PREGÃO ELETRÔNICO Nº 05/2018
CONSELHO DE ARQUITETURA E URBANISMO DO BRASIL – CAU/BR
(Processo Administrativo n.º 002/2018)

O **CONSELHO DE ARQUITETURA E URBANISMO DO BRASIL – CAU/BR**, por intermédio de sua pregoeira e equipe de apoio, designados pela Portaria PRES nº 204, de 13 de outubro de 2017, torna público e faz comunicar aos que interessar possa que realizará licitação na modalidade **PREGÃO ELETRÔNICO**, do tipo **MENOR PREÇO GLOBAL**. O procedimento licitatório obedecerá à Lei nº 10.520, de 2002, ao Decreto nº 3.555, de 2000, e, subsidiariamente, à Lei nº 8.666, de 1993, assim como à legislação correlata, e demais exigências previstas neste Edital e em seus Anexos.

RECEBIMENTO DAS PROPOSTAS E CREDENCIAMENTO: até às 9h59 do dia 29 de maio de 2018 (Horário de Brasília – DF).

ABERTURA DA SESSÃO PÚBLICA DO PREGÃO: às 10h do dia 29 de maio de 2018 (Horário de Brasília – DF).

LOCAL: Portal de Compras do Governo Federal – www.comprasgovernamentais.gov.br.

CAPÍTULO 1. DO OBJETO

1.1. O objeto da presente licitação é a escolha da proposta mais vantajosa para a contratação de suporte técnico especializado na área de informática – infraestrutura de redes, incluída cessão em comodato de equipamentos e dispositivos de rede para prestação de serviços de sustentação de infraestrutura, contemplando fornecimento de serviços de segurança da informação; de controle, operação e administração de rede; de acesso à rede local WI-FI com segurança, controle, identificação e gerenciamento; de operação e execução de rotinas e procedimentos de *backup*s; de monitoramento e gerenciamento de ativos de rede; e de serviços de gestão da rede (incluindo medição de indicadores e realização de consultoria, projetos, diagnósticos e laudos), com o objetivo de implantar e manter infraestrutura de Tecnologia de Informação em conformidade com níveis de serviço previamente determinados e de acordo com as boas práticas vigentes, consoante especificações do Termo de Referência, Anexo I deste Edital.

CAPÍTULO 2. DAS INFORMAÇÕES PRELIMINARES

2.1. O inteiro teor deste Edital poderá ser obtido gratuitamente no sítio eletrônico do Conselho de Arquitetura e Urbanismo do Brasil (CAU/BR), www.caubr.gov.br, ou solicitado ao pregoeiro ou equipe de apoio na sede do Conselho, no horário de 9h00 às 12h00 e das 14h00 às 17h00, mediante pagamento pelas cópias reprográficas.

2.2. Se por qualquer motivo não houver expediente no CAU/BR no dia agendado para abertura da sessão pública, esta ficará automaticamente transferida para o primeiro dia útil seguinte, no mesmo horário, independente de comunicação.

2.3. Das decisões do pregoeiro dar-se-á publicidade no sítio eletrônico do CAU/BR, salvo em relação àquelas cuja publicação e ciência puderem ser feitas diretamente aos licitantes participantes da sessão pública, principalmente, quanto ao resultado de:

2.3.1. Julgamento da licitação;
2.3.2. Recursos porventura interpostos.
2.4. Os esclarecimentos e decisões quanto à impugnação e recursos serão divulgados no sítio eletrônico do CAU/BR, www.caubr.gov.br, quando houver impossibilidade de fazê-lo no Comprasnet.
2.5. A participação na licitação, sem que tenha sido tempestivamente impugnado o Edital importa em total e irrestrito conhecimento e aceitação das condições estatuídas, ou seja, de que os elementos são suficientes, claros e precisos, não cabendo, portanto, posterior reclamação.
2.6. Os licitantes deverão observar o disposto no subitem 2.3, sob pena de arcar com os prejuízos decorrentes da inobservância das publicações oficiais.
2.7. O Termo de Referência é parte integrante deste Edital, como se transcrito estivesse.

CAPÍTULO 3. DOS RECURSOS ORÇAMENTÁRIOS

3.1. As despesas para atender a esta licitação estão programadas em dotação orçamentária própria, prevista no orçamento do Conselho de Arquitetura e Urbanismo do Brasil (CAU/BR), a saber:
3.1.1. Orçamento CAU/BR 2018;
3.1.2. Conta: 6.2.2.1.1.01.04.04.031 - Serviços de Manutenção Sistema de Informática;
3.1.3 Centro de Custo: 4.02.05.001 - Manutenção da Gerência Administrativa;
3.1.4. As despesas referentes aos próximos exercícios deverão ser consignadas em orçamento próprio, nos respectivos exercícios financeiros.

CAPÍTULO 4. DO CREDENCIAMENTO

4.1. O Credenciamento é o nível básico do registro cadastral no SICAF, que permite a participação dos interessados na modalidade licitatória Pregão, em sua forma eletrônica.
4.2. O cadastro no SICAF poderá ser iniciado no Portal de Compras do Governo Federal, no sítio www.comprasgovernamentais.gov.br, com a solicitação de login e senha pelo interessado.
4.3. 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.
4.4. O uso da senha de acesso pelo licitante é de sua responsabilidade exclusiva, incluindo qualquer transação efetuada diretamente ou por seu representante, não cabendo ao provedor do sistema, ou ao órgão ou entidade responsável por esta licitação, responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.
4.5. A perda da senha ou a quebra de sigilo deverão ser comunicadas imediatamente ao provedor do sistema para imediato bloqueio de acesso.

CAPÍTULO 5. DAS CONDIÇÕES DE PARTICIPAÇÃO NO PREGÃO.

5.1. Poderão participar da licitação os interessados que estiverem previamente credenciados no Sistema de Cadastramento Unificado de Fornecedores (SICAF) e perante o sistema eletrônico provido pela Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão (SLTI), por meio do sítio www.comprasnet.gov.br, atendidas as demais exigências do Edital.

5.2. Para ter acesso ao sistema eletrônico, os interessados em participar deste Pregão deverão dispor de chave de identificação e senha pessoal, obtidas junto à SLTI, onde também deverão informar-se a respeito do seu funcionamento e regulamento e receber instruções detalhadas para sua correta utilização.

5.3. O uso da senha de acesso pelo licitante é de sua responsabilidade exclusiva, incluindo qualquer transação por ele efetuada diretamente, ou por seu representante, não cabendo ao provedor do sistema ou ao CAU/BR responsabilidade por eventuais danos decorrentes do uso indevido da senha, ainda que por terceiros.

5.4. Não poderão participar desta licitação os interessados:

5.4.1. Suspensos de participar de licitação e impedidos de contratar com o CAU/BR, durante o prazo da sanção aplicada; (não lembro se essa é a redação padrão, no entanto, considero mais correto assim, se concordarem...)

5.4.2. Declarados inidôneos para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação;

5.4.3. Impedidos de licitar e contratar com a União, durante o prazo da sanção aplicada;

5.4.4. Sociedade estrangeira não autorizada a funcionar no País;

5.4.5. Pessoa Jurídica cujo estatuto ou contrato social não inclua o objeto deste Pregão;

5.4.6. Que se encontrem em processo de dissolução, recuperação judicial;

5.4.7. Sociedades integrantes de um mesmo grupo econômico, assim entendidas aquelas que tenham diretores, sócios ou representantes legais comuns, ou que utilizem recursos materiais, tecnológicos ou humanos em comum, exceto se demonstrado que não agem representando interesse econômico em comum;

5.4.8. Dirigentes, conselheiros e colaboradores do CAU/BR, inclusive familiares, na forma prevista no art. 7º do Decreto nº 7.203, de 2010;

5.4.9. Consórcio de empresa, qualquer que seja sua forma de constituição.

5.5. As demais condições para participação neste certame licitatório estão consignadas no Termo de Referência, Anexo I deste Edital.

CAPÍTULO 6. DO ENVIO DA PROPOSTA

6.1. O licitante deverá encaminhar a proposta por meio do sistema eletrônico até a data e horário marcados para abertura da sessão, quando, então, encerrar-se-á automaticamente a fase de recebimento de propostas.

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

6.3. 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.

6.4. 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.

6.5. O licitante deverá consignar, na forma expressa no sistema eletrônico, o valor global da proposta, já considerados e inclusos todos custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais, fretes e quaisquer outros que incidam direta ou indiretamente na prestação dos serviços.

6.5.1. A Contratada deverá arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, caso o previsto não seja satisfatório para o atendimento do objeto da licitação, exceto quando ocorrer algum dos eventos arrolados nos incisos do §1° do artigo 57 da Lei n° 8.666, de 1993.
6.5.2. O licitante deverá declarar em campo próprio do Sistema, a descrição do serviço ofertado.
6.5.3. O licitante deverá declarar, em campo próprio do sistema eletrônico, que cumpre plenamente os requisitos de habilitação e que sua proposta está em conformidade com as exigências do Edital.
6.5.4. O licitante deverá declarar, em campo próprio do Sistema, sob pena de inabilitação, que não emprega menores de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre, nem menores de 16 (dezesseis) anos em qualquer trabalho, salvo na condição de aprendiz, a partir dos 14 (quatorze) anos.
6.5.5. O licitante enquadrado como microempresa ou empresa de pequeno porte deverá declarar, em campo próprio do Sistema, que atende aos requisitos do art. 3º da Lei Complementar nº 123, de 2006, para fazer jus aos benefícios previstos nesta Lei.
6.5.6. Em se tratando de Microempreendedor Individual – MEI, o licitante deverá incluir, no campo das condições da proposta do sistema eletrônico, o valor correspondente à contribuição prevista no art. 18-B da Lei Complementar n. 123, de 2006.
6.5.7. A declaração falsa relativa ao cumprimento dos requisitos de habilitação, à conformidade da proposta ou ao enquadramento como microempresa ou empresa de pequeno porte ou ao direito de preferência sujeitará o licitante às sanções previstas neste Edital e no Termo de Referência.
6.6. As propostas ficarão disponíveis no sistema eletrônico.
6.6.1. Qualquer elemento que possa identificar o licitante importa desclassificação da proposta, sem prejuízo das sanções previstas neste Edital.
6.6.2. Até a abertura da sessão, o licitante poderá retirar ou substituir a proposta anteriormente encaminhada.
6.7. As propostas terão validade de 60 (sessenta) dias, contados da data de abertura da sessão pública estabelecida no preâmbulo deste Edital.
6.7.1. Decorrido o prazo de validade das propostas, sem convocação para contratação, ficam os licitantes liberados dos compromissos assumidos. Todas as especificações do objeto contidas na proposta vinculam a Contratada.

CAPÍTULO 7. DA ABERTURA DA SESSÃO PÚBLICA

7.1. A abertura da sessão pública deste Pregão, conduzida pelo pregoeiro, ocorrerá na data e na hora indicadas no preâmbulo deste Edital, no sítio eletrônico www.comprasnet.gov.br.
7.1.1. Durante a sessão pública, a comunicação entre o pregoeiro e os licitantes ocorrerá exclusivamente mediante troca de mensagens, em campo próprio do sistema eletrônico.
7.2. Cabe 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 qualquer mensagem emitida pelo sistema ou de sua desconexão.

CAPÍTULO 8. DA CLASSIFICAÇÃO DAS PROPOSTAS

8.1. O pregoeiro verificará as propostas apresentadas e desclassificará, desde logo e motivadamente, aquelas que não estejam em conformidade com os requisitos estabelecidos neste Edital ou contenham vícios insanáveis ou ilegalidades.

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

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

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

CAPÍTULO 9. DA FORMULAÇÃO DE LANCES

9.1. Iniciada a etapa competitiva, os licitantes classificados poderão encaminhar lances sucessivos, exclusivamente por meio do sistema eletrônico, sendo imediatamente informados do horário e valor consignados no registro de cada lance.

9.1.1. O lance ofertado deverá ser referente ao valor global do contrato.

9.2. O licitante somente poderá oferecer lance inferior ao último por ele ofertado e registrado no sistema.

9.3. Durante o transcurso da sessão, os licitantes serão informados, em tempo real, do valor do menor lance registrado, mantendo-se em sigilo a identificação do ofertante.

9.4. Em caso de empate, prevalecerá o lance recebido e registrado primeiro.

9.5. Os lances apresentados e levados em consideração para efeito de julgamento serão de exclusiva e total responsabilidade do licitante, não lhe cabendo o direito de pleitear qualquer alteração.

9.6. Durante a fase de lances, o pregoeiro poderá excluir, justificadamente, lance cujo valor seja manifestamente inexequível.

9.7. Se ocorrer a desconexão do pregoeiro no decorrer da etapa de lances, e o sistema eletrônico permanecer acessível aos licitantes**,** os lances continuarão sendo recebidos, sem prejuízo dos atos realizados.

9.8. No caso de a desconexão do pregoeiro persistir por tempo superior a 10 (dez) minutos, a sessão do Pregão será suspensa automaticamente e terá reinício somente após comunicação expressa aos participantes no sítio www.comprasnet.gov.br.

9.9. O encerramento da etapa de lances será decidido pelo pregoeiro, que informará, com antecedência de 1 (um) a 60 (sessenta) minutos, o prazo para início do tempo de iminência.

9.10. Decorrido o prazo fixado pelo pregoeiro, o sistema eletrônico encaminhará aviso de fechamento iminente dos lances, após o que transcorrerá período de tempo de até 30 (trinta) minutos, aleatoriamente determinado pelo sistema, findo o qual será automaticamente encerrada a fase de lances.

9.11. Após a fase de lances, em atendimento ao disposto no artigo 44 da Lei Complementar nº 123/06, que assegura preferência de contratação como critério de desempate técnico, caso a proposta mais bem classificada não tenha sido ofertada por microempresa ou empresa de pequeno porte e houver proposta apresentada por microempresa ou empresa de pequeno porte igual ou até 5% (cinco por cento) superior à proposta de menor preço, proceder-se-á da seguinte forma:

9.11.1. A microempresa ou a empresa de pequeno porte mais bem classificada poderá, no prazo de 5 (cinco) minutos, que se iniciará após a fase de lances, apresentar uma última oferta, necessariamente inferior àquela apresentada pela primeira colocada, situação em que, atendidas as exigências habilitatórias, será adjudicado em seu favor o objeto deste Pregão;
9.11.2. Não ocorrendo a contratação da microempresa ou empresa de pequeno porte, na forma determinada anteriormente, serão convocadas as remanescentes que porventura se enquadrem na hipótese de microempresas e empresas de pequeno porte, na ordem classificatória, para o exercício do mesmo direito;
9.11.3. No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.
9.11.4. Na hipótese da não contratação nos termos do subitem 9.11, o objeto licitado será adjudicado em favor da proposta originalmente vencedora do certame.

CAPÍTULO 10. DA NEGOCIAÇÃO

10.1 O pregoeiro poderá encaminhar contraproposta diretamente ao licitante que tenha apresentado o lance mais vantajoso, observado o critério de julgamento e o valor estimado para a contratação.
10.2. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

CAPÍTULO 11. DA ACEITABILIDADE DA PROPOSTA VENCEDORA

11.1. Encerrada a etapa de lances e depois da verificação de possível empate, o Pregoeiro examinará a proposta classificada em primeiro lugar quanto ao preço, a sua exequibilidade, bem como quanto ao cumprimento das especificações do objeto.
11.2. O licitante classificado provisoriamente em primeiro lugar deverá encaminhar a proposta de preço adequada ao último lance, acompanhada da planilha de preços (conforme modelo apresentado no Anexo V deste Edital), observadas as demais condições relacionadas no Capítulo 9 do Termo de Referência, Anexo I deste Edital, no prazo de 3 (três) horas, contado da convocação efetuada pelo pregoeiro por meio da opção “Enviar Anexo” no sistema Comprasnet.
11.2.1. A partir da solicitação do pregoeiro no sistema eletrônico, relativa ao envio de documentos de habilitação complementares, poderá ser usado (caso não seja possível enviá-los pelo sistema Comprasnet), preferencialmente, o endereço eletrônico licitacao@caubr.gov.br, ou outros meios, conforme Instrução Normativa nº 1, de 26 de março de 2014, da Secretária de Logística e Tecnologia da Informação do MPOG.
11.3. Os documentos remetidos por meio da opção “Enviar Anexo” do sistema Comprasnet poderão ser solicitados em original ou por cópia autenticada a qualquer momento, os quais deverão ser entregues no prazo máximo de 5 (cinco) dias, na sede do CAU/BR, conforme subitem 11.3.2.
11.3.1. O prazo para a entrega dos documentos poderá ser prorrogado uma única vez, por igual período, quando solicitado pelo licitante vencedor durante o seu transcurso, desde que ocorra motivo justificado e aceito pelo pregoeiro.

11.3.2. Os originais ou cópias autenticadas, caso sejam solicitados, deverão ser encaminhados ao Setor de Compras do CAU/BR, situada no Setor Comercial Sul, Quadra 2, Bloco C, Entrada 22, Ed. Serra Dourada, Salas 401 a 409, CEP 70.300-902, Brasília (DF).

11.4. O licitante que abandonar o certame, deixando de enviar a documentação indicada nesta seção, será desclassificado e sujeitar-se-á às sanções previstas neste Edital e no Termo de Referência.

11.5. O pregoeiro examinará a proposta mais bem classificada quanto à compatibilidade do preço ofertado com o valor estimado e à compatibilidade da proposta com as especificações técnicas do objeto.

11.6. O pregoeiro poderá solicitar parecer de técnicos pertencentes ao quadro de pessoal do CAU/BR ou, ainda, de pessoas físicas ou jurídicas estranhas a ele, para orientar sua decisão.

11.7. Não se considerará qualquer oferta de vantagem não prevista neste Edital, inclusive financiamentos subsidiados ou a fundo perdido.

11.8. Não se admitirá proposta que apresente valores simbólicos, irrisórios ou de valor zero, incompatíveis com os preços de mercado, exceto quando se referirem a materiais e instalações de propriedade do licitante, para os quais ele renuncie à parcela ou à totalidade de remuneração.

11.9. Não serão aceitas propostas com valores unitários e global superiores aos estimados ou com preços manifestamente inexequíveis.

11.9.1. 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, a exemplo das enumeradas no item 9.4 do Anexo VII-A, da SEGES/MPDG IN. 5, de 2017.

11.10. O CAU/BR poderá realizar diligências objetivando comprovar a veracidade das informações prestadas pelo licitante. Caso fique caracterizada atitude inidônea do licitante, esse estará sujeito às penalidades previstas em lei.

11.11. Se a proposta ou lance vencedor for desclassificado, o Pregoeiro examinará a proposta ou lance subsequente, e, assim sucessivamente, na ordem de classificação.

11.11.1. Também nas hipóteses em que o Pregoeiro não aceitar a proposta e passar à subsequente, poderá negociar com o licitante para que seja obtido preço melhor.

11.12. Havendo necessidade, o Pregoeiro suspenderá a sessão, informando no "*chat*" a nova data e horário para a continuidade da mesma.

CAPÍTULO 12. DA HABILITAÇÃO

12.1. As disposições inerentes à habilitação (Qualificação Técnica; Qualificação econômico-financeira; Regularidade fiscal e trabalhista; Declarações e Habilitação Jurídica) constam do Capítulo 8 do Termo de Referência, Anexo I deste Edital, e demais disposições aplicáveis.

CAPÍTULO 13. DA REABERTURA DA SESSÃO PÚBLICA

13.1. A sessão pública poderá ser reaberta:

13.1.1. 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.

13.1.2. 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, nos termos do art. 43, §1º da LC nº 123/2006. Nessas hipóteses, serão adotados os procedimentos imediatamente posteriores ao encerramento da etapa de lances.
13.2. Todos os licitantes remanescentes deverão ser convocados para acompanhar a sessão reaberta.
13.2.1. A convocação se dará por meio do sistema eletrônico ("chat") e do sítio oficial deste Conselho.

CAPÍTULO 14. DOS RECURSOS

14.1. Declarado o vencedor, o pregoeiro abrirá prazo de 20 minutos, durante o qual qualquer licitante poderá, de forma imediata e motivada, em campo próprio do sistema, manifestar sua intenção de recurso.
14.1.1. A falta de manifestação no prazo estabelecido autoriza o pregoeiro a adjudicar o objeto ao licitante vencedor.
14.1.2. O pregoeiro examinará a intenção de recurso, aceitando-a ou, motivadamente, rejeitando-a, em campo próprio do sistema.
14.1.2.1. Nesse momento o Pregoeiro não adentrará no mérito recursal, mas apenas verificará a presença dos pressupostos recursais.
14.1.3. O licitante que tiver sua intenção de recurso aceita deverá registrar as razões do recurso, em campo próprio do sistema, no prazo de 3 (três) dias, ficando os demais licitantes, desde logo, intimados a apresentar contrarrazões, também via sistema, em igual prazo, que começará a correr do término do prazo da recorrente.
14.1.4. Para efeito do disposto no art. 109, § 5º da Lei nº 8.666, de 1993, fica a vista do respectivo processo administrativo franqueada aos interessados.
14.2. As intenções de recurso não admitidas e os recursos rejeitados pelo pregoeiro serão apreciados pelo Presidente do CAU/BR.
14.3. O acolhimento do recurso implicará a invalidação apenas dos atos insuscetíveis de aproveitamento.

CAPÍTULO 15. DA ADJUDICAÇÃO E HOMOLOGAÇÃO

15.1. O objeto deste Pregão será adjudicado ao licitante declarado vencedor, por ato do Pregoeiro, salvo quando houver interposição de recurso, hipótese em que a adjudicação caberá à autoridade competente para homologação, após a regular decisão dos recursos apresentados.
15.2. A homologação do Pregão compete ao Presidente do CAU/BR.
15.3. O objeto do Pregão será adjudicado globalmente ao licitante vencedor.

CAPÍTULO 16. DA GARANTIA DE EXECUÇÃO

16.1. A garantia de execução do contrato será regida pelo disposto no Capítulo 13 do Termo de Referência, Anexo I deste Edital.

CAPÍTULO 17. DO INSTRUMENTO CONTRATUAL

17.1. Após a homologação do resultado do Pregão, o licitante vencedor será convocado para assinatura do contrato, dentro do prazo de 5 (cinco) dias úteis, sob pena de decair o direito à contratação, para assinar o Contrato, sem prejuízo das sanções previstas neste Edital e Anexos.

17.1.1. O prazo para assinatura do contrato poderá, em situação excepcionalíssima, ser prorrogado uma única vez, por igual período, quando solicitado pela licitante vencedora em até 48h (quarenta e oito horas), a contar do recebimento da comunicação, desde que ocorra motivo relevante e aceito pelo CAU/BR.

17.2. Previamente à contratação, a Administração realizará consulta "online" ao SICAF, cujo resultado será anexado aos autos do processo.

17.2.1. 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.

17.3. Na celebração do contrato serão exigidas as mesmas condições de habilitação.

17.4. Alternativamente à convocação para comparecer perante o órgão ou entidade para a assinatura do Contrato, a Administração poderá encaminhá-lo para assinatura, mediante correspondência postal com aviso de recebimento (AR) ou meio eletrônico, para que seja assinado no prazo de 05 (cinco) dias corridos, a contar da data de seu recebimento.

17.5. O prazo previsto para assinatura ou aceite poderá ser prorrogado, por igual período, por solicitação justificada do adjudicatário e aceita pela Administração.

17.6. A vigência do contrato terá início na data da sua assinatura e se estenderá por 48 (quarenta e oito) meses, nos termos do art. 57, IV, da Lei 8.666/93.

17.7. Pela inexecução total ou parcial do contrato poderá ser aplicada à Contratada as sanções de que tratam os arts. 86 a 88 da Lei nº 8.666/1993, garantidos o contraditório e a ampla defesa, bem como as sanções e penalidades previstas neste Termo de Referência.

CAPÍTULO 18. DO ACOMPANHAMENTO E FISCALIZAÇÃO

18.1. Os critérios de acompanhamento e de fiscalização do contrato estão previstos no Termo de Referência, Anexo I deste Edital.

CAPÍTULO 19. DAS OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

19.1. As obrigações da Contratante e da Contratada são as estabelecidas no Termo de Referência, Anexo I deste Edital.

CAPÍTULO 20. DO PAGAMENTO

20.1. O pagamento será efetuado pela Contratante segundo as condições estabelecidas no Termo de Referência, Anexo I deste Edital.

CAPÍTULO 21. DAS SANÇÕES ADMINISTRATIVAS

21.1. As sanções a serem aplicadas ao licitante obedecerão ao disposto no Termo de Referência, Anexo I deste Edital.

CAPÍTULO 22. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

22.1. Até 02 (dois) dias úteis antes da data designada para a abertura da sessão pública, qualquer pessoa física ou jurídica, poderá impugnar o ato convocatório deste Pregão mediante petição a ser enviada exclusivamente para o endereço eletrônico licitacao@caubr.gov.br.

22.2. Caberá ao Pregoeiro, auxiliado pelo setor técnico competente, decidir sobre a impugnação no prazo de até 24 (vinte e quatro) horas.

22.3. Acolhida a impugnação, será definida e publicada nova data para a realização do certame, exceto quando, inquestionavelmente, a alteração não afetar a formulação das propostas.

22.4. Os pedidos de esclarecimentos referentes a este processo licitatório deverão ser enviados ao Pregoeiro, até 03 (três) dias úteis anteriores à data designada para abertura da sessão pública, exclusivamente para o endereço eletrônico licitacao@caubr.gov.br.

22.5. As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.

22.6. As respostas às impugnações e os esclarecimentos prestados pelo Pregoeiro serão disponibilizados no sistema eletrônico e entranhados nos autos do processo licitatório, permanecendo disponíveis para consulta por qualquer interessado.

CAPÍTULO 23. DAS DISPOSIÇÕES GERAIS

23.1. Ao Presidente do CAU/BR compete anular este Pregão por ilegalidade, de ofício ou por provocação de qualquer pessoa, e revogar o certame por considerá-lo inoportuno ou inconveniente diante de fato superveniente, mediante ato escrito e fundamentado.

23.1.1. A anulação do pregão induz à do contrato.

23.1.2. Os licitantes não terão direito à indenização em decorrência da anulação do procedimento licitatório, ressalvado o direito do contratado de boa-fé de ser ressarcido pelos encargos que tiver suportado no cumprimento do contrato.

23.2. É facultado ao pregoeiro ou à autoridade superior, em qualquer fase deste Pregão, promover diligência destinada a esclarecer ou complementar a instrução do processo, vedada a inclusão posterior de informações ou de documentos que deveriam ter sido apresentados para fins de classificação e habilitação.

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

23.4. Caso os prazos definidos neste Edital não estejam expressamente indicados na proposta, eles serão considerados como aceitos no julgamento do Pregão.

23.5. Os documentos eletrônicos produzidos com a utilização de processo de certificação disponibilizada pela ICP-Brasil, nos termos da Medida Provisória nº 2.200-2, de 24 de agosto de 2001, serão recebidos e presumidos verdadeiros em relação aos signatários, dispensando-se o envio de documentos originais e cópias autenticadas em papel.

23.6. Aplicam-se às cooperativas enquadradas na situação do art. 34 da Lei nº 11.488, de 15 de junho de 2007, todas as disposições relativas às microempresas e empresas de pequeno porte.

23.7. Em caso de divergência entre normas infralegais e as contidas neste Edital, prevalecerão as últimas.
23.8. Este Pregão poderá ter a data de abertura da sessão pública transferida por conveniência do CAU/BR, sem prejuízo do disposto no art. 4, inciso V, da Lei nº 10.520, de 2002.
23.9. A homologação do resultado desta licitação não implicará direito à contratação.
23.10. 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.
23.11. 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 no CAU/BR.
23.12. 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.
23.13. Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital.
23.14. Integram este Edital, para todos os fins e efeitos, os seguintes anexos:
23.14.1. ANEXO I – Termo de Referência;
23.14.2. ANEXO II – Modelo de declaração de habilitação (poderá ser substituída pela declaração de mesmo teor, extraída do Sistema Eletrônico);
23.14.3. ANEXO III – Modelo de declaração de trabalho do menor (poderá ser substituída pela declaração de mesmo teor, extraída do Sistema Eletrônico);
23.14.4. ANEXO IV – Modelo de declaração de idoneidade;
23.14.5. ANEXO V – Modelo de planilha de preços;
23.14.6. ANEXO VI – Modelo de declaração para ME e EPP – Poderá ser substituída pela declaração de mesmo teor, extraída do Sistema Eletrônico;
23.14.7. ANEXO VII – Minuta de contrato.
23.15. Sempre que o sistema de pregão eletrônico disponibilizar as declarações citadas, o licitante poderá utilizar as opções pelo meio eletrônico.

Brasília, 16 de maio de 2018.

RICARDO DE FREITAS FRATESCHI JÚNIOR
Gerente Administrativo CAU/BR

Processo Administrativo nº 002/2018

PREGÃO ELETRÔNICO Nº 05/2018

ANEXO I – TERMO DE REFERÊNCIA

TERMO DE REFERÊNCIA

CAPÍTULO 1. DO OBJETO

1.1. Contratação de suporte técnico especializado na área de informática – infraestrutura de redes, incluído cessão em comodato de equipamentos e dispositivos de rede para prestação de serviços de sustentação de infraestrutura, contemplando fornecimento de serviços de segurança da informação; de controle, operação e administração de rede; de acesso à rede local WI-FI com segurança, controle, identificação e gerenciamento; de operação e execução de rotinas e procedimentos de *backup*s; de monitoramento e gerenciamento de ativos de rede; e de serviços de gestão da rede (incluindo medição de indicadores e realização de consultoria, projetos, diagnósticos e laudos), com o objetivo de implantar e manter infraestrutura de Tecnologia de Informação em conformidade com níveis de serviço previamente determinados e de acordo com as boas práticas vigentes.

CAPÍTULO 2. DA JUSTIFICATIVA

2.1. Visando garantir aos profissionais de Arquitetura e Urbanismo vinculados a este órgão o acesso aos serviços prestados pelo CAU/BR, é crucial a garantia de continuidade e progressiva expansão e melhoria da estrutura de alta disponibilidade em sala de segurança que se possui atualmente. Os serviços de sala de segurança estão ativos desde setembro de 2012 e com o aumento da demanda interna e externa, somado ao crescimento do quadro de pessoal do CAU/BR e dos usuários a nível nacional, verificou-se a necessidade de fazer nova licitação para adequar a prestação de serviços especializados da sala de segurança ao CAU/BR.

CAPÍTULO 3. DO PROVIMENTO DE SERVIÇOS DE INFRAESTRUTURA DE REDE

3.1. Fornecimento de infraestrutura de rede, incluindo cessão em comodato de equipamentos e dispositivos de rede (hardware, software, ativos de rede) para provimento dos seguintes serviços:

3.1.1. Fornecimento de serviço de firewall de rede para uso na sede do CAU/BR, com características técnicas mínimas que atendam às especificações do Anexo I - B;

3.1.2. Suporte em servidores virtuais para rede local de computadores, com sistema operacional Windows Server (versão 2008 ou superior) que hospedam os seguintes serviços:

3.1.2.1. Serviço file server, implementado em máquina virtual com espaço de armazenamento de dados inicial de 4 Terabytes, podendo aumentar a capacidade em até 50% no período de até 2 (dois) anos;

3.1.2.2. Serviço DHCP - implementado em máquina virtual;

3.1.2.3. Serviço DNS interno - principal e redundante, implementados em máquinas virtuais distintas, para prevenir falhas;

3.1.2.4. Serviço de atualização permanente e automático de *patches* e *hot-fixes* para servidores e estações de trabalho Windows (WSUS) implementado em máquina virtual, para manter a rede interna do CAU/BR atualizada;

3.1.2.5. Serviço de diretório e autenticação de usuários *MS-Active Directory*, fornecido em duas instâncias (principal e redundante), implementadas em máquinas virtuais distintas.

3.2. Serviço de provimento de antivírus, para até 200 *endpoints*, com atualização diária de vacinas e console central de gerenciamento, em conformidade com as especificações do Anexo I - B, item 3 – Segurança de estações de trabalho e servidores.
3.3. Serviço de realização de *backups/restore* dos arquivos armazenados em servidor de arquivos (servidor virtual), em conformidade com a especificação contida no Anexo I - E.
3.4. Fornecimento de serviços e equipamentos de acesso à rede sem fio, com capacidades mínimas em conformidade com as especificações do Anexo I - D.
3.5. Fornecimento de serviços e de switches de rede, com capacidades mínimas em conformidade com as especificações do Anexo I - G, para atender a demanda de conexão de até 264 (duzentos e sessenta e quatro) pontos.

CAPÍTULO 4. DO SUPORTE TÉCNICO E CONSULTORIA
4.1. A prestação dos serviços abrangerá a identificação e diagnóstico de problemas de infraestrutura de Tecnologia da Informação e Comunicação (TIC) no ambiente de produção do CAU/BR sob demanda, contemplando a medição e avaliação de seus parâmetros ou atributos, por meio da prestação de serviços de técnico especializado. Os parâmetros e/ou atributos a serem considerados neste trabalho são os listados abaixo:
4.1.1. Performance (tempo de resposta dos serviços de TIC);
4.1.2. Disponibilidade (índice de tempo em que os serviços permanecem disponíveis para seus usuários);
4.1.3. Confiabilidade (capacidade do sistema em operar nas condições para as quais foi projetado, eventualmente operando em regime de contingência);
4.1.4. Segurança (proteção do sistema - capacidade do sistema em identificar e repelir ações maliciosas, não autorizadas ou ilegítimas, acidentais ou propositais);
4.1.5. Escalabilidade (Capacidade de expansão do sistema para acomodar maior demanda, sem que sejam necessárias alterações fundamentais no seu projeto);
4.1.6. Resiliência (capacidade de o sistema manter operação normal mesmo em condições adversas);
4.1.7. Compatibilidade (capacidade de estabelecer conexões serviços, dispositivos ou ambientes de terceiros);
4.1.8. Topologia (segmentação física e lógica das conexões de dados);
4.1.9. Custo;
4.2. Além da infraestrutura de tecnologia, o escopo dos serviços de avaliação também inclui os processos de trabalho adotados para implantar e operar os recursos de TIC do CAU/BR.
4.3. As não conformidades detectadas serão objeto de diagnóstico específico. Cada diagnóstico deverá apresentar as causas e efeitos do problema, bem como a recomendação(ões) de solução(ões). A abrangência deste trabalho de avaliação compreende a lista de itens descrita a seguir:
4.3.1. *Cabling;*
4.3.1.1. Topologia física;
4.3.1.2. Topologias lógica;
4.3.1.3. Segmentação;
4.3.1.4. Pontos de rede – identificação, documentação As-Built;
4.3.2. Serviços de rede;
4.3.2.1. Servidores de rede e serviços de rede em operação em cada servidor (compartilhamento de arquivos, impressão, proxy Web, firewall, acesso à Internet, e-mail, intranet, autenticação, etc.);
4.3.3. Ativos;
4.3.3.1. Teste e monitoramento das portas de Hub/Switch;
4.3.3.2. Captura e análise de logs de servidores e roteadores – performance, taxa de utilização de recursos, exceções;
4.3.3.3. Refrigerações / ventilações dos ativos de rede;

4. 3.3.4. Inventários de funcionalidades de Switches (mirror, trunck, VLAN, etc.);
4. 3.3.5. Configurações;
4.3.4. Tráfego;
4.3.4.1. Monitoramentos de colisões Ethernet;
4.3.4.2. Taxa de utilização de banda;
4.3.4.3. Endereçamento TCP/IP;
4.3.4.4. Serviços DNS, DHCP;
4.3.4.5. Impacto de bancos de dados sem recursos no tráfego de rede;
4.3.5. Parque de equipamentos;
4.3.5.1. Inventários de Hardware;
4.3.5.2. Inventários de Software;
4.3.5. Segurança e Integridade;
4.3.5.1. Antivírus;
4.3.5.2. Firewall;
4.3.5.3. *Backup*s;
4.3.5.4. Gerência de servidores, switches e estações;
4.3.5.5. Logs;
4.3.6. Governança;
4.3.6.1. Políticas;
4.3.6.2. Procedimentos;
4.3.6 3. Planos;
4.4. Os serviços a serem prestados pela CONTRATADA ao CAU/BR deverão contemplar, no mínimo, os seguintes tópicos:
4.4.1. Elaboração ou reformulação de projetos de infraestrutura de TIC;
4.4.2. Suporte técnico para implantar os projetos elaborados;
4.4.3. Suporte técnico para realizar intervenções (manutenção corretiva ou preventiva) nos servidores e ativos de rede do CAU/BR;
4.4.4. Executar o plano de manutenção preventiva, proposto pela CONTRATADA e aprovado pelo CAU/BR, no período de até 30 (trinta) dias após a assinatura do contrato;
4.4.5. Atualizar a documentação da infraestrutura de TI do CAU/BR;
4.4.6. Definir e implantar os critérios, permissões, procedimentos e planos para manter, administrar, gerenciar e evoluir a plataforma de TIC do CAU/BR;
4.4.7. Participar de reuniões e atividades do CAU/BR que demandem o apoio da área de informática, interagindo com as áreas do CAU/BR e atendendo suas demandas por meio da alocação de profissionais qualificados;
4.4.8. Respeitar as políticas e acordos de nível de serviço vigentes no CAU/BR;
4.5. Suporte técnico remoto (em primeiro nível) e on-site (em segundo nível), conforme descrito abaixo, para os servidores, dispositivos e serviços de rede fornecidos ao CAU/BR;
4.5.1. Os serviços de suporte e de atendimento somente poderão ser realizados por técnicos especializados da CONTRATADA ou por esta autorizados, sob pena de responder por perdas e danos causados aos equipamentos/sistema durante o período de vigência do contrato.
4.5.2. Os serviços de suporte contemplam o funcionamento adequado dos produtos componentes da solução fornecida, o direito aos patches de correção, e apoio na atualização das versões, pelo período de vigência do contrato.
4.5.3. Os serviços de suporte incluem atender solicitações de suporte técnico relacionados a problemas, erros apresentados e forma de utilização da solução fornecida, e correções necessárias para o restabelecimento de suas funcionalidades.
4.6. Os atendimentos e o suporte técnico para quaisquer assuntos pertinentes ao objeto desta licitação deverão ser prestados via e-mail, telefone ou acesso remoto, e deverão ser iniciadas pela CONTRATADA em até 30 (trinta) minutos a contar da data e hora de abertura do chamado, em horário comercial, de segunda-feira a sexta-feira, das 8h00 às 19h00. Quando comprovada a necessidade de intervenção presencial, os atendimentos deverão ser

prestados pela CONTRATADA na sede do CAU/BR, sem nenhum ônus adicional, e sem limite de número de chamados.
4.6.1. Os serviços de suporte incluem prestar informações e orientações necessárias à utilização e ao perfeito funcionamento da infraestrutura fornecida, incluindo hardware, software e serviços;
4.6.2. As chamadas de suporte terão origem em decorrência de qualquer problema verificado pelo CONTRATANTE no tocante ao pleno funcionamento da solução CONTRATADA;
4.6.3. Quando necessária a retirada para reparos ou qualquer outro motivo de algum equipamento fornecido como serviço pela CONTRATADA ao CAU/BR, a CONTRATADA deverá disponibilizar para uso do CAU/BR, durante o período em que o equipamento estiver em manutenção, outro de capacidade igual ou superior, evitando a interrupção dos serviços de rede;
4.6.4. A CONTRATADA deverá prover e disponibilizar acesso para a CONTRATANTE ao sistema de abertura de chamados, de forma que o CAU/BR possa registrar e acompanhar o andamento de seus chamados por meio deste sistema, via Internet.

CAPÍTULO 5. DO GERENCIAMENTO DE ATIVOS DE REDE E DOS *APPLIANCES* DE SEGURANÇA DO CAU/BR
5.1. A CONTRATADA deverá prover e disponibilizar acesso para o CAU/BR a sistema de monitoramento dos ativos, servidores e serviços de rede, em regime ininterrupto (24 horas, 7 dias por semana), com emissão de relatórios e alertas para falhas ou sobrecarga de utilização, conforme descrito a seguir:
5.1.1. Deverá gerar relatórios diários, semanais e mensais, contendo informações pré-configuradas, tais como desempenho dos elementos existentes nos ativos monitorados, conforme descritos no Anexo I - F deste Termo de Referência.
5.2. Deverá possuir sistema de alerta automatizado que permita informar por meio de SMTP (e-mail) quando ocorrer eventos críticos, ou pré-configurados.
5.3. Deverá gerar alerta de ocorrência de:
5.3.1. Alta utilização de memória;
5.3.2. Alta utilização do processador;
5.3.3. Alta utilização das interfaces de rede;
5.3.4. Alta utilização do disco do ativo de rede;
5.3.5. Indisponibilidade de ativo de rede;
5.3.6. Indisponibilidade de determinado serviço do ativo;
5.3.7. Alto número de processos;
5.3.8. Alto número de utilização de memória de um determinado processo;
5.3.9. Alto número de utilização de CPU de um determinado processo;
5.3.10. Alto número de *ARPs* na tabela de *ARP* dos ativos de rede;
5.4. Possibilitar geração de tela de resumo do sistema de monitoramento, mostrando número de notificações na semana, estado de ativos e serviços, disponibilidade de ativos, dados de licença e dados de ultima coleta;

CAPÍTULO 6. DOS SERVIÇOS DE INSTALAÇÃO, CONFIGURAÇÃO E TREINAMENTO DA SOLUÇÃO E DOS PRAZOS DE ENTREGA
6.1. A Contratada deverá efetuar:
6.1.1. Instalação e configuração de toda a solução fornecida, incluindo montagem no “rack” de equipamentos na sede do CAU/BR e dos dispositivos Wireless nas salas onde ficarão em funcionamento.
6.1.2. Integração do firewall ao *MS-AD*, e criação de políticas de segurança de domínio (*GPO*)
6.1.3. Reorganização de contas de usuários e suas associações aos grupos.
6.1.4. Revisão e configuração/reconfiguração de permissionamento de pastas de servidores.
6.1.5. Criação das *GPO*:

6.1.5.1. *Login-scripts*
6.2. Fornecimento, durante a vigência do contrato, dos serviços de garantia:
6.2.1. De software e de atualizações de versões durante o período do contrato para toda a solução fornecida;
6.2.2. A CONTRATADA obriga-se a substituir, sem ônus para o CONTRATANTE, todas as partes ou peças defeituosas, salvo quando o defeito for provocado por uso inadequado dos equipamentos, devidamente comprovado.
6.3. Fornecimento de treinamento para operação da solução para a equipe de TI do CAU/BR:
6.3.1. Treinamento para 5 (cinco) pessoas em toda a solução oferecida, em Brasília - DF, a ser realizado nas instalações do CAU/BR;
6.3.2. Fornecimento dos materiais apropriados e necessários para os treinamentos, para todos participantes.
6.4. Fornecimento de documentação da solução e do projeto de rede contendo no mínimo:
6.4.1. Topologia Física e Lógica;
6.4.2. Plano de endereçamento IP;
6.4.3. Plano de nomenclatura de rede;
6.4.4. Definição dos serviços de rede, identificando a distribuição dos serviços por servidor;
6.4.5. Plano de *backup*;
6.4.6. Plano de manutenção preventiva da rede LAN do CAU/BR, incluindo *check-lists* e especificação de procedimentos;
6.4.7. Procedimentos de administração e gerência;
6.4.8. Todos os serviços de infraestrutura de rede, bem como todos os itens descritos neste Termo de Referência devem ser passivos de remoção e reinstalação na possibilidade de alteração da sede física do CAU/BR (sede própria em Brasília), garantindo no mínimo os mesmos níveis de disponibilidade e funcionalidade. Tal mudança deve ser realizada pela equipe da CONTRATADA, em tempo hábil e definido e formalizado em conjunto com a Coordenadoria de TI do CAU/BR.
6.5. O prazo máximo de entrega dos equipamentos e serviços será de 15 (quinze) dias, a contar da comunicação do CAU/BR.
6.6. A CONTRATADA deverá arcar com todos os custos referentes ao fornecimento, instalação e atualização dos softwares e hardwares, transporte e tudo o mais que for necessário ao cumprimento do objeto.
6.7. O local de prestação dos serviços e eventuais entregas de equipamentos será na Sede do CAU/BR, em Brasília-DF, observando-se o disposto no item 6.4.10 deste Termo de Referência.

CAPÍTULO 7. REQUISITOS OBRIGATÓRIOS DO HARDWARE

7.1. Os componentes de hardware que farão parte da solução ofertada deverão ser fornecidos pela empresa CONTRATADA, em comodato, e não serão de propriedade do CAU/BR.

CAPÍTULO 8. CONDIÇÕES PARA PARTICIPAR DA LICITAÇÃO

8.1. DAS CONDIÇÕES E VEDAÇÕES

8.1.1. Poderão participar do certame licitatório os interessados que atenderem a todas as exigências estabelecidas e que estiverem previamente credenciados no Sistema de Cadastramento Unificado de Fornecedores (SICAF) e perante o sistema eletrônico provido pela Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão (SLTI), por meio do sítio www.comprasnet.gov.br, não sendo admitida, seja a que título for, a participação de dirigentes, conselheiros e colaboradores do CAU/BR, inclusive familiares, na forma prevista no art. 7º do Decreto nº 7.203, de 2010.

8.1.1.1. Para ter acesso ao sistema eletrônico, os interessados em participar deste Pregão deverão dispor de chave de identificação e senha pessoal, obtidas junto à SLTI, onde também deverão informar-se a respeito do seu funcionamento e regulamento e receber instruções detalhadas para sua correta utilização/.
8.1.1.2. O uso da senha de acesso pelo licitante é de sua responsabilidade exclusiva, incluindo qualquer transação por ele efetuada diretamente, ou por seu representante, não cabendo ao provedor do sistema ou ao CAU/BR responsabilidade por eventuais danos decorrentes do uso indevido da senha, ainda que por terceiros.
8.1.2. Não poderão participar deste Pregão:
8.1.2.1. Empresário suspenso de participar de licitação e impedido de contratar com o CAU/BR, durante o prazo da sanção aplicada.
8.1.2.2. Empresário declarado inidôneo para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação.
8.1.2.3. Empresário impedido de licitar e contratar com o CAU/BR, durante o prazo da sanção aplicada.
8.1.2.4. Sociedade estrangeira não autorizada a funcionar no País.
8.1.2.5. Empresário cujo estatuto ou contrato social não inclua o objeto deste Pregão.
8.1.2.6. Empresário que se encontre em processo de dissolução ou recuperação judicial.
8.1.2.7. Sociedades integrantes de um mesmo grupo econômico, assim entendidas aquelas que tenham diretores, sócios ou representantes legais comuns, ou que utilizem recursos materiais, tecnológicos ou humanos em comum, exceto se demonstrado que não agem representando interesse econômico em comum.
8.1.2.8. Consórcio de empresa, qualquer que seja sua forma de constituição, por se tratar execução de objeto que envolve a prestação de trabalho não eventual por pessoas físicas, com relação de subordinação ou dependência, em face da CONTRATANTE, conforme redação dada pelo Decreto nº 57.159/2011.
8.1.3. A participação na licitação importa em total e irrestrito conhecimento e submissão às condições estatuídas neste Edital.
8.1.4. O descumprimento de qualquer condição de participação acarretará a inabilitação do licitante.

8.2. DA QUALIFICAÇÃO ECONÔMICO-FINANCEIRA
8.2.1. Os licitantes deverão apresentar balanço patrimonial do último exercício social exigível, apresentado na forma da lei.
8.2.2. Deverá ser apresentada certidão negativa de feitos sobre falência, recuperação judicial ou recuperação extrajudicial, expedida pelo distribuidor da sede da licitante.
8.2.3. Os documentos exigidos para fins de qualificação econômico-financeira deverão comprovar o seguinte:
8.2.3.1. Índices de Liquidez Geral (LG), Liquidez Corrente (LC) e Solvência Geral (SG) superiores a 1.
8.2.3.2. Capital Circulante Líquido (CCL) ou Capital de Giro (Ativo Circulante – Passivo Circulante) de, no mínimo, 8,33% (oito inteiros e trinta e três centésimos por cento) do valor estimado para a contratação.
8.2.3.3. Patrimônio Líquido igual ou superior a 10% (dez por cento) do valor estimado para a contratação.
8.2.4. É vedada a substituição do Balanço Patrimonial por balancetes ou balanços provisórios. Caso o exercício financeiro anterior ao da licitação esteja encerrado há mais de 3 (três) meses da data da sessão pública de abertura deste Pregão, o Balanço Patrimonial poderá ser atualizado por índices oficiais.

8.3. DA REGULARIDADE FISCAL E TRABALHISTA

8.3.1. A habilitação das licitantes será verificada por meio do SICAF (habilitação parcial) e da documentação complementar especificada neste Edital.
8.3.2. As licitantes que não atenderem às exigências de habilitação parcial no SICAF deverão apresentar documentos que supram tais exigências, quais sejam:
8.3.2.1. Comprovantes de Inscrição no Cadastro Nacional da Pessoa Jurídica do Ministério da Fazenda (CNPJ/MF).
8.3.2.2. Provas de inscrição no cadastro de contribuintes estadual ou municipal, se houver, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual.
8.3.2.3. Certificados de Regularidade perante o Fundo de Garantia por Tempo de Serviço, emitido pela Caixa Econômica Federal.
8.3.2.4. Certidão Negativa de Débitos perante o Instituto Nacional do Seguro Social.
8.3.2.5. Provas de Regularidade para com as Fazendas Federal, Estadual ou do Distrito Federal e Municipal.
8.3.2.6. Prova de Regularidade trabalhista por meio de apresentação da Certidão Negativa de Débitos Trabalhistas.
8.3.3. Realizada a habilitação parcial no SICAF, serão verificados outros eventuais descumprimentos, mediante consulta ao:
8.3.3.1. SICAF, a fim de verificar a composição societária das empresas e certificar eventual participação indireta que ofenda ao art. 9º, III, da Lei nº 8.666/93;
8.3.3.2. Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa, mantido pelo Conselho Nacional de Justiça – CNJ, no endereço eletrônico www.cnj.jus.br/improbidade_adm/consultar_requerido.php;
8.3.3.3. Cadastro Nacional das Empresas Inidôneas e Suspensas – CEIS, no endereço eletrônico www.portaldatransparencia.gov.br/ceis.
8.3.4. As consultas previstas na Condição anterior realizar-se-ão em nome da sociedade empresária licitante e também de eventual matriz ou filial e de seu sócio majoritário.
8.3.5. Efetuada a verificação referente ao cumprimento das condições de participação no certame, a habilitação das licitantes será realizada mediante a apresentação da seguinte documentação complementar, para fins de comprovação de regularidade trabalhista: Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão 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, tendo em vista o disposto no art. 3º da Lei nº 12.440, de 7 de julho de 2011.

8.4. DAS DECLARAÇÕES
8.4.1. Declaração que cumpre plenamente os requisitos exigidos para habilitação e sujeita-se aos termos e condições da licitação.
8.4.2. Declaração de não possuir em seu quadro de pessoal empregado menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e menor de 16 (dezesseis) anos em qualquer trabalho, salvo na condição de aprendiz a partir de 14 (quatorze) anos.
8.4.3. Declaração do proponente que não está suspenso do direito de licitar e não tenha sido declarado inidôneo por qualquer órgão ou entidade do Governo Federal, Estadual ou do Distrito Federal e Municipal.

8.5. DA HABILITAÇÃO JURÍDICA
8.5.1. Registro comercial, no caso de empresa individual.
8.5.2. Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, em se tratando de sociedades comerciais, e, no caso de sociedades por ações, acompanhado dos documentos de eleição de seus administradores. Havendo alterações ou consolidações, estas deverão acompanhar os demais documentos.
8.5.3. Tratando-se de sociedade cooperativa, serão exigidos ainda:

8.5.3.1. Ata de fundação.
8.5.3.2. Comprovante de registro na Organização das Cooperativas Brasileiras ou na entidade estadual, se houver, conforme art. 107 da Lei nº 5.764/1971.
8.5.3.3. O resultado da última auditoria contábil-financeira da cooperativa, conforme dispõe o art. 112 da Lei nº 5.764, de 1971, ou uma declaração, sob as penas da lei de que tal auditoria não foi exigida pelo órgão fiscalizador.
8.5.3.4. Relação dos cooperados que atendem aos requisitos técnicos exigidos para a contratação e que executarão o objeto, respeitado o disposto nos artigos. 4º, XI, 21, I e 42, §§ 2º a 6º da Lei nº 5.764, de 1971.
8.5.3.5. Declaração de regularidade de situação do contribuinte individual – DRSCI de cada um dos cooperados relacionados.
8.5.4. Decreto de autorização, devidamente publicado, em se tratando de empresa ou sociedade estrangeira em funcionamento no país e ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir.
8.5.5. Inscrição do ato constitutivo, no caso de sociedades civis, acompanhada de prova de investidura ou nomeação da diretoria em exercício.
8.5.6. No caso de o licitante ser microempresa ou empresa de pequeno porte, deverá apresentar certidão ou declaração de enquadramento no citado regime.
8.5.7. Cédula de identidade ou equivalente do(s) representantes legais.

8.6. DA QUALIFICAÇÃO TÉCNICA
8.6.1. Apresentar um ou mais atestados de Capacidade Técnica, fornecido por pessoa jurídica de direito público ou privado, comprovando que a empresa licitante executou a prestação de serviço compatível, em características, quantidades e prazo de no mínimo 12 (doze) meses, com o objeto descrito no termo de referência, bem como capacidade de prestar serviços de instalação, configuração e/ou suporte técnico.
8.6.2. O atestado deverá possuir informações suficientes para qualificar o seu objeto, bem como possibilitar ao CONTRATANTE confirmar sua veracidade junto à instituição emissora do atestado.
8.6.3. Será admitido o somatório de atestados técnicos, desde que pelo menos um deles corresponda ao período de 12 (doze) meses especificado no item 8.6.1.
8.6.4. O(s) atestado(s) deverá(ão) comprovar explicitamente a experiência e capacidade de realização em relação aos seguintes itens:
8.6.4.1. Segurança;
8.6.4.2. Firewall de rede;
8.6.4.3. Firewall WAF;
8.6.4.4. Antivírus;
8.6.4.5. Wireless e controle de acesso;
8.6.4.6. *Backup;*
8.6.4.7. VPN;
8.6.4.8. Suporte técnico gerenciado;
8.6.4.9. Administração e gestão de redes;
8.6.4.10. Suporte técnico nos serviços *MS-AD, DNS, File Server, DHCP, WSUS.*
8.7. A CONTRATADA deverá apresentar declaração ou certificado do fabricante dos equipamentos e softwares utilizados para a prestação do serviço, comprovando que é parceiro autorizado e que possui competência técnica para implantar o serviço.
8.8. A CONTRATADA deverá comprovar ter no mínimo 01 (um) profissional com exigência de certificação ou treinamento oficial do fabricante na(s) ferramenta(s) ofertada(s), comprovando que o profissional é certificado pelo fabricante dos equipamentos da solução ofertada e com vínculo empregatício, contratual ou sociedade do profissional indicado com a empresa CONTRATADA.

8.9. O CAU/BR poderá, a seu exclusivo critério, efetuar diligências para verificação da veracidade das informações, incluindo visita ao local do data center.

CAPÍTULO 9. DAS OBRIGAÇÕES DA CONTRATADA

9.1. Desenvolver e apresentar planejamento da instalação, indicando as atividades que serão realizadas, incluindo:
9.1.1. Definição/requisitos de redes e seus componentes;
9.1.2. Montagem e instalação física dos equipamentos da solução, instalação no rack (firewall) e nos tetos dos andares (acesso points) de acordo com as recomendações do fabricante, conexões lógicas e elétricas e testes de funcionamento, atualizações de software, patches, drivers e firmwares para suas versões mais recentes;
9.1.3. Customização e operacionalização de todos os equipamentos envolvidos;
9.1.4. Apresentar testes de funcionamento;
9.1.5. Executar o processo de integração dos equipamentos com os atualmente em operação, fazendo a devida compatibilidade técnica-operacional, garantindo desta forma que o ambiente atual possa ser integrado plenamente ao novo. Qualquer problema ou incompatibilidade deverá ser resolvido pela CONTRATADA;
9.1.6. A CONTRATADA será eximida da aplicação das sanções administrativas para os respectivos chamados em que sejam descumpridos os tempos de solução, desde que comprovadas as seguintes situações:
9.1.6.1. Quando constatado que o problema está relacionado a *"bug"* no produto e que o fabricante não possui uma correção imediata para tal, sendo este fato declarado pelo próprio;
9.1.6.2. Uma vez constatado a necessidade de escalar o problema para o suporte do Fabricante, a CONTRATADA deverá notificar a CONTRATANTE da necessidade e consequentemente, monitorar e gerenciar os chamados abertos;
9.1.6.3. Quando a CONTRATADA tomou todas as medidas possíveis visando providenciar solução de contorno.
9.2. Devem ser contempladas na proposta, obrigatoriamente e sem custos adicionais para o CAU/BR, os custos das licenças, atualizações, a administração, ativos de rede e configuração serviços, a migração dos serviços atuais e a execução das rotinas de *backup* e *restore* durante a vigência do contrato, bem como repositório de armazenamento das cópias de segurança realizadas em disco, disco virtual ou unidade LTO.

9.3. Solução de Hardware e Software

9.3.1. A CONTRATADA é responsável pela manutenção preventiva e corretiva dos equipamentos por ela ofertados e pelo fornecimento de subscrição dos softwares ofertados durante a vigência do contrato (atualização de versões e releases).

9.4. Implantação das Soluções

9.4.1. A CONTRATADA deverá elaborar um projeto de implantação, em conjunto com as áreas técnicas do CAU/BR, onde deverão constar:
a) Desenho da solução (topologia, configurações de rede, endereçamentos IP etc.);
b) As atividades de migração e preparação do ambiente, customização, testes e implantação;
c) Para cada atividade detectada deve ser identificado o responsável pela mesma;
d) O cronograma de implantação.
9.4.2. As regras de segurança implementadas na solução deverão atender à política de segurança do CAU/BR.
9.4.3. Os procedimentos operacionais deverão atender às necessidades do CAU/BR;
9.4.4. A implantação da solução deverá ser realizada pela CONTRATADA, podendo todas as atividades envolvidas serem acompanhadas e coordenadas por analistas e técnicos do CAU/BR;
9.4.5. A coordenação dos trabalhos será feita pela CORTI do CAU/BR.

9.4.6. A implantação da solução será realizada no ambiente de produção, portanto, se necessário, as atividades deverão ocorrer após o expediente (horários noturnos ou em finais de semana e feriados, a critério do CAU/BR).
9.4.7. Para implantação dos serviços, o CAU/BR irá definir equipe que poderá acompanhar e interagir com a equipe da CONTRATADA.
9.4.8. Na conclusão, o CAU/BR emitirá o respectivo Termo de Recebimento Provisório, e após 15 (quinze) dias consecutivos de funcionamento, emitirá o respectivo Termo de Recebimento Definitivo.
9.4.9. Após a implantação de toda a solução, a CONTRATADA deverá entregar ao CAU/BR relatório contendo:
a) Especificação dos servidores virtuais e suas configurações (quando houver);
b) Especificação dos produtos instalados (nome do produto, versão e fabricante);
c) Políticas e regras implementadas;
d) Demais informações necessárias para documentação da solução implantada.
9.4.9.1 Esta documentação deverá ser entregue no prazo de até 45 (quarenta e cinco) dias, contados do aceite definitivo de cada implantação.

9.5. Prestação dos Serviços
9.5.1. Características exigidas dos serviços de Manutenção Preventiva, Evolutiva e Corretiva
9.5.1.1. Manutenção Preventiva – A CONTRATADA deverá efetuar, durante toda vigência do contrato, manutenção preventiva destinada a reduzir a probabilidade de falha ou de degradação do funcionamento da rede, executando rotinas periódicas de manutenção preventiva.
9.5.1.2. A CONTRATADA deverá elaborar um Plano de Manutenção Preventiva, especificando os itens a serem verificados e sua respectiva periodicidade, indicando o cronograma/agenda de realização.
9.5.1.3. A agenda de manutenção preventiva deverá estar cadastrada no Portal de Serviços gerando os *Tickets* de manutenção preventiva, com no mínimo 1 (um) mês de antecedência.
9.5.1.4. Independentemente da agenda prevista, o CONTRATANTE poderá solicitar à CONTRATADA, a qualquer tempo, execução de atividades de manutenção preventiva
9.5.1.5. Fazem parte da relação mínima de itens a serem executados e/ou verificados: ajustes às especificações do fabricante, manutenção do bom estado de conservação dos equipamentos, configurações necessárias com objetivo de atualização dos equipamentos, execução de rotinas de testes padronizados e verificação da existência de danos físicos no equipamento, entre outras ações que garantam a operacionalidade dos equipamentos, sem fornecimento de peças, licenças de softwares, mídias, e sem apresentar qualquer ônus adicional para o CONTRATANTE.
9.5.1.6. As atividades de manutenção Preventiva deverão estar registradas no Portal de Serviços e seus registros deverão compor os relatórios periódicos a serem emitidos pela CONTRATADA.
9.5.1.7. A CONTRATADA deverá realizar, no mínimo, 1 (uma) visita mensal para execução de rotinas de manutenção preventiva, nos seguintes componentes:
a) Todos os componentes de hardware e software fornecidos pelo CONTRATANTE (tais como, mas, não limitando-se a: Firewall, módulos de software, equipamentos de ponto de acesso sem fio, sistemas de monitoramento).
b) Servidores e ativos de rede do CAU/BR, físicos ou virtuais, conforme relação apresentada no Capitulo 3.
9.5.1.8. A CONTRATADA deverá executar todas as rotinas e procedimentos necessários para verificar e prevenir falhas, em conformidade com as recomendações e boas práticas divulgadas pelos fabricantes.

9.5.1.9. Independentemente do disposto no parágrafo anterior, fazem parte da pauta de atividades das visitas de manutenção preventiva – no mínimo – as seguintes atividades da rede LAN/WAN do CAU/BR:
a) Verificação de atualização dos softwares e componentes de softwares (patch Management).
b) Verificação de inventário de hardware dos ativos contemplados pelos serviços, detectando e informando acréscimos e diminuições em relação à visita anterior.
c) Verificação de inventário de software dos ativos contemplados pelos serviços, detectando e informando acréscimos e diminuições em relação à visita anterior.
d) Análise dos logs de sistema, aplicações e de segurança dos servidores do CAU/BR.
e) Análise de integridade do sistema de diretórios, incluindo:
I) Estado das bases de dados do serviço de autenticação;
II) Estado da replicação das bases de dados de autenticação;
III) Verificação de existência de contas de usuários inativas há mais de 7 dias.
f) Coleta de indicadores de gestão, contemplando no mínimo:
I) Quantidade de hosts total;
II) Quantidade de hosts com antivírus instalado;
III) Quantidade de hosts com antivírus atualizado;
IV) Índice de disponibilidade de servidores e serviços de rede;
V) Estatísticas de sucesso e fracasso de Jobs de *backup*.

9.5.1.2. Manutenção Evolutiva
9.5.1.2.1. A CONTRATADA deverá efetuar, durante toda vigência do contrato, manutenção evolutiva destinada a atualizar periodicamente os softwares e firmwares de ativos em funcionamento na rede do CONTRATANTE, inclusive aqueles fornecidos pela CONTRATADA, com objetivo de diminuir vulnerabilidades e manter o ambiente compatível com as especificações mais atuais.

9.5.1.3. Manutenção Corretiva
9.5.1.3.1. A CONTRATADA deverá efetuar manutenção corretiva nos componentes objeto dos serviços deste certame sempre que estes apresentem problemas ou falhas que impeçam o seu funcionamento normal e/ou requeiram a intervenção de técnico especializado, com o objetivo de reestabelecer o pleno funcionamento da rede e de seus serviços.
9.5.1.3.2. Os serviços de manutenção corretiva deverão obedecer, no mínimo, as seguintes características:
9.5.1.3.2.1. Fazem parte da relação de componentes cobertos pelos serviços de manutenção corretiva, os itens de software relacionados a servidores e ativos de rede do CAU/BR, físicos ou virtuais, conforme relação apresentada no Capítulo 3;
9.5.1.3.2.2. Os serviços de manutenção corretiva incluem substituição de equipamentos e/ou peças e/ou suprimentos em equipamentos de propriedade da CONTRATADA;
9.5.1.3.2.3. Os serviços de manutenção corretiva não contemplam substituição de peças e/ou suprimentos em equipamentos de propriedade do CONTRATANTE.
9.5.1.3.3. Nos casos em que as atividades de manutenção corretiva provoquem interrupção de funcionamento em hardware, software ou serviços de rede, o CONTRATANTE deve ser notificado para providenciar a aprovação da manutenção, ou agendar nova data para execução das atividades
9.5.1.3.4. As ferramentas, softwares e/ou equipamentos necessários à manutenção corretiva aplicável ao objeto deste certame serão de responsabilidade da CONTRATADA.

9.6. Requisitos válidos para ferramentas, equipamentos, softwares e componentes a serem fornecidos ou empregados como parte dos serviços contratados:

9.6.1. São requisitos mínimos aplicáveis aos itens fornecidos pela CONTRATADA para prestação dos serviços:
9.6.1.1. Todos os hardwares e/ou softwares devem estar em linha de produção e sendo comercializados pelo Fabricante;
9.6.1.2. Todos os hardwares e/ou softwares devem ser fornecidos com a última versão de software e/ou firmware disponível pelo Fabricante no momento da aquisição;
9.6.1.3. Todos os hardwares e/ou softwares devem vir acompanhados de manuais (em português ou inglês);
9.6.1.4. Todos os hardwares e/ou softwares não podem constar na situação de "final de produção" ("*end of life*") devendo estar em linha de produção, ou seja, sendo produzidos pelo fabricante no momento da proposta;
9.6.1.5. Todos os hardwares e/ou softwares não podem constar na situação de "solicitação de venda encerrada" ("*end of sale*") ou "solicitação de pedido suspensa" ("*end of order*") pelo fabricante no momento da proposta;
9.6.1.6. Caso algum módulo ofertado pela PROPONENTE para este Termo de Referência não esteja disponível no momento da aquisição, o licitante vencedor deve comprovar as mesmas características técnicas mínimas obrigatórias para o item que o substituir;
9.6.1.7. Os seguintes serviços de garantias e de atualizações, aplicáveis aos equipamentos fornecidos pela CONTRATADA, fazem parte do objeto dos serviços:
9.6.1.7.1. Fornecimento de garantia de hardware, contemplando a substituição de peças e – se necessário – de todo o equipamento desde que este seja equivalente ou superior ao instalado nas dependências do CONTRATANTE
9.6.1.7.2. Em caso de necessidade de retirada com substituição provisória descrita no parágrafo anterior, a CONTRATADA se compromete a providenciar solução de contorno dentro dos prazos de nível de serviço estipulados por este Termo de Referência, e fornecer o equipamento de substituição até o final do próximo dia útil subsequente (n*ext business day - NBD*) ao do registro da solicitação.
9.6.1.7.3. Atualizações de versões de software: A aplicação de atualizações que causem impacto (interrupção do serviço ou degradação de performance de funcionamento) deve ser formalmente comunicada previamente pela CONTRATADA e formalmente agendada e autorizada pelo CONTRATANTE.

9.7. Instalações e desinstalações de hardware, software e componentes
9.7.1. São requisitos mínimos aplicáveis aos serviços de instalação prestados pela CONTRATADA:
9.7.1.1. A instalação deverá ser efetuada de forma a não comprometer o funcionamento dos sistemas, recursos ou equipamentos em operação no CONTRATANTE;
9.7.1.2. Havendo necessidade de interrupção de sistemas, recursos, equipamentos ou da rotina dos trabalhos em decorrência da instalação a ser efetuada, esta deverá estar devidamente planejada, agendada e ser necessariamente aprovada pelo CONTRATANTE;
9.7.1.3. Todos os componentes a serem instalados na rede da CONTRATADA deverão ser previamente testados;
9.7.1.4. Obrigatoriamente, a CONTRATADA deverá registrar em seu Portal de Serviços as atividades de instalação e/ou desinstalação;
9.7.1.5. Quando o componente instalado ou desinstalado pertencer à CONTRATADA, esta deverá – além de registrar a atividade no Portal de Serviços - emitir documento, em duas vias iguais, para permitir a atualização dos registros de custódia.

9.8. Atendimento às solicitações de serviço e aos serviços previamente programados
9.8.1. Os serviços de suporte técnico serão solicitados pelo CONTRATANTE, por meio de telefone, via portal de serviços da CONTRATADA e/ou e-mail, por intermédio de seus colaboradores autorizados, previamente informados pelo CONTRATANTE à CONTRATADA.

9.8.2. A CONTRATADA deverá disponibilizar estrutura de atendimento adequada, incluindo número de telefone local em Brasília-DF (ou equivalente de ligação gratuita), para acionamento dos serviços.
9.8.3. A CONTRATADA deverá atender as solicitações do CONTRATANTE em língua portuguesa.
9.8.4. A CONTRATADA fornecerá aos prepostos do CONTRATANTE previamente identificados e autorizados acesso via internet ao seu Portal de Serviços, para registrar, interagir, acompanhar, abrir e encerrar chamados. Os chamados somente poderão ser encerrados pela CONTRATANTE.
9.8.5. O Portal de Serviços da CONTRATADA deverá permanecer disponível para acesso pelo CONTRATANTE via Internet initerruptamente, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.
9.8.6. A CONTRATADA deverá registrar todas as solicitações de serviço em seu Portal de Serviços, comprometendo-se a manter registros dos mesmos durante toda a vigência do contrato.
9.8.7. Para cada atendimento realizado, a CONTRATADA deverá registrar um *"Ticket*" em seu Portal de Serviços (*Service-Desk*), contendo o número do protocolo, a data e hora do registro do chamado, bem como histórico das providências adotadas, e demais informações relevantes e pertinentes.
9.8.8. Ao receber uma ligação para um chamado já aberto, o atendente da CONTRATADA deverá solicitar o número que lhe foi atribuído por ocasião da abertura (para solicitações anteriores), registrar as novas informações passadas e transmiti-las ao técnico responsável pelo acompanhamento e resolução.
9.8.9. Quando solucionados, os chamados serão fechados pela equipe do CONTRATANTE, ou poderão ser fechados pela CONTRATADA em comum acordo com o CONTRATANTE, não sendo admitido, em nenhuma hipótese, o fechamento de chamados sem este consentimento.
9.8.10. Os registros de solicitações de serviços de suporte técnico efetuados pelo CONTRATANTE deverão, logo que registradas, estar disponíveis para consultas no Portal de Serviços disponibilizado pela empresa CONTRATADA, durante todo o período de vigência do contrato
9.8.11. O Portal de Serviços deverá permitir a realização de consultas e impressão de relatórios, individualizados ou cumulativos, por número do chamado, fila de atendimento, status, data/período de abertura, pessoa responsável pela abertura, e técnico encarregado do atendimento.
9.8.12. Os serviços de suporte técnico poderão ser prestados pela CONTRATADA inicialmente fora das dependências internas do CONTRATANTE (modalidade remota) e, em caso de necessidade, continuados presencialmente na sede do CONTRATANTE.
9.8.13. No início de cada atendimento, cabe à CONTRATADA agir de acordo com os procedimentos de segurança visando garantir a integridade dos dados e/ou equipamentos de rede envolvidos no respectivo chamado, verificando no mínimo:
9.8.13.1. Certificação de existência de cópias de segurança (*backups*) de arquivos.
9.8.13.2. Cumprimento dos procedimentos de execução estabelecidos pelo CONTRATANTE, quando for o caso.
9.8.13.3. O CONTRATANTE colocará seu ambiente computacional e sua rede de computadores à disposição da CONTRATADA para execução dos serviços de suporte técnico, com acompanhamento de sua equipe e – caso necessário – permitindo para tal fim interrupções de funcionamento de equipamentos e serviços de seu ambiente:
9.8.14. Os técnicos da CONTRATADA, previamente identificados, terão pleno e livre acesso às instalações, e equipamentos, programas, componentes de ambiente e/ou de rede do CONTRATANTE objeto dos serviços deste certame, e também aqueles componentes aos quais estão interligados e/ou integrados, a fim de permitir a realização de diagnósticos, testes

e execução dos serviços de manutenção e suporte, respeitadas as normas de segurança vigentes nas dependências do CONTRATANTE.
9.8.15. A CONTRATADA e o CONTRATANTE sempre agendarão previamente as datas e horários de atividades de manutenção preventiva e evolutiva que impliquem na interrupção dos serviços de rede.
9.8.16. A CONTRATADA garante que, para a execução eficaz e eficiente dos serviços objeto desse contrato, somente pessoal capacitado, devidamente treinado e habilitado, será encarregado e responsável pelo atendimento técnico.
9.8.17. Os Serviços de Suporte Técnico serão prestados em dias úteis, durante o horário comercial (de 08h00 às 18h00).
9.8.18. Os serviços de Suporte Técnico objeto deste certame serão solicitados pelo CONTRATANTE à CONTRATADA nestes mesmos dias e horários.
9.8.19. O CONTRATANTE poderá solicitar os serviços quantas vezes entender necessário, não havendo limites ou franquias de quantidades para as solicitações dos serviços.

9.9. Acompanhamento e Controle da Execução
9.9.1. Tanto a CONTRATANTE quanto a CONTRATADA designarão, no mínimo, 1 (um) representante de seus respectivos quadros de colaboradores para acompanhar e fiscalizar a entrega dos serviços.
9.9.1.1. São atribuições do Representante da CONTRATADA:
9.9.1.1.1. Tratar, junto ao CONTRATANTE, termos e condições complementares a este documento para a realização dos serviços;
9.9.1.1.2. Gerenciar e supervisionar a execução dos serviços, franqueando ao CONTRATANTE, a qualquer tempo, o acesso a seus registros, para efeito de acompanhamento e fiscalização de serviços técnicos efetivamente utilizados;
9.9.1.1.3. Tratar com o CONTRATANTE questões relevantes a sua execução e providenciar a regularização de falhas ou defeitos observados;
9.9.1.1.4. Providenciar a entrega de todos os produtos, documentação, relatórios técnicos e outros documentos referentes ao objeto deste Termo de Referência;
9.9.1.1.5. Acompanhar e controlar as atividades do serviço da equipe da CONTRATADA, visando garantir o atendimento dentro dos níveis de serviço acordados;
9.9.1.1.6. Acompanhar, controlar e avaliar a produção dos profissionais que prestam os serviços, monitorando reclamações, alocando profissionais para execução dos serviços, considerando as prioridades e prazos estabelecidos;
9.9.1.1.7. Dimensionar adequadamente os recursos sob sua gestão visando atender os níveis de serviço acordados e a demanda presente ou expectativa futura;
9.9.1.1.8. Suprir os profissionais envolvidos de informações e recursos logísticos e tecnológicos, necessários à realização dos serviços;
9.9.1.1.9. Repassar orientações recebidas do CONTRATANTE e inseri-las na rotina de operações;
9.9.1.1.10. Participar de apresentações programadas pelo CONTRATANTE sobre mudanças efetuadas ou programadas em serviços ou processos atendidos pelo serviço e repassá-las aos profissionais sob sua responsabilidade;
9.9.1.1.11. Efetuar levantamentos históricos e emitir relatórios estatísticos sobre a prestação de serviço para análise pelo Gestor do Contrato;
9.9.1.1.12. Analisar, de forma quantitativa e qualitativa, as estatísticas dos processos operacionais, propondo, quando necessário, mudanças nos processos internos;
9.9.1.1.13. Informar a ocorrência de incidentes generalizados ou de grande impacto, reclamações e sugestões para serem repassadas ao CONTRATANTE;
9.9.1.1.14. Garantir a boa utilização e conservação dos recursos de infraestrutura tecnológica e de ambiente físico disponíveis aos profissionais sob sua coordenação;

9.9.1.1.15. Garantir a adequação da apresentação e da postura profissional, vocabulário, disciplina, respeito, regras de conduta e cordialidade na prestação do serviço;
9.9.1.1.16. Identificar e reportar ao CONTRATANTE a necessidade de adequação da infraestrutura física necessária para a prestação dos serviços;
9.9.1.1.17. Apresentar propostas de melhoria, correção e ajuste dos serviços.
9.9.1.1.18. Representar a CONTRATADA administrativamente, realizar coordenação operacional da execução dos serviços e pela interlocução com o representante da CONTRATANTE.
9.9.1.2. São atribuições do Representante do CONTRATANTE:
9.9.1.2.1. Tratar, junto à CONTRATADA, termos e condições complementares a este documento para a realização dos serviços;
9.9.1.2.2. Suprir os profissionais envolvidos de informações e recursos logísticos e tecnológicos, necessários à realização dos serviços;
9.9.1.2.3. Repassar orientações recebidas da CONTRATADA e inseri-las na rotina de operações;
9.9.1.2.4. Participar de apresentações programadas pela CONTRATADA sobre mudanças efetuadas ou programadas em serviços ou processos atendidos pelo serviço e repassá-las aos profissionais sob sua responsabilidade;
9.9.1.2.5. Informar a ocorrência de incidentes generalizados ou de grande impacto, reclamações e sugestões para serem repassadas à CONTRATADA;
9.9.1.2.6. Garantir a boa utilização e conservação dos recursos de infraestrutura tecnológica e de ambiente físico necessárias ao cumprimento do objeto deste certame sob sua coordenação;
9.9.1.2.7. Providenciar a adequação da infraestrutura física necessária para a prestação dos serviços;
9.9.1.2.8. Analisar e deliberar propostas de melhoria, correção e ajuste dos serviços encaminhadas pela CONTRATADA.
9.9.1.2.9. Representar o CONTRATANTE administrativamente, realizar coordenação operacional da execução dos serviços e pela interlocução com o representante da CONTRATADA.
9.9.1.2.10. O CONTRATANTE poderá solicitar o afastamento de qualquer profissional ou preposto da CONTRATADA que venha causar embaraço à fiscalização ou que adote procedimentos incompatíveis com o exercício das funções que lhe forem atribuídas.
9.9.1.2.11. A existência de fiscalização do CONTRATANTE de nenhum modo diminui ou altera a responsabilidade da CONTRATADA na prestação dos serviços a serem executados;
9.9.2. Deverão ser realizadas, por solicitação tanto do CONTRATANTE quanto da CONTRATADA, reuniões, presenciais ou não, entre o Gestor (CONTRATANTE) e o interlocutor da CONTRATADA para avaliação, acompanhamento, troca de informações e deliberações sobre o(s) serviço(s) prestado(s) no período e verificação do atendimento, bem como planejamento de atividades futuras.
9.9.2.1. As reuniões deverão ser agendadas com – no mínimo – 48 (quarenta e oito) horas de antecedência.

9.10. Estruturação dos Serviços
9.10.1. Os membros da CONTRATADA e do CONTRATANTE deverão trabalhar em colaboração, envidando os seus melhores esforços, com objetivo de atingir os resultados pretendidos pelos serviços objeto deste certame.
9.10.1.1. O objetivo do trabalho em equipe é fazer com que o máximo de solicitações de caráter operacional seja resolvido nesse nível de prestação de serviço, e na impossibilidade disso:

9.10.1.1.1. Minimizar o impacto dos incidentes identificando soluções de contorno, submetendo-as ao CONTRATANTE para homologação e aplicando-as, enquanto não houver soluções definitivas;
9.10.1.1.2. Coletar e registrar informações para agilizar a execução de atividades, o tratamento de assuntos ou incidentes pelos próximos níveis das partes responsáveis.
9.10.1.1.3. As solicitações que não puderem ser tratadas em nível operacional deverão ser encaminhadas aos Gestores do Contrato/prepostos das partes.
9.10.2. A Área de Tecnologia da Informação do CAU/BR será a área demandante dos serviços contratados.
9.10.3. A não realização de uma atividade solicitada pelo CONTRATANTE deverá ser documentada pela CONTRATADA, mediante exposição de motivos, e encaminhada para o Gestor do Contrato, a quem caberá aceitar ou não os motivos alegados. Caso não haja concordância, poderão ser aplicadas penalidades previstas contratualmente.
9.10.4. Não poderão nem deverão ser utilizadas pela CONTRATADA quaisquer ferramentas não licenciadas para uso no CONTRATANTE. Caso se trate de ferramentas baseadas em software livre, a utilização dessas deverá ser aprovada pelo Gestor de Contrato.
9.10.5. A área técnica demandante fiscalizará a execução das atividades solicitadas e/ou previstas. As atividades pendentes não executadas apropriadamente deverão ser alvo de avaliação por parte da área demandante e encaminhadas ao Gestor do Contrato para providências cabíveis;

9.11. Relatórios
9.11.1. A CONTRATADA deverá, mensalmente, elaborar Relatório de Progresso, apresentando-o ao CONTRATANTE até o 10º dia do mês subsequente ao da prestação do serviço. Os relatórios deverão conter, no mínimo:
a) Conteúdo;
b) Indicadores;
c) Periodicidade;
9.11.2. Nos relatórios deverão constar, entre outras informações:
9.11.2.1. Os indicadores/metas de níveis de serviços definidos e os alcançados;
9.11.2.2. Atividades realizadas no período;
9.11.2.3. Recomendações técnicas, administrativas e gerenciais para o próximo período;
9.11.2.4. Registros detalhados dos serviços executados ou em execução, contendo também os seguintes resumos:
9.11.2.4.1. Relação completa dos *Tickets* abertos e seu respectivo estado atual;
9.11.2.4.2. Quantidade de *Tickets* abertos por usuário demandante;
9.11.2.4.3. Quantidade de *Tickets* atendidos por cada técnico da CONTRATADA;
9.11.2.4.4. Quantidade de *Tickets* por status atual;
9.11.2.4.5. Quantidade de *Tickets* por fila de atendimento;
9.11.2.5. Indicadores de *monitoring;*
9.11.2.6. Indicadores de gestão;
9.11.2.7. Os níveis de serviço alcançados, os ajustes eventualmente efetuados, e as mudanças, problemas e indisponibilidades que impactaram os níveis de serviço;
9.11.2.8. Quaisquer outras informações relevantes para a gestão contratual.

9.12. Início da prestação dos serviços
9.12.1. A CONTRATADA deverá iniciar a execução dos serviços, incluindo a instalação de todos os equipamentos necessários, contido no objeto deste Termo de Referência, até 10 (dez) dias úteis após a assinatura do contrato, findo o qual se aplicarão as penalidades contratuais cabíveis.

9.13. Entrega, Avaliação e Recebimento dos Serviços

9.13.1. A CONTRATADA terá 15 (quinze) dias úteis após a assinatura do contrato para efetuar a implantação completa de seus serviços, incluindo a entrega e configuração dos equipamentos e softwares que serão utilizados na prestação dos serviços.
9.13.2. É facultado à CONTRATADA, para cumprir com o prazo definido no parágrafo anterior, implantar provisoriamente equipamentos sobressalentes até o recebimento de equipamentos definitivos, desde que os sobressalentes possuam todas as funcionalidades e sejam de desempenho igual ou superior às especificações deste Edital.
9.13.3. A aceitação dos equipamentos será considerada como de caráter provisório. A aceitação definitiva dar-se-á – uma vez recebidos os equipamentos e componentes definitivos - após verificação do atendimento às especificações técnicas constantes deste Termo de Referência.
9.13.4. Os equipamentos e serviços serão aceitos se e somente se houver comprovação de que todos os requisitos técnicos especificados neste Termo de Referência tenham sido atendidos. Essa comprovação será feita mediante observação direta das características dos equipamentos, conduta à documentação técnica fornecida e verificação dos serviços de instalação e configuração.
9.13.5. O termo de aceite não retira da CONTRATADA a obrigação de trocar qualquer equipamento que apresente algum defeito ou esteja em desconformidade com e especificado no termo após a emissão do aceite
9.13.6. O CONTRATANTE, mensalmente e por meio do Gestor do Contrato, procederá a análise dos relatórios encaminhados pela CONTRATADA em até 5 (cinco) dias, a contar da data de seu recebimento.
9.13.7. Caso os relatórios sejam homologados:
9.13.7.1. A homologação se dará por meio de assinatura do Gestor do Contrato e encaminhamento da Nota Fiscal/Fatura para pagamento (Atesto).
9.13.8. Os serviços de infraestrutura do CAU/BR deverão ser disponibilizados pela CONTRATADA na modalidade 8x5 (oito horas por dia, 5 dias na semana);
9.13.9. O início da prestação dos serviços de manutenção e de suporte técnico se dará quando da emissão do Termo de Recebimento Provisório;
9.13.10. Os softwares ofertados, quando possível, devem sempre estar com a versão mais atual disponível no mercado. A versão anterior não poderá permanecer instalada mais do que 03 (três) meses, após o lançamento da última versão homologada, podendo permanecer instalada por tempo maior, desde que acordado com a CORTI do CAU/BR;
9.13.11. A CONTRATADA deverá interagir com os analistas e técnicos da CORTI do CAU/BR para tirar dúvidas relacionadas ao serviço prestado.

9.14. Manutenção das Regras, Políticas de Segurança e Versões dos Softwares

9.14.1. Toda e qualquer alteração na configuração da solução (aplicação de novas regras, exclusão de regras, atualização de versões, aplicações de “patches” etc.) deve ocorrer mediante autorização formal do CAU/BR e deve ser previamente planejada;
9.14.2. As alterações das configurações deverão sempre ocorrer em horários pré-determinados pelo CAU/BR preferencialmente após as 19:00 horas.

9.15. Controle dos Serviços Realizados pela CONTRATADA

9.15.1. Para o controle e administração dos serviços realizados pela CONTRATADA, o CAU/BR poderá nomear até 06 (seis) representantes autorizados a interagir com a CONTRATADA.
9.15.2. Deverão ocorrer reuniões quando solicitado pelo CAU/BR, para dirimir dúvidas sobre o serviço contratado, análise e entendimento dos relatórios gerenciais e administrativos e revisão das configurações e procedimentos implementados.

9.16. Armazenamento dos registros de Auditoria

9.16.1. Os registros de acesso aos servidores, logs de firewall, IDS, IPS e demais equipamentos de perímetros que componham a solução dos últimos 90 (noventa) dias deverão estar disponíveis para acesso mediante solicitação. Os registros gravados, superiores a 30 (trinta) dias, deverão ser disponibilizados para o CAU/BR em, no máximo, 3 (três) dias úteis, a contar da data da solicitação.

9.17. Ocorrência de Incidentes

9.17.1. No caso de detecção de algum incidente de segurança, a CONTRATADA deverá acionar o CAU/BR imediatamente, para que sejam tomadas as medidas corretivas e necessárias, devendo observar o limite de tempo descrito abaixo:

Incidente	**SLA**
Notificação de Incidentes emergenciais	Até 30 minutos
Iniciar atendimento para correção de problemas, vulnerabilidades e/ou incidentes de segurança	Até 60 minutos

9.17.2. São considerados incidentes de segurança: os acessos indevidos, instalação de códigos maliciosos, negação dos serviços (DoS), ataques por força bruta, ou qualquer outra ação que vise prejudicar a funcionalidade dos serviços do CAU/BR.
9.17.3. As tentativas de acessos indevidos, de instalação de códigos maliciosos, ou de qualquer outra ação que venham pôr em risco a segurança do ambiente do CAU/BR, sem sucesso, mas que seja detectada insistência por parte da pessoa mal-intencionada, a CONTRATADA deverá ser comunicada imediatamente para que possam ser tomadas ações preventivas.
9.17.4. A CONTRATADA deverá disponibilizar no Portal de Acompanhamento de Serviços todas as informações necessárias (origem do ataque, tipo de ataque, data e hora, *logs*, etc.) para que sejam apurados os incidentes de segurança reportados. O CAU/BR deverá informar previamente as pessoas autorizadas a solicitar e obter estas informações.
9.17.5. Dependendo do grau do incidente, a CONTRATADA deverá deslocar recurso técnico capaz de dar suporte ao problema, para compor o Time de Resposta do CAU/BR, visando tirar quaisquer dúvidas e dar suporte nas providências a serem customizadas.
9.17.6. O eventual deslocamento de técnicos para as dependências do CAU/BR, localizadas em Brasília, não deve gerar ônus adicionais para o CONTRATANTE.
9.17.7. O atendimento referido neste item se dará em horário comercial, sendo de segunda a sexta-feira, exceto feriados nacionais, de 08:00 às 18:00hs.

9.18. Segurança e Armazenamento dos dados

9.18.1. A CONTRATADA deverá garantir a segurança e armazenamento dos dados através dos recursos disponibilizados para o atendimento ao cenário proposto, a fim de mitigar a inviolabilidade dos dados e dos serviços prestados.
9.18.2. A inviolabilidade deverá ser garantida no armazenamento, tráfego, e eventual manuseio dos dados, ou seja, durante qualquer intervenção técnica a ser realizada.

9.19. Finalização do Contrato

9.19.1. Ao final do contrato, a CONTRATADA deverá disponibilizar profissionais técnicos com o objetivo de viabilizar a transferência de conhecimento para a equipe do CAU/BR ou para a próxima empresa contratada;
9.19.2. Após a transferência integral do conteúdo e configurações e aceite formal do CAU/BR será emitido um termo atestando a funcionalidade do ambiente.

9.20. Portal de Acompanhamento dos Serviços / Gerência

9.20.1. A CONTRATADA deverá disponibilizar um sistema de monitoramento para verificação da disponibilidade dos serviços e servidores contratados e quando alguma anormalidade for detectada, alertas deverão ser emitidos visualmente e através de uso de sistemas de comunicação como e-mail ou SMS.
9.20.2. A CONTRATADA deverá dispor de sistema para abertura de chamados para atendimento a problemas identificados, solicitações de alteração/implementação de configurações de serviços.
9.20.3. Os sistemas deverão ser acessíveis pela Internet, por intermédio de navegador de internet, utilizando o protocolo HTTP ou HTTPS.
9.20.4. O CAU/BR irá proceder junto à empresa, o credenciamento dos funcionários autorizados a ter acesso ao Portal e a interagir com os técnicos responsáveis pela manutenção dos serviços disponíveis.
9.20.5. A autenticação dos funcionários do CAU/BR no Portal deverá ser realizada por intermédio de credenciais de acesso (nome da conta e senha).
9.20.6. Através do Portal, todos os servidores credenciados pelo CAU/BR poderão ter acesso às seguintes informações e serviços, mediante solicitação por equipe autorizada:
9.20.7. Visualização, recuperação e geração de relatórios a partir dos logs dos serviços disponibilizados;
9.20.8. Visualização detalhada da utilização dos recursos de hardware, bem como relatórios semanais de utilização e tráfego;
9.20.9. Solicitações de informações e serviços gerais.
9.20.10. O Portal deverá estar disponível 7 (sete) dias por semana, 24 (vinte e quatro) horas por dia.
9.20.11. O sistema para abertura de chamados deverá ser capaz de fornecer o acompanhamento de todos os chamados, independentemente da forma pela qual os mesmos foram abertos.
9.20.12. O sistema para abertura de chamados deverá permitir consultas de *Tickets* por período (diário, semanal e mensal), apuração de nível do serviço de atendimento dos chamados (*SLA*), relação de incidentes de segurança e seus devidos tratamentos por parte da CONTRATADA.

9.21. Licenças dos Softwares
9.21.1. Para todas as despesas relacionadas às demandas de softwares que estiverem previstas na solução, sejam elas de qualquer natureza, determina-se que CONTRATADA deverá arcar com todos os custos e deverá licenciar os sistemas operacionais, bancos de dados, softwares necessários para oferta dos serviços e *backup*.
9.21.2. Em relação à atualização destes, a empresa CONTRATADA deverá ser responsável pela atualização das licenças que compõe a solução.

9.22. Resolução de Problemas
9.22.1. Os atendimentos de suporte técnico serão categorizados nos níveis de severidade descritos na tabela abaixo, devendo ter seu atendimento iniciado nos prazos especificados:

Níveis de severidade	Descrição	Prazo para início do atendimento remoto	Prazo para início do atendimento presencial (se necessário)
1	Manutenção Corretiva - Serviços totalmente indisponíveis	30 minutos	60 minutos
2	Manutenção Corretiva - Serviços	30 minutos	120 minutos

	parcialmente indisponíveis		
3	Consultas sobre problemas, dúvidas gerais sobre a execução de configurações, orientações para administração da solução, e demais questionamentos sobre a utilização da solução	4 horas	24 horas
4	Manutenção Evolutiva e Manutenção Preventiva não programada	48 horas	48 horas
5	Atividades de consultoria, Informações, agendamento de atividades, outras	Não se aplica	96 horas

9.23. A CONTRATADA obriga-se, ainda, a:
9.23.1. Adotar todas as providências necessárias para a fiel execução do objeto em conformidade com as disposições deste Termo de Referência, do Edital e do Contrato, prestando o serviço com eficiência, presteza e pontualidade e em conformidade com os prazos e demais condições estabelecidas.
9.23.2. Assumir a responsabilidade pelos encargos fiscais e comerciais decorrentes da prestação dos serviços objeto deste Termo de Referência.
9.23.3. Assumir todas as responsabilidades pelos encargos trabalhistas, previdenciários e fiscais, decorrentes do objeto deste Termo de Referência, observando, inclusive, as Normas Regulamentadoras, eximindo o CAU/BR do estabelecimento de quaisquer vínculos trabalhistas.
9.23.4. O CAU/BR poderá reter pagamentos equivalentes a quantias suficientes à garantia de eventuais indenizações trabalhistas, até o trânsito em julgado das respectivas sentenças, sendo que o licitante ressarcirá o CAU/BR de qualquer despesa que este vier a ser condenado a pagar, uma vez que não haverá qualquer vínculo de emprego do CAU/BR com os colaboradores da CONTRATADA.
9.23.5. Nos valores propostos deverão estar inclusos todos os tributos, taxas e emolumentos, Federais, Estaduais ou do Distrito Federal e Municipais, inclusive encargos sociais, previdenciários, securitários e quaisquer outros que incidam ou venham a incidir sobre o objeto deste Termo de Referência, ficando desde logo estabelecido que o CAU/BR nada deverá quanto a tais encargos vez que já estão incluídos no preço total da contratação.
9.23.6. Garantir que os serviços sejam prestados em conformidade com as exigências do CONTRATANTE.
9.23.7. Acatar as instruções e observações formuladas pela fiscalização, estabelecidas neste Termo de Referência, no contrato e/ou legislação pertinente, ficando, desde logo, ressaltado que a atuação da fiscalização não exime a CONTRATADA de sua total e exclusiva responsabilidade sobre todos os serviços prestados.

CAPÍTULO 10. DAS OBRIGAÇÕES DO CONTRATANTE

10.1. Proporcionar todas as facilidades e prestar as informações e esclarecimentos que venham a ser solicitados pelo licitante e necessários ao desenvolvimento das atividades relativas às obrigações assumidas.
10.2. Pagar os valores correspondentes à remuneração do objeto do contrato pactuados neste Termo de Referência.
10.3. Acompanhar e fiscalizar o objeto deste Termo de Referência por meio de agente designado, o qual anotará em registro próprio todas as ocorrências constatadas.
10.4. Atestar os documentos fiscais correspondentes aos serviços contratados, quando executados a contento e aceitos.

10.5. Notificar o licitante Contratado, por escrito, sobre imperfeições, falhas ou irregularidades constatadas na prestação dos serviços objeto deste Termo de Referência para que sejam adotadas as medidas corretivas necessárias.
10.6. Manter arquivado, junto ao processo administrativo ao qual está vinculado o presente Termo de Referência, toda a documentação referente à contratação.
10.7. Notificar a CONTRATADA, por escrito, da aplicação de eventuais penalidades, garantindo-lhe o direito ao contraditório e à ampla defesa.

CAPÍTULO 11. DA DOTAÇÃO ORÇAMENTÁRIA
11.1. Os recursos necessários ao atendimento das despesas contratuais, correrão à conta dos recursos orçamentários deste Conselho, estão previstos na **Conta** 6.2.2.1.1.01.04.04.031 - Serviços de Manutenção Sistema de Informática, **Centro de Custo** 4.02.05.001 - Manutenção da Gerência Administrativa. O CAU/BR compromete-se, durante a vigência contratual, a consignar em seu Orçamento as despesas contratuais remanescentes a cada respectivo exercício financeiro que se seguir.

CAPÍTULO 12. DO ACOMPANHAMENTO E FISCALIZAÇÃO
12.1. A execução do contrato será acompanhada e fiscalizada por colaborador que venha a ser designado pelo CAU/BR, compreendendo-se no acompanhamento e na fiscalização:
12.1.1. Supervisionar a prestação dos serviços, garantindo que todas as providências sejam tomadas para regularização de falhas ou defeitos observados;
12.1.2. Levar ao conhecimento do representante da CONTRATADA qualquer irregularidade fora de sua competência;
12.1.3. Exigir da CONTRATADA todas as providências necessárias à boa execução do contrato, anexando aos autos do processo de contratação cópias dos documentos escritos que comprovem as solicitações de providências;
12.1.4. Acompanhar os serviços executados, atestar sua prestação e indicar as ocorrências de indisponibilidade dos serviços contratados;
12.1.5. Encaminhar ao representante legal da CONTRATADA os documentos relacionados às multas aplicadas à CONTRATADA, bem como os referentes a pagamentos;
12.1.6. Verificar a entrega do comprovante de pagamento do Fundo de Garantia do Tempo de Serviço (FGTS), de salários e demais verbas, assim como todos e quaisquer pagamentos no que se refere às obrigações para com os prestadores de serviços designados a trabalhar nas dependências do CAU/BR, inclusive benefícios constantes em norma coletiva.
12.1.7. O acompanhamento e a fiscalização não excluirão a responsabilidade da CONTRATADA nem conferirão ao CAU/BR responsabilidade solidária ou subsidiária, inclusive perante terceiros, por quaisquer irregularidades e/ou informações incorretas na execução dos serviços contratados.
12.1.8. As determinações e as solicitações formuladas pelo representante do CAU/BR, encarregado da fiscalização do contrato, deverão ser prontamente atendidas pela CONTRATADA, ou na impossibilidade, justificada por escrito.

CAPÍTULO 13. DA GARANTIA CONTRATUAL
13.1. Será exigida da CONTRATADA, no prazo máximo de 10 (dez) dias, a partir da assinatura do contrato, prestação de garantia contratual em favor do CAU/BR, correspondente a 5% (cinco por cento) do valor total do contrato, numa das seguintes modalidades:
13.1.1. Caução em dinheiro ou títulos da dívida pública federal.
13.1.2. Seguro-garantia.
13.1.3. Fiança bancária.
13.2. Caso a CONTRATADA opte por apresentar títulos da dívida pública, deverão ter valor de mercado compatível com aquele a ser garantido, preferencialmente em consonância com

as espécies recomendadas pelo Governo Federal, como os previstos no art. 2º da Lei nº 10.179/2001.

13.3. Caso o licitante opte pela caução em dinheiro, deve providenciar o depósito perante instituição financeira indicada pelo CAU/BR, em conta remunerada, para os fins específicos a que se destina, sendo o recibo de depósito o único meio hábil para comprovar essa exigência.

13.4. Se o valor da garantia for utilizado, total ou parcialmente, em pagamento de qualquer obrigação, a CONTRATADA deverá proceder à respectiva reposição no prazo de até 3 (três) dias úteis, contados da data em que for notificado pelo CAU/BR, sob pena de rescisão contratual, multa e responsabilização da CONTRATADA pelos danos eventuais causados ao CAU/BR.

13.5. A garantia será restituída à CONTRATADA após total cumprimento das obrigações pactuadas no contrato, nos termos da legislação vigente.

13.6. A garantia somente será liberada ante a comprovação de que a adjudicatária pagou todas as verbas rescisórias trabalhistas decorrentes da contratação e que, caso esse pagamento não ocorra até o fim do segundo mês após o encerramento da vigência contratual, a garantia será utilizada para o pagamento dessas verbas trabalhistas diretamente pelo CAU/BR.

CAPÍTULO 14. DA ACEITAÇÃO E DO PAGAMENTO

14.1. Os pagamentos serão realizados após a apresentação do documento fiscal exigível em conformidade com a legislação de regência e com eles as informações sobre o banco, agência e número da conta corrente da CONTRATADA.

14.1.1. A CONTRATADA deverá encaminhar o documento fiscal exigível, discriminando todas as importâncias devidas, correspondentes aos serviços efetivamente prestados.

14.1.2. O documento fiscal referido no subitem 14.1 deverá destacar as retenções previstas na Instrução Normativa RFB nº 1.234, de 11 de janeiro de 2012 e demais legislações pertinentes. A retenção também será realizada nos moldes da Lei Complementar nº 116/2003 e outras legislações de regência.

14.1.3. Na hipótese de a CONTRATADA ser optante do Simples, a fim de fazer incidir a não retenção de tributos, conforme art. 4º, XI, da Instrução Normativa RFB nº 1.234/2012, deverá anexar à fatura, declaração devidamente assinada por seu representante legal, sob as penas da lei.

14.2. Recebido o documento fiscal exigível, o CAU/BR providenciará sua aferição e, após aceitação dos serviços prestados, efetuará o pagamento no prazo de 10 (dez) dias úteis, contados da apresentação da respectiva nota fiscal/fatura.

14.3. O atraso no pagamento do documento fiscal emitido, desde que a CONTRATADA não tenha concorrido de alguma forma para tanto, sujeitará o CAU/BR ao pagamento de juros moratório de 0,5% (cinco décimos por cento) ao mês, até o efetivo pagamento, além da devida atualização monetária.

14.4. O CAU/BR reserva-se no direito de não efetuar o pagamento se, no ato da atestação, a prestação dos serviços não atender as situações descritas neste Termo de Referência, inclusive no caso de a CONTRATADA deixar de apresentar a documentação de regularidade fiscal para com o Fundo de Garantia por Tempo de Serviço, Instituto Nacional do Seguro Social, as Fazendas Públicas Federal, Estadual ou do Distrito Federal e Municipal, e regularidade trabalhista.

14.5. O CAU/BR não pagará qualquer valor não constante ou fora dos critérios estabelecidos neste Termo de Referência.

14.6. Nenhum pagamento será efetuado à CONTRATADA enquanto pendente de liquidação qualquer obrigação financeira em virtude de penalidade ou inadimplência contratual, sem que isso gere direito à alteração dos preços, ou de compensação financeira por atraso de pagamento. O CAU/BR poderá deduzir do montante a pagar os valores correspondentes a multas ou indenizações devidas pela CONTRATADA, conforme este Termo de Referência.

14.7. Havendo erro na emissão do documento de cobrança ou circunstância que impeça a liquidação da despesa, como rasuras, entrelinhas, ou falta de algum dos documentos, a nota fiscal/fatura será devolvida à CONTRATADA e o pagamento ficará pendente até que sejam sanados os problemas.
14.7.1. Nesta hipótese, o prazo para pagamento será reiniciado após a regularização da situação ou reapresentação dos documentos, não acarretando quaisquer ônus para o CAU/BR.
14.8. A simples existência da relação contratual sem a contraprestação do serviço não enseja nenhum pagamento à CONTRATADA.
14.9. O CAU/BR não se responsabilizará pelo pagamento de quaisquer serviços realizados sem a solicitação e autorização do fiscal do contrato.

CAPÍTULO 15. DA RESPONSABILIDADE CIVIL
15.1. O licitante responderá por quaisquer prejuízos ou danos, por culpa ou dolo, causados por seus empregados ou prepostos ao CAU/BR e/ou a terceiros, em decorrência da prestação dos serviços, seja a que título for.
15.2. O CAU/BR estipulará prazo para a devida reparação, a depender da gravidade e extensão dos danos.

CAPÍTULO 16. DO CONTRATO
16.1. Após a adjudicação e homologação do procedimento licitatório, convocar-se-á o licitante vencedor para assinatura do instrumento contratual, que deverá ocorrer, impreterivelmente, no prazo de até 5 (cinco) dias úteis, a contar da comunicação, sob pena de decair do direito à contratação e sem prejuízo das sanções previstas neste Termo de Referência e no art. 81 da Lei nº 8.666, de 1993.
16.2. O prazo para assinatura do contrato poderá, em situação excepcionalíssima, ser prorrogado uma única vez, por igual período, quando solicitado pelo licitante vencedor em até 48h (quarenta e oito horas), a contar do recebimento da comunicação constante do item 16.1, desde que ocorra motivo relevante e aceito pelo CAU/BR.
16.3. Na celebração do contrato serão exigidas as mesmas condições de habilitação.
16.4. Pela inexecução total ou parcial do contrato poderá, garantidos o contraditório e a ampla defesa, ser aplicada ao contratado as sanções de que tratam os artigos 86 a 88 da Lei nº 8.666, de 1993, bem como as sanções e penalidades previstas neste Termo de Referência.

CAPÍTULO 17. DAS SANÇÕES E PENALIDADES
17.1. Incorre em infração administrativa nos termos da Lei nº 8.666/1993 e da Lei nº 10.520/2002 a CONTRATADA que:
17.1.1. Inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação.
17.1.2. Ensejar o retardamento da execução do objeto.
17.1.3. Fraudar a execução do contrato.
17.1.4. Comportar-se de modo inidôneo.
17.1.5. Cometer fraude fiscal.
17.1.6. Não manter a proposta apresentada.
17.2. A CONTRATADA que cometer qualquer das infrações discriminadas no subitem acima ficará sujeita, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:
17.2.1. Advertência, por escrito, nos casos de infrações de menor gravidade que não ocasionem prejuízos ao CONTRATANTE;
17.2.2. Multa:
17.2.2.1. Multa moratória de 0,5% (meio por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 30 (trinta) dias;

17.2.2.2. Multa compensatória de 1% (um por cento) sobre o valor total da proposta, quando houver até 3 (três) ocorrências, devidamente registradas pelo fiscal do contrato, como falta de prestador de serviço não reposto a tempo e modo, serviço em desacordo com o estabelecido neste Termo de Referência sem a devida correção, entre outras circunstâncias descritas neste Termo de Referência e não observados pela CONTRATADA;
17.2.2.3. Multa compensatória de 5% (cinco por cento) sobre o valor total da proposta, quando da 4ª (quarta) a 5ª (quinta) ocorrência, devidamente registradas pelo fiscal do contrato;
17.2.2.4. Multa compensatória de 10% (dez por cento) sobre o valor total da proposta quando da 6ª (sexta) ocorrência, caso em que será considerada total inadimplência contratual, gerando a rescisão contratual.
17.2.3. Suspensão do direito de licitar e impedimento de contratar com o CAU/BR, pelo prazo de até dois anos;
17.2.4. Impedimento de licitar e contratar com a União, e consequente descredenciamento no SICAF pelo prazo de até cinco anos;
17.2.5. Declaração de inidoneidade para licitar ou contratar com a administração pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a contratada ressarcir o contratante pelos prejuízos causados;
17.3. Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, a Contratada que:
17.3.1 Tenha sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;
17.3.2 Tenha praticado atos ilícitos visando a frustrar os objetivos da licitação;
17.3.3 Demonstre não possuir idoneidade para contratar com a administração em virtude de atos ilícitos praticados.
17.4. 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;
17.5. As multas serão descontadas dos pagamentos a que a CONTRATADA tiver direito, ou recolhidas diretamente ao CAU/BR, no prazo de 15 (quinze) dias, contados da data de sua comunicação, ou ainda, quando for o caso, cobrados judicialmente.
17.6. 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 ao Contratante, observado o princípio da proporcionalidade.
17.7. As penalidades serão obrigatoriamente registradas no SICAF.
17.8. As hipóteses de rescisão contratual serão regidas pelos artigos 77 a 80 da Lei nº 8.666, de 1993.

CAPÍTULO 18. DO PRAZO DE VIGÊNCIA

18.1. O prazo de vigência do contrato será 48 (quarenta e oito) meses, nos termos do art. 57, IV, da Lei 8.666/93.
18.2. A CONTRATADA fica 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, conforme legislação vigente.

CAPÍTULO 19. DO REAJUSTE DE PREÇOS

19.1. Decorrido o prazo de 12 (doze) meses da data da apresentação da proposta, poderá a CONTRATADA fazer jus ao reajuste do valor contratual que deverá retratar a variação efetiva do custo de produção ou dos insumos utilizados na consecução do objeto contratual, limitado pelo Índice Nacional de Preços ao Consumidor (INPC), na forma do que dispõem o art. 40, XI, da Lei nº 8.666, de 1993.

19.2. Os reajustes deverão ser precedidos de solicitação da CONTRATADA.
19.3. A CONTRATADA poderá exercer, perante o CONTRATANTE, seu direito ao reajuste dos preços do contrato até a data da prorrogação contratual subsequente.
19.3.1. Caso a CONTRATADA não solicite tempestivamente o reajuste e prorrogue o contrato sem pleiteá-lo, ocorrerá a preclusão do direito de reajustar.
19.4. O CONTRATANTE deverá assegurar-se de que os preços contratados são compatíveis com aqueles praticados no mercado, de forma a garantir a continuidade da contratação mais vantajosa.

CAPÍTULO 20. ESCOLHA DA MODALIDADE LICITATÓRIA
20.1. Considerando que os padrões, os níveis de qualidade, a qualificação técnica, as quantificações e as especificações dos produtos a serem adquiridos estão adequadamente definidos por meio de especificações usuais no mercado e de modo objetivo no presente Termo de Referência, entende-se que a contratação que ora se pretende está enquadrada como serviço comum, sendo obrigatória a adoção da modalidade Pregão Eletrônico do tipo Menor Preço, na forma de execução indireta, conforme Decreto nº 5.450/2005.

CAPÍTULO 21. DA ESTIMATIVA DE CUSTO
21.1. O valor estimado para a contratação de que trata este Termo de Referência é de **R$ 1.490.179,54** (um milhão quatrocentos e noventa mil cento e setenta e nove reais e cinquenta e quatro centavos).

CAPÍTULO 22. DAS DISPOSIÇÕES FINAIS
22.1. Esclarecimentos relativos ao Termo de Referência serão prestados pela Gerência Administrativa, no horário de 8h30 as 12h30 e 14h00 as 18h00, SCS Quadra 02, Bloco “C”, Entrada 22, Sala 401 a 409, Edifício Serra Dourada, CEP: 70300-902 Telefone: (61) 3204-9500.

Brasília, 16 de maio de 2018.

À consideração superior,

WARLEY DE MORAES VIRIATO
Coordenador de TI CSC - CAU/BR

De acordo. Aprovo o Termo de Referência nos moldes delineados, à vista de todo o detalhamento descrito e encaminho à Comissão de Licitação para as providências devidas quanto à elaboração do Edital de licitação e demais procedimentos.

ANDREI CANDIOTA
Gerente Geral - CAU/BR

ANEXO I - A

1. Especificação do Objeto:

Item	Descrição
1	Serviços de Segurança de Rede, incluindo alocação de equipamento do tipo Firewall de rede com funcionalidades de controle de conteúdo, controle de aplicações, VPN, WAF, integração com dispositivos de ponto de acesso sem-fio (AP Wireless), integração com endpoint e balanceamento de links.
2	Provimento de serviços gerenciados de operação e administração de Rede e Servidores de Rede, incluindo suporte técnico preventivo, corretivo e evolutivo.
3	Serviços de Acesso Wireless gerenciado e seguro à rede local, incluindo alocação de equipamento do tipo ponto de acesso de Rede Sem-fio (AP), integrado ao firewall e com funcionalidades de Captive Portal.
4	Serviços Gerenciados de Operação de *Backup*s.
5	Serviços Gerenciados de Monitoramento e Gestão de Rede, incluindo a emissão periódica de relatórios de acompanhamento contendo indicadores de gestão e de progresso/acompanhamento de projetos.
6	Serviços de Segurança de Rede, incluindo alocação de swithes conforme especificação Anexo I - G.

1.1. Item 01: Serviços de Segurança da Informação – Fornecimento de serviços técnicos especializados e gerenciados de segurança da informação e de redes, incluindo provimento/fornecimento, durante a vigência do contrato, de equipamento firewall de rede, com respectivas assinaturas de módulos e softwares para firewall de rede, firewall de aplicação Web (WAF) e para sua integração com dispositivos de ponto de acesso sem-fio e *endpoints* e seus respectivos serviços de manutenção preventiva, corretiva e evolutiva, além de serviços de suporte técnico credenciado com acordo de nível de serviço, incluindo visitas mensais de manutenção preventiva e emissão de relatórios, conforme especificado no Anexo I - B.

1.2 Item 02: Serviços de operação e administração de Rede e Servidores de Rede – Fornecimento de serviço especializado e gerenciado de suporte técnico a redes de computadores, com nível de serviço, contemplando manutenção preventiva, corretiva, e evolutiva, para plataformas Windows Server e Linux, Virtualização VMWare, Redes Ethernet e TCP/IP (incluindo alocação de ativos de redes) conforme especificações Anexo I - G, visitas mensais de manutenção preventiva e emissão de relatórios, conforme *Ticket*s de serviços de acesso gerenciado e seguro à rede local sem-fio, incluindo fornecimento, durante a vigência do contrato, de software e hardware de equipamento *Access Point* e suas respectivas atualizações de software, garantias e assinaturas de módulos; e de suporte técnico credenciado com acordo de nível de serviço para o serviço de acesso sem-fio, incluindo visitas mensais de manutenção preventiva e emissão de relatórios, conforme especificado no Anexo I - D.

1.3. Item 03: Serviços de Acesso Wireless gerenciado e seguro à rede local, incluindo alocação de equipamento do tipo Ponto de acesso de Rede Sem-fio (AP), integrado ao firewall e com funcionalidades de Captive Portal.

1.4. Item 04: Serviços de Operação de *Backup*s – Fornecimento de serviços de operação e administração de *backup*s, com acordo de nível de serviço e emissão de relatórios, para *backup*s de dados de servidores e de configurações de ativos de redes, conforme especificado no Anexo I - E.

1.5. Item 05: Serviços de Monitoramento e Gestão de Rede – Fornecimento de serviços de monitoramento e gestão de rede, com emissão de relatórios e gráficos, conforme especificado no Anexo I - F.
2. Local de prestação dos serviços e entregas: Sede do CAU/BR, localizada no SCS, Quadra 2, Ed. Serra Dourada, 4° Andar, salas 401 a 409, Brasília/DF, CEP:70300-902 ou outro endereço que venha a ser definido durante a vigência contratual, desde que em Brasília/DF.

ANEXO I - B

1. ESPECIFICAÇÕES GERAIS DO SERVIÇO DE SEGURANÇA

1.1. Deverão ser fornecidas as licenças para atualização de todos os componentes de software, vacinas de antivírus/malwares, endpoints, softwares de criptografia de armazenamento em nuvem e assinaturas de IPS, filtro de conteúdo web, controle de aplicações e proteção de firewall de aplicação web sem custo adicional, durante o período contratual.

2. Segurança de rede

Fornecimento de solução de segurança de rede composta por 1 (um) firewall em *appliance*, em comodato (na modalidade *Security as a Service*), compreendendo equipamentos (hardwares), softwares e prestação de serviços, conforme especificações a seguir:

2.1. Características Gerais:

2.1.1. Tecnologia *Next-Generation Firewall* (NGFW) para proteção de informação perimetral e de rede interna que inclui inspeção profunda de pacotes, para controle de tráfego de dados por identificação de usuários e por camada 7, com controle de aplicação, administração de largura de banda (QoS), VPN IPsec e SSL, IPS, prevenção contra ameaças de vírus, *malwares,* Filtro de URL, inspeção de tráfego criptografado e proteção de firewall de aplicação Web. Deverá ser fornecido console de gerenciamento dos equipamentos e permitir a centralização de logs em hardware específico ou virtualizado.
2.1.2. A solução deverá estar licenciada para quantidade ilimitada de usuários e também de endereços IP.
2.1.3. Para os itens que representem bens materiais, a CONTRATADA deverá fornecer produtos novos, sem uso anterior.
2.1.4. Não serão aceitos equipamentos, servidores e sistema operacional de uso genérico.
2.1.5. Por cada *appliance* físico que compõe a plataforma de segurança, entende-se o hardware, software e as licenças necessárias para o seu funcionamento.
2.1.6. Cada *appliance* deverá ser capaz de executar a totalidade das capacidades exigidas para cada função, não sendo aceitos somatórias para atingir os limites mínimos.
2.1.7. O hardware e o software fornecidos não podem constar, no momento da apresentação da proposta, em listas de *end-of-sale, end-of-support, end-of-engineering-support* ou *end-of-life* do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante.
2.1.8. O software deverá ser fornecido em sua versão mais atualizada.

2.2. Especificações Técnicas Gerais:

2.2.1. A solução deve consistir de *appliance* de proteção de rede com funcionalidades de *Next Generation Firewall* (NGFW), e console de gerência, monitoramento e logs.
2.2.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões.
2.2.3. As funcionalidades de proteção de rede que compõem a plataforma de segurança podem funcionar em múltiplos *appliances* desde que obedeçam a todos os requisitos desta especificação.
2.2.4. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7.
2.2.5. O firewall deverá possibilitar monitoração de falha de link.
2.2.6. Uma interface completa de comando de linha (*CLI command-line-interface*) deverá ser acessível através da interface gráfica e via porta serial.
2.2.7. A atualização de software deverá enviar avisos de atualização automáticos.
2.2.8. O Firewall deverá permitir a definição de redes, serviços, hosts períodos de tempos, usuários e grupos, clientes e servidores.

2.2.9. O *backup* e o reestabelecimento de configuração deverá ser feito localmente, via FTP ou e-mail com frequência diária, semanal ou mensal, podendo também ser realizado por demanda.
2.2.10. As notificações de monitoramento deverão ser realizadas via e-mail e SNMP.
2.2.11. O Firewall deverá cumprir as seguintes especificações:
2.2.11.1. Protocolos *SNMP e Netflow*.
2.2.11.2. O firewall deverá possuir capacidade de inspeção profunda de pacotes.
2.2.11.3. Deverá permitir estabelecer políticas de conversão de endereços (NAT) customizáveis para cada regra.
2.2.11.4. Deverá possuir proteção contra *flood*, com mecanismos contra *DoS (Denial of Service), DdoS (Distributed DoS)* e bloqueio de *portscan*.
2.2.11.5. Deverá possuir proteção contra *anti-spoofing*.
2.2.11.6. Possuir suporte a IPv4 e IPv6.
2.2.11.7. Em IPv6 deve suportar os tunelamentos 6in4, 6to4, 4in6 e IPv6 *Rapid Deployment* (6rd) de acordo com a RFC 5969.
2.2.11.8. Suporte aos roteamentos estáticos, dinâmico (RIP, BGP e OSPF) e *multicast* (PIM-SM e IGMP).
2.2.11.9. Deverá suportar a definição de VLANs no firewall conforme padrão IEEE 802.1q e tagging de VLAN.
2.2.11.10. Possuir balanceamento de link WAN que permita múltiplas conexões de links Internet, checagem automática do estado de links*, failover* automático e balanceamento por peso.
2.2.11.11. Deverá permitir *port-aggregation* de interfaces de firewall suportando o protocolo 802.3ad, para escolhas entre aumento de *throughput* e alta disponibilidade de interfaces;
2.2.11.12. Deverá implementar os serviços de DNS, *Dynamic* DNS, DHCP e NTP, de forma que o Firewall seja o provedor destes serviços para a rede;
2.2.11.13. Possuir funcionalidade de qualidade de serviço do tipo traffic shapping (QoS) baseada em rede ou usuário.
2.2.11.14. Deverá permitir estabelecimento de cotas cíclicas ou não-cíclicas, por usuários, para upload/download e pelo tráfego total.
2.2.11.15. Possuir otimização em tempo real de tráfego VoIP (voz sobre IP).
2.2.11.16. Implementar o protocolo de negociação *Link Aggregation Control Protocol* (LACP).

2.3. Especificações de desempenho do Firewall:
2.3.1. Performance mínima de 22 Gbps de t*hroughput* para firewall.
2.3.2. Performance mínima de 5 Gbps de *throughput* de IPS.
2.3.3. Performance mínima de 3 Gbps de *throughput* para controle de Antivírus/proxy.
2.3.4. Performance mínima de 2 Gbps de *throughput* de VPN.
2.3.5. Suporte a, no mínimo, 15.000.000 (quinze milhões) de conexões simultâneas.
2.3.6. Suporte a, no mínimo, 180.000 (cento e oitenta mil) novas conexões por segundo.
2.3.7. Possuir número irrestrito de usuários licenciados.
2.3.8. Possuir armazenamento interno de no mínimo 120GB SSD para quarentena local, logs e relatórios.
2.3.9. Possuir no mínimo 8 (oito) GB de memória RAM.
2.3.10. Possuir no mínimo 8 (oito) interfaces de rede 1000Base-TX.
2.3.11. Possuir 1 (uma) interface do tipo console ou similar, além das 8 (oito) interfaces de uso especificadas no item acima.
2.3.12. Permitir instalação de no mínimo 1 (um) módulo de expansão de interfaces
2.3.13. Possuir 1 (uma) fonte 100-240VAC.

2.4. Políticas de Controle de Firewall:

2.4.1. O controle de políticas deverá monitorar as políticas de redes, usuários, grupos e tempo, bem como identificar as regras não-utilizadas, desabilitadas, modificadas e novas políticas.
2.4.2. As políticas deverão ter controle de tempo de acesso por usuário e grupo, sendo aplicadas por zonas (rede interna, DMZ, rede externa), redes e por tipos de serviços.
2.4.3. As políticas de controle deverão ainda: suportar controles por porta e protocolos TCP/UDP, origem/destino e identificação de usuários; possuir controle de políticas por países via localização por IP; dar suporte a objetos e regras IPV6 e a objetos e regras multicast.

2.5. Prevenção de Ameaças
2.5.1. Para fins de prevenção de ameaças, o firewall deverá:
2.5.1.1. Possuir módulo de IPS, Antivírus, Anti-Malware e Firewall de Proteção Web (WAF) integrados no próprio appliance de Firewall ou entregue em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação.
2.5.1.2. Possuir integração com os endpoints antivírus especificados no item 3 a seguir, de modo que ameaças identificadas pelo endpoint sejam comunicadas automaticamente ao firewall e deste para os demais endpoints da rede, automatizando processo de resposta aos incidentes originados por malware ou outras ameaças detectadas pelos endpoints.
2.5.1.3. Realizar a inspeção profunda de pacotes para prevenção de intrusão (IPS) e deve incluir assinaturas de prevenção de intrusão (IPS).
2.5.1.4. Permitir a customização de assinaturas de prevenção de intrusão (IPS).
2.5.1.5. Permitir configurar exceções por usuário, grupo de usuários, IP de origem ou de destino nas regras;
2.5.1.6. Permitir configurar de maneira granular as políticas de IPS, Antivírus e *Anti-Malware*, possibilitando a criação de diferentes politicas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens, com customização completa;
2.5.1.7. Bloquear todas as formas de vírus, *web malwares, trojans e spyware em HTTP e HTTPS, FTP e web-emails*.
2.5.1.8. Possuir capacidade de realizar a proteção com emulação *JavaScript*.
2.5.1.9. Possuir proteção em tempo real contra novas ameaças criadas.
2.5.1.10. Possuir pelo menos duas engines de antivírus independentes e de diferentes fabricantes para a detecção de malware, podendo ser configuradas isoladamente ou simultaneamente.
2.5.1.11. Permitir o bloqueio de vulnerabilidades.
2.5.1.12. Permitir o bloqueio de *exploits* conhecidos.
2.5.1.13. Detectar e bloquear o tráfego de rede que busque acesso a *contact command* e servidores de controle utilizando múltiplas camadas de *DNS, AFC e firewall*.
2.5.1.14. Incluir proteção contra ataques de negação de serviços.
2.5.1.15. Ser imune e capaz de impedir ataques básicos tais como: *SYN flood, ICMP flood, UDP Flood*.
2.5.1.16. Suportar bloqueio de arquivos por tipo.
2.5.1.17. Registrar no console de monitoramento as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo.
2.5.1.18. Permitir a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas de segurança considerando uma das opções ou a combinação de todas elas: usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por usuários, grupos de usuários, origem, destino, zonas de segurança.
2.5.1.19. Possuir - no mínimo mas não limitado a - proteção contra os seguintes ataques: SQL injection e Cross-site scripting.
2.5.2. Os eventos devem identificar o país de onde partiu a ameaça.

2.5.3. O firewall de aplicação Web (WAF) deverá ter a função de reverse proxy, com a função de URL *hardening* realizando *deep-linking* e prevenção dos ataques de *path traversal* ou *directory traversal*.
2.5.4. O firewall de aplicação Web (WAF) deverá realizar cookie signing com assinaturas digitais, roteamento baseado por caminho, autenticações reversas e básicas para acesso do servidor.
2.5.5. O firewall de aplicação Web (WAF) deverá possuir a função de balanceamento de carga de visitantes por múltiplos servidores, com a possibilidade de modificação dos parâmetros de performance do WAF e permissão e bloqueio de ranges de IP

2.6. Controle e Proteção de Aplicações
2.6.1. Possuir a capacidade de reconhecer aplicações por assinaturas e camada 7, utilizando portas padrões (80 e 443), portas não padrões, port hopping e túnel através de tráfego SSL encriptado.
2.6.1.1. Em relação ao tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de *payload* para checagem de assinaturas de aplicações conhecidas pelo fabricante.
2.6.2. Reconhecer pelo menos 2.000 (duas mil) aplicações diferentes, classificadas por nível de risco, características e tecnologia, incluindo, mas não limitado a: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, serviços de rede, VoIP, streaming de mídia, proxy e tunelamento, mensageiros instantâneos, compartilhamento de arquivos, web e-mail e update de softwares.
2.6.3. Reconhecer no mínimo as seguintes aplicações: 4Shared File Transfer, Active Directory/SMB, Citrix ICA, DHCP Protocol, Dropbox Download, Easy Proxy, Facebook Graph API, Firefox Update, Freegate Proxy, FreeVPN Proxy, Gmail Video, Chat Streaming, Gmail WebChat, Gmail WebMail, Gmail-Way2SMS WebMail, Gtalk Messenger, Gtalk Messenger File Transfer, Gtalk-Way2SMS, HTTP Tunnel Proxy, HTTPort Proxy, LogMeIn Remote Access, NTP, Oracle database, RAR File Download, Redtube Streaming, RPC over HTTP Proxy, Skydrive, Skype, Skype Services, skyZIP, SNMP Trap, TeamViewer Conferencing e File Transfer, TOR Proxy, Torrent Clients P2P, Ultrasurf Proxy, UltraVPN, VNC Remote Access, VNC Web Remote Access, WhatsApp, WhatsApp File Transfer e WhatsApp Web.
2.6.4. Realizar o escaneamento e controle de micro app's, incluindo mas não limitado a: Facebook (Applications, Chat, Commenting, Events, Games, Like Plugin, Message, Pics Download e Upload, Plugin, Post Attachment, Posting, Questions, Status Update, Video Chat, Video Playback, Video Upload, Website), Freegate Proxy, Gmail (Android Application, Attachment), Google Drive (Base, File Download, File Upload), Google Earth Application, Google Plus, LinkedIN (Company Search, Compose Webmail, Job Search, Mail Inbox, Status Update), SkyDrive File Upload e Download, Twitter (Message, Status Update, Upload, Website), Yahoo (WebMail, WebMail File Attach) e Youtube (Video Search, Video Streaming, Upload, Website)
2.6.4.1. O escaneamento de micro app deverá ser habilitado via console gráfica (GUI) e também via comando de linha (CLI).
2.6.5. Atualizar a base de assinaturas de aplicações automaticamente.
2.6.6. Reconhecer aplicações em IPv6.
2.6.7. Limitar a banda usada por aplicações (*traffic shaping*).
2.6.8. Possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no *Domain Controller*, nem nas estações dos usuários.
2.6.9. 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.

2.6.10. Permitir o uso individual de diferentes aplicativos para usuários que pertencem ao mesmo grupo de usuários, sem que seja necessária a mudança de grupo ou a criação de um novo grupo. Os demais usuários deste mesmo grupo que não possuírem acesso a estes aplicativos devem ter a utilização bloqueada.

2.7. Controle e Proteção para Aplicações WEB

2.7.1. Deve permitir especificar política de navegação Web por tempo, ou seja, a definição de regras para um determinado dia da semana e horário de início e fim, permitindo a adição de múltiplos dias e horários na mesma definição de política por tempo. Esta regra de tempo pode ser recorrente ou aplicada em uma única vez.
2.7.2. Deve permitir a criação de políticas por usuários, grupos de usuários, IPs e redes.
2.7.3. Deve ter capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via LDAP, *Active Directory*, Radius, *E-directory* e base de dados local.
2.7.4. Deve explicitar em todos os logs de URL as informações dos usuários conforme descrito na integração com serviços de diretório.
2.7.5. Deve possuir pelo menos 70 categorias de URLs.
2.7.6. Deve suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL.
2.7.7. Deve ter capacidade de forçar o uso da opção "*Safe Search*" em sites de busca.
2.7.8. Deve ser capaz de categorizar as URLs a partir de base ou cache de URLs locais ou através de consultas dinâmicas na nuvem do fabricante, independentemente do método de classificação a categorização não deve causar atraso na comunicação ao usuário.
2.7.9. Deve suportar a criação categorias de URLs customizadas.
2.7.10. Deve suportar a opção de bloqueio de categoria HTTP e liberação da categoria apenas em HTTPS.
2.7.11. Deve permitir a customização de página de bloqueio.
2.7.12. Deve suportar a inclusão nos logs do produto de informações das atividades dos usuários.
2.7.13. Deve salvar nos logs as informações adequadas para geração de relatórios indicando usuário, tempo de acesso, bytes trafegados e site acessado.
2.7.14. Deve realizar caching do conteúdo web.
2.7.15. Deve realizar filtragem por mime-type, extensão e tipos de conteúdos ativos, tais como, mas não limitado a: ActiveX, applets e cookies.

2.8. Identificação de Usuários

2.8.1. Permitir a criação de políticas baseadas na visibilidade e controle de quem (usuário) está utilizando quais aplicações através da integração com serviços de diretório, autenticando via LDAP, *Active Directory, Radius, eDirectory, TACACS+* e via base de dados local, para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários.
2.8.2. 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*).
2.8.3. Possuir suporte à identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços.
2.8.4. Permitir autenticação em modos: transparente, autenticação proxy (NTLM e Kerberos) e autenticação via clientes nas estações com os sistemas operacionais Windows, MAC OS X e Linux 32/64.
2.8.5. Possuir a autenticação Single sign-on para, pelo menos, os sistemas de diretórios Active Directory e eDirectory.

2.8.6. Possuir portal do usuário para que os usuários tenham acesso ao uso de internet pessoal, troquem senhas da base local e façam o download de softwares para as estações presentes na solução por meio de autosserviço.

2.9. Qualidade de Serviço (QoS)
2.9.1. Para controlar aplicações e tráfego cujo consumo possa ser excessivo e ter um alto consumo de largura de banda, é exigido que o firewall, além da capacidade de permitir ou negar esses tipos de aplicações, deverá também ter a capacidade de controlá-las por políticas de largura de banda máxima, quando forem solicitadas por diferentes usuários ou aplicações.
2.9.2. A solução deverá suportar *Traffic Shaping* (QoS) e a criação de políticas baseadas em categoria web e aplicação por: endereço de origem; endereço de destino; usuário e grupo do LDAP/AD.
2.9.3. A solução deverá possibilitar a configuração de limite e garantia de upload/download, bem como priorização o tráfego total e bit-rate de modo individual ou compartilhado.
2.9.4. A solução deverá suportar priorização de tempo real (*Real-Time)* de protocolos de voz (VoIP).

2.10. Redes Privadas Virtuais (VPN)
2.10.1. Suportar VPN *Site-to-Site e Cliente-to-Site*.
2.10.2. Suportar IPsec VPN.
2.10.3. Suportar SSL VPN.
2.10.4. Suportar L2TP e PPTP.
2.10.5. Suportar acesso remoto SSL, IPSec e VPN Client para Android e iPhone/iPAD.
2.10.6. Deve ser disponibilizado o acesso remoto ilimitado, até o limite suportado de túneis VPN pelo equipamento, sem a necessidade de aquisição/aplicação de novas licenças e sem qualquer custo adicional para o licenciamento de clientes SSL para estações Windows.
2.10.7. Deve possuir o acesso via o portal de usuário para o download e configuração do cliente SSL para Windows.
2.10.8. Deve possuir um portal encriptado baseado em HTML5 para suporte pelo menos a: RDP, HTTP, HTTPS, SSH, Telnet e VNC, sem a necessidade de instalação de clientes VPN nas estações de acesso.
2.10.9. A VPN IPsec deve suportar: DES e 3DES, Autenticação MD5 e SHA-1;*Diffie-Hellman Group 1, Group 2, Group 5 e Group 14*; Algoritmo Internet Key Exchange (IKE); AES 128, 192 e 256 (*Advanced Encryption Standard*); SHA 256, 384 e 512; Autenticação via certificado PKI (X.509) e Pre-shared key (PSK).
2.10.10. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Dell SonicWALL, Fortinet, Huawei, Juniper, Sophos e Palo Alto Networks.
2.10.11. Deve pPermitir criar políticas de controle de aplicações, IPS, Antivírus, *Anti-Malware* e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL.
2.10.12. Suportar autenticação via AD/LDAP, *Token* e base de usuários local.
2.10.13. Permitir estabelecer um túnel SSL VPN com uma solução de autenticação via LDAP, *Active Directory, Radius, eDirectory, TACACS+* e via base de dados local.

2.11. Gerência Administrativa Centralizada
2.11.1. A solução fornecida deverá possuir Gerência Administrativa Centralizada que atenda aos requisitos mínimos abaixo elencados:
2.11.1.1. Possuir solução de gerenciamento centralizado, possibilitando o gerenciamento do Firewall ou de seus diversos equipamentos em um único console central, com administração de privilégios e funções;
2.11.1.2. Estar licenciada para gerenciar as soluções de firewall de próxima geração;

2.11.1.3. Fornecer soluções virtuais ou via appliances desde que obedeçam a todos os requisitos desta especificação;
2.11.1.4. Centralizar a gerência de todas as políticas e configurações do firewall sem necessidade de acesso direto aos equipamentos;
2.11.1.5. Permitir a criação de Templates para configurações;
2.11.1.6. Possuir indicadores do estado de equipamentos e rede;
2.11.1.7. Emitir alertas baseados em thresholds customizáveis, incluindo também alertas de expiração de subscrição, mudança de status de gateways, uso excessivo de disco, eventos ATP, IPS, ameaças de vírus, navegação, entre outros;
2.11.1.8. Permitir a criação de grupos de equipamentos por nome, modelo, firmware e regiões;
2.11.1.9. Ter controle de privilégios administrativos, com granularidade de funções (VPN admin, App e Web admin, IPS admin, etc);
2.11.1.10. Ter controle das alterações feitas por usuários administrativos, comparar diferentes versões de configurações e realizar o processo de roll-back de configurações para mudanças indesejadas;
2.11.1.11. Ter logs de auditoria de uso administrativo e atividades realizadas nos equipamentos (trilha de auditoria);
2.11.1.12. Possuir integração com solução de logs e relatórios, habilitando o provisionamento automático de novos equipamentos e a sincronização dos administradores da centralização da gerência com a centralização de logs e relatórios.
2.11.1.13. Possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança.

2.12. Gerência Centralizada de Logs e Relatórios
2.12.1. A solução fornecida deverá possuir Gerência Centralizada de Logs e Relatórios que atenda aos requisitos mínimos abaixo elencados:
2.12.1.1. Possuir solução de logs e relatórios centralizados, possibilitando a consolidação total de todas as atividades da solução através de uma único console central;
2.12.1.2. Estar licenciada para o firewall;
2.12.1.3. Fornecer soluções virtuais ou via appliances desde que obedeçam a todos os requisitos desta especificação, com armazenamento mínimo de 100 GB de dados;
2.12.1.4. Prover relatórios baseados em usuários, com visibilidade sobre acesso a aplicações, navegação, eventos ATP, downloads e consumo de banda, independente em qual rede ou IP o usuário esteja se conectando;
2.12.1.5. Possibilitar a identificação de ataques como a identificação de malware identificados pelos eventos ATP, usuários suspeitos, tráfegos anômalos incluindo tráfego ICMP e consumo não-usual de banda;
2.12.1.6. Conter relatórios pré-configurados, pelo menos de: aplicações, navegação, web server (WAF), IPS, ATP e VPN;
2.12.1.7. Forcnecer relatórios históricos para análises de mudanças e comportamentos;
2.12.1.8. Conter customizações dos relatórios para inserção de logotipos próprios;
2.12.1.9. Deve permitir a exportação via PDF ou Excel;
2.12.1.10. Deve fornecer relatórios sobre os acessos de procura no Google, Yahoo, Bing e Wikipédia;
2.12.1.11. Deve fornecer relatórios de tendências;
2.12.1.12. Deve fornecer logs em tempo real, de auditoria e arquivados;
2.12.1.13. Deve possuir mecanismo de procura de logs arquivados;
2.12.1.14. Deve ter acesso baseado em Web com controles administrativos distintos.

3. Segurança de estações de trabalho e Servidores
3.1. Características Gerais

3.1.1. *Next-Generation Endpoint* (NGE) para proteção de equipamentos de 200 usuários finais (considerar 3 dispositivos por usuário), integrados ao firewall e monitorados por meio de uma central única de monitoração, para proteção *antimalware, live protection*, prevenção de *exploits* e análise de comportamento, reputação de *downloads*, controle de aplicativos, dispositivos e filtro de URL, detecção de tráfego malicioso, sincronização com AD, políticas por usuários e console de gerenciamento.

3.2. Especificações de Next Generation EndPoint

3.2.1. Deve ser fornecida solução de *Next-Generation Endpoint* (NGE) para proteção de equipamentos de 200 usuários finais em Windows, considerando o uso de até 2 dispositivos simultâneos por usuário;

3.2.2. A solução deve oferecer, pelo menos, proteção *antimalware, live protection*, prevenção de *exploits* e análise de comportamento, reputação de downloads, controle de aplicativos, dispositivos e filtro de URL, detecção de tráfego malicioso, sincronização com AD, políticas por usuários, e console de gerenciamento.

3.2.3. O monitoramento e a configuração deverão ser realizados por meio de um Console Central único, que deverá conter todas a ferramentas para o monitoramento e controle da proteção dos dispositivos.

3.2.4. O console deverá apresentar *Dashboard* com o resumo dos status de proteção dos computadores e usuários, bem como indicar os alertas de eventos de criticidades alta, média e informacional.

3.2.5. O console deverá possuir capacidade de criar e editar diferentes políticas para a aplicação das proteções exigidas e aplicadas em nível de usuários, não importando em que equipamentos eles estejam acessando.

3.2.6. Prover no *endpoint* a solução de HIPS (*Host Instrusion Prevention System*) para a detecção automática e proteção contra comportamentos maliciosos (análise de comportamento) e deverá ser atualizado diariamente.

3.2.7. Prover proteção automática contra web sites infectados e maliciosos, assim como prevenir o ataque de vulnerabilidades de browser via *web exploits*.

3.2.8. Permitir o monitoramento e o controle de dispositivos removíveis nos equipamentos dos usuários, como dispositivos USB, periféricos da própria estação de trabalho e redes sem fio, estando sempre atrelado ao usuário e não ao dispositivo.

3.2.9. O controle de dispositivos deve ser realizado no nível de permissão, somente leitura ou bloqueio.

3.2.10. No mínimo, os seguintes dispositivos deverão ser gerenciados pelo *endpoint*: HD (hard disks) externos, *pendrives* USB, *storages* removíveis seguras, CD, DVD, *Blu-ray, floppy* drives, interfaces de rede sem fio, modems, *bluetooth*, infra-vermelho, MTP (*Media Transfer Protocol*) tais como *Blackberry*, *iPhone* e *Android* smartphone e PTP (*Picture Transfer Protocol*) como câmeras digitais.

3.2.11. A solução deve permitir o escaneamento HTTPS e de múltiplos protocolos, gerenciando tanto o tráfego *inbound* quanto *outbound* para proteção completa dos dados.

3.2.12. A solução deve fornecer gerenciamento de arquivos armazenados em nuvem (por exemplo *Dropbox*), garantindo que o processo de upload de arquivos seja monitorado e gerenciado, bem como realizar automaticamente o escaneamento do arquivo contra *malwares*, realizar pesquisa de palavras chaves ou informações confidenciais. O bloqueio do upload ou a remoção da informação confidencial deverá ser executado antes do envio do arquivo (upload).

3.2.13. A solução deve fornecer o controle de aplicativos para o bloqueio e liberação de aplicações não maliciosas, tais como, mas não limitada a: mensagens instantâneas, acesso remoto, jogos, entre outras.

3.2.14. A solução deve possuir mecanismo de isolamento automático de *endpoints* comprometidos da rede, limitando o uso de recursos da rede até a remediação automática e completa da vulnerabilidade do *endpoint*, retornando ao estado de proteção segura.
3.2.15. A solução deve informar ao administrador os bloqueios de ameaças web, as violações e alertas de políticas, bem como indicar qual procedimento o operador realizou após a recepção deste alerta.
3.2.16. A solução deve permitir sincronização com o *Active Directory (AD)* para gestão de usuários e grupos integrados às políticas de proteção.
3.2.17. A solução deve fornecer a gestão por usuários, com a informação do equipamento que este está acessando, eventos e políticas aplicadas.
3.2.18. A solução deve permitir o uso de múltiplas políticas para diferentes usuários e grupos de usuários.
3.2.19. A solução deve permitir exclusões de escaneamento para um determinado website, arquivo ou aplicação, tanto em nível geral quanto específico em uma determinada política.
3.2.20. A solução deve possuir mecanismo contra a desinstalação do endpoint pelo usuário e cada dispositivo deverá ter uma senha única, não sendo autorizada soluções com senha única válida para todos os dispositivos.
3.2.21. A solução deve prover cache para updates dos endpoints, para um equipamento específico presente na rede interna ou para múltiplos computadores.
3.2.22. A instalação deve ser realizada via cliente específico por download da gerência central e também via e-mail de configuração. O instalador deverá permitir a distribuição do cliente via Active Directory (AD) para múltiplas máquinas.
3.2.23. A solução deve conter relatórios para análise e controle dos usuários e endpoints. Os relatórios deverão ser divididos, no mínimo, em relatórios de: eventos, usuários, controle de aplicativos, periféricos e web, indicando todas as funções solicitadas para os endpoints.

4. Disposições finais específicas do serviço de segurança
4.1. Instalação e configuração
4.1.1. Deverá ocorrer reunião de planejamento para implementação e transferência de conhecimento da solução de segurança, a fim de alinhar os requisitos do projeto;
4.1.2. A reunião mencionada no item anterior deverá ocorrer antes da entrega dos equipamentos;
4.1.3. A reunião de planejamento de implementação, bem como de alinhamento dos requisitos técnicos, ocorrerá entre a equipe técnica do CONTRATANTE e a equipe técnica da CONTRATADA responsável pela instalação;
4.1.4. Na reunião deverão ser tratados no mínimo os seguintes assuntos: alinhamento inicial, cronograma de instalação e transferência de conhecimento;
4.1.5. Na reunião inicial deverá ser feita a exposição técnica das funcionalidades presentes no Firewall, para definição, por parte da equipe técnica do CONTRATANTE, com apoio da CONTRATADA, das configurações, topologias e outras definições a serem implementadas;
4.1.6. O produto da reunião inicial será um plano de implementação, podendo ser efetuadas reuniões adicionais para concluir a sua elaboração;
4.1.7. Os equipamentos deverão ser instalados, física e logicamente, pelos técnicos da CONTRATADA, com acompanhamento dos técnicos do CONTRATANTE e segundo as configurações definidas no plano de implementação;
4.1.8. Todos os custos de pessoal para efetuar a implementação dos equipamentos, tais como passagens áreas ou terrestres, hospedagem, alimentação, deslocamentos e demais custos, serão de responsabilidade da CONTRATADA;
4.1.9. Os técnicos da CONTRATADA envolvidos na instalação e configuração dos equipamentos adquiridos deverão ser certificados pelo fabricante;
4.1.10. Os serviços de instalação também englobarão as seguintes atividades:
4.1.10.1. Desempacotamento dos equipamentos, verificação e conferência dos componentes;

4.1.10.2. Definição dos procedimentos e melhores práticas de instalação;
4.1.10.3. Montagem física dos equipamentos, instalação básica dos equipamentos de acordo com as recomendações do fabricante, realizar conexões do tipo física, lógica e elétrica;
4.1.10.4. Instalação física de todos os hardwares fornecidos, incluindo montagem no "rack" de equipamentos na sede do CAU/BR, conexão lógica, atualizações de softwares, patches, drivers e firmwares para suas mais recentes versões suportadas antes da ativação dos mesmos em produção;
4.1.10.5. Realizar a ativação e configuração do acesso de gerenciamento remoto dos equipamentos fornecidos;
4.1.10.6. Configuração das ferramentas de gerenciamento e administração do equipamento;
4.1.10.7. Configuração dos equipamentos, conforme definido no plano de implementação;
4.1.10.8. Realização de testes de verificação ao término da instalação;
4.1.10.9. Desinstalação física e lógica do firewall atual e instalação física e lógica do novo firewall, por parte da CONTRATADA, preservando a continuidade das operações e todas as configurações previamente efetuadas para o ambiente da Autarquia;

4.2. Requisitos de Suporte Técnico específicos para os serviços de segurança
4.2.1. Além das condições de prestação dos serviços especificadas no Anexo I - G deste Termo de Referência, serão exigidas da CONTRATADA as condições listadas abaixo, específicas para suporte técnico ao Firewall:
4.2.1.1. Os serviços de suporte devem contemplar atualizações de firmware e versões de software disponibilizadas pelo fabricante da solução, ajustes e configurações de acordo com as melhores práticas e recomendações do fabricante da solução, procedimentos destinados a manter e/ou recolocar a solução em pleno e perfeito estado de uso, nos casos de inoperância total ou parcial, defeito ou mau funcionamento;
4.2.1.2. Os serviços de suporte incluem o atendimento às solicitações de suporte técnico relacionado a problemas, erros apresentados e forma de utilização da solução e correções necessárias para o restabelecimento das suas funcionalidades, de acordo com as melhores práticas e recomendações do fabricante do Firewall;
4.2.1.3. Os serviços de suporte incluem a prestação de informações e orientações necessárias à atualização e ao perfeito funcionamento da solução;
4.2.1.4. Os serviços de suporte contemplam o funcionamento adequado do produto, aplicação de patches de correção e apoio na atualização das versões, incluindo:
4.2.1.4.1. Atualizações de módulos e softwares;
4.2.1.4.2. Atualização das assinaturas de software de subscrição (módulos) durante o período de vigência do contrato, fornecidos pelo seu fabricante;
4.2.1.4.3. Garantia de hardware, incluindo a substituição de peças defeituosas sem ônus para a CONTRATANTE durante a vigência do contrato.
4.2.1.5. Na eventualidade de o CONTRATANTE necessitar dos serviços de garantia de hardware ou houver a retirada de equipamento para manutenção externa pela CONTRATADA, esta deverá disponibilizar outro firewall de capacidade igual ou superior para uso do CONTRATANTE em caráter provisório e temporário, e sem perda das funções em utilização, durante o período em que o equipamento estiver em manutenção, evitando a interrupção dos serviços de rede do CONTRATANTE, até que o equipamento removido seja restituído devidamente reparado, em perfeitas e plenas condições de uso.
4.2.1.6. Em caso de necessidade de retirada com substituição provisória descrita no parágrafo anterior, a CONTRATADA se compromete a providenciar solução de contorno dentro dos prazos de nível de serviço estipulados por este Edital, e fornecer o equipamento de substituição em até 4 (quatro) horas úteis ao do registro da solicitação.

4.3. Treinamento

4.3.1. A CONTRATADA deverá ministrar treinamento relativo à instalação, operacionalização, manuseio, configuração e utilização da solução de segurança, visando garantir a transferência de conhecimento para até 4 (quatro) pessoas indicadas pelo CONTRATANTE.
4.3.2. O treinamento deverá possuir carga horária mínima de 20 (vinte) horas, observando-se que o treinamento deverá conter todo o conteúdo descrito no item anterior.
4.3.3. As datas e horários para realização dos treinamentos serão definidos pelo CONTRATANTE em comum acordo com a CONTRATADA.
4.3.4. O treinamento deverá ser realizado nas instalações (sede) do CONTRATANTE, e seu conteúdo programático (ementa) deverá ser apresentado com antecedência mínima de 5 (cinco) dias úteis antes de seu início.
4.3.5. Deverão ser utilizadas apostilas impressas, uma por participante, e o instrutor deverá possuir experiência em treinamentos desta natureza, bem como certificação no Firewall.
4.3.6. Deverá ser emitido certificado aos participantes do treinamento que cumprirem frequência mínima de 80%.

ANEXO I - C

1. Características e especificações dos serviços de operação e Administração da Rede e Servidores de Rede - Caberá à CONTRATADA realizar continuamente a operação, administração, manutenção (preventiva, corretiva e evolutiva) e monitoramento de servidores, equipamentos ativos em operação na rede LAN, e serviços de rede em produção no ambiente de TI do CONTRATANTE, prestando serviços que, além das especificações constantes nos demais itens e anexos deste Edital, também deverão atender aos seguintes critérios:

1.1. Realizar periodicamente as rotinas de manutenção preventiva e evolutiva, conforme os Planos de Manutenção Preventiva, que – entre outros itens – contempla:
1.1.1. Atualizar patches, correções e versões ou releases mais recentes dos softwares;
1.1.2. Executar cópia de segurança (*backup*) do *system state* do serviço de diretórios MS-AD em produção no CONTRATANTE, e verificar a integridade do sistema de diretórios;
1.1.3. Verificar o espaço em disco e partições de disco de servidores, e – caso necessário – encaminhar ou executar as providências necessárias para evitar problemas decorrentes de falta de espaço de armazenamento;
1.1.4. Verificar Logs de servidores e ativos de rede, e tomar as providências cabíveis para prevenir e/ou corrigir falhas e/ou problemas;
1.1.5. Executar rotinas operacionais e acompanhar a correta conclusão de rotinas agendadas;
1.1.6. Acompanhar a correta conclusão de rotinas agendadas, tais como (mas não limitado a) *backup*s de dados, *backup*s de configurações de sistema (system state), limpeza e cópia de registros de eventos e inicializações dos servidores;
1.1.7. Realizar visitas mensais presenciais para execução das rotinas de manutenção preventiva, independente de outros chamados de suporte técnico (corretivos, evolutivos, preventivos) demandados pelo CONTRATANTE ou que a própria CONTRATADA julgue necessários.

1.2. Realizar atendimentos eventuais, atividades de manutenção corretiva e provimento de serviço de suporte técnico, contemplando:
1.2.1. Instalar, desinstalar, configurar, migrar servidores, serviços de rede, máquinas virtuais, sistemas operacionais de rede e ativos de rede, conforme demandas da CONTRATANTE ou projetos desenvolvidos para a rede do CAU/BR;
1.2.2. Executar procedimentos, resolver problemas e esclarecer dúvidas relacionadas com instalação, configuração, atualização, funcionamento e uso dos equipamentos necessários ao funcionamento da rede;
1.2.3. Monitorar e resolver problemas de mau funcionamento, baixo desempenho ou de excessivo consumo de recursos dos equipamentos componentes da rede do CONTRATANTE;
1.2.4. Prover suporte técnico para realizar intervenções (manutenção corretiva ou preventiva) nos servidores e ativos de rede do CAU/BR;
1.2.4.1. Os serviços de suporte incluem prestar informações e orientações necessárias à utilização e ao perfeito funcionamento da solução.

1.3. Realizar as atividades de gestão e administração da rede, que contempla:
1.3.1. Manter atualizada a documentação da rede do CAU/BR;
1.3.2. Implantar os critérios, permissões, procedimentos e planos definidos/elaborados pelo CAU/BR, para manter, administrar, gerenciar e evoluir a plataforma de TI do CAU/BR;
1.3.3. Elaboração e/ou reformulação de projetos de infraestrutura de TIC;
1.3.4. Manter, com atualização semanal, os registros e documentação de inventário de hardware e de software para toda a rede do CAU/BR, incluindo servidores, ativos e estações de trabalho;

1.3.4.1. Notificar o CAU/BR sobre inclusões e exclusões de hardwares e softwares em sua rede;
1.3.5. Administrar e acompanhar, com atualização semanal, as atualizações de vacinas de antivírus em servidores e estações, reportando ao CAU/BR os seguintes casos:
1.3.5.1. Ocorrência de servidor ou estação sem antivírus instalado;
1.3.5.2. Ocorrência de servidor ou estação com antivírus desatualizado;
1.3.5.3. Ocorrência de detecção de vírus em estações ou servidores;
1.3.5.4. Reincidências.
1.3.6. Administrar e acompanhar, com atualização semanal, as atualizações de software (patch Management) em servidores e estações, incluindo:
1.3.6.1. Agendar o download centralizado de patches para sistemas operacionais e aplicativos Microsoft;
1.3.6.2. Aprovar a aplicação das atualizações e patches Microsoft, após anuência do CONTRATANTE.
1.3.7. Prover acesso remoto seguro à rede do CAU/BR, para seus colaboradores e prepostos previamente autorizados, por meio VPN;
1.3.8. Emitir relatório semanal contendo informações de uso dos links de internet, contemplando no mínimo:
1.3.8.1. Gráfico do consumo total de banda (download e upload);
1.3.8.2. As 10 aplicações mais bloqueadas e acessadas;
1.3.8.3. Os 10 usuários que mais consumiram link internet.
1.3.9. Elaborar projetos para implantação, ativação ou desativação de servidores, ativos e serviços de rede;
1.3.9.1. Prover suporte técnico para implantar e acompanhar os projetos elaborados;
1.3.9.2. A CONTRATADA deverá sempre que necessário realizar em conjunto com o CONTRATANTE atividades como a indicação de boas práticas para viabilidade de novos projetos, consolidação de processos de trabalho, emissão de parecer especializado, entre outros cuja característica e escopo estejam contemplados pela natureza dos serviços objeto deste Edital e seus anexos.
1.3.10. Emitir, mensalmente, relatórios com informações sobre chamados (também denominados *Tickets* ou Ordens de Serviço) abertos junto à Equipe de Suporte Técnico da CONTRATADA;
1.3.11. Avaliar periodicamente o acervo de dados armazenados nos servidores do CAU/BR, propondo com base em informações de estatísticas de acessos e datas de modificações o arquivamento permanente (*Archiving*) de dados e informações (arquivos, documentos, logs, *backup*s, versões, etc);
1.3.12. Realizar verificações periódicas de conformidade em relação aos planos, procedimentos, processos e diretrizes de operação, suporte e administração da rede vigentes.

1.4. Realizar serviços de consultoria e governança
1.4.1. Elaborar e/ou revisar, e implantar, projetos, políticas, planos e procedimentos cujo escopo seja objeto dos serviços contratados por meio deste Edital e seus anexos.
1.4.1.1. Faz parte do escopo deste item realizar em conjunto com o CONTRATANTE atividades especiais, tais como a indicação de boas práticas para viabilidade de novos projetos, consolidação de processos de trabalho, emissão de parecer especializado, entre outros.
1.4.2. Emitir, a pedido do CONTRATANTE, pareceres, laudos, diagnósticos ou outros documentos sobre os serviços objeto deste Edital e seus anexos.
1.4.3. Apoiar e/ou participar, dentro do escopo dos serviços objeto desta Licitação e sempre que solicitado pelo CONTRATANTE, de grupos de trabalho, reuniões e/ou projetos. A título de exemplificação, são exemplos de projetos e/ou atividades que demandam este tipo de participação (sem esgotar a lista) eleições informatizadas, implantação e auditoria de

procedimentos de Certificação de Qualidade ISO 9001, adequações em plataformas de TI visando obtenção de conformidade legal, entre outras.
1.4.4. Propor a definição, e com base nos critérios definidos pelo CONTRATANTE, elaborar:
1.4.4.1. Política/procedimento de controle de mudanças (*Change Management*) para conformidade de execução de atividades de manutenção, operação e administração da rede, e respectivas definições das responsabilidades e prerrogativas de cada membro da equipe nestes processos;
1.4.4.2. No caso específico de elaboração de *Change Control Management* para aplicação/uso em administração e firewall, a política/procedimento deverá contemplar no mínimo os seguintes itens:
1.4.4.2.1. Criação/alteração/exclusão de objetos/entidades;
1.4.4.2.2. Criação/alteração/exclusão de regras de filtragem;
1.4.4.2.3. Criação/alteração/exclusão de políticas/perfis de usuários;
1.4.4.2.4. Modificações de configurações/parâmetros do sistema;
1.4.4.2.5. Patching (atualizações corretivas e/ou evolutivas);
1.4.4.2.6. Testing (homologação de modificações realizadas);
1.4.4.2.7. Janelas de manutenção;
1.4.4.2.8. *Backup* de configurações;
1.4.5. Elaborar, especificamente para a operação e administração de objetos da rede, os seguintes planos/regras/diretrizes:
1.4.5.1. Nomenclatura de entidades;
1.4.5.2. Nomenclatura de comentários e observações a serem utilizados em relatórios, configurações de ativos e outros documentos;
1.4.5.3. Nomenclatura de termos para uso em *Tickets* (Service-desk);
1.4.5.4. Identidade visual (ícones a serem associados às entidades, políticas, etc) em gráficos usados em documentação e consoles de administração;
1.4.5.5. Ordem, organização e agrupamento de regras e políticas de firewall;
1.4.5.6. Padrões de termos e textos para notificações automáticas de ocorrência de eventos, textos de chamados, textos de avisos/alertas.

1.5. Realizar diagnósticos em caso de problemas
1.5.1. Os diagnósticos poderão ser solicitados sob demanda pelo CONTRATANTE, ou realizados por iniciativa da CONTRATADA.
1.5.2. Os diagnósticos têm por objetivo a identificação de problemas de infraestrutura de TIC no ambiente de produção do CAU/BR (descrito no Anexo I - B), contemplando a medição e avaliação de seus parâmetros ou atributos. Os parâmetros e/ou atributos a serem considerados neste trabalho são os listados abaixo:
1.5.2.1. Performance (tempo de resposta dos serviços de TIC);
1.5.2.2. Disponibilidade (índice de tempo em que os serviços permanecem disponíveis para seus usuários);
1.5.2.3. Confiabilidade (capacidade do sistema em operar nas condições para as quais foi projetado, eventualmente operando em regime de contingência);
1.5.2.4. Segurança (proteção do sistema - capacidade do sistema em identificar e repelir ações maliciosas, não autorizadas ou ilegítimas, acidentais ou propositais);
1.5.2.5. Escalabilidade (Capacidade de expansão do sistema para acomodar maior demanda, sem que sejam necessárias alterações fundamentais no seu projeto);
1.5.2.6. Resiliência (capacidade do sistema manter operação normal mesmo em condições adversas);
1.5.2.7. Compatibilidade (capacidade de estabelecer conexões serviços, dispositivos ou ambientes de terceiros);
1.5.2.8. Topologia (segmentação física e lógica das conexões de dados).

1.5.3. Além da infraestrutura de tecnologia, o escopo dos serviços de avaliação também inclui os processos de trabalho adotados para implantar e operar os recursos de TIC do CAU/BR. As não-conformidades detectadas serão objeto de diagnóstico específico. Cada diagnóstico deverá apresentar as causas e efeitos do problema, bem como a(s) recomendação(ões) de solução(ões). A abrangência deste trabalho de avaliação compreende a lista de itens descrita a seguir:

Cabling (topologia física)
1.5.3.1. Topologia física;
1.5.3.2. Segmentação;
1.5.3.3. Pontos de rede – identificação, documentação As-Built.

Projeto da Rede
1.5.3.4. Topologia lógica;
1.5.3.5. Endereçamento de rede TCP/IP;
1.5.3.6. Regras de nomenclatura;
1.5.3.7. Resolução de nomes (Tais como DNS, WINS, gatekeeper).

Serviços de rede
1.5.3.8. Servidores de rede e distribuição dos serviços de rede em operação em cada servidor (tais como – sem esgotar a lista - compartilhamento de arquivos, DNS, DHCP, NTP, impressão, proxy Web, firewall, acesso à Internet, e-mail, intranet, autenticação, etc).

Ativos
1.5.3.9. Captura e análise de logs de servidores e ativos de rede;
1.5.3.10. Refrigeração / ventilação dos ativos de rede;
1.5.3.11. Configuração dos ativos de rede.

Tráfego
1.5.3.12. Captura e análise de tráfego na rede;
1.5.3.13. Identificação de gargalos, sobre utilização, colisões (camada 2) e outras causas que impactam na performance da rede;
1.5.3.14. Os diagnósticos e propostas de solução deverão contemplar, no mínimo, os seguintes tópicos:
1.5.3.14.1. Elaboração ou reformulação de projetos;
1.5.3.14.2. Suporte técnico para implantar os projetos elaborados
1.5.3.14.3. Suporte técnico para realizar intervenções (manutenção corretiva ou preventiva) nos servidores e ativos de rede do CAU/BR.

ANEXO I - D

Especificações dos Serviços de Acesso Wireless gerenciado e seguro à rede local

1. Acesso à rede Sem fio (Wireless) Seguro e Gerenciado: fornecimento de solução de acesso à rede sem-fio como serviço, com gerenciamento e segurança, composta por 8 (oito) equipamentos de ponto de acesso (*Access Points* - AP), compreendendo equipamentos (hardwares), softwares e prestação de serviços, conforme especificações a seguir:

1.1. Integração:
1.1.1. Os equipamentos de ponto de acesso (*Access Points)* deverão ser de mesma marca (ou completamente compatíveis) com o Firewall (vide ANEXO I - A), e funcionar de maneira integrada, conforme especificado abaixo:
1.1.1.1. O Firewall deverá atuar como controlador dos equipamentos de ponto de acesso sem-fio, gerenciando o tráfego da WLAN (Wireless LAN);
1.1.1.2. Os usuários da rede sem fio deverão ser controlados e autenticados pelo Firewall, por meio de *Captive Portal;*
1.1.1.3. Permitir a administração centralizada dos APs sem a necessidade de configurar os APs individualmente;
1.1.1.4. A instalação dos equipamentos AP deverá ser do tipo "*plug-and-play*", com detecção automática pelo Firewall;
1.1.1.5. Integração com as funcionalidades de autenticação do Firewall e do serviço de diretório da rede do CAU/BR (MS-AD).

1.2. Características Técnicas dos equipamentos Access Points:
1.2.1. Para instalação *Indoor*, em teto, cor predominante branca;
1.2.2. Implementar os padrões abertos de gerência de rede SNMP;
1.2.3. Operar simultaneamente nas frequências de 2.4GHz e 5GHz, com rádios distintos;
1.2.4. Permitir a criação de – no mínimo – 8 SSID's – para cada rádio;
1.2.5. Permitir a configuração de *Hidden SSID's* (SSID's ocultos);
1.2.6. Suportar os padrões IEEE 802.11 a/b/g/n/ac;
1.2.7. Suportar o padrão 802.11r (*fast transition*);
1.2.8. Permitir alimentação elétrica por meio de Power Over Ethernet (PoE), padrão 802.3at;
1.2.9. Possuir capacidade de selecionar dinamicamente a frequência de operação (DFS);
1.2.10. Permitir o controle da potência de transmissão (*Transmit Power Control* - TPC);
1.2.11. Funcionar em modo *Bridge* para LAN e/ou VLAN, com capacidade de isolamento dos dispositivos clientes;
1.2.12. Suportar padrão de criptografia WPA2 Personal e WPA2 Enterprise;
1.2.13. Capacidade de detectar "*Rogue AP"*, ou seja, detectar a existência em funcionamento de outros equipamentos AP cuja instalação/operação/sinal de rádio não tenha sido autorizado para uso no CAU/BR (ilegítimo);
1.2.14. Capacidade de detectar interferência;
1.2.15. Possuir funcionalidade de visualização de dispositivos conectados e histórico das conexões;
1.2.16. Permitir atualização de firmware automática;
1.2.17. Possuir capacidade de alta disponibilidade (HA);
1.2.18. Possuir funcionalidades de segurança específicas para controle de dispositivos *BYOD;*

1.3. Características exigidas da funcionalidade *Captive Portal*:
1.3.1. Permitir personalizar o portal de conexão e autenticação com a logomarca do CAU/BR;
1.3.2. Permitir acesso de convidados com navegação controlada para acesso a aplicações, redes e serviços de rede (*walled garden);*

1.3.3. Possuir capacidade de emitir vouchers com senha do dia e/ou cota de tempo para acesso a Internet;
1.3.4. Possuir funcionalidade de *T&C Acceptance (Terms and Conditions)*, exibindo para os usuários da rede Wireless os termos e condições de aceitação para fazer uso da rede sem fio, e exigindo a concordância do usuário para permitir sua conexão.

2. Características específicas do serviço de acesso sem-fio
2.1. Instalação e configuração
2.1.1. Os equipamentos deverão ser instalados, física e logicamente, pelos técnicos da CONTRATADA, com acompanhamento dos técnicos do CONTRATANTE.
2.1.2. Fisicamente, os equipamentos AP fornecidos como serviço deverão substituir aqueles atualmente em uso no CAU/BR, nos mesmos locais e utilizando os mesmos pontos de rede já instalados.
2.1.3. Todos os custos de pessoal para efetuar a implementação dos equipamentos, tais como passagens áreas ou terrestres, hospedagem, alimentação, deslocamentos e demais custos, serão de responsabilidade da CONTRATADA.
2.1.4. Os técnicos da CONTRATADA envolvidos na instalação e configuração dos equipamentos adquiridos deverão ser certificados pelo fabricante.
2.1.5. Os serviços de instalação também englobarão as seguintes atividades:
2.1.5.1. Desempacotamento dos equipamentos, verificação e conferência dos componentes;
2.1.5.2. Definição dos procedimentos e melhores práticas de instalação;
2.1.5.3. Montagem física dos equipamentos, instalação básica dos equipamentos de acordo com as recomendações do fabricante, realizar conexões do tipo física, lógica e elétrica;
2.1.5.4. Instalação física de todos os hardwares fornecidos na sede do CAU/BR, conexão lógica, atualizações de softwares, patches, drivers e firmwares para suas mais recentes versões suportadas antes da ativação dos mesmos em produção;
2.1.5.5. Realizar a ativação e configuração do acesso de gerenciamento remoto dos equipamentos fornecidos;
2.1.5.6. Configuração das ferramentas de gerenciamento e administração do equipamento;
2.1.5.7. Configuração dos equipamentos, conforme definido pela CONTRATANTE;
2.1.5.8. Realização de testes de verificação ao término da instalação;
2.1.5.9. Desinstalação física e lógica dos equipamentos AP atualmente em uso, preservando a continuidade das operações e todas as configurações previamente efetuadas para o ambiente da Autarquia.

3. Requisitos de Suporte Técnico específicos para os serviços de acesso à rede sem fio
3.1. As condições listadas abaixo, específicas para suporte técnico aos serviços de acesso à rede sem-fio serão exigidas da CONTRADA.
3.1.1. Os serviços de suporte devem contemplar atualizações de firmware e versões de software disponibilizadas pelo fabricante da solução, ajustes e configurações de acordo com as melhores práticas e recomendações do fabricante da solução, procedimentos destinados a manter e/ou recolocar a solução em pleno e perfeito estado de uso, nos casos de inoperância total ou parcial, defeito ou mau funcionamento;
3.1.2. Os serviços de suporte incluem atender solicitações de suporte técnico relacionado a problemas, erros apresentados e forma de utilização da solução e correções necessárias para o restabelecimento das suas funcionalidades, de acordo com as melhores práticas e recomendações do fabricante dos equipamentos AP;
3.1.3. Os serviços de suporte incluem prestar informações e orientações necessárias à atualização e ao perfeito funcionamento da solução;
3.1.4. Os serviços de suporte contemplam o funcionamento adequado do produto, aplicação de patches de correção e apoio na atualização das versões, incluindo:
3.1.4.1. Atualizações de módulos e softwares;

3.1.4.1.1. Atualização das assinaturas de software de subscrição (módulos) durante o período de vigência do contrato, fornecidos pelo seu fabricante;
3.1.4.2. Garantias de hardware;
3.1.4.2.1. A garantia de hardware deverá incluir a substituição de peças defeituosas sem ônus para o CONTRATANTE durante a vigência do contrato;
3.1.4.2.2. Na eventualidade de o CONTRATANTE necessitar dos serviços de garantia de hardware ou houver a retirada de equipamento para manutenção externa pela CONTRATADA, esta deverá disponibilizar outro equipamento de capacidade igual ou superior para uso do CONTRATANTE em caráter provisório e temporário, e sem perda das funções em utilização, durante o período em que o equipamento estiver em manutenção, evitando a interrupção dos serviços de rede doCONTRATANTE, até que o equipamento removido seja restituído devidamente reparado, em perfeitas e plenas condições de uso.
3.1.4.2.3. Em caso de necessidade de retirada com substituição provisória descrita no parágrafo anterior, a CONTRATADA se compromete a providenciar solução de contorno dentro dos prazos de nível de serviço estipulados por este Edital, e fornecer o equipamento de substituição até o final do próximo dia útil subsequente (*next business day - NBD*) ao do registro da solicitação.
3.2. Treinamento de Operação e administração da solução de acesso sem-fio.
3.2.1. A CONTRATADA deverá ministrar treinamento relativo à instalação, operacionalização, manuseio, configuração e utilização da solução de Acesso sem-fio, visando garantir a transferência de conhecimento para até 4 (quatro) pessoas indicadas pelo CONTRATANTE.
3.2.2. O treinamento deverá possuir carga horária mínima de 10 (dez) horas, observando-se que o treinamento deverá conter todo o conteúdo descrito no item anterior.
3.2.3. As datas e horários para realização dos treinamentos serão definidos pelo CONTRATANTE em comum acordo com a CONTRATADA.
3.2.4. O treinamento deverá ser realizado nas instalações (sede) do CONTRATANTE, e seu conteúdo programático (ementa) deverá ser apresentado com antecedência mínima de 5 (cinco) dias úteis antes de seu início.
3.2.5. Deverão ser utilizadas apostilas impressas, uma por participante, e o instrutor deverá possuir experiência em treinamentos desta natureza, bem como certificação do fabricante.
3.2.6. Deverá ser emitido certificado aos participantes do treinamento que cumprirem frequência mínima de 80%.

ANEXO I - E

Especificações dos Serviços de Operação de *Backup*s

1. Atividades de operação, configuração e gerenciamento de Cópias de Segurança de Dados (*backup*s)

1.1. O serviço de operação, configuração, gerenciamento e monitoramento de cópias de segurança de dados (*backups*) será prestado pela CONTRATADA.

1.1.1. A CONTRATADA deverá fornecer ferramenta (software e/ou *appliance* de *backup*), durante toda a vigência do contrato, conforme especificações técnicas deste Anexo.

1.1.2. Caso a CONTRATADA opte por utilizar ferramenta em software, o CONTRATANTE cederá 1 (uma) máquina virtual, para uso da CONTRATADA, com a finalidade específica de instalação de sua ferramenta.

1.1.3. O CONTRATANTE permitirá a instalação de agentes e/ou softwares componentes da ferramenta de *backup* em seus servidores/hosts, para a finalidade exclusiva de realização das cópias de *backup*.

1.1.4. O CONTRATANTE é responsável por fornecer as mídias e/ou acesso às áreas de armazenamento onde as cópias de *backup* deverão ser armazenadas.

1.2. A CONTRATADA deverá realizar os serviços de *Backup* em conformidade com o Plano de *Backup* fornecido pelo CONTRATANTE.

1.2.1. O Plano de *Backup* especificará as tarefas (Jobs) de *backup* a serem realizadas, e seus respectivos dados de frequência/periodicidade, origem dos dados, destino (repositório) dos dados, período de retenção da informação de *backup*, bem como o período de tempo (janela de *backup*) disponível para execução de cada tarefa ou para um conjunto de tarefas.

1.3. As atividades de *backup* compreenderão a realização de cópias de segurança de máquinas virtuais, bancos de dados, arquivos em servidores, configurações de ativos de rede, bem como a restauração, em caso de necessidade, destas cópias de segurança.

1.4. Fazem parte das atribuições da CONTRATADA:

1.4.1. Realizar configurações na ferramenta de *backup*, como criação de tarefas (jobs), políticas de *backup*, agendamentos, volumes, adicionar drives e mídias, gerenciamento de máquinas clientes e qualquer outra configuração que se fizer necessária para adequada administração da solução de *backup*;

1.4.2. Revisar as políticas de *Backup*, com apoio do CONTRATANTE, identificando possíveis alterações que favoreçam o desempenho da solução assim como manter a organização lógica e estruturada dos itens de configuração;

1.4.3. Configurar e reconfigurar políticas e tarefas de *backup* adicionando ou eliminando máquinas servidoras (físicas e/ou virtuais), pastas e arquivos objetos de *backup* e agendamentos;

1.4.4. Realizar operações de *backup* e restauração de dados sob demanda;

1.4.5. Realizar as operações periódicas de *Backup* conforme o plano de *Backup*, e verificar o resultado de sua execução;

1.4.5.1. Em caso de ocorrência de falha na execução de uma tarefa (*Job*) de *backup*, a CONTRATADA deverá registrar um chamado (*Ticket*) no sistema de *service-desk.*

1.4.6. Monitorar e analisar tarefas de *backup* (jobs) e políticas, e em caso de incidentes, obter soluções e resoluções de problemas, mensagens de erros e logs relativos aos status dos *backup*s realizados ou que falharam;

1.4.7. Elaborar planos de configuração visando melhorias na performance e usabilidade, incluindo procedimentos de *Disaster Recovery*;

1.4.8. Apoiar o registro, o diagnóstico, a solução de problemas e outras atividades correlatas;

1.4.9. Testar as cópias de *backup*, periodicamente, conforme frequência estabelecida no Plano de *Backup*, restaurando os arquivos em área de testes (não-produção) e verificando sua integridade e disponibilidade para uso;

1.5. Sobre a restauração/recuperação de informações:
1.5.1. Em caso de necessidade, o CONTRATANTE registrará um chamado de suporte técnico (*Ticket*) solicitando à CONTRATADA a recuperação de arquivo ou arquivos, a partir das cópias de *backup* disponíveis. A solicitação deverá indicar o local onde o arquivo/arquivos deverão ser gravados.
1.5.2. O atendimento à solicitação de restauração/recuperação de *backup* deverá ser executado pela CONTRATADA conforme as condições, termos e exigências de suporte técnico deste Edital aplicáveis, com o cuidado adicional de verificar o local onde a restauração/recuperação deverá ser gravada.
1.5.3. Exportar semanalmente backup de arquivos considerados essenciais em HDs externos a serem fornecidos pela contratante, visando possível necessidade de *disaster recovery*;
1.5.4 Em caso de necessidade, realizar procedimento de *disaster recovery* com a finalidade de restaurar em ambiente a ser definido pela CONTRATANTE os arquivos exportados semanalmente em discos externos

2. Especificação técnica mínima para a ferramenta de Cópias de Segurança de Dados (*backup*s)

2.1. Especificações gerais do serviço de segurança
2.1.1. Fornecimento como serviço de solução de cópia (*backup*) de dados para ambiente virtualizado do CAU/BR, para criação de ambiente de cópia / recuperação (*backup*/restore), local e remoto, para discos e unidade de fitas e solução de replicação/DR (*Disaster Recovery*) entre estruturas heterogêneas de diferentes fabricantes.
2.1.2. A garantia de funcionamento e atualização da ferramenta, bem como o seu suporte técnico preventivo, evolutivo e corretivo, para a solução, durante a toda vigência do contrato.
2.1.3. A solução deverá contemplar as rotinas de *backup* dos seguintes ativos:
2.1.3.1. Até 20 (vinte) servidores virtuais – plataforma *MS VM-Ware*, hospedados nos servidores físicos;
2.1.3.2. Até 02 (dois) servidores físicos – Servidores Vmware;
2.1.3.2.1. Servidores *Dell PowerEdge* R730;
2.1.3.2.2. Sistema Operacional: *VMware ESXi* 6.0.0 build-3073146;
2.1.3.2.3. CPU: x2 Intel(R) Xeon(R) CPU E5-2630 v3 @ 2.40GHz 8 Núcleos;
2.1.3.2.4. RAM: 128 GB DDR 4.
2.1.4. A solução deverá incluir funcionalidades de proteção (*backup*) e replicação integradas em uma única solução, incluindo retorno (*rollback*) de réplicas e replicação desde e até a infraestrutura virtualizada.
2.1.5. A solução deverá garantir, no mínimo, a proteção de máquinas virtuais e seus dados, gerenciadas através das soluções de virtualização VMware.
2.1.6. A solução deverá ter a capacidade de replicação de dados armazenados entre *storages* ou máquinas de configuração e de fabricantes diferentes.
2.1.7. A solução deverá proteger o ambiente, sem interromper a atividade das máquinas virtuais e sem prejudicar sua performance, facilitando as tarefas de proteção (*backup*) e migrações em conjunto.
2.1.8. A solução deverá ter a capacidade de testar a consistência do *backup* e replicação (S.O., aplicação, VM), emitindo relatório de auditoria para garantir a capacidade de recuperação.
2.1.9. A solução deverá prover a deduplicação e compressão das máquinas virtuais diretamente e durante a operação de *backup*.
2.1.10. A solução deverá ser capaz de proteger, de forma indistinta uma máquina virtual completa ou discos virtuais específicos de uma máquina virtual.
2.1.11. Deverá ser fornecida ferramenta de gestão de arquivos para os administradores de máquinas virtuais no console do operador.

2.1.12. A solução deverá ter a capacidade de integração através de API's dos fabricantes de infraestrutura virtualizada para a proteção de dados.
2.1.13. A solução deverá ter a capacidade de realizar proteção (*backup*) incremental e replicação diferencial, aproveitando a tecnologia de "rastreio de blocos modificados" (CBT – *changed block tracking*), reduzindo ao mínimo necessário, o tempo de *backup* e possibilitando proteção (*backup* e replicação).
2.1.14. A solução deverá oferecer múltiplas estratégias e opções de transporte de dados para as áreas de proteção (*backup*) a saber:
2.1.14.1. Diretamente através de *Storage Area Network (SAN);*
2.1.14.2. Diretamente do *storage*, através do *hypervisor I/O* (*Virtual Appliance*);
2.1.14.3. Mediante uso da rede local (LAN);
2.1.15. A solução deverá poder manter um *backup* sintético, eliminando assim a necessidade de realizar *backup*s completos *(full)* periódicos, incremental permanente, o que permitirá economizar tempo e espaço.
2.1.16. A solução deverá contar com tecnologia de deduplicação também para o ambiente de máquinas virtuais para gerar economia de espaço de armazenamento no repositório de *backup*s sem a necessidade de *hardware* de terceiros (*appliance deduplicadora*).
2.1.17. A solução deverá proporcionar proteção quase contínua de dados (*near-CDP*), permitindo a minimização dos Objetivos de Pontos de Recuperação (RPO).
2.1.18. A solução deverá prover/devolver o serviço aos usuários através da inicialização da máquina virtual que falhou, diretamente do arquivo de *backup*, armazenado no repositório de *backup* de segurança, sem necessidade, inclusive de "hidratação" dos dados gravado no repositório do *backup*, os quais obrigatoriamente deverão estar "deduplicados" e também "comprimidos".
2.1.19. A solução deverá permitir a recuperação de mais de uma máquina virtual e/ou ponto de restauração simultâneo, permitindo assim, ter múltiplos pontos de tempo de uma ou mais máquinas virtuais.
2.1.20. Todo serviço de migração das máquinas virtuais do repositório de *backup* até o armazenamento na produção restabelecida, não deverá afetar a disponibilidade e acesso pelo usuário, sem paradas.
2.1.21. A solução deverá prover acesso ao conteúdo das máquinas virtuais, para recuperação de arquivos, pastas ou anexos, diretamente do ambiente protegido (repositório de *backup*) ou replicados, sem a necessidade de recuperar completamente o *backup* e inicializar.
2.1.22. A solução deverá permitir realizar buscas rápidas mediante os índices dos arquivos que sejam controlados por um sistema operacional Windows, quando este seja o sistema operacional executado dentro da máquina virtual da qual se tenha realizado o *backup*.
2.1.23. A solução deverá assegurar a consistência de aplicações transacionais de forma automática por meio da integração com Microsoft VSS, dentro de sistemas operacionais Windows.
2.1.24. A solução deverá permitir realizar a truncagem de logs transacionais (*transaction logs*).
2.1.25. A solução deverá permitir notificações por correio eletrônico, *SNMP* ou através dos atributos da máquina virtual do resultado da execução de seus trabalhos.
2.1.26. A solução deverá permitir recuperar no nível de objetos de qualquer aplicação virtualizada, em qualquer sistema operacional, utilizando as ferramentas de gestão das aplicações existentes.
2.1.27. A solução deverá incluir ferramentas de recuperação, mediante as quais os administradores dos servidores de serviços de diretório, tais como Microsoft *Active Directory*, possam recuperar objetos individuais, tais como usuários, grupos, contas, Objetos de Política de Grupo *(GPOs)*, registros do *Microsoft DNS* integrados ao *Active Directory* entre outros, sem a necessidade de recuperar os arquivos das máquinas virtuais como um todo ou reiniciar a mesma.

2.1.28. A solução deverá incluir ferramentas de recuperação, mediante as quais os administradores dos servidores de banco de dados, possam recuperar objetos individuais, tais como bases, tabelas, registros, entre outros, sem a necessidade de recuperar os arquivos das máquinas virtuais como um todo ou reiniciar a mesma.
2.1.29. A solução deverá oferecer testes automatizados de recuperação para todas as máquinas virtuais protegidas, gerando confiabilidade de 100% na execução correta das máquinas virtuais e de suas aplicações (*DNS Server*, Controlador de domínio, etc.).
2.1.30. A solução deverá permitir criar uma cópia da máquina virtual de produção, para criação de ambiente de homologação, teste, QA, etc; em qualquer estado anterior para a resolução de problemas, provas de procedimentos, capacitação, entre outros. Deverá ser possível executar uma ou várias máquinas virtuais a partir do arquivo de *backup*, em um ambiente isolado, sem a necessidade de espaço de armazenamento adicional e sem modificar os arquivos de *backup* (*read-only*).
2.1.31. A solução deverá oferecer trabalhos de cópia de *backup* com implementação de políticas de retenção.
2.1.32. A solução deverá ser fornecida com a funcionalidade de acelerar a rede “WAN” para geração de cópia ou replicação das máquinas virtuais, sem utilização de agentes, nem configurações de rede especiais.
2.1.33. A solução deverá incluir suporte para VMware.
2.1.34. A solução deverá incluir um plug-in para *VMware vSphere Web Client*, afim de permitir o monitoramento da infraestrutura de *backup* diretamente do *vSphere Web Client*, com visibilidade detalhada e geral do estado dos trabalhos e recursos de *backup*.
2.1.35. A solução deverá operar em ambientes virtualizados através das soluções da *VMware*, incluido: *VMware vSphere 5.5* e superiores.
2.1.36. A solução deverá ter a capacidade de monitoramento em tempo real, sem a necessidade de agentes, da infraestrutura virtual e de *backup*, inclusive máquinas virtuais *VMware*, com notificação de problemas de *backup* e desempenho, com geração de alertas e base de conhecimento embutida para resolução dos mesmos.
2.1.37. A solução deverá ter a capacidade de monitoramento e análise de capacidade do ambiente para crescimento, ajustes e planejamentos de crescimento.
2.1.38. A solução deverá garantir a recuperação granular e consistente, sem necessidade de agentes adicionais para o ambiente virtualizado através das soluções acima, principalmente para os seguintes softwares:
2.1.38.1. Microsoft Active Directory Server 2008 SP2 em diante;
2.1.39. A solução deverá ser capaz de realizar réplicas em outros sites ou infraestruturas a partir dos *backup*s realizados.
2.1.40. A solução deverá regular de forma dinâmica e parametrizável, a exigência sobre os sistemas protegidos, de forma tal, que se possa definir limites de utilização de performance em discos para diminuir o impacto na infraestrutura de produção, durante as atividades de *backup*.
2.1.41. A solução deverá permitir um método de fácil de recuperação, desde ambientes de contingência, com as ações pré-configuradas para evitar ações manuais em caso de desastre, similar a um botão de emergência.
2.1.42. A solução deverá oferecer a possibilidade de armazenar os arquivos de *backup* de forma criptografada, com algoritmo mínimo de 256 bits, ativando e desativando tal operação, assim como assegurar o trânsito da informação através desse cenário, mesmo que impacte a performance da gravação.
2.1.43. A solução deverá permitir a criação de níveis de delegação de tarefas (perfis) de recuperação no nível de elementos da aplicação, inclusive para outros usuários, de forma a diminuir a carga de atividades executadas pelo administrador da plataforma.

2.1.44. A solução deverá dispor de funcionalidades integradas que permitam a seleção de um repositório de *backup* que esteja alojado em um provedor de serviços na nuvem (*backup* ou replicação na nuvem – *cloud providers*).
2.1.45. A solução deverá integrar uma solução unificada de monitoração de ambientes virtualizados, com fornecimento de relatórios capazes de apresentar informações do tipo:
2.1.45.1. Relatórios que permitam o planejamento de capacidade;
2.1.45.2. Relatórios que permitam determinar a ineficiência dos recursos em uso;
2.1.45.3. Relatórios que facilitem a visibilidade de tendências negativas e anomalias;
2.1.45.4. Quadros de controle claros, apresentáveis e integráveis em sites web.
2.1.46. A solução deverá correlacionar a execução de trabalhos de *backup* e réplica com os objetos do ambiente virtual.
2.1.47. A solução deverá oferecer a capacidade de relatar o cumprimento das políticas de proteção de dados e disponibilidade de acordo com parâmetros definidos.
2.1.48. A solução deve suportar múltiplas operações dos componentes/servidores participantes da estrutura de *backup*, permitindo atividades de *backup* e recuperação simultâneas;
2.1.49. A solução deve suportar repositório de *backup* com aumento de escala ilimitado para o armazenamento de dados com suporte aos seguintes sistemas de armazenamento:
2.1.49.1. *Microsoft Windows*;
2.1.49.2. *Linux*;
2.1.49.3. Pastas compartilhadas;
2.1.49.4. *Appliances deduplicadoras*.
2.1.50. A solução deve suportar servidores proxy de *backup* virtuais ou físicos para *backup* de máquinas virtuais;
2.1.51. A solução deve estar homologada para os sistemas operacionais Windows ou Linux sem a necessidade de instalação de agentes;
2.1.52. A solução deve possuir a funcionalidade de recuperar dados para servidores diferentes do equipamento de origem;
2.1.53. A solução deve estar licenciada para utilização de no mínimo 1 biblioteca de fita com número independentemente da quantidade de drives e slots operando simultaneamente e com compartilhamento entre os *jobs* de *backup*;
2.1.54. Deve ser ofertada a versão mais atual do *software* de *backup*, liberada oficialmente pelo fabricante do software. Caso haja necessidade, por razões de compatibilidade com os demais componentes de hardware e software do ambiente de *backup*, o CONTRATANTE se reserva no direito de utilizar a versão do software imediatamente anterior à versão mais atual, sem nenhum ônus adicional para o CONTRATANTE;
2.1.55. A solução deve possuir compatibilidade com a ferramenta *BitLooker.*
2.2. *Backup* e Restore
2.2.1. As rotinas de *Backup* e Restore deverão ser executadas pela CONTRATADA conforme frequência estabelecida na política de segurança do CAU/BR;
2.2.2. Os *backup*s dos serviços e pastas serão definidos pela CORTI;
2.2.3. Os *backup*s devem ser armazenados em infraestrutura da CONTRATADA;
2.2.4. A CONTRATADA deverá disponibilizar software e hardware de *backup* e restore;
2.2.5. O *backup* deverá ser realizado de acordo com a seguinte agenda:

Semana\Dia	Segunda	Terça	Quarta	Quinta	Sexta	Sábado	Domingo
1 semana	+	+	+	+	+	+	++
2 semana	+	+	+	+	+	+	++
3 semana	+	+	+	+	+	+	++
4 semana	+	+	+	+	+	+	+++

+ Incremental

++ Completo Semanal
+++ Completo Mensal

2.2.6. O período de retenção dos *backup*s deverá ser 6 (seis) meses e respeitar mensalmente a seguinte quantidade de *backup*s:
2.2.6.1. *Backups* diários incrementais;
2.2.6.2. *Backup* Normal por semana;
2.2.6.3. *Backups* normais mensais (a serem armazenadas).

ANEXO I - F

Especificações do Serviço de Monitoramento e Gestão de Rede

1. Especificações gerais do serviço de monitoramento

1.1. Caberá à CONTRATADA realizar continuamente o monitoramento de equipamentos, serviços e aplicações em produção no ambiente de TI da CONTRATANTE, por meio de verificações, testes de comunicações, ferramenta de monitoramento, *check-lists*, *scripts* e outras ferramentas que se fizerem necessárias para execução das atividades, e ainda:

1.2. Monitorar o funcionamento e desempenho dos Serviços e Sistemas integrantes do ambiente de TI do CAU/BR, nas versões atualmente instaladas ou quaisquer outras que venham a ser adotadas.

1.3. A critério do CONTRATANTE, a CONTRATADA deverá incluir, alterar, ou remover itens a serem monitorados nos equipamentos, serviços e aplicações adotados no ambiente de TI do CAU/BR, monitorando, ainda, o desempenho de Sistemas Operacionais e aplicativos, inclusive os que vierem a ser utilizados futuramente.

1.3.1. O serviço de monitoramento deverá contemplar: Servidores Linux e Windows, roteadores, switches, dispositivos access-point, firewalls, outros ativos de rede desde que compatíveis com os protocolos de monitoramento SMNP.

1.4. A CONTRATADA deverá prover e disponibilizar acesso para o CAU/BR ao sistema de monitoramento dos ativos, servidores e serviços de rede, em regime ininterrupto 24x7 (24 horas, 7 dias por semana), com emissão de relatórios e alertas para falhas ou sobrecarga de utilização, conforme descrito a seguir:

1.4.1. A CONTRATADA deverá, além de operar e disponibilizar acesso ao seu próprio sistema de monitoramento externo, implantar uma instância de sistema e/ou ferramenta de monitoramento para funcionar na rede local do CAU/BR, configurada e mantida em funcionamento para gerar as mesmas métricas e informações, evitando que eventuais indisponibilidades em links de acesso impeçam a coleta de indicadores e emissão de alertas.

1.4.1.1. Exclusivamente para a finalidade descrita no item anterior, o CONTRATANTE cederá para uso da CONTRATADA 1 (uma) Máquina Virtual sem sistema operacional. A CONTRATADA poderá implantar sua ferramenta de monitoramento nesta Máquina Virtual, ou a seu exclusivo critério, utilizar hardware próprio;

1.4.1.2. A Implantação desta ferramenta será supervisionada e homologada pelo CONTRATANTE, para que seu funcionamento não introduza riscos à rede do CAU/BR.

1.4.2. O monitoramento deverá gerar gráficos de utilização dos ativos em tempo real.

1.4.3. O monitoramento deverá gerar relatórios diários, semanais e mensais emitidos automaticamente e enviados via e-mail para a equipe técnica do CONTRATANTE.

1.4.4. O monitoramento deverá disponibilizar mapa customizado da rede, com representação gráfica por meio de ícones dos principais ativos e links de rede, e informações de banda dos links utilizados, para permitir ampla visualização do ambiente de rede e dos ativos monitorados, com fácil acesso ao monitoramento destes ativos e atualização em tempo real.

1.4.4.1. O mapa customizado deverá representar graficamente os ativos de rede e os links de acesso de acesso com cores distintas conforme o estado de sua disponibilidade (no mínimo duas cores, uma cor para indisponível outra cor para representar funcionamento normal).

1.4.5. O monitoramento deverá possuir sistema de alerta automatizado que permita informar por meio de SMTP (e-mail) ocorrências de eventos críticos ou pré-configurados:

1.4.5.1. Alta utilização de memória;

1.4.5.2. Alta utilização de processador;

1.4.5.3. Alta utilização das interfaces de rede;

1.4.5.4. Alta utilização do disco e/ou espaço(s) de armazenamento permanente(s) de ativo de rede;

1.4.5.5. Alta utilização de links de comunicação de dados.

1.4.6. A ferramenta deverá monitorar as ocorrências de indisponibilidade de:
1.4.6.1. Ativos de rede;
1.4.6.2. Serviços de rede (tais como DHCP, DNS, etc);
1.4.6.3. Aplicações WEB;
1.4.6.4. Serviços de Streaming de áudio e vídeo;
1.4.6.5. Links de comunicação de dados do CAU/BR.
1.4.7. O monitoramento deverá possuir sistema de alerta automatizado que notifique as mudanças de status de "disponível" para "indisponível" e vice-versa, conforme critérios de verificação de disponibilidade definidos pelo CONTRATANTE.
1.4.7.1. As notificações de indisponibilidade detectadas pela instância interna deverão, automaticamente, registrar um chamado (abertura de *Ticket*) no sistema de registro de serviços;
1.4.7.2. O monitoramento não deverá registrar mais de um alerta nem mais de um chamado para uma mesma ocorrência de indisponibilidade, evitando as "tempestades de alertas";
1.4.7.3. Os índices de disponibilidade de ativos e serviços monitorados, medidos em períodos mensais, deverão obrigatoriamente compor o Relatório Mensal de Progresso e Acompanhamento.

ANEXO I - G

1. Especificações técnicas mínimas relativas ao item 3.5 do Termo de Referência (Portas Necessárias 264)

1.1. Deve possuir no mínimo 24 portas Switch Gigabit Ethernet 10/100/1000BaseT com conectores RJ 45 diretamente no equipamento não sendo permitido o uso de conectores do tipo TELCO ou harmônicas;
1.2. Deve suportar no mínimo a instalação de 2 portas 1000BaseX, podendo ser configurada com interfaces 1000BaseSX ou 1000BaseLX;
1.3. Deve possuir Power Over Ethernet (PoE), IEE 802.3af e IEE 802.3at;
1.4. Todas as portas devem ser autosense, suportando auto negociação de banda 10Mbps, 100Mbps ou 1000Mbps e também auto negociação de modo Full-Duplex ou Half-Duplex;
1.5. Deve possuir capacidade de switching de no mínimo 48 (quarenta e oito) Gbps;
1.6. Deve possuir 4 filas de prioridade com suporte ao protocolo 802.1p e WRR (Weighted Round Robin);
1.7. Deve permitir a configuração de 64 VLANs no protocolo 802.1Q;
1.8. Deve suportar a configuração de no mínimo 4 grupos de portas, contendo até 8 portas por grupo;
1.9. As fontes de operação deverão operar em tensões de 100 a 240 V e em frequências de 50 a 60 Hz;
1.10. Deve conter tabela de endereços MAC com capacidade para no mínimo 8000 endereços MAC;
1.11. Deve possuir LEDs de indicação de status da porta, velocidade e atividade;
1.12. Deve vir acompanhado do kit de suporte específico para montagem em Rack de 19";
1.13. Todas as portas deverão ser auto configuráveis MDI/MDIX;
1.14. Deve suportar gerenciamento via interface Web, com as seguintes facilidades mínimas de configuração:
1.14.1. Velocidade da porta e modo de operação full-duplex;
1.14.2. Protocolo Spanning Tree;
1.14.3. VLANs;
1.14.4. IGMP snooping;
1.14.5. Link aggregation;
1.14.6. IGMP query;
1.14.7. Monitoramento de Tráfego;
1.14.8. Controle de Broadcast;
1.15. Deve possuir garantia da revenda de, no mínimo, 1 ano;
1.16. Deve suportar configuração através de TELNET;
1.17. Deve suportar as seguintes MIBs: MIB II, Bridge MIB e RMON MIB;
1.18. Deve permitir a configuração através de porta serial padrão RS232 ou RJ-45 com conexão a terminal;
1.19. Implementar Gerenciamento via Web;
1.20. Deve suportar gerenciamento RMON implementando no mínimo 4 grupos;
1.21. Deve suportar configuração de endereço IP através de DHCP;
1.22. Deve suportar gerenciamento por SSHv2, HTTP e SNMP v1, v2 e v3;
1.23. Deve Implementar cliente NTP;
1.24. Deve implementar autenticação de acesso ao switch por servidor RADIUS;
1.25. Deve possibilitar a limitação da quantidade de sessões de gerência simultâneas;
1.26. Deve permitir a restrição do endereço MAC e do endereço IP da console de gerência para acesso ao switch;

1.27. Deve implementar espelhamento de tráfego para uma porta de monitoração. Deverá ser possível o espelhamento de tráfego de várias portas em uma porta;
1.28. Deve possibilitar *backup* e restore de sua configuração em arquivo texto;
1.29. Deve implementar FTP e TFTP server;
1.30. Deve implementar proteção BPDU;
1.31. Deve implementar CHAP, PAP, EAPoL, PEAP e EAP-TLS para autenticação 802.1x;
1.32. Deve ser capaz de armazenar múltiplas imagens de software simultaneamente.
1.33. O fabricante do switch deve possuir certificação ISO9001.

Processo Administrativo nº 002/2018

PREGÃO ELETRÔNICO Nº 05/2018

ANEXO II – DECLARAÇÃO DE HABILITAÇÃO

(Licitante), pessoa jurídica de direito privado, inscrita no CNPJ/MF sob o nº _____, sediada na _____, representada por _____, (nacionalidade), (estado civil), (profissão), portador(a) da Cédula de Identidade nº _____, inscrito no CPF sob o nº _____, (residência e domicílio), DECLARA que cumpre plenamente os requisitos exigidos para habilitação, conforme prescreve o art. 4º, inciso VII, da Lei nº 10.520, de 17 de julho de 2002, referente ao Pregão Eletrônico nº 05/2018, promovido pelo Conselho de Arquitetura e Urbanismo do Brasil (CAU/BR), estando ciente das penalidades aplicáveis em caso de descumprimento ou declaração inverídica.

Local e data.

Nome e assinatura do representante legal

Processo Administrativo nº 002/2018

PREGÃO ELETRÔNICO Nº 05/2018

ANEXO III – DECLARAÇÃO DE TRABALHO DO MENOR

(Licitante), pessoa jurídica de direito privado, inscrita no CNPJ/MF sob o nº _____, sediada na _____, representada por _____, (nacionalidade), (estado civil), (profissão), portador(a) da Cédula de Identidade nº _____, inscrito no CPF sob o nº _____, (residência e domicílio), DECLARA, para fins de participação no Pregão Eletrônico nº 05/2018, promovido pelo Conselho de Arquitetura e Urbanismo do Brasil (CAU/BR), que atende ao disposto no art. 7º, inciso XXXIII, da Constituição Federal e art. 27, inciso V, da Lei nº 8.666, de 1993, não empregando menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre, e menor de 16 (dezesseis) anos, estando ciente das penalidades aplicáveis em caso de descumprimento ou declaração inverídica.
Ressalva: emprega menor, a partir de 14 (quatorze) anos, na condição de aprendiz, nos termos do art. 429 da Consolidação das Leis do Trabalho. **(se houver)**

Local e data.

Nome e assinatura do representante legal

Processo Administrativo nº 002/2018

PREGÃO ELETRÔNICO Nº 05/2018

ANEXO IV – DECLARAÇÃO DE IDONEIDADE

(Licitante), pessoa jurídica de direito privado, inscrita no CNPJ/MF sob o nº _____, sediada na _____, representada por _____, (nacionalidade), (estado civil), (profissão), portador(a) da Cédula de Identidade nº _____, inscrito no CPF sob o nº _____, (residência e domicílio), DECLARA, para fins de participação no Pregão Eletrônico nº 05/2018, promovido pelo Conselho de Arquitetura e Urbanismo do Brasil (CAU/BR), ser idônea a participar de processo licitatório e contratar com órgãos e entidades da Administração Pública Direta e Indireta Federal, Estadual, do Distrito Federal e Municipal, assim como inexistem fatos supervenientes impeditivos de habilitação, estando ciente das penalidades aplicáveis em caso de descumprimento ou declaração inverídica.

Local e data.

Nome e assinatura do representante legal

Processo Administrativo nº 002/2018

PREGÃO ELETRÔNICO Nº 05/2018

ANEXO V – MODELO DE PLANILHA DE PREÇOS

Item	Descrição	Valor mensal	Valor anual	Valor para o período de vigência do contrato (48 meses)
1	Serviços de Segurança de Rede, incluindo alocação de equipamento do tipo Firewall de rede com funcionalidades de controle de conteúdo, controle de aplicações, VPN, WAF, integração com dispositivos de ponto de acesso sem-fio (AP Wireless), integração com endpoint e balanceamento de links.	R$ XX,XX	R$ XX,XX	R$ XX,XX
2	Provimento de serviços gerenciados de operação e administração de Rede e Servidores de Rede, incluindo suporte técnico preventivo, corretivo e evolutivo.	R$ XX,XX	R$ XX,XX	R$ XX,XX
3	Serviços de Acesso Wireless gerenciado e seguro à rede local, incluindo alocação de equipamento do tipo ponto de acesso de Rede Sem-fio (AP), integrado ao firewall e com funcionalidades de Captive Portal.	R$ XX,XX	R$ XX,XX	R$ XX,XX
4	Serviços Gerenciados de Operação de *Backup*s.	R$ XX,XX	R$ XX,XX	R$ XX,XX
5	Serviços Gerenciados de Monitoramento e Gestão de Rede, incluindo a emissão periódica de relatórios de acompanhamento contendo indicadores de gestão e de progresso/acompanhamento de projetos.	R$ XX,XX	R$ XX,XX	R$ XX,XX
6	Serviços de Segurança de Rede, incluindo alocação de swithes conforme especificação Anexo I - G.	R$ XX,XX	R$ XX,XX	R$ XX,XX
Valor total mensal		R$ XX,XX	R$ XX,XX	R$ XX,XX
Valor total anual				
Valor global para o período de vigência do contrato (48 meses)				

Processo Administrativo nº 002/2018

PREGÃO ELETRÔNICO Nº 05/2018

ANEXO VI – DECLARAÇÃO PARA ME E EPP

(Nome da empresa), estabelecida na _____ (rua; nº e cidade), por seu representante legal _____ (nome do representante, nacionalidade, estado civil, profissão, RG, CPF, endereço domiciliar), DECLARA, sob as penas da lei penal e civil, que a ora declarante está classificada como Microempresa (ME) ou Empresa de Pequeno Porte (EPP) perante (Receita Federal e/ou Secretaria da Fazenda do Estado), assim entendida por preencher os requisitos do artigo 3º da Lei Complementar nº 123, de 2006, do art. 6º do Decreto nº 8.538, de 2015 e, ainda, por praticarem atividades pertinentes ao objeto licitado, comprometendo-se a informar, de imediato, caso deixe de ser enquadrada na condição de Microempresa (ME), nos termos da lei.

Local e data.

Nome e assinatura do representante legal

Processo Administrativo nº 002/2018

PREGÃO ELETRÔNICO Nº 05/2018

ANEXO VII – MINUTA DO CONTRATO

CONTRATO DE PRESTAÇÃO DE SERVIÇOS CAU/BR N° XX/XXXX

Das Partes:

I – CONSELHO DE ARQUITETURA E URBANISMO DO BRASIL (CAU/BR), autarquia federal de fiscalização profissional regida pela Lei n° 12.378, de 31 de dezembro de 2010, inscrito no CNPJ sob o n° XXXXXXX, com sede no XXXX, em Cidade, Estado, CEP XXXX, representado neste ato pelo Presidente, **NOMEAR**, nacionalidade, profissão, portador da Carteira de Identidade nº XXX, expedida pela XXX, e do CPF nº XXX, residente e domiciliado em Cidade, Estado, doravante designado **CAU/BR ou CONTRATANTE**;

II – CONTRATADA, pessoa jurídica de direito privado, inscrita no CNPJ sob o n° XXXXXXXXXXX, com sede na XXXXXXXXXX, Cidade, Estado, CEP XXXX, representada neste ato pelo Cargo, **NOMEAR**, nacionalidade, profissão, portador da Carteira de Identidade nº XXX, expedida pela XXX, e do CPF nº XXX, residente e domiciliado em Cidade, Estado, doravante designada **CONTRATADA**;

RESOLVEM, tendo em vista o constante no Processo Administrativo nº 002/2018, celebrar o presente Contrato de Prestação de Serviços, na forma descrita no Termo de Referência, o que fazem mediante as cláusulas e condições a seguir:

CLÁUSULA PRIMEIRA – DO FUNDAMENTO LEGAL

1.1. O presente contrato é firmado com amparo da Lei nº 10.520, de 17 de julho de 2002, e, subsidiariamente, na Lei nº 8.666, de 21 de junho de 1993, e ainda, no resultado da licitação promovida pelo CAU/BR, por meio do Pregão Eletrônico nº 05/2018 – Processo CAU/BR nº 2/2018, realizada em xx de xxxxx de 2018, e homologada em xx de xxxxx de 2018, pelo Senhor Presidente do CAU/BR, vinculando-se ao presente contrato, como se nele estivessem transcritos de forma integrante e inseparável:

1.1.1. Termo de Referência;

1.1.2. Edital do Pregão Eletrônico CAU/BR nº XX/2018 e seus anexos;

1.1.3. Proposta de preços da CONTRATADA;

1.1.4. Demais elementos constantes do Processo Administrativo nº 002/2018.

CLÁUSULA SEGUNDA – DO OBJETO E SUA DESCRIÇÃO

2.1. O objeto da presente licitação é a escolha da proposta mais vantajosa para a contratação de suporte técnico especializado na área de informática – infraestrutura de redes, incluída cessão em comodato de equipamentos e dispositivos de rede para prestação de serviços de sustentação de infraestrutura, contemplando fornecimento de serviços de segurança da informação; de controle, operação e administração de rede; de acesso à rede local WI-FI com segurança, controle, identificação e gerenciamento; de operação e execução de rotinas e procedimentos de *backup*s; de monitoramento e gerenciamento de ativos de rede; e de serviços de gestão da rede (incluindo medição de indicadores e realização de consultoria, projetos, diagnósticos e laudos), com o objetivo de implantar e manter infraestrutura de Tecnologia de Informação em conformidade com níveis de serviço previamente determinados e de acordo com as boas práticas vigentes, consoante especificações do Termo de Referência, Anexo I do Edital do Pregão Eletrônico nº XX/2018.
2.2. As especificações dos serviços constam do Termo de Referência, Anexo I do Edital do Pregão Eletrônico nº 05/2018.

CLÁUSULA TERCEIRA – DOS VALORES E DOS PAGAMENTOS
3.1. Pela prestação dos serviços, objeto deste Contrato, o CONTRATANTE pagará a CONTRATADA o valor mensal de R$ xxxxxx; o valor anual de R$ xxxxxx e o valor global de R$ XXXXXXXXX, de acordo com a planilha de preços abaixo especificada:

Item	Descrição	Valor mensal	Valor anual	Valor para o período de vigência do contrato (48 meses)
1	Serviços de Segurança de Rede, incluindo alocação de equipamento do tipo Firewall de rede com funcionalidades de controle de conteúdo, controle de aplicações, VPN, WAF, integração com dispositivos de ponto de acesso sem-fio (AP Wireless), integração com endpoint e balanceamento de links.	R$ XX,XX	R$ XX,XX	R$ XX,XX
2	Provimento de serviços gerenciados de operação e administração de Rede e Servidores de Rede, incluindo suporte técnico preventivo, corretivo e evolutivo.	R$ XX,XX	R$ XX,XX	R$ XX,XX
3	Serviços de Acesso Wireless gerenciado e seguro à rede local, incluindo alocação de equipamento do tipo ponto de acesso de Rede Sem-fio (AP), integrado ao firewall e com funcionalidades de Captive Portal.	R$ XX,XX	R$ XX,XX	R$ XX,XX
4	Serviços Gerenciados de Operação de *Backup*s.	R$ XX,XX	R$ XX,XX	R$ XX,XX
5	Serviços Gerenciados de Monitoramento e Gestão de Rede, incluindo a emissão periódica de relatórios de acompanhamento contendo indicadores de gestão e de progresso/acompanhamento de projetos.	R$ XX,XX	R$ XX,XX	R$ XX,XX
6	Serviços de Segurança de Rede, incluindo alocação de swithes conforme especificação Anexo I - G.	R$ XX,XX	R$ XX,XX	R$ XX,XX

Valor total mensal	R$ XX,XX	R$ XX,XX	R$ XX,XX
Valor total anual			
Valor global para o período de vigência do contrato (48 meses)			

3.2. Os pagamentos serão regidos pelo que dispõe o Termo de Referência, Anexo I do Edital do Pregão Eletrônico nº 05/2018.

CLÁUSULA QUARTA – DA DOTAÇÃO ORÇAMENTÁRIA

4.1. As despesas correrão à conta da dotação orçamentária do Conselho de Arquitetura e Urbanismo do Brasil (CAU/BR), a saber:

4.1.1. Fonte: Orçamento CAU/BR 2018;

4.1.2. Conta: 6.2.2.1.1.01.04.04.031 - Serviços de Manutenção Sistema de Informática

4.1.3. Centro de Custo: 4.02.05.001 - Manutenção da Gerência Administrativa

4.2. As despesas referentes aos próximos exercícios deverão ser consignadas em orçamento próprio, nos respectivos exercícios financeiros, e deverão ser confirmadas pelo Gestor do Contrato.

4.3. Fica estabelecido, com a concordância das partes, que a continuidade da execução do contrato será dependente da consignação, nos Orçamentos seguintes, de dotações orçamentárias suficientes ao seu custeio.

CLÁUSULA QUINTA – DA VIGÊNCIA DO CONTRATO E DAS ALTERAÇÕES

5.1. A vigência do contrato terá início na data da sua assinatura e se estenderá por 48 (quarenta e oito) meses, nos termos no art. 57, IV, da Lei 8.666/93.

5.2. A contratada fica 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, conforme legislação vigente.

5.3. O presente contrato poderá ser alterado, mediante a lavratura de Termo Aditivo, conforme previsão legal do art. 65 da Lei nº 8.666, de 1993.

CLÁUSULA SEXTA – DO REAJUSTE

6.1. O reajuste deste Contrato obedecerá às disposições contidas no Capítulo 19 do Termo de Referência, Anexo I do Edital do Pregão Eletrônico nº 05/2018.

CLÁUSULA SÉTIMA – DAS OBRIGAÇÕES DA CONTRATADA

7.1. As responsabilidades e obrigações da Contratada serão regidas pelas disposições do Capítulo 9 do Termo de Referência, Anexo I do Edital do Pregão Eletrônico nº 05/2018 e demais disposições legais aplicáveis.

CLÁUSULA OITAVA – DAS OBRIGAÇÕES DO CONTRATANTE

8.1 As obrigações e responsabilidades assumidas pelo Contratante constam do Capítulo 10 do Termo de Referência, Anexo I do Edital do Pregão Eletrônico nº 05/2018.

CLÁUSULA NONA – DA GARANTIA

9.1. A Contratada compromete-se a prestar a garantia dos serviços conforme descritos no Capítulo 13 do Termo de Referência, Anexo I do Edital do Pregão Eletrônico nº 05/2018.

CLÁUSULA DÉCIMA – DAS SANÇÕES ADMINISTRATIVAS

10.1. A inexecução parcial ou total das condições pactuadas, erro de execução, mora na execução, sujeitará a CONTRATADA às penalidades e determinações descritas no Capítulo 17 do Termo de Referência, Anexo I do Edital do Pregão Eletrônico nº 05/2018 e demais disposições legais aplicáveis.

CLÁUSULA DÉCIMA PRIMEIRA – DA CESSÃO E TRANSFERÊNCIA

11.1. É vedada a cessão ou transferência total ou parcial dos direitos e/ou obrigações inerentes ao Termo de Referência, por quaisquer das partes, sem prévia e expressa autorização da outra.

CLÁUSULA DÉCIMA SEGUNDA – DA TOLERÂNCIA/NOVAÇÃO

12.1. A tolerância não enseja em novação, sendo que qualquer alteração, por mais simples que seja, deverá ser feita obrigatoriamente por ajuste escrito entre as partes.

CLÁUSULA DÉCIMA TERCEIRA – DAS DISPOSIÇÕES ESPECIAIS

13.1. São partes integrantes do presente contrato, para todos os fins de direito, independente de transcrições ou referências, todo o conteúdo do Processo Administrativo CAU/BR nº 002/2018, em cujos autos foi promovido o Pregão Eletrônico nº 05/2018, especialmente o Edital, Termo de Referência e Proposta Comercial apresentada pela CONTRATADA.

13.2. As partes contratantes observarão as disposições constantes do Termo de Referência, anexo a este instrumento, em especial os capítulos que tratam do objeto, das condições de execução dos serviços, da garantia e suporte técnico, das obrigações da contratada e contratante, da aceitação e do pagamento, do acompanhamento e fiscalização e das penalidades.

CLÁUSULA DÉCIMA QUARTA – DO FORO

14.1. O foro competente para dirimir quaisquer dúvidas oriundas do presente contrato, com exclusão de qualquer outro por mais privilegiado que seja, é o da Justiça Federal, Seção Judiciária do Distrito Federal.

E por estarem acordes as partes contratantes, por seus representantes legais, firmam o presente contrato em duas vias de igual teor e forma, na presença das testemunhas abaixo identificadas.

Brasília (DF), XX de XXXXXXX de XXXX.

CONTRATANTE:
CONSELHO DE ARQUITETURA E URBANISMO DO BRASIL

NOMEAR
Presidente do CAU/BR

CONTRATADA:

NOMEAR
Cargo

TESTEMUNHAS:

Assinatura:
Nome:
CPF:

Assinatura:
Nome:
CPF: