Devem ser monitorados no mínimo os links de internet e de comunicação entre a contratada e o CREA-SP.

4.6.3 REQUISITOS DE OPERAÇÃO

1 A CONTRATADA deverá disponibilizar uma equipe de pessoas tecnicamente capacitadas, as quais serão responsáveis pela operação total do Ambiente.

2 Pelo menos um membro da equipe de operação deverá ficar locado na Sede do CREA-SP, na Avenida BrigadeiroFaria Lima, 1059, PINHEIROS no período de 9:00 as 18:00, cinco dias por semana.

2.1 Será responsabilidade da contratada arcar com todos os custos, referentes ao recurso locado na sede doCREA, sem nenhum ônus financeiro, ou vínculo empregatício para o CREA-SP.

2.2 A função deste recurso é facilitar a comunicação entre o CREA-SP e as demais equipes da CONTRATADA (Redes, Servidores, Segurança, etc.), de forma a garantir o cumprimento de todos os níveis de serviço, e priorizaras atividades de acordo com as necessidades do CREA-SP.

3 Com exceção do recurso especificado no item 1, os demais membros da equipe, poderão também, à critério da CONTRATADA, com a finalidade de atender aos Níveis de Serviço definidos, ficar locados na Sede do CREA-SP, na Avenida Brigadeiro Faria Lima, 1059, PINHEIROS.

4 A equipe deverá cuidar da operação da rede em regime 24 x 7 x 365 (vinte e quatro horas por dia, sete dias porsemana, trezentos e sessenta e cinco dias por ano)

5 A equipe deve ser formada de, no mínimo 01 profissional de cada uma das seguintes áreas de atuação:

5.1 Redes e comunicação de dados (Roteadores, Switches, Firewals, etc)

5.2 Segurança (Firewall/Waf, EDR, etc)

5.3 Banco de Dados (Db2 e SQLServer)

5.4 Virtualização

5.5 Sistemas operacionais (Windows e Linux)

6 Responsabilidades e atividades da Equipe

6.1 Realizar todos os serviços de operação da solução.

6.2 Realizar os serviços de monitoramento.

6.3 Realizar os serviços de operação do sistema de Segurança (SOC).

6.4 Realizar o atendimento de tickes/chamados abertos pela CONTRATADA no sistema da CONTRATANTE.

6.5 Realizar operações de mudança (Gerencia de Mudanças) aprovadas pelo CREA.

6.6 Realizar a interface entre as necessidades do CREA e os profissionais da CONTRATADA responsáveis porexecutar as atividades.

7 Capacitação mínima dos profissionais

7.1 Suporte em SO Windows/Linux e Hypervisor VM

7.1.1 Skills: Windows Servers (AD, core, etc), VMWare, VCenter, Linux (CentOS/RedHat).

7.2 Suporte em Firewall/Segurança da Informação e Segurança de Redes

7.2.1 Skills: TCP/IP, Switching, Routing, Firewalling, WAF, Segurança da Informação.

7.3 Banco de dados – DBA

7.3.1 Skills: Profissional que possa gerenciar as bases db2 (IBM) e sql server (Microsoft).

4.6.3.1 REQUISITOS DO SERVIÇO DE OPERAÇÃO DO SISTEMA DE SEGURANÇA

1 A CONTRATADA deverá oferecer uma plataforma inteligente com uma visão unificada da segurança dos ativosde TI contratados.

2 A CONTRATADA deverá investigar, identificar e responder às ameaças em tempo real.

3 A CONTRATADA deverá implementar o processo de gestão de vulnerabilidades do ambiente.

3.1 A CONTRATADA deverá fornecer relatórios periódicos das vulnerabilidades do ambiente de TI (servidoresde virtualização, IBM, WAF, SIEM, equipamentos de rede, firewalls, etc. -não inclui os servidores virtuais) contratado, com planos de ação para o tratamento das mesmas.

4 A operação do ambiente de segurança deverá seguir as normas previstas na ISO27001 de segurança dainformação.

5 A CONTRATADA deverá fornecer usuários com permissão de leitura, com acesso (gráfico e terminal - caso haja) a todos os equipamentos e sistemas que compõe o ambiente de identificação, prevenção, detecção, mitigação, logs e resposta de ameaças para os analistas do CREA-SP acompanharem a operação do ambiente.

5 - DEVERES E RESPONSABILIDADES DA CONTRATANTE

5.1 OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATANTE

1 Observar e fazer cumprir fielmente o que estabelece este Termo de Referência;

2 Receber o objeto no prazo e condições estabelecidas no Termo de Referência;

3 Prestaras informações e os esclarecimentos que venham a ser solicitados pela CONTRATADA;

4 Comunicará a CONTRATADA toda e qualquer ocorrência relacionada com a execução do Contrato;

5 Acompanhar e fiscalizar o cumprimento das obrigações da CONTRATADA por meio de um fiscal;

6 Colocar à disposição da CONTRATADA os elementos e informações necessárias à consecução do objeto doContrato;

7 Aplicar à CONTRATADA as penalidades contratuais e regulamentares cabíveis, garantidos o contraditório e a ampladefesa;

8 Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com as cláusulas contratuaise os termos de sua proposta.

9 Nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execuçãodos contratos;

10 Encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com oscritérios estabelecidos no Termo de Referência;

11 Receber o objeto fornecido pela contratada que esteja em conformidade com a proposta aceita, conforme inspeçõesrealizadas;

12 Aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;

13 Liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;

14 Comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;

15 Prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos eprodutos, cuja criação ou alteração seja, objeto da relação contratual pertençam à Administração, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, justificando os casos em queisso não ocorrer;

16 Verificar, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes doEdital e da proposta, para fins de aceitação e, posterior, recebimento definitivo;

6 - DEVERES E RESPONSABILIDADES DA CONTRATADA

OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATADA

1 Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

2 Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, quaisquer danos diretamente causados à contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamentoda execução dos serviços pela contratante;

3 Propiciar todos os meios necessários à fiscalização do contrato pela contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão;

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

5 Quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;

6 Quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante aexecução do contrato; e

7 Ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados à Administração;

8 Executar o objeto do certame em estreita observância dos ditames estabelecido pela Lei nº 13.709, de 14 de agostode 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).

9 Executar os serviços conforme especificações deste Termo de Referência e de sua

proposta;

10 Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com os artigos 14 e 17 a 27,do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);

11 Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere responsabilidade à CONTRATANTE;

12 Relatar à CONTRATANTE toda e qualquer irregularidade verificada no decorrer da prestação dos serviços;

13 Executar o objeto do certame em estrita observância dos ditames estabelecido pela Lei 13.709/2018 (Lei Geral deProteção de Dados Pessoais (LGPD)).

14 Prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATANTE por intermédio depreposto designado para acompanhamento do contrato).

15 Indicar no prazo máximo de 24 horas úteis após a assinatura do contrato, junto à CONTRATANTE, um preposto para representar a CONTRATADA, principalmente no tocante à eficiência e agilidade da execução dos serviços objeto deste Termo de Referência, e que deverá responder pela fiel execução do contrato; Na hipótese de afastamento do preposto definitivamente ou temporariamente, a CONTRATADA deverá comunicar ao Gestor do Contrato por escrito o nome e a forma de comunicação de seu substituto até o fim do próximo dia útil.

16 Reconhecer o Gestor do Contrato, bem como outros servidores que forem indicados pela CONTRATANTE, pararealizar as solicitações relativas ao contrato firmado, tais como manutenção, configuração, entre outras;

17 Apresentar Nota Fiscal/Fatura com a descrição dos serviços prestados, nas condições deste Termo de Referência, como forma de dar início ao processo de pagamento pela CONTRATANTE;

18 Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes àexecução do objeto contratual;

19 Assumir as responsabilidades pelos encargos fiscais e comerciais resultantes da contratação.

20 Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado em contrato, osserviços efetuados em que se verificarem vícios, defeitos ou incorreções resultantes da execução;

21 Propiciar todos os meios necessários à fiscalização do contrato pela CONTRATANTE, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, sempre que considerar a medida necessária;

22 Acatar as orientações da CONTRATANTE, sujeitando-se à mais ampla e irrestrita fiscalização, prestando osesclarecimentos solicitados e atendendo as reclamações formuladas;

23 Prestar esclarecimentos à CONTRATANTE sobre eventuais atos ou fatos noticiados que se refiram àCONTRATADA, independente de solicitação;

24 Comunicar à CONTRATANTE, por escrito, qualquer anormalidade nos serviços e prestar os esclarecimentosjulgados necessários;

25 Não veicular publicidade ou qualquer outra informação acerca da prestação dos serviços do Contrato, sem préviaautorização da CONTRATANTE;

26 Não fazer uso das informações prestadas pela CONTRATANTE para fins diversos do estrito e absoluto cumprimentodo contrato em questão;

7 - MODELO DE EXECUÇÃO DO CONTRATO

7.1 - Rotinas de Execução

7.1.1 DA REUNIÃO INICIAL DO CONTRATO

1 As partes, CONTRANTE e CONTRATADA deverão, em até 05 (cinco) dias úteis após a assinatura do contrato, prorrogáveis uma única vez, a pedido justificado pela CONTRATADA, promover a reunião inicial do Contrato (“kick off”)para o estabelecimento e planejamento dos procedimentos relacionados ao Plano de Inserção da CONTRATADA.

2 Nesta reunião deverão ocorrer as seguintes atividades:

2.1 Apresentação do preposto titular e preposto substituto pela CONTRATADA;

2.2 Apresentação do gestor e fiscais do contrato pela CONTRATANTE;

2.3 Proposição de um Plano de Comunicação pela CONTRATADA;

2.4 Definição dos procedimentos de gestão, demanda, acompanhamento e validação dos trabalhos;

2.5 Definição da data de início da execução contratual;

2.6 Definição dos modelos de relatórios de prestação de serviços, de acompanhamento dos NMS’s;

2.7 Apresentação, pela CONTRATADA da minuta do Plano de Inserção da CONTRATADA.

2.8 Ajuste do início da execução dos serviços;

7.1.2 PLANO DE INSERÇÃO DA CONTRATADA

1 Conceitua-se "Plano de Inserção" o processo no qual o CREA-SP repassa à

CONTRATADA informações e atividades, conforme os padrões de execução até então realizados, para que não haja quebra de continuidade dos serviços e a partir do qual a CONTRATADA assume o início da execução dos serviços, passando a ser responsável pelos resultados obtidos, ressalvados os ajustes de NMS.

2 Os primeiros 90 (noventa) dias após o início da execução dos serviços serão considerados como período de inserçãoda CONTRATADA.

3 Após o período de inserção, caso a CONTRATADA não tenha realizado as tarefas de migração necessárias para queo ambiente de hospedagem esteja completamente transferido para sua administração, será de sua responsabilidade arcar com os custos da manutenção da hospedagem no Datacenter atualmente contratado pelo CREA-SP.

4 O período de Inserção é reservado para que a CONTRATADA realize as seguintes atividades:

4.1 Conhecer, analisar e entender o ambiente computacional e sua dinâmica atual, procedimentos, diretrizes, políticas, normas, planos e programas, dentre outros que deverão ser considerados na execução contratual;

4.2 Apresentar a equipe de operação devidamente capacitada;

4.3 Implantar processos de atendimento, em conformidade com o disposto na contratação;

4.4 Definir as rotinas de serviços, entre outras atividades necessárias à execução do objeto, durante as quais os níveis de serviços acordados serão ajustados, em comum acordo entre a CONTRATANTE e a CONTRATADA.

5 Durante os períodos de inserção e execução, a CONTRATADA deverá manter, quantitativa e qualitativamente, equipe suficiente para executar as atividades do plano de Migração, que inclui a central de serviços.

6 O Plano de Inserção deve ser elaborado pela CONTRATADA e entregue ao CREA-SP para validação até o 10º dia útil após o início da execução dos serviços contratados, contemplando as seguintes premissas/atividades para o prazo de90 dias:

6.1 Formalização do supervisor do serviço de Gestão;

6.2 Formalização das equipes operação e administração;

6.3 Validação ou atualização dos Níveis Mínimos de Serviço, considerando as especificidades do ambientecomputacional do CREA-SP;

6.4 Cronograma de mapeamento e registro da situação do licenciamento de softwares;

6.5 O prazo de entrega do sistema de Monitoramento;

6.6 O prazo para entrega do Planejamento de instalação e Migração;

6.7 O Prazo para que o plano de migração esteja completo.

6.8 O prazo para que a solução Hospedagem, esteja instalada e em condições para início da migração;

6.9 Em conjunto com a CONTRATANTE estabelecer o cronograma para implantação do sistema de hospedagemredundante;

6.10 O Prazo para que o serviço de interligação esteja completo, pronto para interligar o Datacenter da Contratadaao CREA-SP.

6.11 Modelos de documentos para gestão de mudanças e incidentes;

6.12 Modelos de documentos e relatórios do serviço de Gestão;

6.13 Treinamento dos servidores do CREA-SP nas funcionalidades de auditoria para efeito de acompanhamento,aferição e fiscalização dos serviços;

6.14 Plano para início dos atendimentos dos chamados de suporte técnico do CREA-SP;

6.15 Entrega dos manuais de procedimentos para abertura de chamados na Central de Serviços para disseminaçãoaos usuários de TIC do CREA-SP.

7.1.3 FASE DE OPERAÇÃO

1. A Fase de operação inicia com o final do processo de inserção da Contratada, conforme negociado entre a CONTRATADA ea CONTRATANTE por ocasião da reunião inicial.

2. A Fase de operação termina com o término do contrato.

3. Durante a Fase de Operação, a CONTRATADA entra em regime de operação, conforme requisitos definidos neste termo dereferência.

7.1.4 DA TRANSIÇÃO CONTRATUAL

1. Em casos de interrupção contratual e ocorrendo mudança de fornecedor da solução, todo conhecimento adquirido ou desenvolvido, bem como toda informação produzida pelos atendimentos de chamados de suporte deverão ser disponibilizadosà CONTRATANTE ou empresa por ela designada em até 30 (trinta) dias corridos após o encerramento do contrato. As informações disponibilizadas devem ser em formato digital, inteligível para humanos, e na língua portuguesa.

2. A CONTRATADA deverá elaborar o Plano de Transição, no prazo de 60 (sessenta) dias corridos antes do encerramento docontrato, para a transferência integral e irrestrita dos conhecimentos e das competências necessárias e suficientes para promover a continuidade dos serviços.

3. A CONTRATANTE poderá estabelecer prazo inferior caso haja rescisão contratual.

4. Nenhum pagamento será devido à CONTRATADA pela elaboração ou pela execução do Plano de Transição. O fato da empresa CONTRATADA ou seus representantes não cooperarem ou reterem qualquer informação ou dado solicitado pela CONTRATANTE, que venha a prejudicar, de alguma forma, o andamento da transição das tarefas e serviços para um novo prestador, constituirá quebra de contrato, sujeitando-a as obrigações em relação a todos os danos causados à CONTRATANTE.

5. A CONTRATADA deverá oferecer a CONTRATANTE uma opção de aquisição do ambiente de hospedagem.

7.1.5 MANUTENÇÃO DO SIGILO E NORMAS DE SEGURANÇA

1 A Contratada deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

2 O **Termo de Compromisso e Manutenção de Sigilo**, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal da Contratada, e **Termo de Ciência**,a ser assinado por todos os empregados da Contratada diretamente envolvidos na contratação, encontram-se nos ANEXOS modelo-termo-de-compromisso-de-manutencao-do-sigilo-v1-0 e modelo-termo-de-ciencia-v1-0.docx.

7.2 - Quantidade Mínima de Bens ou Serviços para Comparação e Controle

1 A avaliação da qualidade e da adequação dos serviços ocorrerá na através da avaliação dos relatórios mensais dosserviços prestados definidos nos **REQUISITOS DO SERVIÇO DE GESTÃO**.

2 A Avaliação da qualidade será realizada pelo Fiscal Técnico do Contrato com base nos indicadores definidos no item**REQUISITOS GERIAS DE NÍVEL DE SERVIÇO MÍNIMO (NMS)** deste termo de referência, aos quais a CONTRATADA deverá atender.

7.2.1 1 A CONTRATADA estará sujeita, garantido o contraditório e a ampla defesa, às sanções administrativas em função dosindicadores obtidos abaixo da faixa de ajuste.

7.2.2 1 A aplicação dos ajustes (glosas) do pagamento pelo não atendimento dos Níveis mínimos de Serviço não exclui a aplicação de multas e sanções previstas neste documento.

7.3 - Mecanismos Formais de Comunicação entre a Contratada e a Administração

INTERAÇÃO ENTRE CONTRATANTE E CONTRATADA

1 São mecanismos formais de comunicação entre a CONTRATADA e a CONTRATANTE:

1.1 E-mails: forma rápida de comunicação para tratar de informações cotidianas;

1.2 Ofícios: Comunicação para tratar de assuntos gerais;

2 Toda a comunicação entre a CONTRATANTE e a CONTRATADA deverá ser sempre formal como regra, exceto emcasos excepcionais que justifiquem outro canal de comunicação.

7.4 - Forma de Pagamento em Função dos Resultados

7.4.1 **1** O pagamento será efetuado, mensalmente, mediante crédito em conta-corrente após:

1.1 O atesto do fiscal do contrato do cumprimento da perfeita realização da entrega dos serviços.

1.2 Prévia verificação da regularidade fiscal da licitante vencedora feita.

7.4.2 DA NOTA FISCAL

1 O CREA-SP efetuará o pagamento até o 15o (décimo quinto) dia após a apresentação da nota fiscal/fatura, a qual deverá ser entregue na Sede Faria Lima, na Equipe de Suporte e Sustentação de TI, localizada na Av. Brigadeiro Faria Lima, 1059 – Pinheiros – CEP 01452-920 – São Paulo/SP, ficando a CONTRATADA obrigada a manter durante execução dos serviços os documentos abaixo relacionados acompanhados da nota fiscal/fatura:

2 Comprovante de regularidade com o Sistema e Seguridade Social– Certidão Negativa de Débito – CND.

3 Comprovante de Regularidade com o Fundo de Garantia do Tempo de Serviço– Certificado de Regularidade doFGTS CRF.

4 Comprovante de regularidade para com a Fazenda Federal– Certidão Conjunta Negativa.

5 Comprovante de inexistência de débitos inadimplidos perante a Justiçado Trabalho, mediante a apresentação deCertidão

6 Negativa de Débitos Trabalhistas – CNDT, nos Termos do Título VII-A da Consolidação das Leis de Trabalho,aprovada pelo Decreto-Lei no 5.452, de 1o de maio de 1943.

7 A nota fiscal/fatura será analisada, minimamente, quanto aos itens a seguir descritos:

7.1 Correlação entre os valores indicados na nota fiscal/fatura o da proposta da empresa.

7.2 Ausência de emendas ou rasuras na nota fiscal/fatura.

7.3 O correto preenchimento dos dados do CREA-SP (nome, CNPJ, dados contratuais) e da discriminação dosserviços;

7.4 Pertinência dos cálculos aritméticos da nota fiscal/fatura – o valor total deverá corresponder ao somatório dosvalores individuais lançados na mesma,

7.5 Correlação entre o valor da nota fiscal e os valores empenhados;

7.6 Correlação entre o CNPJ da CONTRATADA e o constante na proposta e na nota de empenho;

8 O Crea-SP efetuará retenção de impostos eventualmente incidentes sobre o valor do bem/serviço, conforme previstona Lei Federal no 9.430, de 27 de dezembro de 1996 e Instrução Normativa RFB no 1.234,de 11 de janeiro de 2012 e anexo;

9 A CONTRATADA é responsável pelos encargos fiscais, trabalhistas e previdenciários incidentes sobre os serviçoscontratados;

10 Se a CONTRATADA descumprir qualquer termo ou condição a que se obrigar no presente certame, por sua exclusiva culpa, poderá a Administração reter o pagamento, até que seja sanado o respectivo inadimplemento, não sobrevindo, portanto, qualquer ônus ao Conselho resultante desta situação;

11 Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pelo CREA-SP, entre a data do vencimento e o efetivo adimplemento da parcela, é calculada mediante a aplicação da seguinte fórmula, conforme previsto no ANEXO XI da IN 05/2017:

EM = I x N x VP, sendo:
EM = Encargos moratórios;
N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;
VP = Valor da parcela a ser paga;
I = Índice de compensação financeira = 0,00016438, assim apurado:

I = (TX)	I =	(6 / 100) 365	I = 0,00016438
TX = Percentual da taxa anual = 6%			

7.4.3 CRONOGRAMA FÍSICO FINANCEIRO

1. A Tabela a seguir lista os principais marcos e eventos que ocorrerão durante a execução do Contrato:

		ANO 1	ANO 2	ANO 3
Etapas	**Atividades**	**Pagamento correspondente**	**Pagamento correspondente**	**Pagamento correspondente**
Início do Contrato				
Fase de Inserção da Contratada	Entrega dos Serviços de Interligação	início do pagamento dos Serviços de interligação	**N.A.**	
	Entrega do plano de migração		**N.A.**	
	Migração dos Servidores e Banco de Dados	início do pagamento dos serviços de	**N.A.**	

		hospedagem		
	Termino da Migração e atualização dos sistemas	Pagamento dos serviços de Migração e atualização	**N.A.**	
	Apresentação do Supervisor de Gestão	início do pagamento dos serviços de Gestão	**N.A.**	
	Implantação do Sistema de Monitoramento Apresentação da equipe de operação	início do pagamento dos serviços de Administração e operação	**N.A.**	
	TÉRMINO DA INSTALAÇÃO E MIGRAÇÃO	Pagamento do SERVIÇODE MIGRAÇÃO	**N.A.**	
Fase de Operação	atividades de operação: SERVIÇO DE GESTÃO SERVIÇO DE ADMINISTRAÇÃO SERVIÇO DE HOSPEDAGEM SERVIÇO DE ARMAZENAMENTO SERVIÇO DE INTERLIGAÇÃO	Pagamento dos serviços de hospedagem, interligação, Gestão, Administração e Armazenamento	Pagamento Mensal Correspondente	Pagamento Mensal Correspondente

7.4.4 DO REAJUSTE

1. Os preços são fixos e irreajustáveis no prazo de um ano contado da data limite para a apresentação das propostas.

2. Dentro do prazo de vigência do contrato e mediante solicitação da contratada, os preços contratados poderão sofrer reajusteapós o interregno de um ano, aplicando-se o índice ICTI (Índice de Custo da Tecnologia da Informação), previsto no art. 24 da Instrução Normativa nº 1, de 4 de Abril de 2019, do Ministério da Economia/Secretaria Especial de Desburocratização, Gestão e Governo Digital/Secretaria do Governo Digital:

"...Art. 24. Nas contratações de serviços de Tecnologia da Informação em que haja previsão de reajuste de preços por aplicação de índice de correção monetária, é obrigatória a adoção do Índice de Custos de Tecnologia da Informação - ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada – IPEA".

3. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros doúltimo reajuste.

8 - MODELO DE GESTÃO DO CONTRATO

8.1 - Metodologia/Formas de Avaliação da Qualidade e Adequação da Solução às Especificações Funcionais e Tecnológicas

8.1.1 1 Nos termos do artigo 67 da Lei Federal n.º 8.666/93, a responsabilidade pela gestão desta contratação ficará do Gestor indicado o qual será auxiliado pela fiscalização técnica e administrativa, conforme designação por funcionário doCREA-SP competente.

2 A Avaliação será realizada utilizando minimamente os critérios definidos no item **REQUISITOS GERAIS DE NÍVELDE SERVIÇO MÍNIMO (NMS)** deste documento.

9 - PROCEDIMENTOS DE FISCALIZAÇÃO DA EXECUÇÃO CONTRATUAL

9.1 PAPEIS E RESPONSABILIDADES

9.1.1 PAPEIS E RESPONSABILIDADES DO CREA NA FISCALIZAÇÃO DO CONTRATO

9.1.1.1 GESTOR DO CONTRATO

1 Servidor com atribuições gerenciais, designado para coordenar e comandar o processo de gestão e fiscalizaçãoda execução contratual, indicado por autoridade competente.

9.1.1.2 FISCAL TÉCNICO

1 Servidor representante da Área de Tecnologia da Informação, indicado pela autoridade competente dessa áreapara fiscalizar tecnicamente o contrato.

9.1.1.3 FISCAL ADMINISTRATIVO

1 Servidor representante da Área Administrativa, indicado pela autoridade competente dessa área para fiscalizar ocontrato quanto aos aspectos administrativos.

9.1.2 PAPEIS E RESPONSABILIDADES DA CONTRATADA NA FISCALIZAÇÃO CONTRATUAL

9.1.2.1 PREPOSTO

1 Representante da CONTRATADA, responsável por acompanhar a execução do contrato e atuar como interlocutor principal junto ao Órgão, incumbido de receber, diligenciar, encaminhar e responder às principais questões técnicas, legais e administrativas referentes ao andamento contratual:

1.1 Fazer a gestão geral do contrato, mantendo o controle de todas os chamados, com o objetivo de garantir aexecução dos serviços dentro dos prazos estabelecidos, atendendo a todos os requisitos de qualidade;

1.2 Realizar a gestão, por parte da CONTRATADA, quanto aos aspectos de caráter administrativo e legal docontrato;

1.3 Informar ao CREA-SP sobre problemas de qualquer natureza que possam impedir o andamento normal dosserviços;

1.4 Garantir a elaboração e entrega dos documentos e relatórios mensais de Gestão, referentes ao cumprimentodos Níveis mínimos de Serviço (NMS);

1.5 Garantir a execução dos procedimentos administrativos referentes aos recursos envolvidos na execução dosserviços contratados;

1.6 Estar apto a prestar tempestivamente todas as informações (por meio de documentos impressos ou digitais) sobre as regularidades fiscais e financeiras da empresa, bem como a manutenção de todos os requisitos contratuais. Irregularidades administrativas ou contratuais poderão ensejar rescisão contratual;

1.7 Supervisionar todos os processos do trabalho, garantindo a qualidade dos serviços prestados e ocumprimento dos Níveis Mínimos de Serviço estabelecidos;

1.8 Propor novas rotinas, processos e fluxos de trabalho, visando maior eficácia no serviço prestado;

1.9 Gerenciar o cumprimento de prazos e prioridades estabelecidos;

1.10 Gerenciar e acompanhar o desempenho da prestação de serviço.

9.2 CONTROLE E FISCALIZAÇÃO DA EXECUÇÃO

1 O acompanhamento e a fiscalização da execução do contrato consistem na verificação da conformidade da prestaçãodos serviços e da alocação dos recursos necessários, de forma a assegurar o perfeito cumprimento do ajuste, devendo ser exercidos por um ou mais representantes da CONTRATANTE, especialmente designados, na forma dos arts. 67 e 73da Lei nº 8.666, de 1993, e do art. 10 do Decreto nº 9.507, de 2018.

2 O representante da CONTRATANTE deverá ter a experiência necessária para o acompanhamento e controle daexecução dos serviços e do contrato.

3 A verificação da adequação da prestação do serviço deverá ser realizada com base nos critérios previstos nesteTermo de Referência e Anexos.

4 A execução do contrato será acompanhada e fiscalizada por meio de instrumentos de controle, que compreendam amensuração dos aspectos mencionados no art. 47 e no ANEXO V, item 2.6, i, ambos da IN nº 05/2017.

5 A fiscalização técnica do contrato avaliará constantemente a execução do objeto e utilizará o Instrumento de Mediçãode Resultado (IMR), conforme previsto na TABELA DE NÍVEIS MÍNIMOS DE SERVIÇOS (NMS) deste Termo de Referência, ou outro instrumento substituto para aferição da qualidade da prestação dos serviços, devendo haver o redimensionamento no pagamento com base nos indicadores estabelecidos, sempre que a CONTRATADA:

5.1 Não produzir os resultados, deixar de executar, ou não executar com a qualidade mínima exigida as atividadescontratadas; ou

5.2 Deixar de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizá-los comqualidade ou quantidade inferior à demandada.

6 A utilização da tabela NMS não impede a aplicação concomitante de outros mecanismos para a avaliação daprestação dos serviços.

7 Durante a execução do objeto, o fiscal técnico deverá monitorar constantemente o nível de qualidade dos serviços para evitar a sua degeneração, devendo intervir para requerer à CONTRATADA a correção das faltas, falhas e

Irregularidades constatadas.

9.3 ENTREGA E CRITÉRIOS DE ACEITAÇÃO DO OBJETO

1 Os Serviços de suporte continuado serão aceitos mensalmente pelo gestor do contrato, através do seu Atesto. Os Critérios utilizados para dar aceitação são os definidos no NMS (Nível mínimo de Serviço) deste Termo de Referência.

9.3.1 DA NÃO ACEITAÇÃO DO OBJETO

1. A recusa parcial ou total de um relatório de serviços emitido, será oficiada à CONTRATADA pela CONTRATANTE, quedeverá prontamente prestar o serviço de acordo com o solicitado e em acordo com os requisitos estabelecidos pelo contrato;

9.3.2 DO RECEBIMENTO E ACEITAÇÃO DO OBJETO

1 A emissão da Nota Fiscal/Fatura deve ser precedida do recebimento definitivo do objeto contratual, nos termosabaixo.

2 No prazo de até 5 dias corridos do adimplemento da parcela, a CONTRATADA deverá entregar toda adocumentação comprobatória do cumprimento da obrigação contratual;

3 O recebimento provisório será realizado pelo fiscal técnico e setorial ou pela equipe de fiscalização após a entregada documentação acima, da seguinte forma:

3.1 A contratante realizará inspeção minuciosa de todos os serviços executados, por meio de profissionais técnicoscompetentes, acompanhados dos profissionais encarregados pelo serviço, com a finalidade de verificar a adequação dos serviços e constatar e relacionar os arremates, retoques e revisões finais que se fizerem necessários.

3.1.1 Para efeito de recebimento provisório, ao final de cada período de faturamento, o fiscal técnico do contrato irá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenhoe qualidade da prestação dos serviços realizados em consonância com os indicadores previstos, que poderá resultar no redimensionamento de valores a serem pagos à contratada, registrando em relatório a ser encaminhado ao gestor do contrato

3.1.2 A Contratada fica obrigada a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, notodo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução oumateriais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

3.1.3 O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes decampo e à entrega dos Manuais e Instruções exigíveis.

3.2 No prazo de até 10 dias corridos a partir do recebimento dos documentos da CONTRATADA, cada fiscal ou aequipe de fiscalização deverá elaborar Relatório Circunstanciado em consonância com suas atribuições, e encaminhá-lo ao gestor do contrato.

3.2.1 Quando a fiscalização for exercida por um único servidor, o relatório circunstanciado deverá conter o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, em relação à fiscalizaçãotécnica e administrativa e demais documentos que julgar necessários, devendo encaminhá-los ao gestor docontrato para recebimento definitivo.

3.2.2 Será considerado como ocorrido o recebimento provisório com a entrega do relatório circunstanciado ou,em havendo mais de um a ser feito, com a entrega do último.

3.2.2.1 Na hipótese de a verificação a que se refere o parágrafo anterior não ser procedida tempestivamente, reputar-se-á como realizada, consumando-se o recebimento provisório no dia do esgotamento do prazo.

4 No prazo de até 10 (dez) dias corridos a partir do recebimento provisório dos serviços, o Gestor do Contrato deveráprovidenciar o recebimento definitivo, ato que concretiza o ateste da execução dos serviços, obedecendo as seguintes diretrizes:

4.1 Realizar a análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes,solicitando à CONTRATADA, por escrito, as respectivas correções;

4.2 Emitir Termo Circunstanciado para efeito de recebimento definitivo dos serviços prestados, com base nosrelatórios e documentações apresentadas; e

4.3 Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pelafiscalização, com base no Instrumento de Medição de Resultado (IMR), ou instrumento substituto.

5 O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da Contratada pelos prejuízosresultantes da incorreta execução do contrato, ou, em qualquer época, das garantias concedidas e das responsabilidades assumidas em contrato e por força das disposições legais em vigor (Lei n° 10.406, de 2002).

6 1.6.Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo

com as especificações constantes neste Termo de Referência e na proposta, devendo ser corrigidos/refeitos/substituídos no prazo fixado pelofiscal do contrato, às custas da Contratada, sem prejuízo da aplicação de penalidades.

10 - Bens e Serviços					
	Bem/Serviço	**Qtd.**	**Unidade**	**Valor Unitário (R$)**	**Valor Total (R$)**
1	Serviço de Hospedagem em Datacenter; Composto dos Preços da Tabela AT - Serviços de hospedagem.	36	Serviço		
2	Serviço de interligação conforme Tabela BT - Serviços de Interligação. (Serviço compagamento mensal, por 36 meses)	36	Serviço		
3	Serviços de Gestão conforme descrito Tabela CT - Serviços de Gestão. (Serviço com pagamento mensal, por 36 meses)	36	Serviço		
4	Serviços de Administração e Operação conforme Tabela DT - Serviços de Administração. (Serviço com pagamentomensal, por 36 meses)	36	Serviço		
5	Serviço de Planejamento e instalação conforme Tabela ET - Serviços de Planejamento e Instalação. (Serviço com pagamento único mediante entrega)	1	Serviço		
6	Serviço de Área de Armazenamento (Storage), conforme tabela FT - Serviço deArmazenamento	36	Meses		
Valor Total (R$)					

11 - ESTIMATIVA DAS QUANTIDADES

1. A memória de cálculo e justificativas de quantitativos estão nos Estudos Técnicos Preliminares.

MAPEAMENTO DE SERVIÇOS/PRODUTOS

2. Devido à complexidade da solução fazemos um mapeamento para o leitor identificar os itens das tabelas e a memória decálculo utilizada para calcular o quantitativo necessário, onde essa memória de cálculo se aplica, onde não e onde deve sercalculado pela CONTRATADA, baseado no Hardware a ser fornecido.

Tabela A - Serviços de hospedagem

Item	**Descrição**	**Qtd**	**Unidade deMedida**

1	Hosting com Serviço de Virtualização com sistema de gerenciamento gráfico via web, com as devidas licenças Calculadas pela CONTRATADA, de acordo com o hardware fornecido para atender o ambiente vCloud, item8 desta tabela.	1	Licenciamento
2	Licenciamento do SO Windows Server Data Center, fornecido por Core, sem a necessidade de cobrança dos hosts virtuais instalados no ambiente virtual. Calculado de acordo com os servidores utilizados para oserviço de Hosting.	1	Licenciamento
3	Licenciamento Banco de Dados IBM DB2;	1	Licenciamento
4	Licenciamento Banco de Dados MS SQL ServerEnterprise;	4	licença para 02Cores
5	Licenciamento Banco de Dados MS SQL ServerStandard;	8	licença para 02Cores
6	Certificado Wildcard	1	Certificado Digital para 3 anos
7	Hosting para sistema Operacional IBM AIX;	1	Servidor Físico
8	Ambiente de VCloud composto pelos servidores físicos, de acordo com os Requisitos de Sistema de Virtualização	1	Ambiente
9	Serviços de segurança; (Firewall, IPS/IDS, WAF, Gerenciamento de vulnerabilidades e ameaças, Cofre deSenhas para 10 usuários), conforme descrito no itens REQUISITOS GERAIS DE SEGURANÇA	1	Serviço
10	SIEM (Sistema de informações e eventos de segurança).conforme descrito no item requisitos de gerenciamento de eventos de segurança da informação (SIEM)	150 GB/dia	Serviço
11	Load Balancer, conforme descrito no item Requisitos de Balanceamento de Carga Local	1	Serviço
12	Serviço de Backup e Restauração	1	Serviço
13	Rede de Comunicação TCP/IP, conforme descrito no item requisitos de comunicação	1	Rede

Tabela B - Serviços de Interligação

Item	**Descrição**	**Largura de banda**	**Qtde**
1	Link de Fibra óptica Redundante (Sistema Ativo/Ativo com balanceamento de Carga)	10 Gbps, dedicado, full duplex	1
2	Banda IP (fornecida através de um link redundante com capacidade de 200Mbps);	200 Mbps, dedicado, full duplex	1
3	Total - Valor a Ser transportado para a Tabela Sumarizadora, do objeto da Contratação		

Tabela C - Serviços de Gestão

Item	**Descrição**	**Qtde**	Unidade
1	Serviço de Gestão da Solução	1	Serviço
2	Serviço de Relatórios de Gestão	1	Serviço

Tabela D - Serviços de Administração

Item	**Descrição**	**Qtde**	**Unidade**
1	Serviços de OPERAÇÃO, compostos pela administração das Maquinas, virtuais, Bancos de Dados, Redes, Segurança, etc.	1	Serviço
2	Serviços de Manutenção e Monitoramento	1	Serviço
3	Serviço de Suporte e Gestão de incidentes	1	Serviço

Tabela E - Serviços de Planejamento e Instalação

Item	Descrição	**Qtde**	**Unidade**
1	Serviços de Planejamento	1	Serviço

2	Serviço de Instalação	1	Serviço
3	Serviço de Migração / Replicação	1	Serviço

TABELA F - Serviço de Armazenamento

Item	Descrição	Qtde Inicial Mínima (TB)	Qtde Máxima(TB)	Unidade
1	Área em storage Comum (Servidores Windows eLinux);	170	340	TeraBytes
2	Área de Storage DB2, conectada ao Servidor AIX	50	110	TeraBytes

12 - PLANILHA PARA COTAÇÃO DE PREÇO

Tabela SUMARIZADORA de Precificação

item	Descrição	Qtde (meses)	Valor Mensal (R$)	Valor Total (R$)
1	Serviço de Hospedagem em Datacenter; Composto dos Preços da Tabela AT - Serviços de hospedagem.	36		
2	Serviço de interligação conforme Tabela BT - Serviços de Interligação. (Serviço com pagamento mensal, por 36 meses)	36		
3	Serviços de Gestão conforme descrito Tabela CT - Serviços de Gestão. (Serviço com pagamento mensal, por 36 meses)	36		
4	Serviços de Administração e Operação conforme Tabela DT - Serviços de Administração. (Serviço com pagamento mensal, por36 meses)	36		
5	Serviço de Planejamento e instalação conforme Tabela ET - Serviços de Planejamento e Instalação. (Serviço com pagamento único mediante entrega) (neste caso o valor mensal é o valor unitário e deve ser o mesmo do valor total)	1	N.A.	
6	Serviço de Área de Armazenamento (Storage) conforme tabela FT -Serviço de Armazenamento	36		
	TOTAL GERAL			

Tabela AT - Serviços de hospedagem:

Item	Descrição	Qtd	Unidade de Medida	Valor Unitário Mensal	Valor Total 36 meses
1	Hosting com Serviço de Virtualização com sistema de gerenciamento gráfico via web, com as devidas licenças Calculadas pela CONTRATADA, de acordo com o hardware fornecido para atender o ambiente vCloud, item 8 desta tabela.	1	Licenciamento		

2	Licenciamento do SO Windows Server Data Center, fornecido por Core, sem a necessidade de cobrança dos hosts virtuais instalados no ambiente virtual. Calculado de acordo com os servidores utilizados para oserviço de Hosting.	1	Licenciamento		
3	Licenciamento Banco de Dados IBM DB2;	1	Licenciamento		
4	Licenciamento Banco de Dados MS SQL Server Enterprise;	4	licença para 02 Cores		
5	Licenciamento Banco de Dados MS SQL Server Standard;	8	licença para 02 Cores		
6	Certificado Wildcard	1	Certificado Digitalpara 3 anos		
7	Hosting para sistema Operacional IBM AIX;	1	Servidor Físico		
8	Ambiente de VCloud composto pelos servidores físicos,de acordo com os Requisitos de Sistema de Virtualização	1	Ambiente		

9	Serviços de segurança; (Firewall, IPS/IDS, WAF, Gerenciamento de vulnerabilidades e ameaças, Cofre deSenhas para 10 usuários), conforme descrito no itens REQUISITOS GERAIS DE SEGURANÇA	1	Serviço		
10	SIEM (Sistema de informações e eventos de segurança). conforme descrito no item REQUISITOS DE GERENCIAMENTO DE DE EVENTOS DE SEGURANÇA DA INFORMAÇÃO (SIEM)	150 GB/dia	Serviço		
11	Load Balancer, conforme descrito no item Requisitos deBalanceamento de Carga Local	1	Serviço		
12	Serviço de Backup e Restauração	1	Serviço		
13	Rede de Comunicação TCP/IP, conforme descrito no itemrequisitos de comunicação	1	Rede		
14	TOTAL A ser transportado para o item 1 da tabela SUMARIZADORA de Precificação				

Tabela BT - Serviços de Interligação

Item	Descrição	Largura de banda	Qtde	Valor Mensal	Valor Total
1	Link de Fibra óptica Redundante (Sistema Ativo/Ativo com balanceamento de Carga)	10 Gbps, dedicado, full duplex	1		
2	Banda IP (fornecida através de um link redundante com capacidade de 200Mbps);	200 Mbps, dedicado, full duplex	1		
3	TOTAL A ser transportado para o item 2 da tabela SUMARIZADORA de Precificação				

Tabela CT - Serviços de Gestão

Item	Descrição	Qtde	Unidade	Valor Mensal	Valor Total
1	Serviço de Gestão da Solução	1	Serviço		
2	Serviço de Relatórios de Gestão	1	Serviço		

	TOTAL A ser transportado para o item 3 da tabela SUMARIZADORA de Precificação		

Tabela DT - Serviços de Administração

Item	Descrição	Qtde	Unidade	Valor Mensal	Valor Total
1	Serviços de OPERAÇÃO, compostos pela administração das Maquinas, virtuais, Bancos de Dados, Redes, Segurança, etc.	1	Serviço		
2	Serviços de Manutenção e Monitoramento	1	Serviço		
3	Serviço de Suporte e Gestão de incidentes	1	Serviço		
4	TOTAL a Ser trasnportado para o item 4 da tabela SUMARIZADORA de Precificação				

Tabela ET - Serviços de Planejamento e Instalação

Item	Descrição	Qtde	Unidade	Valot Total
1	Serviços de Planejamento	1	Serviço	
2	Serviço de Instalação	1	Serviço	
3	Serviço de Migração / Replicação	1	Serviço	
4	TOTAL a Ser trasnportado para o item 5 da tabela SUMARIZADORA de Precificação			

Tabela FT - Serviço de Armazenamento

Item	Descrição	Qtde Inicial Mínima (múltiplos de 10 TB)	Qtde Máxima Projetada (múltiplos de10 TB)	Unidade	Valou unitário (10 TB) Mensa	Valor Total 36 meses
1	Área em storage Comum (Servidores Windows e Linux);	17 (Totalizando 170 TB)	34 (totalizando 340 TB)	TeraBytes		
2	Área de Storage DB2, conectada ao Servidor AIX	5 (Totalizando 50 TB)	11 (Totalizando 110 TB)	TeraBytes		
3	TOTAL a Ser transportado para o item 6 da tabela SUMARIZADORA de Precificação					

Obs. Note-se que a unidade mínima utilizada é 10 TB

13 - FONTE DE RECURSOS ORÇAMENTÁRIOS

13.1 DOTAÇÃO ORÇAMENTÁRIA

Os recursos orçamentários para a presente contratação são oriundos:

- **Conta Contábil:** 6.2.2.1.1.01.04.09.005
- **Centro de Custo:** 01.03.17.09.01.01

14 - LOCAIS DE ENTREGA

14.1 **1** Endereço: Av. Brigadeiro Faria Lima, 1059 - Pinheiros - São Paulo - SP

2 Telefone para informações: (11) 3095 - 6484

15 - CRITÉRIOS DE SELEÇÃO DO FORNECEDOR			
REGIME DE EXECUÇÃO	( ) Empreitada	(X) Preço Global	( ) Preço Unitário
ADJUDICAÇÃO DO OBJETO	(X) Global	( ) Por Lote	( ) Por Item

15.1 - Qualificação Técnica

15.1.1 JUSTIFICATIVA QUALIFICAÇÃO TÉCNICA

1 Em face da criticidade dos equipamentos que suportam toda a infraestrutura de redes corporativa do CREA-SP, atenderem a todas as áreas de negócio da empresa e necessitarem de atendimento técnico especializado, com a possibilidade de troca de equipamentos, faz-se necessário que a empresa CONTRATADA demonstre a comprovação deaptidão aos serviços contratados através de atestado(s) de serviços similares de complexidade tecnológica.

15.1.2 **1** É necessária comprovação de aptidão para a para o fornecimento de licenças, produtos, manutenção, atualização esuporte dos mesmos. Serviços de implantação e migração com a devida transferência de conhecimento em características, quantidades e prazos compatíveis com o objeto desta licitação, por meio de apresentação de Atestado fornecido por pessoas jurídicas de direito público ou privado.

2 O(s) atestado(s) deverão ser apresentados em papel timbrado do emitente, conter identificação do signatário, nome, endereço, telefone e se for o caso, correio eletrônico para contato, a fim de possibilitar possíveis diligências.

15.1.3 A Licitante Vencedora deverá apresentar obrigatoriamente, **na assinatura do Contrato** comprovação de que o datacenter fornecido possui a certificação mínima **Tier III**.

15.1.4 A Licitante Vencedora deverá apresentar obrigatoriamente, na assinatura do Contrato comprovação de que o datacenter fornecido possui as certificações de Segurança Mínimas, ISO **27017 e 27018**.

15.2 - Critérios de Seleção

15.2.1 - Critérios Gerais

15.2.1.1 REGIME DE EXECUÇÃO

1. O regime da execução dos contratos é de EMPREITADA POR PREÇO GLOBAL.

15.2.2 - Subcontratação

É vedada a subcontratação completa ou da parcela principal da obrigação;

A subcontratação depende de autorização prévia da Contratante, a quem incumbe avaliar se a subcontratada cumpre osrequisitos de qualificação técnica necessários para a execução do objeto.

Em qualquer hipótese de subcontratação, permanece a responsabilidade integral da Contratada pela perfeita execução contratual, cabendo-lhe realizar a supervisão e coordenação das atividades da subcontratada, bem como responder perante aContratante pelo rigoroso cumprimento das obrigações contratuais correspondentes ao objeto da subcontratação.

Será permitida subcontratação para o seguintes itens:

- Montagem (instalação física) do serviço de monitoramento nas dependências da CONTRATANTE.

15.2.3 - Formação de Consórcios

15.2.3.1 Não Será permitida formação de Consórcio.

15.2.4 - Alteração Subjetiva

15.2.4.1 É admissível a fusão, cisão ou incorporação da CONTRATADA com/por outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas asdemais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato.

15.2.5 - Garantia Contratual

15.2.5.1. Não será exigida a prestação de garantia de execução para celebrar a contratação decorrente deste certame licitatório

16 - PROCEDIMENTOS PARA APLICAÇÃO DAS SANÇÕES

16.1 - Sanções Aplicáveis

Item	**Evento**	**Ocorrência**	**Sanção/Multa**
1	Não atender ao nível mínimo de assertividade de serviço NMS (Nível Mínimo de Serviço)	1	Glosa de 10% sobre o valor do serviço mensal para valores de assertividade entre 80% e 89%
2	Não atender a qualquer nível mínimo de assertividade de NMS (NívelMínimo de Serviço)	2	o dobro da glosa da ocorrência 1

3	Não atender ao nível mínimo de assertividade de serviço NMS (Nível Mínimo de Serviço)	1	Glosa de 20% sobre o valor do serviço mensal para valores de assertividade abaixo de79%
4	Não atender ao nível mínimo de assertividade de serviço NMS (Nível Mínimo de Serviço)	1	Glosa de 5% sobre o valor do serviço mensal para valores de assertividade entre 90% e 95% (90% e 99% no caso de atividades programadas).
5	Não Atender ao NMS (Nível Mínimo de Serviço) de Gestão entregando os relatórios depois do prazo de 5 dias úteis do início do mês	1	Advertência
6	Não Atender ao NMS (Nível Mínimo de Serviço) de Gestão entregando os relatórios depois do prazo de 5 dias úteis do início do mês	2	Glosa de 10% sobre o valor do serviço de gestão mensal
7	Não Atender ao NMS (Nível Mínimo de Serviço) de Gestão entregando os relatórios depois do prazo de 5 dias úteis do início do mês	3	Glosa de 20% sobre o valor do Serviço Mensal
8	Não Atender ao NMS (Nível Mínimo de Serviço) de Gestão entregando os relatórios depois do prazo de 5 dias úteis do início do mês	4	Glosa de 30% do valor do serviço Mensal, podendo ensejar o início das tratativas de encerramento do contrato
9	Não atender a qualquer nível mínimo de assertividade de NMS (NívelMínimo de Serviço)	3	A mesma Glosa da segunda ocorrência, podendo ensejar o início das tratativas de encerramento de contrato
16.2 - Sanções Administrativas			

16.2.1 1. Comete infração administrativa nos termos da Lei nº 10.520, de 2002, a CONTRATADA que:

a) Falhar na execução do contrato, pela inexecução, total ou parcial, de quaisquer das obrigações assumidas nacontratação;

b) Ensejar o retardamento da execução do objeto;

c) Fraudar na execução do contrato;

d) Comportar-se de modo inidôneo; ou

e) Cometer fraude fiscal.

2. Pela inexecução total ou parcial do objeto deste contrato, a Administração pode aplicar à CONTRATADA as seguintessanções:

i) **Advertência por escrito**, quando do não cumprimento de quaisquer das obrigações contratuais consideradas faltas leves, assim entendidas aquelas que não acarretam prejuízos significativos para o serviço contratado;

ii) **Multa de**:

(1) 0,1% (um décimo por cento) até 0,2% (dois décimos por cento) por dia sobre o valor adjudicado em caso de atraso na execução dos serviços, limitada a incidência a 15 (quinze) dias. Após o décimo quinto dia e a critério daAdministração, no caso de execução com atraso, poderá ocorrer a não-aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença;

(2) 0,1% (um décimo por cento) até 10% (dez por cento) sobre o valor adjudicado, em caso de atraso na execução do objeto, por período superior ao previsto no subitem acima, ou de inexecução parcial da obrigação assumida; (3)0,1% (um décimo por cento) até 15% (quinze por cento) sobre o valor adjudicado, em caso de inexecução totalda obrigação assumida;

(4) 0,2% a 3,2% por dia sobre o valor mensal do contrato, conforme detalhamento constante das **tabelas 1 e 2**,abaixo; e

(5) As penalidades de multa decorrentes de fatos diversos serão consideradas independentes entre si.

iii) Suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual aAdministração Pública opera e atua concretamente, pelo prazo de até dois anos;

iv) Sanção de impedimento de licitar e contratar com órgãos e entidades da União, com o consequentedescredenciamento no SICAF pelo prazo de até cinco anos.

3.A Sanção de impedimento de licitar e contratar prevista no subitem “iv” também é aplicável em quaisquer das hipótesesprevistas como infração administrativa neste Termo de Referência.

4. As sanções previstas nos subitens “i”, “iii” e “iv” poderão ser aplicadas à CONTRATADA

juntamente com as de multa,descontando-a dos pagamentos a serem efetuados.

5. Para efeito de aplicação de multas, às infrações são atribuídos graus, de acordo com as tabelas 1 e 2:

Tabela 1

GRAU	CORRESPONDÊNCIA
1	0,2% ao dia sobre o valor mensal do contrato
2	0,4% ao dia sobre o valor mensal do contrato
3	0,8% ao dia sobre o valor mensal do contrato
4	1,6% ao dia sobre o valor mensal do contrato
5	3,2% ao dia sobre o valor mensal do contrato

Tabela 2

INFRAÇÃO		
ITEM	**DESCRIÇÃO**	**GRAU**
1	Permitir situação que crie a possibilidade de causar dano físico, lesão corporalou consequências letais, por ocorrência;	05
2	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, osserviços contratuais por dia e por unidade de atendimento;	04
3	Manter funcionário sem qualificação para executar os serviços contratados, porempregado e por dia;	03
4	Recusar-se a executar serviço determinado pela fiscalização, por serviço e pordia;	02
5	Retirar funcionários ou encarregados do serviço durante o expediente, sem aanuência prévia do CONTRATANTE, por empregado e por dia;	03
Para os itens a seguir, deixar de:		
6	Registrar e controlar, diariamente, a assiduidade e a pontualidade de seupessoal, por funcionário e por dia;	01
7	Cumprir determinação formal ou instrução complementar do órgão	02

	fiscalizador,por ocorrência;	
8	Substituir empregado que se conduza de modo inconveniente ou não atenda àsnecessidades do serviço, por funcionário e por dia;	01
9	Cumprir quaisquer dos itens do Edital e seus Anexos não previstos nesta tabelade multas, após reincidência formalmente notificada pelo órgão fiscalizador, por item e por ocorrência;	03
10	Indicar e manter durante a execução do contrato os prepostos previstos noedital/contrato;	01
11	Providenciar treinamento para seus funcionários conforme previsto na relaçãode obrigações da CONTRATADA	01

6. Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, as empresas ou profissionais que: 6.1. Tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquertributos;

6.2. Tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

6.3. Demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

7.A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à CONTRATADA, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente a Lei nº 9.784, de 1999.

8. As multas devidas e/ou prejuízos causados à Contratante serão deduzidos dos valores a serem pagos, ou recolhidos emfavor da União, ou deduzidos da garantia, ou ainda, quando for o caso, serão inscritos na Dívida Ativa da União e cobrados judicialmente.

8.1. Caso a Contratante determine, a multa deverá ser recolhida no prazo máximo de 10 (dez) dias, a contar da datado recebimento da comunicação enviada pela autoridade competente.

9. Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do licitante, a União ou Entidadepoderá cobrar o valor remanescente judicialmente, conforme artigo 419 do Código Civil.

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

11.Se, durante o processo de aplicação de penalidade, houver indícios de prática de infração administrativa tipificada pela Leinº 12.846, de 1º de agosto de 2013, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da

responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização - PAR.

12.A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Públicanacional ou estrangeira nos termos da Lei nº 12.846, de 1º de agosto de 2013, seguirão seu rito normal na unidade administrativa.

13.O processamento do PAR não interfere no seguimento regular dos processos administrativos específicos para apuração daocorrência de danos e prejuízos à Administração Pública Federal resultantes de ato lesivo cometido por pessoa jurídica, com ou sem a participação de agente público.

14.As penalidades serão obrigatoriamente registradas no SICAF.

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

ANEXO II
MODELO PROPOSTA DE PREÇOS

Ao CREA-SP
Pregão Eletrônico nº 007/2022 Processo Administrativo nº V-0050/2020

A empresa _____, sediada à Av. / Rua _____, Cidade, Bairro e CEP, inscrita no CNPJ/MF sob o nº _____, Inscrição Municipal _____ Inscrição Estadual _____, vem através desta apresentar proposta de preço, conforme solicitado. CONTATO: nome _____ Telefone: ( ) _____ e-mail ____.

TABELA SUMARIZADORA DE PRECIFICAÇÃO

ITEM	Bem/Serviço	Qtd.	Unidade	Valor Unitário	Valor Total
1	Serviço de Hospedagem em Datacenter. Composto dos Preços da **Tabela AT - Serviços de hospedagem**.	36	Serviço	R$	R$
2	Serviço de interligação conforme **Tabela BT - Serviços de Interligação**. (Serviço com pagamento mensal, por 36 meses)	36	Serviço	R$	R$
3	Serviços de Gestão conforme descrito **Tabela CT - Serviços de Gestão**. (Serviço com pagamento mensal, por 36 meses)	36	Serviço	R$	R$
4	Serviços de Administração e Operação conforme **Tabela DT - Serviços de Administração**. (Serviço com pagamento mensal, por 36 meses)	36	Serviço	R$	R$
5	Serviço de Planejamento e instalação conforme **Tabela ET - Serviços de Planejamento e Instalação**. (Serviço com pagamento único mediante entrega)	1	Serviço	R$	R$
6	Serviço de Área de Armazenamento (Storage), conforme **Tabela FT - Serviço de Armazenamento**.	36	Meses	R$	R$
Valor Total_____					R$

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

Tabela AT - Serviços de hospedagem:

Item	Descrição	Qtd	Unidade de Medida	Valor Unitário	Valor Total
1	Hosting com Serviço de Virtualização com sistema de gerenciamento gráfico via web, com as devidas licenças Calculadas pela CONTRATADA, de acordo com o hardware fornecido para atender o ambiente vCloud, item 8 desta tabela.	1	Licenciamento		
2	Licenciamento do SO Windows Server Data Center, fornecido por Core, sem a necessidade de cobrança dos hosts virtuais instalados no ambiente virtual. Calculado de acordo com os servidores utilizados para o serviço de Hosting.	1	Licenciamento		
3	Licenciamento Banco de Dados IBM DB2;	1	Licenciamento		
4	Licenciamento Banco de Dados MS SQL Server Enterprise;	4	licença para 02 Cores		
5	Licenciamento Banco de Dados MS SQL Server Standard;	8	licença para 02 Cores		
6	Certificado Wildcard	1	Certificado Digital para 3 anos		
7	Hosting para sistema Operacional IBM AIX;	1	Servidor Físico		
8	Ambiente de VCloud composto pelos servidores físicos, de acordo com os Requisitos de Sistema de Virtualização	1	Ambiente		
9	Serviços de segurança; (Firewall, IPS/IDS, WAF, Gerenciamento de vulnerabilidades e ameaças, Cofre de Senhas para 10 usuários), conforme descrito no itens REQUISITOS GERAIS DE SEGURANÇA	1	Serviço		
10	SIEM (Sistema de informações e eventos de segurança). conforme descrito no item REQUISITOS DE GERENCIAMENTO DE DE EVENTOS DE SEGURANÇA DA INFORMAÇÃO (SIEM)	150 GB/dia	Serviço		
11	Load Balancer, conforme descrito no item Requisitos de Balanceamento de Carga Local	1	Serviço		
12	Serviço de Backup e Restauração	1	Serviço		
13	Rede de Comunicação TCP/IP, conforme descrito no item requisitos de comunicação	1	Rede		
14	**Total - A ser transportado para o item 1 da tabela SUMARIZADORA DE PRECIFICAÇÃO**				

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

Tabela BT - Serviços de Interligação

Item	Descrição	Largura de banda	Qtde	Valor Mensal	Valor Total
1	Link de Fibra Óptica Redundante (Sistema Ativo/Ativo com balanceamento de Carga)	10 Gbps, dedicado, full duplex	36		
2	Banda IP (fornecida através de um link redundante com capacidade de 200Mbps);	200 Mbps, dedicado, full duplex	36		
3	**Total - Valor a Ser transportado para o item 2 da Tabela SUMARIZADORA**				

Tabela CT - Serviços de Gestão

Item	Descrição	Qtde	Unidade	Valor Unitário Mensal	Valor Total
1	Serviço de Gestão da Solução	36	Serviço		
2	Serviço de Relatórios de Gestão	36	Serviço		
3	**Valor Total a ser transportado para o item 3 da tabela SUMARIZADORA**				

Tabela DT - Serviços de Administração

Item	Descrição	Qtde	Unidade	Valor Unitário Mensal	Valor Total
1	Serviços de OPERAÇÃO, compostos pela administração das Maquinas, virtuais, Bancos de Dados, Redes, Segurança, etc.	36	Serviço		
2	Serviços de Manutenção e Monitoramento	36	Serviço		
3	Serviço de Suporte e Gestão de incidentes	36	Serviço		
4	**Valor Total a ser transportado para o item 4 da tabela SUMARIZADORA**				

Tabela ET - Serviços de Planejamento e Instalação

Item	Descrição	Qtde	Unidade	Valor Unitário	Valor Total
1	Serviços de Planejamento	1	Serviço		
2	Serviço de Instalação	1	Serviço		
3	Serviço de Migração / Replicação	1	Serviço		
4	**Valor Total a ser transportado para o item 5 da Tabela SUMARIZADORA**				

Tabela FT - Serviço de Armazenamento

Item	Descrição	Qtde Inicial Mínima (múltiplos de 10 TB)	Qtde Máxima Projetada (múltiplos de 10 TB)	Unidade	Valou unitário (10 TB) Mensal	Valor Total Mensal para a quantidade máxima projetada	Valor total do Contrato 36 Meses
1	Área em storage Comum (Servidores Windows e Linux);	17 (Totalizando 170 TB)	34 (totalizando 340 TB)	TeraBytes			
2	Área de Storage DB2, conectada ao Servidor AIX	5 (Totalizando 50 TB)	11 (Totalizando 110 TB)	TeraBytes			
3	**Total a Ser transportado para o item 6 da tabela SUMARIZADORA**						

Obs. Note-se que a unidade mínima utilizada é 10 TB

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

Deverá constar na proposta comercial:

1) **Validade da Proposta:** não inferior a 60 (sessenta) dias a contar da data de abertura da licitação;

2) **Dados bancários para pagamento:** Banco; número da conta; agência;

3) **Para fins de assinatura contrato, informar:**

3.1) Razão Social;

3.2) CNPJ, Inscrição Estadual e Municipal;

3.3) Endereço completo da empresa, inclusive CEP;

3.4) Telefone e *e-mail* do responsável (preposto);

3.5) Nome, número do CPF, número do RG e cargo do Representante Legal da empresa com poderes para assinatura do contrato;

3.6) Nome, número do CPF, número do RG do responsável (preposto), que deverá ser mantido, aceito pelo CREA-SP, para representa-la na execução do contrato.

4 Custos contemplados na Proposta: nos preços apresentados acima já estão computados todos os custos necessários decorrentes da prestação dos serviços, bem como já incluídos todos os impostos, encargos trabalhistas, previdenciários, fiscais, comerciais, taxas, seguros, deslocamentos de pessoal e quaisquer outros que incidam direta ou indiretamente.

Deverá ser observado ainda, conforme disposto no item "4.4.4.2 – requisitos gerais dos equipamentos de rede", do Termo de Referência – Anexo I do Edital:

5 O fabricante e o modelo dos equipamentos ofertados bem como seus respectivos Part Numbers para tornar mais fácil e clara a identificação do produto ofertado;

5.1 Os equipamentos ofertados devem ser novo e em plena fabricação. Não serão aceitos equipamentos com avisos de "End of Life", ou seja, aviso de que o produto está fora de linha de fabricação emitida pelo fabricante;

5.2 Os equipamentos ofertados devem possuir garantia e suporte de 36 meses com direito a atualização de firmware, troca de peças no próximo dia útil em horário comercial e abertura de chamados no fabricante. Tal procedimento se justifica pelo fato de que, de forma geral a contratação, de serviços de manutenção para ativos fora de garantia, usualmente é mais onerosa para a Administração do que quando o bem é adquirido com garantia para toda sua vida útil;

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

5.3 Os equipamentos ofertados devem possuir homologação junto a ANATEL conforme a resolução nº 242, de 30 de novembro de 2000. A exigência de certificação de Produtos de Telecomunicação classificáveis nas Categorias I, II e III do art. 4o da Resolução Anatel 242/2000 é pré-requisito obrigatório para fins de comercialização e utilização no país, para atendimento ao disposto no parágrafo único do art. 20 da Resolução 242 da Anatel. Todas as certificações necessárias devem estar disponíveis publicamente no sítio eletrônico da agencia reguladora conforme endereço eletrônico http://sistemas.anatel.gov.br/sgch/.

(Local) ....., de 2022.

Nome e Assinatura do Representante Legal
Cargo/Função
Carimbo do CNPJ
(Apresentar em papel timbrado do licitante)

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

ANEXO III
MINUTA DO TERMO DE CONTRATO

Contrato nº /2022
Processo Administrativo nº V-0050/2020

TERMO DE CONTRATO DE EMPRESA ESPECIALIZADA EM SERVIÇOS DE HOSPEDAGEM DE SISTEMAS DE SOFTWARE E ARQUIVOS, COM SEUS RESPECTIVOS SISTEMAS OPERACIONAIS, APLICAÇÕES E BANCOS DE DADOS, COMPOSTO POR SEUS EQUIPAMENTOS (HARDWARE), SOFTWARES, LICENCIAMENTO, PLANEJAMENTO, INSTALAÇÃO, MIGRAÇÃO DE DADOS E APLICAÇÕES, MANUTENÇÃO, COMUNICAÇÃO DE DADOS, SUPORTE, OPERAÇÃO, TREINAMENTO E GERENCIAMENTO DA SOLUÇÃO DE HOSPEDAGEM.

O **CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DO ESTADO DE SÃO PAULO – CREA-SP**, instituído pelo Decreto Federal nº 23.569, de 11 de dezembro de 1933 e mantido pela Lei Federal nº 5.194, de 24 de dezembro de 1966, com sede e foro na Avenida Brigadeiro Faria Lima nº 1.059, nesta Capital, inscrito no CNPJ sob nº 60.985.017/0001-77, neste ato representado por seu Presidente, o Engenheiro **VINICIUS MARCHESE MARINELLI**, brasileiro, portador da cédula de identidade RG nº 34.123.915-X – SSP/SP e inscrito no CPF/MF nº 304.423.178-75, registrado no **CREA-SP** sob nº **5062051089**, doravante denominado simplesmente **CONTRATANTE**, e de outro lado a Empresa _____, com sede na _____, ____ – _____ – _____/____ - CEP: _____, inscrita no CNPJ sob o nº _____, Inscrição Estadual _____, CCM nº _____, neste ato representado por seu _____, _____, portador da Cédula de Identidade RG. nº _____ e CPF sob nº _____, doravante denominada simplesmente **CONTRATADA**, resolvem de comum acordo firmar o presente Contrato, conforme Edital de Pregão Eletrônico nº 007/2022 e respeitável despacho de fls. ____, nos termos da Lei nº 10.520, de 17/07/2002, do Decreto nº 3.555 de 8/08/2000, Decreto n° 10.024, de 20/09/2019, e, subsidiariamente, a Lei nº 8.666, de 21/06/1993, e suas atualizações, contidos nos autos do Processo Administrativo nº V-0050/2020, e regido pelas seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA – DO OBJETO

1.1. O presente instrumento tem como objeto a contratação de empresa especializada em serviços de hospedagem de sistemas de software e arquivos, com seus respectivos sistemas operacionais, aplicações e bancos de dados, composto por seus equipamentos (hardware), softwares, licenciamento, planejamento, instalação, migração de dados e aplicações, manutenção, comunicação de dados, suporte, operação, treinamento e gerenciamento da solução de Hospedagem.

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

1.2. Este Termo de Contrato vincula-se ao Edital do Pregão, identificado no preâmbulo e à proposta vencedora, independentemente de transcrição.

CLÁUSULA SEGUNDA – DO PREÇO

2.1. O valor deste Termo de Contrato é de R$ _____ (_____)**.**

2.1.1. Descrição, quantitativos e preços conforme proposta comercial anexa.

2.1.2. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

CLÁUSULA TERCEIRA – DA VIGÊNCIA

3.1. Será firmado contrato com cláusula de vigência de 36 (trinta e seis) meses, a contar da data de assinatura do Contrato, podendo ser prorrogado até o limite de 60 (sessenta) meses, na forma da Lei nº 8.666/93, e suas atualizações.

3.2. O contrato poderá ser rescindido nos termos e hipóteses dos artigos 77 a 80 da Lei nº 8.666/93 e suas atualizações.

CLÁUSULA QUARTA – DA DOTAÇÃO ORÇAMENTÁRIA

4.1. A despesa para atender a esta licitação está programada em dotação orçamentária própria da Equipe de Infraestrutura e Segurança da Informação - EISI da Gerência de Desenvolvimento e Execução de Projetos - GDEP da Superintendência de Tecnologia e Inovação - SUPTEC, prevista no orçamento do CREA-SP no exercício de financeiro de 2022, oriundo das contas nº 6.2.2.1.1.01.04.09.005 – Serviços de Informática – PJ.

4.2. A despesa com a execução dos serviços de que trata o objeto desta licitação é estimada no período de 36 (trinta e seis) meses.

CLÁUSULA QUINTA – FORMA DO PAGAMENTO EM FUNÇÃO DOS RESULTADOS

5.1. As regras acerca do pagamento são as estabelecidas no item “7.4 – forma de pagamento em função dos resultados do item 7.4.1 até o item 7.4.3 – cronograma físico financeiro”, do Termo de Referência – Anexo I do Edital.

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

CLÁUSULA SEXTA – DA DESCRIÇÃO DA SOLUÇÃO E DA ESTIMATIVA DAS QUANTIDADES

6.1. A descrição geral da solução e a estimativa das quantidades estão previstas nos itens "3 – descrição da solução" e "11 – estimativa das quantidades" do Termo de Referência – Anexo I do Edital.

CLÁUSULA SÉTIMA – ESPECIFICAÇÃO TÉCNICA

7.1. A descrição da especificação técnica está prevista no item "4 – especificação técnica" do Termo de Referência – Anexo I do Edital.

CLÁUSULA OITAVA – DO MODELO DE EXECUÇÃO DO CONTRATO

8.1. A descrição das rotinas de execução do contrato está prevista no item "7.1.1 – da reunião inicial do contrato" até o item "7.3 – mecanismos formais de comunicação entre a contratada e a administração" do Termo de Referência – Anexo I do Edital.

CLÁUSULA NONA – DO PROCEDIMENTO DE FISCALIZAÇÃO DA EXECUÇÃO CONTRATUAL

9.1. Os procedimentos de fiscalização da execução contratual são os estabelecidos no item "9 – procedimentos de fiscalização da execução contratual" do Termo de Referência – Anexo I do Edital.

CLÁUSULA DÉCIMA – DO LOCAL DE ENTREGA

10.1. A definição do local de entrega encontra-se descrito no item "14 – locais de entrega" do Termo de Referência – Anexo I do Edital.

CLÁUSULA DÉCIMA PRIMEIRA – DA FORMA DE REAJUSTAMENTO DO VALOR CONTRATUAL

11.1. A prorrogação contratual somente será concretizada quando:

11.1.1. Ficar caracterizado, mediante pesquisa a ser realizada pelo Contratante, que os preços a serem praticados na prorrogação contratual serão condizentes aos praticados no mercado, e

11.1.1. Houver comunicação formal do Contratante à Contratada, com no mínimo 30 (trinta) dias anteriores ao do vencimento do Contrato.

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

11.2. Dentro do prazo de vigência do contrato e mediante solicitação da contratada, os preços contratados poderão sofrer reajuste após o interregno de um ano, aplicando-se o índice ICTI (Índice de Custo da Tecnologia da Informação), previsto no art. 24 da Instrução Normativa nº 1, de 4 de abril de 2019, do Ministério da Economia/Secretaria Especial de Desburocratização, Gestão e Governo Digital/Secretaria do Governo Digital.

11.3. A data base de pedido de reajuste será da apresentação da proposta comercial, ou seja, da sessão de abertura do presente certame.

11.4. O reajuste incidirá apenas sobre os serviços não executados, não incidirá sobre os serviços em atrasos.

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

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

CLÁUSULA DÉCIMA SEGUNDA – DA GARANTIA CONTRATUAL

12.1. Não será exigida a prestação de garantia de execução para celebrar a contratação decorrente do certame licitatório.

CLÁUSULA DÉCIMA TERCEIRA – DOS DEVERES E RESPONSABILIDADES DA CONTRATANTE

13.1. Os deveres e responsabilidades da Contratante são os estabelecidos no item “5 – deveres e responsabilidades da contratante” do Termo de Referência – Anexo I do Edital.

CLÁUSULA DÉCIMA QUARTA – DOS DEVERES E RESPONSABILIDADES DA CONTRATADA

14.1. Os deveres e responsabilidades da Contratada são os estabelecidos no item “6 – deveres e responsabilidades da contratada” do Termo de Referência – Anexo I do Edital.

CLÁUSULA DÉCIMA QUINTA – DAS SANÇÕES ADMINISTRATIVAS

15.1. DAS SANÇÕES APLICÁVEIS

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

Item	Evento	Ocorrência	Sanção/Multa
1	Não atender ao nível mínimo de assertividade de serviço NMS (Nível Mínimo de Serviço)	1	Glosa de 10% sobre o valor do serviço mensal para valores de assertividade entre 80% e 89%
2	Não atender a qualquer nível mínimo de assertividade de NMS (NívelMínimo de Serviço)	2	o dobro da glosa da ocorrência 1
3	Não atender ao nível mínimo de assertividade de serviço NMS (Nível Mínimo de Serviço)	1	Glosa de 20% sobre o valor do serviço mensal para valores de assertividade abaixo de 79%
4	Não atender ao nível mínimo de assertividade de serviço NMS (Nível Mínimo de Serviço)	1	Glosa de 5% sobre o valor do serviço mensal para valores de assertividade entre 90% e 95% (90% e 99% no caso de atividades programadas).
5	Não Atender ao NMS (Nível Mínimo de Serviço) de Gestão entregando os relatórios depois do prazo de 5 dias úteis do início do mês	1	Advertência
6	Não Atender ao NMS (Nível Mínimo de Serviço) de Gestão entregando os relatórios depois do prazo de 5 dias úteis do início do mês	2	Glosa de 10% sobre ovalor do serviço de gestão mensal
7	Não Atender ao NMS (Nível Mínimo de Serviço) de Gestão entregando os relatórios depois do prazo de 5 dias úteis do início do mês	3	Glosa de 20% sobre o valor do Serviço Mensal
8	Não Atender ao NMS (Nível Mínimo de Serviço) de Gestão entregando os relatórios depois do prazo de 5 dias úteis do início do mês	4	Glosa de 30% do valordo serviço Mensal, podendo ensejar o início das tratativas de encerramento do contrato
9	Não atender a qualquer nível mínimo de assertividade de NMS (NívelMínimo de Serviço)	3	A mesma Glosa da segunda ocorrência, podendo ensejar o início das tratativas de encerramento de contrato

15.2. Comete infração administrativa nos termos da Lei nº 10.520, de 2002, a Contratada que:

a) Não assinar o Termo de Contrato, quando convocado dentro do prazo de validade da proposta de preços;

b) Falhar na execução do contrato, pela inexecução, total ou parcial, de quaisquer das

obrigações assumidas na contratação;

c) Ensejar o retardamento da execução do objeto;

d) Falhar ou fraudar na execução do contrato;

e) Comportar-se de modo inidôneo; ou

f) Cometer fraude fiscal.

15.3. Pela inexecução total ou parcial do objeto deste contrato, a Administração pode aplicar à CONTRATADA as seguintes sanções:

i) **Advertência por escrito**, quando do não cumprimento de quaisquer das obrigações contratuais consideradas faltas leves, assim entendidas aquelas que não acarretam prejuízos significativos para o serviço contratado;

ii) **Multa de**:

1. 0,1% (um décimo por cento) até 0,2% (dois décimos por cento) por dia sobre o valor adjudicado em caso de atraso na execução dos serviços, limitada a incidência a 15 (quinze) dias. Após o décimo quinto dia e a critério da Administração, no caso de execução com atraso, poderá ocorrer a não aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença;

2. 0,1% (um décimo por cento) até 10% (dez por cento) sobre o valor adjudicado, em caso de atraso na execução do objeto, por período superior ao previsto no subitem acima, ou de inexecução parcial da obrigação assumida;

3. 0,1% (um décimo por cento) até 15% (quinze por cento) sobre o valor adjudicado, em caso de inexecução total da obrigação assumida;

4. 0,2% a 3,2% por dia sobre o valor mensal do contrato, conforme detalhamento constante das tabelas 1 e 2, abaixo.

5. As penalidades de multa decorrentes de fatos diversos serão consideradas independentes entre si.

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

iii) **Suspensão de licitar** e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos;

iv) **Sanção de Impedimento de licitar** e contratar com órgãos e entidades da União com o consequente descredenciamento no SICAF pelo prazo de até cinco anos;

15.4. A Sanção de impedimento de licitar e contratar prevista no subitem "iv" também é aplicável em quaisquer das hipóteses previstas como infração administrativa.

15.5. As sanções previstas nos subitens "i", "iii" e "iv" poderão ser aplicadas à CONTRATADA juntamente com as de multa, descontando-a dos pagamentos a serem efetuados.

15.6. Para efeito de aplicação de multas, às infrações são atribuídos graus, de acordo com as tabelas 1 e 2:

Tabela 1

GRAU	CORRESPONDÊNCIA
1	0,2% ao dia sobre o valor mensal do contrato
2	0,4% ao dia sobre o valor mensal do contrato
3	0,8% ao dia sobre o valor mensal do contrato
4	1,6% ao dia sobre o valor mensal do contrato
5	3,2% ao dia sobre o valor mensal do contrato

Tabela 2

INFRAÇÃO		
ITEM	**DESCRIÇÃO**	**GRAU**
1	Permitir situação que crie a possibilidade de causar dano físico, lesão corporal ou consequências letais, por ocorrência;	**05**
2	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços contratuais por dia e por unidade de atendimento;	**04**
3	Manter funcionário sem qualificação para executar os serviços contratados, por empregado e por dia;	**03**
4	Recusar-se a executar serviço determinado pela fiscalização, por serviço e por dia;	**02**

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

5	Retirar funcionários ou encarregados do serviço durante o expediente, sem a anuência prévia do CONTRATANTE, por empregado e por dia;	**03**
Para os itens a seguir, deixar de:		
6	Registrar e controlar, diariamente, a assiduidade e a pontualidade de seu pessoal, por funcionário e por dia;	**01**
7	Cumprir determinação formal ou instrução complementar do órgão fiscalizador, por ocorrência;	**02**
8	Substituir empregado que se conduza de modo inconveniente ou não atenda às necessidades do serviço, por funcionário e por dia;	**01**
9	Cumprir quaisquer dos itens do Edital e seus Anexos não previstos nesta tabela de multas, após reincidência formalmente notificada pelo órgão fiscalizador, por item e por ocorrência;	**03**
10	Indicar e manter durante a execução do contrato os prepostos previstos no edital/contrato;	**01**
11	Providenciar treinamento para seus funcionários conforme previsto na relação de obrigações da CONTRATADA	**01**

15.7. Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, as empresas ou profissionais que:

15.7.1. tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;

15.7.2. tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

15.7.3. demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

15.8. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à Contratada, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente a Lei nº 9.784, de 1999.

15.9. As multas devidas e/ou prejuízos causados à Contratante serão deduzidos dos valores a serem pagos, ou recolhidos em favor da União, ou deduzidos da garantia, ou ainda, quando for o caso, serão inscritos na Dívida Ativa da União e cobrados judicialmente.

15.9.1. Caso a Contratante determine, a multa deverá ser recolhida no prazo máximo de 10 (dez) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

15.10. Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do licitante, a União ou Entidade poderá cobrar o valor remanescente judicialmente, conforme artigo 419 do Código Civil.

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

15.12. Se, durante o processo de aplicação de penalidade, houver indícios de prática de infração administrativa tipificada pela Lei nº 12.846, de 1º de agosto de 2013, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização - PAR.

15.13. A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei nº 12.846, de 1º de agosto de 2013, seguirão seu rito normal na unidade administrativa.

15.14. O processamento do PAR não interfere no seguimento regular dos processos administrativos específicos para apuração da ocorrência de danos e prejuízos à Administração Pública Federal resultantes de ato lesivo cometido por pessoa jurídica, com ou sem a participação de agente público.

15.15. As penalidades serão obrigatoriamente registradas no SICAF.

CLÁUSULA DÉCIMA SEXTA – DA ALTERAÇÃO SUBJETIVA

16.1. É admissível a fusão, cisão ou incorporação da Contratada com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato.

CLÁUSULA DÉCIMA SÉTIMA – DA SUBCONTRATAÇÃO

17.1. Os parâmetros para a subcontratação encontram-se definidos no item “15.2.2 – subcontratação” do Termo de Referência, Anexo I do Edital.

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

CLÁUSULA DÉCIMA OITAVA - DA CONFIDENCIALIDADE E DO TRATAMENTO E PROTEÇÃO DOS DADOS

Considerando que, na execução de suas atividades o CREA-SP gera e mantém um enorme volume de informações, se tornando inviável o tratamento manual deste vasto acervo informacional e necessária a utilização de infraestrutura, processos e serviços de Tecnologia da Informação e Comunicação (TIC), de modo a restarem caracterizadas as hipóteses previstas nos incisos II e III, do artigo 7º, da Lei nº 13.709/2018;

Considerando que as atividades relacionadas aos serviços de hospedagem de sistemas de software e arquivos resultam no tratamento de dados pessoais de terceiros e o que estabelece a Lei nº 13.709/2018.

18.1. As **PARTES** declaram, concordam e garantem que toda e qualquer atividade de tratamento de dados deve atender às finalidades do Contrato e seus eventuais Aditivos e devem ser realizadas em conformidade com a legislação aplicável, sobretudo, mas não se limitando, à Lei nº 13.709/2018.

18.2. As **PARTES** declaram e concordam que, nos termos do que estabelece a Lei nº 13.709/2018, na presente contratação o **CONTRATANTE** atua na condição de **CONTROLADOR** e o **CONTRATADO**, realizará suas atividades na condição de **OPERADOR** e que, para todo e qualquer tratamento de dados pessoais vinculado a este Contrato, o **OPERADOR** deverá atuar de acordo com as orientações do **CONTROLADOR,** conforme ditames da Lei nº 13.709/2018 ou, quando for o caso, no cumprimento de obrigação legal ou regulatória, no exercício regular de direito, por determinação judicial ou por requisição da Autoridade Nacional de Proteção de Dados (ANPD).

18.2.1. O **OPERADOR** não pode retificar, apagar ou restringir o tratamento de dados pessoais que serão processados em nome do **CONTROLADOR** por sua própria iniciativa, mas somente mediante instruções devidamente documentadas pelo **CONTROLADOR**;

18.2.2. O **OPERADOR** não poderá criar cópias ou duplicar os dados sem que o **CONTROLADOR** tenha conhecimento e demonstre sua concordância, exceto, quando couber para a prestação de serviço, cópias de backup, as quais sejam necessárias para garantir o adequado tratamento dos dados pessoais, bem como, para os dados pessoais necessários, para atender aos requisitos de retenção de dados legalmente exigíveis.

18.3. A duração do tratamento de dados deverá respeitar o objeto contratual, bem como, o disposto na legislação aplicável.

18.4. As **PARTES** adotarão normas relacionadas à implementação de medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de eventos acidentais ou ilícitos de destruição, perda, alteração, comunicação ou difusão ou qualquer outra ocorrência decorrente de tratamento inadequado ou ilícito, implementação de programa de governança em privacidade, estruturação de planos de resposta a incidentes e remediação, sendo que as **PARTES** manterão procedimento para identificar, solucionar e eliminar incidentes envolvendo dados pessoais tratados sob a égide do Contrato e cooperarão uma com a outra na investigação de tais incidentes.

18.5. As **PARTES** reconhecem que os dados pessoais sensíveis estão sujeitos a um maior rigor legal e, portanto, exigem maior proteção técnica e organizacional. Assim, o **OPERADOR** somente poderá realizar operações de tratamento de dados pessoais sensíveis quando estritamente necessário para cumprir com as disposições do Contrato, devendo garantir a implementação de proteções técnicas apropriadas, aptas a manter a integridade, confidencialidade e segurança destas informações.

18.6. As **PARTES** cooperarão entre si no cumprimento das obrigações referentes ao exercício dos direitos dos Titulares previstos na LGPD e nas Leis e Regulamentos de Proteção de Dados em vigor e também no atendimento de requisições e determinações do Poder Judiciário, Ministério Público, Órgãos de controle administrativo.

18.7. Assegurar que todos os tipos de conexões sejam criptografados e que todas as atividades do serviço tenham a garantia de registro das transações realizadas (*log)*, apresentando um adequado controle baseado em função *(role based access control)* e com transparente identificação do perfil dos credenciados, tudo estabelecido como forma de garantir inclusive a rastreabilidade de cada transação e a franca apuração, a qualquer momento, de desvios e falhas, sendo vedado o compartilhamento desses dados com terceiros.

18.8. Encerrada a vigência do contrato ou não havendo mais necessidade de utilização dos dados pessoais, sensíveis ou não, o **OPERADOR** interromperá o tratamento e, em no máximo (30) dias, sob instruções e medidas determinadas pelo **CONTROLADOR**, eliminará completamente os dados pessoais e todas as cópias porventura existentes (em formato digital, físico ou outro qualquer), salvo quando necessite mantê-los para cumprimento de obrigação legal ou outra hipótese legal prevista na LGPD.

18.9. Em caso de o Titular de dados pessoais entrar em contato diretamente com o **OPERADOR** para exercer seus direitos com relação à retificação, eliminação, compartilhamento, confirmação,

acesso, cancelamento ou restrição do tratamento de dados pessoais, o **OPERADOR** deverá encaminhar a solicitação ao **CONTROLADOR** no prazo de 24 (vinte e quatro) horas através do e-mail dpo@creasp.org.br.

18.10. As Partes se comprometem a não tratar ou autorizar o Tratamento de Dados Pessoais fora do território brasileiro sem tomar as medidas garantidoras necessárias para que a transferência esteja em conformidade com a LGPD, o que deve incluir, sem limitações, a observância de regras vinculantes aprovadas pela Autoridade Nacional de Proteção de Dados (ANPD).

CLÁUSULA DÉCIMA NONA – DAS OBRIGAÇÕES DO CONTRATANTE COMO CONTROLADOR DE DADOS

19.1. Garantir que todo o tratamento dos dados pessoais, desde a coleta até o seu compartilhamento com o **OPERADOR** foi realizado de acordo com os princípios da finalidade deste Contrato, da adequação e da necessidade disposto no art 6º, I a III, da LGPD ou qualquer legislação aplicável e que as instruções para o tratamento de dados pessoais pelo **OPERADOR** estão de acordo com tais normas.

19.2. Através de registros formais, fornecer ao **OPERADOR** as instruções e informações relevantes e estabelecer os critérios para que o **OPERADOR** tenha acesso somente aos dados pessoais necessários para o cumprimento da finalidade do tratamento de dados constante deste Contrato.

19.3. Atender a requisições de exercício de direitos por parte dos Titulares ou solicitações da Autoridade Nacional de Proteção de Dados (ANPD) ou qualquer outra autoridade que venha a fiscalizar o tratamento de dados pessoais.

19.4. Garantir que os Titulares dos dados pessoais e a Autoridade Nacional de Proteção de Dados (ANPD) recebam as informações exigidas pela LGPD, principalmente no que tange a possível incidente de dados pessoais, nos termos da LGPD e do presente Contrato, a menos que o **CONTROLADOR** demonstre que o dano resultou de falha exclusiva do **OPERADOR**;

19.5. O **CONTROLADOR** deverá, sem demora e formalmente, informar ao **OPERADOR** sobre mudanças no tratamento de dados que possam vir a afetar os seus deveres. Além disso, o **CONTROLADOR** deverá informar ao **OPERADOR** de ações tomadas por terceiros, entre outras, da Autoridade Nacional de Proteção de Dados (ANPD), com relação ao tratamento de dados objeto do presente Contrato.

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

CLÁUSULA VIGÉSIMA – DAS OBRIGAÇÕES DO CONTRATADO COMO OPERADOR DE DADOS

20.1. Realizar o tratamento de dados pessoais, conforme indicado pelo **CONTROLADOR**, unicamente para operacionalização das relações contratuais previstas, tratando destes dados pessoais no limite do quanto necessário para o bom cumprimento das suas atividades.

20.2. Manter registro de todas as operações de tratamento de dados pessoais que realiza.

20.3. Seguir as instruções do **CONTROLADOR** no tratamento de dados pessoais, e, caso não o faça, assumir as devidas responsabilidades, nos termos da LGPD e qualquer outra lei ou regulamento que venha a tratar deste assunto, quanto as ações tomadas em desacordo com as instruções.

20.4. Prestar assistência ao **CONTROLADOR**, nos limites das obrigações impostas pela LGPD, ou qualquer outra lei que venha a tratar do assunto, caso a Autoridade Nacional de Proteção de Dados (ANPD) ou qualquer outra autoridade governamental, ou, ainda, o Titular de dados pessoais requeira informações quanto à conformidade do tratamento dos dados pessoais com a LGPD, na medida em que tais informações encontrem-se de posse do **OPERADOR** nas atividades de tratamento dos dados pessoais.

20.5. Implementar medidas de segurança, técnicas e administrativas necessárias para proteger os dados pessoais contra a destruição, acidental ou ilícita, a perda, a alteração, a comunicação ou difusão ou o acesso não autorizado, além de garantir documentalmente que o ambiente (seja ele físico ou virtual) utilizado para o tratamento de dados pessoais seja estruturado de forma a atender aos requisitos de segurança mínimos previstos pelo **CONTROLADOR**, aos padrões de boas práticas de governança, aos princípios gerais previstos na LGPD e nas demais leis ou regulamentos aplicáveis.

20.5.1. O **OPERADOR** deve dar conhecimento formal aos seus empregados das obrigações e condições acordadas nesta cláusula, inclusive no tocante à Política de Privacidade do **CONTROLADOR**.

20.6. Estabelecer diretrizes de Segurança da Informação interna de modo a sustentar os pilares de confidencialidade, disponibilidade e integridade dos dados do **CONTROLADOR**, pautadas nos requisitos do negócio, nos riscos envolvidos, na legislação e regulamentação vigente.

20.7. Apresentar ao **CONTROLADOR**, obrigatoriamente, uma Política de Gestão de Segurança da Informação interna, baseada na Norma ABNT NBR ISO/IEC 27002, com a devida descrição dos controles que foram estabelecidos e implementados, os quais devem ser periodicamente monitorados,

analisados e melhorados com o objetivo de identificar riscos, falhas, vulnerabilidades e descumprimentos das medidas de segurança da informação.

20.8. Apresentar ao **CONTROLADOR**, obrigatoriamente, uma Política de Gestão de Privacidade interna.

20.9. Restringir o acesso aos dados pessoais e ao ambiente mediante a definição de pessoas habilitadas e responsáveis pelo tratamento, responsabilizando-se pela confidencialidade dos dados pessoais.

20.10. Garantir a integridade das informações compartilhadas pelo **CONTROLADOR**, não alterando dados pessoais por sua própria iniciativa, mas somente mediante instruções devidamente documentadas pelo **CONTROLADOR**, enquanto perdurar o Contrato.

20.11. Atender imediata e adequadamente a todas as solicitações do **CONTROLADOR** com relação ao tratamento de dados pessoais sob este Contrato, bem como considerar a orientação da Autoridade Nacional de Proteção de Dados (ANPD) com relação ao tratamento de dados pessoais transferidos.

20.12. Manter inventário detalhado dos acessos aos dados pessoais e aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do funcionário ou do responsável pelo acesso e o arquivo acessado, inclusive quando tal acesso é feito para cumprimento das obrigações legais ou determinações definidas por autoridade competente.

20.13. Atender o **CONTROLADOR** em diligências e entrevistas a serem realizadas com a finalidade de averiguação das medidas de segurança aplicadas para a proteção dos dados pessoais (*due-diligence*).

20.14. Atender o **CONTROLADOR** prontamente as solicitações de revisão dos procedimentos de *selfassessment* e/ou *due-diligence.*

20.15. Realizar operações de tratamento de dados pessoais sensíveis somente quando estritamente necessário para cumprir com as disposições do Contrato, devendo garantir a implementação de proteções técnicas apropriadas, aptas a manter a integridade, confidencialidade e segurança destas informações.

20.16. Sempre que necessário e solicitado pelo **CONTROLADOR**, o **OPERADOR** deverá auxiliar no atendimento das requisições realizadas por Titulares ou por qualquer autoridade.

20.17. Quaisquer informações solicitadas pelo **CONTROLADOR** deverão ser atendidas pelo **OPERADOR** de forma imediata ou no prazo máximo de 72 (setenta e duas horas) horas, justificando os motivos da demora.

20.18. O **OPERADOR** se obriga, ainda, a notificar o **CONTROLADOR** imediatamente sobre:

(a) qualquer pedido legalmente vinculativo de divulgação dos dados pessoais por uma Autoridade Pública;

(b) qualquer incidente com os dados pessoais ou serviços prestados; e

(c) qualquer solicitação recebida diretamente dos Titulares dos dados pessoais, ou da Autoridade Nacional de Proteção de Dados (ANPD), sem responder a esse pedido, a menos que tenha sido autorizado de outra forma a fazê-lo.

20.18.1. A notificação deverá:

(i) descrever a natureza do pedido, solicitação ou do incidente;
(ii) descrever as consequências prováveis do incidente;
(iii) descrever as medidas tomadas ou propostas pelo OPERADOR em resposta ao incidente;
(iv) fornecer o contato do DPO - Encarregado de Dados do OPERADOR.

20.19. O **OPERADOR** manterá o **CONTROLADOR** integralmente isento de quaisquer responsabilidades ou reivindicações dos Titulares de dados pessoais compartilhados ou tratados pelo **OPERADOR** em desacordo com as instruções fornecidas pelo **CONTROLADOR** ou, ainda, em descumprimento do Contrato, inclusive com relação aos incidentes.

20.20. Caso sejam ajuizadas ações pelos Titulares dos dados pessoais contra o **CONTROLADOR** ou sejam recebidas pelo **CONTROLADOR** notificações de quaisquer órgãos públicos, com base no uso indevido de dados pessoais decorrente de falha do **OPERADOR**, deverá o **OPERADOR** intervir no processo, reivindicando a condição de demandada e requerendo a exclusão do **CONTROLADOR** e, em caso de condenação do **CONTROLADOR**, o **OPERADOR** deverá ressarci-lo pelo valor principal pago, bem como por todos os danos e todas as despesas envolvidas na demanda.

20.21. Após a expiração ou rescisão do Contrato, o **OPERADOR** eliminará ou devolverá ao **CONTROLADOR** os materiais contendo dados pessoais que lhes foram disponibilizados para os fins dispostos no Contrato, conforme instruções e prazo informados pelo **CONTROLADOR**, não podendo exceder a 30 (trinta) dias e de acordo com os critérios da legislação aplicável.

20.22. Mesmo após a rescisão deste Contrato ou de outros acordos celebrados entre as Partes, as obrigações do **OPERADOR** perdurarão enquanto ele tiver acesso, estiver em posse ou conseguir realizar qualquer operação de tratamento dos dados pessoais envolvendo informações fornecidas pelo **CONTROLADOR**.

20.23. Manter atualizado junto ao **CONTROLADOR** o nome do DPO (*Data Protection Officer*) – Encarregado de Dados, e-mail e telefone de contato por parte do **OPERADOR** para manter as comunicações e solicitações entre as partes.

20.24. É vedada ao **OPERADOR** a subcontratação total ou parcial de operadores para tratamento de dados previsto no objeto do Contrato original.

CLÁUSULA VIGÉSIMA PRIMEIRA – DAS ALTERAÇÕES, ACRÉSCIMOS OU SUPRESSÕES

21.1. Eventuais alterações contratuais reger-se-ão pela disciplina do art. 65 da Lei nº 8.666, de 1993.

21.1.1. A Contratada é obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

21.2. As supressões resultantes de acordo celebrado entre as partes contratantes poderão exceder o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

CLÁUSULA VIGÉSIMA SEGUNDA - DA RESCISÃO

22.1. O presente Termo de Contrato poderá ser rescindido:

22.1.1. Por ato unilateral e escrito da Administração, nas situações previstas nos incisos I a XII e XVII do art. 78 da Lei nº 8.666, de 1993, e com as consequências indicadas no art. 80 da mesma Lei, sem prejuízo da aplicação das sanções previstas no Termo de Referência – Anexo I do Edital;

22.1.2. Amigavelmente, nos termos do art. 79, inciso II, da Lei nº 8.666, de 1993.

22.2. Os casos de rescisão contratual serão formalmente motivados, assegurando-se à Contratada o direito à prévia e ampla defesa.

22.3. A Contratada reconhece os direitos do Contratante em caso de rescisão administrativa prevista no art. 77 da Lei nº 8.666, de 1993.

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

22.4.1. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

22.4.2. Relação dos pagamentos já efetuados e ainda devidos;

22.4.3. Indenizações e multas.

CLÁUSULA VIGÉSIMA TERCEIRA – DA GESTÃO DO CONTRATO

23.1. A gestão do contrato será acompanhada por Gestor a ser indicado através de Portaria da autoridade competente após a assinatura do Contrato.

23.1.1. Será dada ciência da Portaria ao preposto da Contratada.

23.2. O Gestor do Contrato poderá, quando da emissão da Ordem de Serviço, exigir a entrega de relatório do prestador de serviço/fornecedor, referente à execução do Contrato, indicando nesta ocasião o formato e a periodicidade de entrega.

23.3. Os pagamentos devidos serão sempre condicionados a entrega dos relatórios.

CLÁUSULA VIGÉSIMA QUARTA – DO PREPOSTO DA CONTRATADA

24.1. Fica estabelecido que o preposto da Contratada para representá-la perante o Contratante na execução deste Contrato é o(a) Sr.(a). _____, função _____, portador da Cédula de Identidade RG nº _____ e CPF/MF nº _____, endereço eletrônico: ____.

CLÁUSULA VIGÉSIMA QUINTA – DAS VEDAÇÕES

25.1. É vedado à Contratada interromper a execução dos serviços sob alegação de inadimplemento por parte da Contratante, salvo nos casos previstos em lei.

25.2. É permitido à Contratada caucionar ou utilizar este Termo de Contrato para qualquer operação financeira, nos termos e de acordo com os procedimentos previstos na Instrução Normativa SEGES/ME nº 53, de 8 de julho de 2020.

25.3. A cessão de crédito, a ser feita mediante celebração de termo aditivo, dependerá de comprovação da regularidade fiscal e trabalhista da cessionária, bem como da certificação de que a cessionária não se encontra impedida de licitar e contratar com o Poder Público, conforme a legislação em vigor, nos termos do Parecer JL-01, de 18 de maio de 2020.

25.4. A crédito a ser pago à cessionária é exatamente aquele que seria destinado à cedente (Contratada) pela execução do objeto contratual, com o desconto de eventuais multas, glosas e prejuízos causados à Administração, sem prejuízo da utilização de institutos tais como os da conta vinculada e do pagamento direto previstos na IN SEGES/ME nº 5, de 2017, caso aplicáveis.

CLÁUSULA VIGÉSIMA SEXTA – DA PUBLICAÇÃO

26.1. O Contratante providenciará a publicação do extrato deste contrato e de seus eventuais termos aditivos no Diário Oficial da União, a suas expensas, na forma prevista no Parágrafo único do art. 61 da Lei nº 8.666/1993.

CLÁUSULA VIGÉSIMA SÉTIMA – DAS CONSIDERAÇÕES GERAIS

27.1. É vedada a utilização, na execução do objeto pela Contratada, de empregado que seja familiar de agente público ocupante de cargo em comissão ou função de confiança no Contratante, nos termos do art. 7º do Decreto nº 7.203/2010.

27.2. Constituem direitos e prerrogativas do Contratante, além dos previstos em outras leis, os constantes da Lei nº 8.666/1993, que a Contratada aceita e a eles se submete.

27.3. A omissão ou tolerância das partes em exigir o estrito cumprimento das disposições deste Contrato ou em exercer prerrogativa dele decorrente não constituirá novação ou renúncia nem lhes afetará o direito de, a qualquer tempo, exigirem o fiel cumprimento do avençado.

27.4. Fica ressalvada a possibilidade de alteração das condições contratuais, em face da superveniência de normas federais, estaduais ou municipais, bem como em razão da conveniência e oportunidade da Administração, devidamente justificadas.

27.5. A Contratada se compromete a manter durante a execução do presente Contrato, todas as condições de habilitação e qualificação exigidas no Edital do Pregão Eletrônico nº 007/2022.

27.6. Integram o presente Contrato como se nele estivesse transcrito o Edital do Pregão Eletrônico nº 007/2022, seus anexos e a Proposta Comercial de fls. ___ apresentada pela Contratada, anexados no processo administrativo V-0050/2020.

27.7. Este Contrato não autoriza, nem a Contratada tem direito, tampouco poderes e nem deverá comprometer ou vincular a Contratante a qualquer acordo, Contrato ou reconhecimento, nem induzir, renunciar ou transigir quaisquer dos direitos do Contratante ou, ainda, assumir qualquer obrigação em nome deste, a qual não se responsabilizará por quaisquer reclamações de lucros cessantes ou danos pleiteados por Terceiros em decorrência ou relacionados com a celebração, execução ou rescisão deste Contrato.

27.8. Caso qualquer das cláusulas deste Contrato seja ou se torne legalmente ineficaz, a validade do documento como um todo não deverá ser afetada.

CLÁUSULA VIGÉSIMA OITAVA – DOS CASOS OMISSOS

28.1. Os casos omissos serão decididos pelo Contratante, segundo as disposições contidas na Lei nº 8.666, de 1993, na Lei nº 10.520, de 2002 e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

CLÁUSULA VIGÉSIMA NONA – DO FORO DE ELEIÇÃO

29.1. As partes, de comum acordo, elegem o Foro da Justiça Federal de São Paulo para dirimir qualquer lide oriunda deste Contrato, com renúncia expressa de qualquer outro, por mais privilegiado que seja.

E, por estarem assim justas e contratadas, assinam as partes este Contrato, em 02 (duas) vias de igual teor e forma, para os mesmos efeitos, na presença de 02 (duas) testemunhas.

São Paulo, de de 2022.

Ao assinar este Contrato as partes declaram ciência de todo seu conteúdo, independente de rubricas em todas as páginas.

Pela CONTRATADA:
REPRESENTANTE LEGAL:
TESTEMUNHA:

Pelo CREA-SP:
REPRESENTANTE LEGAL:
TESTEMUNHA:

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

ANEXO I

O Termo de Referência Anexo I do Edital será juntado quando da lavratura do instrumento contratual.

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

ANEXO III-A
TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO

INTRODUÇÃO
O Termo de Compromisso de Manutenção de Sigilo registra o comprometimento formal da Contratada em cumprir as condições estabelecidas no documento relativas ao acesso e utilização de informações sigilosas do CREA-SP em decorrência de relaçãocontratual, vigente ou não. **Referência: Art. 18, Inciso V, alínea "a" da IN SGD/ME Nº 1/2019.**

Pelo presente instrumento o CREA-SP, sediado em Av. Brigadeiro Faria Lima, 1059, Pinheiros, São Paulo, SP, CNPJ n° 60.985.017/0001-77, doravante denominado **CONTRATANTE**, e, de outro lado, a <NOME DA EMPRESA>, sediada em <ENDEREÇO>, CNPJ n° <Nº do CNPJ>, doravante denominada **CONTRATADA**;

CONSIDERANDO que, em razão do **CONTRATO nº <nº do contrato>** doravante denominado **CONTRATO PRINCIPAL**, a **CONTRATADA** poderá ter acesso a informações sigilosas do **CONTRATANTE**;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na Política de Segurança da Informação e Privacidade da **CONTRATANTE**;

Resolvem celebrar o presente **TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO,** doravante **TERMO**, vinculado ao **CONTRATO PRINCIPAL**, mediante as seguintes cláusulas e condições abaixo discriminadas.

1 – OBJETO

Constitui objeto deste **TERMO** o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela **CONTRATADA**, no que diz respeito ao trato de informações sigilosas disponibilizadas pela **CONTRATANTE** e a observância às normas de segurança da informação e privacidade por força dos procedimentos necessários para a execução do objeto do **CONTRATO PRINCIPAL** celebrado entre as partes e em acordo com o que dispõem a Lei 12.527, de 18 de novembro de 2011, Lei nº 13.709, de 14 de agosto de 2018, e os Decretos 7.724, de 16 de maio de 2012, e 7.845, de 14 de novembro de 2012, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo.

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

2 – CONCEITOS E DEFINIÇÕES

Para os efeitos deste **TERMO**, são estabelecidos os seguintes conceitos e definições: **INFORMAÇÃO**: dados, processados ou não, que podem ser utilizados para produção etransmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquela abrangida pelas demais hipóteses legais de sigilo.

CONTRATO PRINCIPAL: contrato celebrado entre as partes, ao qual este **TERMO** se vincula.

3 – DA INFORMAÇÃO SIGILOSA

Serão consideradas como informação sigilosa, toda e qualquer informação classificada ou não nos graus de sigilo ultrassecreto, secreto e reservado. O **TERMO** abrangerá todainformação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: *know-how*, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades da **CONTRATANTE** e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao **CONTRATO PRINCIPAL**, doravante denominados **INFORMAÇÕES**, a que diretamente ou pelos seus empregados, a **CONTRATADA** venha a ter acesso, conhecimento ou que venha a lhe serconfiada durante e em razão das atuações de execução do **CONTRATO PRINCIPAL** celebrado entre as partes.

4 – DOS LIMITES DO SIGILO

As obrigações constantes deste **TERMO** não serão aplicadas às **INFORMAÇÕES** que:

I – sejam comprovadamente de domínio público no momento da revelação, exceto setal fato decorrer de ato ou omissão da **CONTRATADA**;

II – tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente **TERMO**;

III – sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

5 – DIREITOS E OBRIGAÇÕES

As partes se comprometem a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do **CONTRATO PRINCIPAL**, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas **INFORMAÇÕES**, que se restringem estritamente ao cumprimento do **CONTRATO PRINCIPAL**.

Parágrafo Primeiro – A **CONTRATADA** se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento prévio e expresso da **CONTRATANTE**.

Parágrafo Segundo – A **CONTRATADA** compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do **CONTRATO PRINCIPAL** sobre a existência deste **TERMO** bem como da natureza sigilosa das informações.

I – A **CONTRATADA** deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente **TERMO** e dará ciência à **CONTRATANTE** dos documentos comprobatórios.

Parágrafo Terceiro – A **CONTRATADA** obriga-se a tomar todas as medidas necessárias àproteção da informação sigilosa da **CONTRATANTE**, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela **CONTRATANTE**.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste **TERMO**.

I – Quando requeridas, as **INFORMAÇÕES** deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto – A **CONTRATADA** obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à **CONTRATADA**, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do **CONTRATO PRINCIPAL**.

Parágrafo Sexto – A **CONTRATADA**, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer titulo ou dispor das **INFORMAÇÕES**, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas eprecauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmos judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das **INFORMAÇÕES**por seus agentes, representantes ou por terceiros;

III – Comunicar à **CONTRATANTE**, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das **INFORMAÇÕES**, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da **CONTRATADA**, terão acesso às informações sigilosas.

6 – VIGÊNCIA

O presente **TERMO** tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a quea **CONTRATADA** teve acesso em razão do **CONTRATO PRINCIPAL**.

7 – PENALIDADES

A quebra do sigilo e/ou da confidencialidade das **INFORMAÇÕES**, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do **CONTRATO PRINCIPAL** firmado entre as **PARTES**. Neste caso, a **CONTRATADA**, estará sujeita, por ação ou omissão, ao pagamento ou recomposição detodas as perdas e danos sofridos pela **CONTRATANTE**, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme Art. 87 da Lei nº. 8.666/93.

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

8 – DISPOSIÇÕES GERAIS

Este **TERMO** de Confidencialidade é parte integrante e inseparável do **CONTRATO PRINCIPAL**.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando- se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa-fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente **TERMO** prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro – Ao assinar o presente instrumento, a **CONTRATADA** manifesta suaconcordância no sentido de que:

I – A **CONTRATANTE** terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da **CONTRATADA**;

II – A **CONTRATADA** deverá disponibilizar, sempre que solicitadas formalmente pela **CONTRATANTE**, todas as informações requeridas pertinentes ao **CONTRATO PRINCIPAL**.

III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV – Todas as condições, termos e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V – O presente **TERMO** somente poderá ser alterado mediante **TERMO** aditivo firmado pelas partes;

VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a **CONTRATADA** não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste **TERMO**, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações, conforme definição do item 3 deste documento, disponibilizadas para a **CONTRATADA**, serão incorporados a este **TERMO**, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descritapara as informações iniciais disponibilizadas, sendo necessário a formalização de **TERMO** aditivo ao **CONTRATO PRINCIPAL**;

VIII – Este **TERMO** não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar **INFORMAÇÕES** para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

9 – FORO

A **CONTRATANTE** elege o foro da Justiça Federal de São Paulo, onde está localizada a sede da **CONTRATANTE**, para dirimir quaisquer dúvidas originadas do presente **TERMO**, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

10 – ASSINATURAS

E, por assim estarem justas e estabelecidas as condições, o presente Termo de Compromisso de Manutenção de Sigilo é assinado pelas partes em 2 vias de igual teor e um só efeito.

São Paulo, de de 2022.

Ao assinar este Termo as partes declaram ciência de todo seu conteúdo, independente de rubricas em todas as páginas.

Pela CONTRATADA:
REPRESENTANTE LEGAL:
TESTEMUNHA:

Pelo CREA-SP:
REPRESENTANTE LEGAL:
TESTEMUNHA:

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

ANEXO III-B
TERMO DE CIÊNCIA

INTRODUÇÃO
O Termo de Ciência visa obter o comprometimento formal dos empregados da contratada diretamente envolvidos na contratação quanto ao conhecimento da declaração de manutenção de sigilo e das normas de segurança vigentes no CREA-SP. No caso de substituição ou inclusão de empregados da contratada, o preposto deveráentregar ao Fiscal Administrativo do Contrato os Termos de Ciência assinados pelos novos empregados envolvidos na execução dos serviços contratados. **Referência: Art. 18, Inciso V, alínea "b" da IN SGD/ME Nº 1/2019.**

1 – IDENTIFICAÇÃO			
CONTRATO Nº	xxxx/aaaa		
OBJETO	<objeto do contrato>		
CONTRATADA	<nome da contratada>	**CNPJ**	xxxxxxxxxxxx
PREPOSTO	<Nome do Preposto da Contratada>		
GESTOR DOCONTRATO	<Nome do Gestor do Contrato>	**MATR.**	xxxxxxxxxxxx

2 – CIÊNCIA

Por este instrumento, os funcionários abaixo identificados declaram ter ciência e conhecer o inteiro teor do Termo de Compromisso de Manutenção de Sigilo e as normas de segurança vigentes da Contratante.

Funcionários da Contratada		
Nome	**Matrícula**	**Assinatura**
<Nome do(a) Funcionário(a)>	<xxxxxxxxxx>	
<Nome do(a) Funcionário(a)>	<xxxxxxxxxx>	
…	…	…

São Paulo, de de 2022.

Pela CONTRATADA:
REPRESENTANTE LEGAL:
TESTEMUNHA: