CONSELHO REGIONAL DE ECONOMIA
2ª REGIÃO – SÃO PAULO

Rua Líbero Badaró, 425 – 14º Andar - CEP 01009-905 - Tel: (11) 3291-8700 - Fax: (11) 3291-8701
Site : www.coreconsp.org.br – E-mail: licitacoes@coreconsp.org.br

PREGÃO ELETRÔNICO Nº 07/2018

PROCESSO Nº L-07/2018

E D I T A L

De ordem do Senhor Presidente do CONSELHO REGIONAL DE ECONOMIA – 2ª REGIÃO - SÃO PAULO, por meio de seu Pregoeiro designado pela Resolução nº 668 de 03/01/2018, torna público que realizará certame licitatório sob a modalidade **PREGÃO ELETRÔNICO** Nº L 07-2018, do tipo **MENOR PREÇO**, conforme enunciado no item 2. DO OBJETO, regido pelo Decreto 5.450/05 de 31.05.2005, pela Lei nº 10.520/02 de 17.07.2002 e, subsidiariamente, pela Lei nº 8.666, de 21.06.1993, e alterações posteriores, nos termos deste Edital e seus Anexos, e de acordo com as disposições que seguem:

1. DATA, HORA E LOCAL DA ABERTURA

1.1. A abertura da presente Licitação dar-se-á em sessão pública, dirigida pelo pregoeiro designado, a ser realizada de acordo com a legislação mencionada no preâmbulo deste Edital e conforme indicado abaixo:

ENDEREÇO ELETRÔNICO: **www.licitacoes-e.com.br**
DATA DO ENCERRAMENTO DO RECEBIMENTO DAS PROPOSTAS: **10/05/2018**
HORÁRIO: **14h**
DATA DA ABERTURA DAS PROPOSTAS: **10/05/2018**
HORÁRIO: **14h30min**
INÍCIO DA SESSÃO DE DISPUTA DE PREÇOS: **10/05/2018**
HORÁRIO: **15h**
REFERÊNCIA DE TEMPO: **Será observado o horário de Brasília (DF)**

1.2. A sessão de disputa de preços terá duração de, **no mínimo, 10 (dez) minutos**, seguida de um tempo aleatório de **até 30 (trinta) minutos**.

2. DO OBJETO

2.1. O objeto da presente licitação consiste em manter ativo o Suporte Técnico e Atualização dos Produtos DELL SONICWALL CGSS Comprehensive Gateway Security Suite for the NSA 2400 Series por 36 meses, para AGSS Advanced Gateway Security Suíte for the NSA 2400 Series por 36 meses, conforme especificações constantes do Termo de Referência (Anexo I).

3. DAS DISPOSIÇÕES PRELIMINARES

3.1. A proponente que tiver dúvidas quanto à interpretação dos termos deste Edital poderá solicitar esclarecimentos ao Pregoeiro, até três dias úteis anteriores à data fixada para início da sessão de disputa, exclusivamente por e-mail no seguinte endereço: licitacoes@coreconsp.org.br.

3.1.1. As respostas ao pedido de esclarecimentos formulados serão divulgadas mediante publicação no site do CORECON-SP, no seguinte endereço: www.coreconsp.org.br, menu "Licitações".

3.1.2. Em hipótese alguma serão atendidas solicitações verbais.

4. DAS CONDIÇÕES PARA PARTICIPAÇÃO

4.1. Poderão participar deste Pregão quaisquer interessados que atenderem todas as exigências constantes deste Edital e seus Anexos, inclusive quanto às de documentação, observadas, para esse efeito, as condições fixadas em Lei:

4.1.1. Atuar no ramo pertinente ao objeto e comprovar possuir os requisitos mínimos de qualificação estabelecidos neste Edital, observando-se o determinado no art. 9º da Lei nº 8.666/93;

4.2. Não poderão participar, os interessados que se encontrem sob falência, concordata, concurso de credores, dissolução, liquidação ou em regime de consórcio, qualquer que seja sua forma de constituição, empresas estrangeiras que não funcionem no País, nem aqueles que tenham sido declarados inidôneos para licitar ou contratar com a Administração Pública ou punidos com suspensão do direito de licitar e contratar com a Administração Pública, nos termos do art. 87, incisos III e IV da Lei nº 8.666/93.

5. DO CREDENCIAMENTO

5.1. Somente poderão participar deste pregão eletrônico as licitantes devidamente credenciadas junto ao provedor do sistema na página eletrônica do Banco do Brasil: www.licitacoes-e.com.br, nos termos do artigo 3º do Decreto nº 5.450/05, devendo o credenciamento ser realizado no prazo de até 03 (três) dias úteis antes da data prevista para realização do pregão, nos termos do inc. III do art. 7° do Decreto n° 3.697/00.

5.2. O credenciamento dar-se-á pela atribuição de chave de identificação e de senha pessoal e intransferível, para acesso ao sistema eletrônico.

5.3. O credenciamento junto ao sistema eletrônico implica a responsabilidade legal do licitante e de seu representante legal pelos atos praticados e a presunção de capacidade técnica para realização das transações inerentes ao pregão eletrônico, não cabendo ao provedor do sistema ou ao CORECON-SP responsabilidade por eventuais danos decorrentes do uso indevido da senha, ainda que por terceiros.

6. DA CONEXÃO COM SISTEMA E DO ENVIO DAS PROPOSTAS

6.1. A participação neste Pregão Eletrônico dar-se-á por meio da conexão do licitante ao sistema eletrônico mencionado, mediante digitação de sua senha privativa e subsequente encaminhamento da proposta de preços, exclusivamente por meio do referido sistema, até a data e horário de encerramento informado no preâmbulo deste edital.

6.2. A licitante será responsável por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo suas propostas e seus lances como firmes e verdadeiros.

6.3. Como requisito para a participação no pregão eletrônico a licitante deverá manifestar, sob as penas da lei, em campo próprio do sistema eletrônico, o pleno conhecimento e atendimento às exigências de habilitação previstas neste Edital.

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

6.5. Durante a disputa, os lances oferecidos deverão referir-se ao valor total do lote.

6.6. No valor total do lote devem estar inclusos todos os encargos financeiros ou previsão inflacionária, incluindo o montante da mão-de-obra, materiais e equipamentos necessários à execução dos serviços, encargos trabalhistas, sociais, previdenciários e fiscais, incluindo-se no preço quaisquer despesas que decorram da execução do objeto do certame, cabendo ao CORECON-SP pagar somente pelo objeto ora licitado.

6.7. No caso da licitação possuir mais de um lote, o licitante não está obrigado a cotar todos eles, porém, em cada lote ofertado deverão estar incluídos todos os respectivos itens que o compõem, sob pena de desclassificação.

6.8. Até a abertura da sessão, a licitante poderá retirar ou substituir a proposta anteriormente encaminhada.

7. DO CRITÉRIO DE ACEITABILIDADE

7.1. Serão desclassificadas as propostas que não atendam às exigências do ato convocatório.

7.2. Não será levada em consideração proposta que contenha vantagem não prevista neste edital, inclusive aquela caracterizada por valor baseado nas ofertas das demais licitantes.

7.3. A validade da proposta será de, no mínimo, 60 (sessenta) dias, contados da data marcada para abertura das propostas. Em caso de omissão do licitante, será considerado o prazo mínimo exigido.

7.4. Serão desclassificadas as propostas que apresentarem preços manifestamente inexequíveis ou excessivos, consoante o inciso II do artigo 48 da Lei Federal nº 8.666/93.

8. DA ABERTURA DAS PROPOSTAS, ENVIO DOS LANCES E JULGAMENTO

8.1. Na data e horário previstos no preâmbulo deste edital serão abertas as propostas de preços, passando o pregoeiro a avaliar a aceitabilidade das mesmas e verificando a sua conformidade com os requisitos estabelecidos neste instrumento convocatório.

8.2. O pregoeiro efetuará o julgamento das propostas pelo critério tipo **MENOR PREÇO**.

8.3. A partir do horário previsto no edital terá início à sessão pública do Pregão Eletrônico, com a divulgação dos preços das propostas aceitas e convite aos licitantes a apresentarem lances.

8.3.1. Em caso de empate no valor das propostas, a classificação será por ordem de entrega de propostas.

8.4. Aberta a etapa competitiva, os licitantes poderão encaminhar lances exclusivamente por meio do sistema eletrônico, sendo o licitante imediatamente informado do seu recebimento e respectivo horário de registro e valor.

8.5. Os licitantes poderão oferecer lances sucessivos, observado o horário fixado e as regras de aceitação dos mesmos.

8.6. Só serão aceitos os lances cujos valores forem inferiores ao último lance anteriormente ofertado pelo respectivo licitante e registrado no sistema.

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

8.8. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado que tenha sido apresentado pelos demais licitantes, sendo vedada a identificação do autor do lance.

8.9. No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do Pregão Eletrônico, o sistema eletrônico poderá permanecer acessível aos licitantes para o recebimento dos lances, retomando o Pregoeiro, quando possível, sua atuação no certame, sem prejuízo dos atos já realizados.

8.10. Quando a desconexão persistir por tempo superior a 10 (dez) minutos, a sessão do Pregão Eletrônico será suspensa e terá reinício somente após comunicação expressa aos participantes, através de mensagem eletrônica (e-mail) ou via fax, divulgando data e hora para a reabertura da sessão.

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

8.12. A etapa de lances da sessão pública, prevista no edital, será encerrada mediante aviso de fechamento iminente dos lances, emitido pelo sistema eletrônico aos licitantes. Após transcorrerá período randômico de até trinta minutos, aleatoriamente determinado pelo sistema eletrônico, findo o qual será automaticamente encerrado o recebimento de lances.

8.13. Não poderá haver desistência dos lances ofertados, sujeitando-se o proponente desistente às penalidades constantes neste edital.

8.14. Encerrada a etapa competitiva, o pregoeiro poderá encaminhar, pelo sistema eletrônico, contraproposta diretamente ao licitante que tenha apresentado o lance de menor valor, para que possa ser obtida proposta melhor, bem como decidir sobre sua aceitação, não se admitindo negociar condições diferentes das previstas neste Edital.

8.15. O pregoeiro anunciará o licitante detentor da melhor proposta imediatamente após o encerramento da etapa de lances da sessão pública ou, quando for o caso, após negociação e decisão do pregoeiro sobre a aceitação do lance de menor valor. Caso não haja lances, o licitante vencedor será aquele que houver ofertado a melhor proposta inicial.

8.16. Caso a empresa detentora da melhor proposta venha a ser desclassificada ou inabilitada, o pregoeiro examinará as ofertas subsequentes e a qualificação dos licitantes na ordem de classificação, e assim sucessivamente, até a apuração de uma que atenda ao edital, sendo o respectivo licitante declarado vencedor.

8.17. O sistema gerará ata circunstanciada da sessão, na qual estarão registrados todos os atos do procedimento e as ocorrências relevantes, que estará disponível para consulta no endereço eletrônico www.licitacoes-e.com.br.

9. DAS MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE

9.1. As microempresas e empresas de pequeno porte deverão, no ato de envio de suas propostas, para efeito de beneficiarem-se na presente licitação do tratamento diferenciado e favorecido disposto na Lei Complementar nº 123/2006 e Decreto nº 6204/2007, declarar, em campo próprio do sistema, que atendem aos requisitos do artigo 3º dessa Lei.

9.2. A declaração falsa relativa ao cumprimento dos requisitos de habilitação e proposta e de enquadramento no regime da Lei nº 123/2006, sujeitará o licitante às sanções previstas no item 18 deste edital.

9.3. Caso as propostas apresentadas por microempresas e empresas de pequeno porte sejam iguais ou até 5% (cinco por cento) superiores à proposta detentora do melhor lance ou valor negociado, será assegurada preferência de contratação, respeitado o seguinte:

9.3.1. A microempresa ou empresa de pequeno porte mais bem classificada poderá apresentar proposta de preço inferior àquela detentora do melhor lance ou valor negociado, no prazo máximo de 5 (cinco) minutos após a solicitação do Pregoeiro, situação em que será adjudicado em seu favor o objeto deste Pregão;

9.3.2. Não ocorrendo a contratação da microempresa ou empresa de pequeno porte, na forma do subitem anterior, serão convocadas as licitantes remanescentes que porventura se enquadrem na hipótese desta Condição, na ordem classificatória, para o exercício do mesmo direito;

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

9.3.4. Na hipótese da não-contratação nos termos previstos nesta Condição, o objeto será adjudicado em favor da proposta originalmente vencedora do certame.

9.4. O disposto nesta Condição somente se aplicará quando a melhor oferta inicial não tiver sido apresentada por microempresa ou empresa de pequeno porte;

10. DOS RECURSOS

10.1. Declarado o vencedor, qualquer licitante poderá manifestar imediata e devidamente motivado a intenção de recorrer, por meio do sistema eletrônico. Após, lhe será concedido o prazo de 3 (três) dias úteis para apresentação das razões do recurso, ficando os demais licitantes, desde logo, intimados a apresentar contrarrazões em igual prazo, que começará a correr a partir do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos autos, disponíveis na sede do CORECON-SP.

10.2. O acolhimento de recurso importará a invalidação apenas dos atos insuscetíveis de aproveitamento.

10.3. A falta de manifestação imediata e motivada do licitante importará a renúncia do direito de recurso e a adjudicação do objeto da licitação pelo pregoeiro ao vencedor.

10.4. O encaminhamento das razões do recurso e de eventuais contrarrazões pelos demais licitantes será realizado exclusivamente por meio do sistema eletrônico, no site www.licitacoes-e.com.br.

10.5. Julgado o recurso, a decisão será publicada nos endereços eletrônicos www.licitacoes-e.com.br e www.coreconsp.org.br.

11. DA HABILITAÇÃO

11.1. Encerrada a etapa competitiva e ordenada de lances, a licitante detentora da melhor proposta deverá transmitir, em no **máximo 01 (uma) hora**, a documentação relacionada abaixo através do fax (11) 3291-8701, ou através do e-mail licitacoes@coreconsp.org.br, devendo, em ambos os casos, a licitante encaminhar posteriormente os documentos originais ou cópias autenticadas, no prazo máximo de **03 (três) dias úteis** contados da data da realização do Pregão, para a sede do CORECON-SP, aos cuidados do Senhor Pregoeiro.

11.1.1. Caso a empresa opte por enviar a documentação via e-mail, estes deverão ser assinados e escaneados, para o envio eletrônico;

11.1.2. Deverá a empresa, após o envio, confirmar se a documentação chegou a seu destino, entrando em contato com o pregoeiro responsável pelo certame;

11.2. Habilitação Jurídica:

11.2.1. Registro comercial, no caso de empresa individual;

11.2.2. Ato constitutivo, estatuto ou contrato social em vigor devidamente registrado, em se tratando de sociedades comerciais e, no caso de sociedades por ações, acompanhado de documentos de eleição de seus administradores;

a) Os documentos em apreço deverão estar acompanhados de todas as alterações ou consolidação respectiva;

11.2.3. Inscrição do ato constitutivo, no caso de sociedades civis, acompanhada de prova de diretoria em exercício;

11.2.4. Decreto de autorização, 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;

11.2.5. Não serão aceitas participações de empresas com sócios comuns.

11.3. Regularidade Fiscal:

11.3.1. Prova de inscrição no Cadastro de Pessoas Físicas (CPF) ou no Cadastro Nacional de Pessoas Jurídicas (CNPJ);

11.3.2. Prova de inscrição no cadastro de contribuintes estadual, municipal ou Distrital, se houver, relativo ao domicílio ou sede da licitante, pertinente ao seu ramo de atividade e compatível com o objeto licitado;

11.3.3. Prova de regularidade para com as Fazendas Federal, Estadual/Distrital e Municipal do domicílio ou sede da licitante, ou outra equivalente, na forma da lei;

11.3.4. Prova de regularidade relativa à Seguridade Social (CND) e ao Fundo de Garantia por Tempo de Serviço (CRF), demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei.

11.3.5. Havendo alguma restrição na comprovação da regularidade fiscal das microempresas e empresas de pequeno porte, será assegurado o prazo de 2 (dois) dias úteis, cujo termo inicial corresponderá ao momento em que o proponente for declarado o vencedor do certame, prorrogáveis por igual período, a critério da Administração, para a regularização da documentação, pagamento ou parcelamento do débito, e emissão de eventuais certidões negativas ou positivas com efeito de certidão negativa.

11.3.6. A não regularização da documentação, no prazo previsto no item acima, implicará decadência do direito à contratação, sem prejuízo das sanções previstas no artigo 81 da Lei nº 8.666/93, sendo facultado à Administração convocar os licitantes remanescentes, na ordem de classificação, para assinatura do contrato, ou revogar a licitação.

11.4. Qualificação Econômico-Financeira:

11.4.1. Balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a

boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrados há mais de 3 (três) meses da data de apresentação da proposta.

11.4.2. O capital mínimo ou o valor do patrimônio líquido a que se refere o parágrafo anterior não poderá ser inferior a 10% (dez por cento) do valor estimado da contratação, devendo a comprovação ser feita relativamente à data da apresentação da proposta, a forma da lei, admitida atualização para esta data através de índices oficiais;

11.4.3. As microempresas e as empresas de pequeno porte estão dispensadas do balanço patrimonial apenas para fins fiscais. Assim, para a presente licitação, é OBRIGATÓRIA a apresentação desta peça, bem como a prova de seu enquadramento como microempresa ou empresa de pequeno porte registrada na Junta Comercial.

11.5. Qualificação Técnica:

11.5.1. Atestado(s) de capacidade técnica, expedido(s) por pessoa(s) jurídica(s) de direito público ou privado, que comprove(m) que a LICITANTE executou ou executa serviços da mesma natureza ou similares ao da presente Licitação, devidamente registrados no Conselho Regional de Engenharia, Arquitetura e Agronomia - CREA;

11.5.2. Certidão negativa de falência ou concordata, expedida pelo distribuidor da sede da pessoa jurídica, ou de execução patrimonial, expedida no domicílio da pessoa física;

11.5.3. Declaração de fato superveniente, na forma do § 2º do artigo 32 da Lei nº 8.666/93, conforme modelo constante do Anexo III, deste Edital;

11.5.4. Declaração da licitante, conforme Anexo IV, de que não possui em seu quadro de pessoal, funcionário(s) com menos de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e de 16 (dezesseis) anos em qualquer trabalho, salvo na condição de aprendiz a partir dos 14 (quatorze) anos, nos termos do inciso V, do art. 27 da Lei nº 8.666/93.

11.6. Sob pena de inabilitação, todos os documentos apresentados para habilitação deverão:

11.6.1. Estar em nome da licitante e, preferencialmente, com número do CNPJ e com o endereço respectivo:

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

b) Se a licitante for a filial, todos os documentos deverão estar em nome da filial, exceto aqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz;

c) Os atestados de capacidade técnica/responsabilidade técnica poderão estar emitidos em nome e com CNPJ da matriz e/ou da(s) filial(ais) da licitante.

11.6.2. Ser apresentados em original ou, se cópias, autenticadas por cartório competente, ou publicação em órgão da imprensa oficial, ou acompanhadas dos respectivos originais para serem autenticadas pela Comissão de Licitações;

a) Serão aceitas somente cópias legíveis;

b) Não serão aceitos documentos cujas datas estejam rasuradas;

11.6.3. Datados dos últimos 180 (cento e oitenta) dias até a data de abertura dos envelopes, quando não tiver prazo estabelecido pelo órgão/empresa competente expedido.

a) Não se enquadram no prazo de que trata o item anterior os documentos cuja validade é indeterminada, como é o caso dos atestados de capacidade/responsabilidade técnica.

11.6.4. A Comissão de Licitações reserva-se o direito de solicitar o original de qualquer documento, sempre que tiver dúvida e julgar necessário.

11.7. Nova planilha de custos contendo os respectivos valores readequados ao valor do lance de menor preço, Anexo VI.

11.8. No caso de microempresa ou empresa de pequeno porte, declaração de que está apta a usufruir o tratamento favorecido estabelecido na lei Complementar nº 123/2006, Anexo II.

12. DA PROPOSTA COMERCIAL

12.1. O fornecedor vencedor deverá enviar, aos cuidados do pregoeiro, juntamente com os documentos de habilitação, a sua proposta comercial original (modelo Anexo VI), assinada e atualizada com os valores finais ofertados neste Pregão, informando o valor apresentado na etapa de lances, bem como atender as seguintes exigências:

a) Conter as especificações do objeto de forma clara, descrevendo detalhadamente as características técnicas de todos os equipamentos, incluindo marca/modelo;

b) Conter o prazo de validade não inferior a 60 (sessenta) dias;

c) Conter o prazo de entrega.

13. DA ADJUDICAÇÃO E HOMOLOGAÇÃO

13.1. Inexistindo manifestação recursal, o Pregoeiro adjudicará o objeto da licitação ao licitante vencedor, com a posterior homologação do resultado pela Autoridade Competente ou, decididos os recursos porventura interpostos, e constatada a regularidade dos atos procedimentais, a Autoridade Competente adjudicará o objeto ao licitante vencedor e homologará o procedimento licitatório.

13.2 Se a licitante classificada em primeiro lugar desatender às exigências habilitatórias, o pregoeiro examinará a oferta subsequente na ordem de

classificação, verificando a sua aceitabilidade e procedendo a sua habilitação, repetindo esse procedimento sucessivamente, se for necessário, até a apuração de uma proposta que atenda ao edital, sendo a respectiva licitante declarada vencedora.

14. DOS PRAZOS

14.1. A licitante vencedora terá até 20 (vinte) dias corridos para a entrega e/ou execução do objeto deste certame, a partir da data de assinatura do contrato.

15. DO CONTRATO

15.1. A minuta de contrato (Anexo V) que acompanha este Edital poderá sofrer alterações para adequá-la à proposta vencedora, bem como para mantê-la integralmente compatível com o edital e seus anexos.

15.2. Decorridos 60 (sessenta) dias da entrega da proposta, sem a prorrogação e/ou a convocação de que trata esta condição, ficam as concorrentes liberadas dos compromissos assumidos.

15.3. A vencedora 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 do Contrato.

15.4. Quaisquer outras condições apresentadas pela licitante vencedora em sua proposta poderão ser acrescentadas, a juízo da Administração, no que couber, ao Contrato a ser assinado, desde que não alterem disposição legal deste certame.

16. DO RECEBIMENTO DO OBJETO

16.1. O objeto será recebido provisoriamente, no ato da entrega, mediante assinatura do recibo da Nota Fiscal, Fatura etc., para posterior verificação da conformidade do material com a especificação e da formulação correta da Nota Fiscal;

16.2. Além do recebimento/aceite dos produtos e/ou execução dos serviços, a Nota Fiscal deverá ser formulada, já constando os impostos que serão retidos, sob pena de devolução para correção, contando-se o prazo para o pagamento a partir do recebimento regular da mesma (IN SRF nº 480 de 15.12.2004 – DOU 29.12.2004).

17. DO PAGAMENTO

17.1. O pagamento será efetuado em até 21 (vinte e um) dias corridos, contados a partir da entrega do objeto, contra apresentação da nota fiscal/ fatura e do boleto bancário, com antecedência de 10 (dez) dias úteis do seu vencimento, que deverá recair sobre o dia 05, 15 ou 25 do mês.

17.2. Havendo erro na nota fiscal ou circunstâncias que impeçam liquidação da despesa, aquela será devolvida e o pagamento ficará pendente até que a licitante vencedora providencie as medidas saneadoras. Nessa hipótese, o prazo para o pagamento iniciar-se-á após a regularização da situação e/ou a reapresentação da nota fiscal, não acarretando qualquer ônus para o Conselho Regional de Economia – 2ª Região – SP.

17.2.1. Solicitamos observarem as Instruções Normativas da Secretaria da Receita Federal nº. 480, de 15 de dezembro de 2004 e nº. 539, de 25 de abril de 2005, que trata da retenção na fonte do Imposto Sobre a Renda da Pessoa Jurídica (IRPJ), da Contribuição Social Sobre o Lucro Líquido (CSLL), da Contribuição Para o Financiamento da Seguridade Social (COFINS) e da Contribuição para o PIS/PASEP. Em obediência às normas legais e tributárias, o Conselho Regional de Economia – 2ª Região – SP, por ser autarquia federal, está sujeita a reter na fonte e recolher os impostos mencionados, independentes do valor da nota ou documento fiscal, conforme a natureza do bem fornecido ou do serviço prestado conforme o Anexo I – Tabela de Retenções da IN SRF nº. 539.

17.3. O Conselho Regional de Economia – 2ª Região – SP poderá deduzir do montante a pagar os valores correspondentes a multas ou indenizações devidas pela licitante vencedora, nos termos deste edital.

17.4. Nenhum pagamento será efetuado à licitante vencedora enquanto pendente de liquidação qualquer obrigação financeira e previdenciária, sem que isso gere direito a reajustamento de preços, compensação financeira ou aplicação de penalidade ao Conselho Regional de Economia – 2ª Região - SP.

17.5. As despesas decorrentes desta licitação correrão pelas seguintes dotações orçamentárias:

LOTES 1 e 2: 3.1.30.02.20 – Serviços de Informática.

17.6. Apenas a título de subsídio e **sem nenhum compromisso** para o futuro, informamos que o valor estimado para a contratação é, aproximadamente: R$ 47.500,00 (quarenta e sete mil e quinhentos reais) para o Lote 1 e R$ 25.500,00 (vinte e cinco mil e quinhentos reais) para o Lote 2.

18. DAS PENALIDADES

18.1. Aos licitantes que ensejarem o retardamento da execução do certame, não mantiverem a proposta, falharem ou fraudarem na execução do contrato, comportarem-se de modo inidôneo, apresentarem documentação ou declaração falsa, cometerem fraude fiscal, poderão ser aplicadas, conforme o caso, sanções previstas no art. 7º, da Lei nº 10.520/02, bem como aos arts. 86 e 87 da Lei nº 8.666/93, sem prejuízo da reparação dos danos causados ao CONSELHO.

18.2. A CONTRATADA ficará sujeita, em caso de atraso injustificado na execução do contrato, sem prejuízo da rescisão unilateral e de outras sanções previstas na Lei Nº 8.666/93, a multa nos seguintes limites:

a) 20% (vinte por cento) sobre o valor da Proposta, em caso de recusa da CONTRATADA em assinar o Contrato dentro de 05 (cinco) dias úteis, contados da data de sua convocação;

b) 0,3% (três décimos por cento) ao dia, até o trigésimo dia de atraso na entrega dos serviços ou material ou equipamento, sobre o valor do contrato não realizado;

c) 20% (vinte por cento) sobre o valor do Contrato não realizado, no caso de:

- Atraso superior a 30 (trinta) dias, na entrega dos serviços;

- Desistência da entrega dos serviços;

18.3. As multas previstas nesta Condição serão aplicadas à licitante vencedora de forma cumulativa.

18.4. O atraso injustificado após o quarto dia será considerado como inexecução total ou parcial do objeto contratado, conforme o caso, sendo aplicável à licitante vencedora, nessa hipótese, a multa correspondente.

18.5. O descumprimento das obrigações estabelecidas no contrato sujeitará a licitante vencedora à multa de 0,3% (zero vírgula três por cento) por dia e por ocorrência, até o máximo de 10% (dez por cento) sobre o valor total do contrato, recolhida no prazo máximo de 15 (quinze) dias corridos, uma vez comunicada oficialmente.

18.6. Pela inexecução total ou parcial do objeto deste edital, a Administração do Conselho Regional de Economia – 2ª Região – SP poderá, garantida a prévia defesa, aplicar à licitante vencedora as seguintes sanções:

18.6.1. Advertência;

18.6.2. Multa, conforme descrito;

18.6.3. 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 licitante ressarcir a Administração do Conselho Regional de Economia – 2ª Região – SP pelos prejuízos resultantes.

18.7. Se o motivo ocorrer por comprovado impedimento ou por motivo de reconhecida força maior, devidamente justificado e aceito pela Administração do CONTRATANTE, a CONTRATADA ficará isenta das penalidades mencionadas.

19. DA IMPUGNAÇÃO DO EDITAL

19.1. É facultado a qualquer cidadão impugnar por escrito os termos do presente Edital, até 05 (cinco) dias úteis antes da data fixada para abertura das propostas, devendo a administração do Conselho Regional de Economia – 2ª Região - SP, por intermédio da Comissão de Licitações, julgar e responder à impugnação em até 03 (três) dias úteis.

19.2. Decairá do direito de impugnar os termos deste Pregão perante a administração do Conselho Regional de Economia – 2ª Região- São Paulo, a licitante que não o fizer até o segundo dia útil que anteceder à data prevista para a abertura das Propostas, apontando as falhas ou irregularidades que o viciariam, hipótese em que tal comunicação não terá efeito de recurso.

19.3. A impugnação feita tempestivamente pela licitante não a impedirá de participar deste Pregão até o trânsito em julgado da decisão a ela pertinente.

19.4. A impugnação interposta deverá ser comunicada à Comissão de Licitações e somente será válida após sua confirmação de recebimento.

19.5. Acolhida a impugnação contra este Edital, será designada nova data para a realização do certame, exceto quando, inquestionavelmente, a alteração não afetar a formulação das propostas.

20. ANEXOS INTEGRANTES DESTE EDITAL

Anexo I - Termo de Referência;
Anexo II - Declaração de ME ou EPP;
Anexo III - Modelo de Superveniência de Fato Impeditivo;
Anexo IV - Declaração de não Emprego de Menor;
Anexo V - Minuta de Contrato;
Anexo VI - Modelo de Proposta Comercial.

21. DAS DISPOSIÇÕES GERAIS

21.1. A apresentação da proposta de licitação coloca a licitante em integral submissão às exigências deste Edital e seus adendos, não podendo mais impugnar quaisquer de seus dispositivos, salvo o que tenha questionado de forma expressa, conforme disposto no item 19 deste instrumento;

21.2. O recebimento das propostas pelo órgão não implica em nenhum direito à proponente ou compromisso do CORECON-SP, além do recebimento das mesmas.

21.3. Farão parte integrante deste Edital as condições estabelecidas, a minuta de contrato e a proposta apresentada pelo licitante;

21.4. As normas que disciplinam este Pregão serão sempre interpretadas em favor da ampliação da disputa entre os proponentes, desde que não comprometam o interesse da Administração, a finalidade e a segurança da contratação.

21.5. É facultado ao pregoeiro, no interesse da Administração, relevar omissões puramente formais observadas na documentação e proposta, desde que não contrariem a legislação vigente e não comprometam a lisura da licitação, sendo possível a promoção de diligência destinada a esclarecer ou a complementar a instrução do processo;

21.6. O objeto do Contrato somente será recebido quando perfeitamente de acordo com as condições deste Edital, da proposta apresentada e dos demais documentos que fizerem parte do ajuste;

21.7. A responsabilidade da contratada pela qualidade, pontualidade, organização, lisura, legalidade e segurança dos serviços subsistirão, na forma da Lei, mesmo após o recebimento definitivo dos objetos desta licitação;

21.8. A tolerância do CONTRATANTE em qualquer atraso ou inadimplência da CONTRATADA, não implicará, sob qualquer forma, em alteração contratual ou renovação;

21.9. A aquisição do objeto deste Pregão será adjudicado globalmente por lote, depois de atendidas as Condições deste Edital.

21.10. O CORECON-SP se reserva o direito de revogar ou anular esta licitação, no todo ou em parte por conveniência administrativa ou interesse público devidamente justificado, sem que caiba ao licitante direito à indenização;

21.11. O CORECON-SP não se responsabilizará por e-mails que, por qualquer motivo, não forem recebidos em virtude de problemas no servidor ou navegador, tanto do CORECON-SP quanto do emissor.

21.12. Cópia do presente Edital e demais documentos relacionados a este Pregão estarão disponíveis no site www.coreconsp.org.br , link "licitações" a partir de 20 de abril de 2018.

21.13. O número do CNPJ do Conselho Regional de Economia – 2ª Região - SP é 62.144.084/0001-94.

São Paulo, 16 de abril de 2018.

José Dutra Vieira Sobrinho
Presidente da Comissão de Licitações

PREGÃO ELETRÔNICO Nº 07/2018

PROCESSO Nº L-07/2018

A N E X O I

Termo de Referência

I – OBJETO

O objeto da presente licitação consiste em manter ativo o Suporte Técnico e Atualização dos Produtos DELL SONICWALL CGSS Comprehensive Gateway Security Suite for the NSA 2400 Series por 36 meses, para AGSS Advanced Gateway Security Suíte for the NSA 2400 Series por 36 meses.

LOTE 1 - SOFTWARE - RENOVAÇÃO CGSS SONICWALL COM ATUALIZAÇÃO PARA AGSS SONICWALL E SUPORTE TÉCNICO PARA EQUIPAMENTO NSA 2400 EM HA PARA 36 MESES.

ITEM	QTD	DESCRIÇÃO
01	01	**DELL SONICWALL CGSS (Comprehensive Gateway Security Suite Bundle for the NSA 2400 Series (3Year) com atualização para AGSS (Advanced Gateway Security Suite) 3 Year.**

Caso a Renovação acima não esteja mais disponível para comercialização no mercado, modelo equivalente/superior do mesmo Fabricante deverá ser oferecido e a origem da comercialização deverá ser proveniente de um Distribuidor Autorizado, comprovado em https://www.sonicwall.com/pt-br/partners/authorized-distributors **com Representante e escritório no Brasil para preservação dos mais de 2700 objetos em operação e mais de 780 regras de negócio, além de diversas configurações de sistemas legados, funcionando desde 2011, poderá ser oferecido na modalidade UPGRADE ou NOVO, desde que tenha o valor igual ou inferior à modalidade UPGRADE e que atenda em sua totalidade os requisitos abaixo.:**

ESPECIFICAÇÃO DO EQUIPAMENTO

Performance de Firewall Stateful Packet Inspection igual ou superior a 3 Gbps."
Performance de todos os serviços ativos UTM (Proteção Anti-Malware e Anti-virus, IDS, IPS e Controle de Aplicação) deverá ser de 600 (seiscentos) Mbps ou superior. Caso o fornecedor não possa comprovar este item em documentações públicas, deve ser comprovado através de testes em bancada com gerador de pacotes (custos destes testes pagos pela CONTRATADA).

Perfomance de Inspeção (decriptografia e criptografia) de tráfego criptografado (SSL) de no mínimo 300 (trezentos) Mbps, os throughputs devem ser comprovados por documento de domínio público do fabricante. Caso o fornecedor não possa comprovar este item em documentações públicas, deve ser comprovado através de testes em bancada com gerador de pacotes (custos destes testes pagos pela CONTRATADA). Não serão aceitos declarações ou cartas de fabricantes para atendimento a este item;

Performance de IPS de 1.400 (Mil e quatrocentos cem) Mbps ou superior"
Suporte a, no mínimo, 1.000.000 (Um milhão) de conexões do tipo SPI simultâneas;
Suporte a, no mínimo, 500.000 (Quinhentos mil) conexões do tipo DPI simultâneas;
Suporte a, no mínimo, 15.000 (quinze mil) novas conexões por segundo;
Disco SSD de no mínimo 16 Gb.
Fonte de alimentação redundante com chaveamento automático de 100-240 VAC.
Deverá possuir pelo menos quatro interfaces de 1 GbE SFP;
12 (doze) interfaces de rede 10/100/1000 base-TX. Todas as interfaces devem possuir mecanismo de autosense e seleção de modo half/full duplex. A seleção da velocidade e duplex deve ser realizada obrigatoriamente através da interface gráfica de gerenciamento. As interfaces devem suportar as seguintes atribuições:

a) Segmento WAN , ou externo.
b) Segmento WAN, secundário com possibilidade de ativação de recurso para redundância de WAN com balanceamento de carga e WAN Failover por aplicação. O equipamento deverá suportar no mínimo balanceamento de 4 links utilizando diferentes métricas pré-definidas pelo sistema e configuráveis pelo administrador.
c) Segmento LAN ou rede interna.
d) Segmento LAN ou rede interna podendo ser configurado como DMZ (Zona desmilitarizada)
e) Segmento LAN ou rede interna ou Porta de sincronismo para funcionamento em alta disponibilidade
f) Segmento ou Zona exclusiva para controle de dispositivos Wireless dedicado, com controle e configuração destes dispositivos.
01 (uma) interface do tipo console ou similar;
01 (uma) interface de rede dedicada para gerenciamento;

A VPN SSL deve ser licenciada para, no mínimo, 2 (dois) usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para no mínimo, 350 (trezentos e cinquenta) usuários simultâneos, com aquisição de licença futura;
Suportar 1000 (Mil) túneis de VPN IPSEC simultâneos;
Suportar, no mínimo, 1500(Mil e quinhentos) Mbps de throughput de VPN IPSEC

Os Throughputs devem ser comprovados por teste de bancada, utilizando ferramentas corporativas de geração de trafego, como exemplo as ferramentas dos fabricantes IXIA ou Spirent. Não será aceito comprovações que utilizem soluções do tipo desktop para geração do trafego.
Não serão aceitas cartas ou declarações de fabricantes para atendimento aos valores de performance solicitados;

"Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e/ou end-of-sale ou situação semelhante;

CARACTERÍSTICAS GERAIS

"Todas as funcionalidades descritas devem funcionar no mesmo appliance sem a necessidade de composição de um ou mais produtos;

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

"O hardware e software que executem as funcionalidades de proteção de rede devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

O equipamento deverá ser baseado em hardware desenvolvido com está finalidade, ou seja, não sendo aceita soluções baseadas em plataforma PC ou equivalente.

Não serão permitidas soluções baseadas em sistemas operacionais abertos(OpenSource) como Free BSD, Debian ou mesmo Linux.

"Todo o ambiente deverá ser gerenciado através de uma única interface sem a necessidade de produtos de terceiros para compor a solução;
Deve ser possível suportar arquitetura de armazenamento de logs redundante, permitindo a configuração de equipamentos distintos;

A solução deverá suportar monitoramento através de SNMP v2 e v3;

Deve oferecer as funcionalidades de backup/restore tanto da configuração quanto do firmware/sistema operacional através da interface gráfica , assim como permitir ao administrador agendar procedimentos de backups da configuração em determinado dia e hora. O appliance deve armazenar no mínimo 02 (duas) versões distintas do sistema operacional, sendo possível escolher qual versão será inicalizada;de backups da configuração em determinado dia e hora.

Suporte a definição de VLAN no firewall, conforme padrão IEEE 802.1q e ser possível criar sub-interfaces lógicas associadas a VLANs e estabelecer regras de filtragem (Stateful Firewall) entre elas;

A solução deve suportar configuração de link-aggregation de interfaces suportando o protocolo 802.3ad para aumento de throughput .

A solução deve suportar configuração de port-redundacy de interfaces para a alta disponibilidade de interfaces;

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

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

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

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

Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas.
Possuir DHCP Server interno;

Suporte a encaminhamento de pacotes UDPs multicast/broadcast entre diferentes interfaces e zonas de segurança como como DHCP Relay, suportando os protocolos e portas:

Time service—UDP porta 37
DNS—UDP porta 53
DHCP—UDP portas 67 e 68
Net-Bios DNS—UDP porta 137
Net-Bios Datagram—UDP porta 138
Wake On LAN—UDP porta 7 e 9
mDNS—UDP porta 5353
Suporte a Jumbo Frames;
Implementar sub-interfaces ethernet lógicas;
Deve suportar os seguintes tipos de NAT:

Nat dinâmico (Many-to-1);
Nat dinâmico (Many-to-Many);
Nat estático (1-to-1);
NAT estático (Many-to-Many);
Nat estático bidirecional 1-to-1;
Tradução de porta (PAT);
NAT de origem;
NAT de destino;

Suportar NAT de origem e NAT de destino simultaneamente.

Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing)
Implementar mecanismo de sincronismo de horário através do protocolo NTP. Para tanto o appliance deve realizar a pesquisa em pelo menos 03 servidores NTP distintos, com a configuração do tempo do intervalo de pesquisa;

Possuir gerenciamento de tráfego de entrada ou saida, por serviços, endereços IP e regra de firewall, permitindo definir banda mínima garantida e máxima permitida em porcentagem (%) para cada regra definida.

Implementar 802.1p e classe de serviços CoS (Class of Service) de DSCP (Differentiated Services Code Points);

Permitir remarcação de pacotes utilizando TOS e/ou DSCP;

Suporte a policy based routing (PBR), com a capacidade de roteamento por endereço de origem, endereço de destino, serviço, interface ou todas as opções simultâneas.
Suporte ao protocolo de roteamento multicast (PIM-SM);

Suportar protocolos de roteamento RIP, RIPng, OSPF, OSPFv3 e BGP;

Suportar Equal Cost Multi-Path (ECMP);

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

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

A solução deve suportar integralmente o padrão IPv6, assim como criação de regras com objetos que utilizem endereços IPv4 e IPv6.

Deve suportar no mínimo as seguintes funcionalidades ou protocolos para o padrão de endereçamento IPv6: Tunel 6 to 4, regras de acesso, objetos de endereço, limitador de conexões IPv6, monitor de conexões, DHCP, gerenciamento HTTPS via IPv6, NAT IPv6, proteção contra ataques to tipo IP Spoofing para IPv6, captura de pacotes IPv6, interface VLAN com endereço IPv6, VPN SSL com o uso do IPv6, controle de URL, Anti-Malware e anti-vírus, controle de aplicação, IPS, IKEv2, ICMP6, SNMP, alta disponibilidade, RFC 1981 Path MTU Discovery for IPv6, RFC 2460 IPv6 specification, RFC 2464 Transmission of IPv6 Packets over Ethernet Networks;
Possui suporte a log via syslog;

Possuir mecanismo para possibilitar a aplicação de correções e atualizações para o firewall remotamente através da interface gráfica;

Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do firewall.

Permitir a geração de gráficos em tempo real, representando os serviços mais utilizados e as máquinas mais acessadas em um dado momento;

Permitir a visualização de estatísticas do uso de CPU do appliance o através da interface gráfica remota em tempo real;

Alta Disponibilidade

Possuir mecanismo de Alta Disponibilidade operando em modo Ativo/Standby, com as implementações de Fail Over.

Não serão permitidas soluções de cluster (HA) que façam com que o equipamento (s) reinicie após qualquer modificação de parâmetro/configuração seja realizada pelo administrador.

O recurso de Alta Disponibilidade deverá ser suportado em modo Bridge

VPN

Criptografia 3DES, AES 128 e AES 256;

Autenticação com MD5, SHA-1, SHA-256 e SHA-384;

Diffie-Hellman: Grupo 2 (1024 bits), Grupo 5 (1536 bits) e Grupo 14 (2048 bits);

Algoritmo Internet Key Exchange (IKE);

Autenticação via certificado IKE PKI;

Deve possuir interoperabilidade com outros fabricantes de acordo com o padrão IPSEC através de RFC`s;

A solução deve suportar VPNs L2TP, incluindo suporte para iPhone, Windows phone, Android com suporte a cliente L2TP;

Solução deve suportar VPNs baseadas em politicas e VPNs baseadas em roteamento estático e dinâmico.

Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo site-to-site com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC.

Solução deve incluir a capacidade de estabelecer VPNs com outros firewalls que utilizam IP públicos dinâmicos;

Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do circuito primário;

Permitir que seja criado políticas de roteamentos estáticos utilizando IPs de origem, destino, serviços e a própria VPN como parte encaminhadora deste tráfego sendo este visto pela regra de roteamento, como uma interface simples de rede para encaminhamento do tráfego.

Suportar a criação de túneis IP sobre IP (IPSEC Tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet;

Autenticação

Permitir a utilização de LDAP, AD e RADIUS;

Permitir o cadastro manual dos usuários e grupos diretamente na interface de gerencia remota do Firewall, caso onde se dispensa um autenticador remoto para o mesmo;

Suporte a uma rede com múltiplos domínios, possibilitando a integração em um ambiente onde existam domínios diferentes e totalmente segregados.

Permitir a integração com qualquer autoridade certificadora emissora de certificados X509 que seguir o padrão de PKI descrito na RFC 2459, inclusive verificando as CRLs emitidas periodicamente pelas autoridades, que devem ser obtidas automaticamente pelo firewall via protocolos HTTP e LDAP;

Permitir o controle de acesso por usuário, para plataformas Windows Me, NT, 2000, 2000, XP, Windows 7 , Windows 8 e Windows 10 de forma transparente, para todos os serviços suportados, de forma que ao efetuar o logon na rede, um determinado usuário tenha seu perfil de acesso automaticamente configurado;

Permitir a restrição de atribuição de perfil de acesso a usuário ou grupo independente ao endereço IP da máquina que o usuário esteja utilizando.

Suportar recurso de autenticação única para todo o ambiente de rede, ou seja, utilizando a plataforma de autenticação atual que pode ser de LDAP ou AD; o perfil de cada usuário deverá ser obtido automaticamente através de regras no Firewall DPI (Deep Packet Inspection) sem a necessidade de uma nova autenticação como por exemplo, para os serviços de navegação a Internet atuando assim de forma toda transparente ao usuário. Serviços como HTTP, HTTPS devem apenas consultar uma base de dados de usuários e grupos de servidores 2008/2012 com AD;

IPS

Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS integrados no próprio appliance de firewall, onde sua console de gerência deverá residir na mesma console centralizada dos appliances de segurança, com suporte a pelo menos 3.000 assinaturas;

A solução de IPS deverá possuir os seguintes mecanismos de detecção: assinaturas e trabalhar em conjunto com o controle de aplicações;

A solução de IPS deve fazer a inspeção de todo o pacote, independentemente do tamanho;

A solução de IPS deve fazer a inspeção de todo o trafego de forma bidirecional, analisando qualquer tamanho de pacote sem degradar a performance do equipamento solicitado neste edital;

Possuir capacidade de remontagem de pacotes para identificação de ataques;

O mecanismo de inspeção deve receber e implementar em tempo real atualizações para os ataques emergentes sem a necessidade de reiniciar o appliance;

Para cada proteção de segurança, deve ser possível consultar informações no site do fabricante.

A ferramenta de log deve possuir a capacidade de criar uma regra de exceção a partir do log visualizado na gerência centralizada;

As regras de exceção devem possuir: origem, destino e serviço;

A solução deve ser capaz de inspecionar tráfego HTTPS.

Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;

Detecção de anomalias;

A solução de IPS deve possuir política capaz de definir o modo de operação (bloqueio ou detecção);

O módulo de IPS deve possuir assinaturas voltadas para ambientes de servidores de SMTP, Web e DNS;

O mecanismo de inspeção deve receber e implementar em tempo real atualizações de novas assinaturas sem a necessidade de reiniciar o appliance;

Para cada proteção, ou para todas as proteções suportadas, deve incluir a opção de adicionar exceções baseado na origem e destino;

A solução deve ser capaz de detectar e bloquear ataques nas camadas de rede e aplicação, protegendo pelo menos os seguintes serviços: Aplicações web, serviços de e-mail, DNS, FTP, SQL Injection, ataques a sistemas operacionais e VOIP;

Deve incluir proteção contra worms;

Deve incluir uma tela de visualização situacional a fim de monitorar graficamente a quantidade de alertas de diferentes severidades e a evolução ao logo do tempo dispondo o sumario quantitativo das ameaças analisadas.

A solução deve possuir esquema de atualização de assinaturas através de um click; Atualização de modo offline, onde poder ser baixado na base do fabricante e posteriormente fazer o upload do arquivo na solução;

A solução deve suportar importar certificados de servidor para inspeções de tráfego seguro HTTP (HTTPS) de entrada. Depois de importar esses certificados, a solução deve permitir o IPS para Inspeção segura HTTP(HTTPS);

A solução deverá ser capaz de inspecionar e proteger apenas hosts internos;

A solução deverá possuir proteções para sistemas SCADA;

Solução deverá permitir que o administrador bloqueie facilmente o tráfego de entrada e/ou saída com base em países, sem a necessidade de gerir manualmente os ranges de endereços IP dos países que deseja bloquear.

Possibilitar operação em modo de detecção baseado em base de assinaturas SNORT.

Aplication Control

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

Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos.
Capacidade para realizar filtragens/inspeções dentro de portas TCP conhecidas por exemplo porta 80 http, buscando por aplicações que potencialmente expõe o ambiente como: P2P, Kazaa, Morpheus, BitTorrent ou messengers.

Controlar o uso dos serviços de Instant Messengers como MSN, YAHOO, Google Talk, ICQ, de acordo com o perfil de cada usuário ou grupo de usuários, de modo a definir, para cada perfil, se ele pode ou não realizar download e/ou upload de arquivos, limitar as extensões dos arquivos que podem ser enviados/recebidos e permissões e bloqueio de sua utilização baseados em horários pré-determinados pelo administrador será obrigatório para este item.

Deverá controlar software FreeProxy tais como ToR, Ultrasurf, Freegate,etc.
Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
Deverá permitir a criação de regras para acesso/bloqueio por subrede de origem e destino;

Atualizar a base de assinaturas de aplicações automaticamente;

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

A solução de controle de aplicação WEB deve criar regras granulares possibilitando adicionar tipos de aplicação WEB e categorias por regra, sendo assim criando controle granular de qualquer tipo de acesso não permitido pela empresa;

Deve implementar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e protocolos;

Caso a solução não tenha assinaturas pré-definida na solução a mesma deverá possibilitar a criação ou importação de assinaturas personalizadas para os seguintes tipos ou protocolos: HTTP, FTP, Email e extensão de arquivos.

O administrador deve ser capaz de configurar quais comandos FTP são aceitos e quais são bloqueados a partir de comandos FTP pré-definidos;

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

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

Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Facebook e bloquear chat;

Deverá possibilitar a diferenciação de aplicações Proxies possuindo granularidade de controle/políticas para os mesmos;

Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:

Nível de risco da aplicação.

Categoria de aplicações.

Filtro de URL

Para prover maior visibilidade e controle dos acessos dos usuários do ambiente, deve ser incluído um módulo de filtro de URL integrado no firewall;
Possuir base contendo no mínimo 20 milhões de sites internet web já registrados e classificados com atualização automática;

Implementar filtro de conteúdo transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das máquinas clientes.

A plataforma de proteção deve possuir as seguintes funcionalidades de filtro de URL:
Permitir a criação de listas personalizadas de URLs permitidas e bloqueadas (lista branca e lista negra);

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

Deve ser possível à criação de políticas por usuários, grupos de usuários, IPs, redes e grupos de redes;

O mecanismo de Controle de aplicação Web/URL deve apresentar contagem de utilização de regra de acordo com a utilização (hit count);

Deverá permitir criar política de confirmação de acesso.

Deve possibilitar a inspeção de tráfego HTTPS (Inbound/Outbound), sendo que para a opção de Outbound não será necessário efetuar o "man-inthe- middle", ou seja, a solução deverá prover mecanismo que irá analisar a conexão HTTPS para verificar se a URL solicitada está na lista de permissões de acesso, de acordo com a política configurada;

O administrador poderá adicionar filtros por palavra-chave de modo específico;

Deverá permitir o bloqueio Web através de senha pré configura pelo administrador
Deverá 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);

A solução deve fornecer um mecanismo para solicitação de categorização de URL caso esta não esteja categorizada ou categorizada incorretamente;

Suportar recurso de autenticação única para todo o ambiente de rede, ou seja, utilizando a plataforma de autenticação atual que pode ser de LDAP ou AD; o perfil de cada usuário deverá ser obtido automaticamente para o controle das políticas de Filtro de Conteúdo sem a necessidade de uma nova autenticação.

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

Suportar base ou cache de URLs local no appliance ou possibilitar a replicação da base de conhecimento de URLs do fabricante via instalação de maquina virtual, a infraestrutura da máquina virtual (VM) para uso desse recurso será fornecida pelo CONTRATANTE , evitando delay de comunicação/validação das URLs;

Possuir pelo menos 50 categorias de URLs;

Suporta a criação de categorias de URLs customizadas;

Suporta a exclusão de URLs do bloqueio, por categoria;

Deverá possibilitar a categorização ou recategorização de URL caso não esteja categorizada ou categorizada incorretamente;
A solução deverá permitir um mecanismo que permita sobrescrever as categorias de URL;
Permite a customização de página de bloqueio;

PROTEÇÃO CONTRA VIRUS E BOT-NETS

Deve possuir módulo de antivírus e anti-bot integrado no próprio appliance de segurança;

A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliances através de assinaturas.

Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego;

Implementar funcionalidade de detecção e bloqueio de callbacks;

A solução deverá ser capaz de detectar e bloquear comportamento suspeito ou anormal da rede;

A solução Antibot deve possuir mecanismo de detecção que inclui, reputação de endereço IP;

Implementar interface gráfica WEB segura, utilizando o protocolo HTTPS.

Implementar interface CLI segura através do protocolo SSH;

Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, IMAP, POP3, FTP, CIFS e TCP Stream;

A solução deve permitir criar regras de exceção de acordo com a proteção;

Deve possuir visualização na própria interface de gerenciamento referente aos top incidentes através de hosts ou incidentes referentes a incidentes de vírus e Bots;

Permitir o bloqueio de malwares (vírus, worms, spyware e etc).

A solução deve ser capaz de proteger contra ataques para DNS.

A solução deverá ser gerenciada a partir de uma console centralizada com políticas granulares.

A solução deve ser capaz de prevenir acesso a websites maliciosos.

A solução deve ser capaz de realizar inspeção de tráfego SSL e SSH.

A solução deverá receber atualizações de um serviço baseado em cloud.

A solução deverá ser capaz de bloquear a entrada de arquivos maliciosos.

A solução Antivírus deverá suportar análise de arquivos que trafegam dentro do protocolo CIFS.

A solução deve suportar funcionalidade de GeoIP, ou seja, a capacidade de identificar, isolar e controlar tráfego baseado na localização (origem e/ou destino), incluindo a capacidade de configuração de listas customizadas para esta mesma finalidade.

PROTEÇÃO CONTRA ATAQUES AVANÇADOS

A solução deverá prover as funcionalidades de inspeção de tráfego de entrada e saída de malwares não conhecidos ou do tipo APT com filtro de ameaças avançadas e análise de execução em tempo real, e inspeção de tráfego de saída de callbacks;

Suportar os protocolos HTTP assim como inspeção de tráfego criptografado através de HTTPS e TLS;

A solução deve ser capaz de inspecionar o tráfego criptografado SSL e SSH;

Identificar e bloquear a existência de malware em comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle;

Implementar mecanismo de bloqueio de vazamento não intencional de dados oriundos de máquinas existentes no ambiente LAN em tempo real;

Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar arquivo PDF com até 10Mb;

Implementar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows XP, Windows 7, Windows 10, MacOS, Android, Linux

Conter ameaças de dia zero permitindo ao usuário final o recebimento do arquivos livres de malware;

A tecnologia de máquina virtual deverá suportar diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas;

A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliance através de assinaturas.

Implementar a visualização dos resultados das análises de malwares de dia zero nos diferentes sistemas operacionais dos ambientes controlados (sandbox) suportados;

Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego;

Conter ameaças avançadas de dia zero;

Toda análise deverá ser realizada de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador;

Implementar mecanismo do tipo múltiplas fases para verificação de malware e/ou códigos maliciosos;

Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real. Não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos;

Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx) e Android APKs no ambiente controlado;

Implementar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;

Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, POP3, FTP , IMAP e CIFS;

Conter ameaças de dia zero de forma transparente para o usuário final;

Conter ameaças de dia zero através de tecnologias em nível de emulação e código de registro;

Implementar mecanismo de pesquisa por diferentes intervalos de tempo;

Conter ameaças de dia zero via tráfego de internet;

Permitir a contenção de ameaças de dia zero sem a alteração da infraestrutura de segurança;

Conter ameaças de dia zero que possam burlar o sistema operacional emulado;

A solução deve permitir a criação de White list baseado no MD5 do arquivo;

Conter ameaças de dia zero antes da execução e evasão de qualquer código malicioso;

Conter exploits avançados.

A análise "In Cloud" ou local deve prover informações sobre as ações do Malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo Malware, gerar assinaturas de Antivírus e Antispyware automaticamente, definir URLs não confiáveis utilizadas pelo novo Malware e prover Informações sobre o usuário infectado (seu endereço IP e seu login de rede);

Suporte a submissão manual de arquivos para análise através do serviço de Sandbox.

ADMINISTRAÇÃO

Suportar no mínimo 20.000 usuários autenticados com serviços ativos e identificados passando por este dispositivo de segurança em um único dispositivo de segurança. Políticas baseadas por grupos de usuários deverão ser suportadas por este dispositivo. Está comprovação poderá ser exigida em testes sobe o ambiente de produção com o fornecimento do produto para comprovação deste e demais itens.

Permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o firewall, cada um responsável por determinadas tarefas da administração;

Fornecer gerência remota, com interface gráfica nativa;
A interface gráfica deverá possuir assistentes para facilitar a configuração inicial e a realização das tarefas mais comuns na administração do firewall, incluindo a configuração de VPN IPSECs, NAT, perfis de acesso e regras de filtragem;

Possuir mecanismo que permita a realização de cópias de segurança (backups) e sua posterior restauração remotamente, através da interface gráfica, sem necessidade de se reinicializar o sistema;

Possuir mecanismo para possibilitar a aplicação de correções e atualizações para o firewall remotamente através da interface gráfica;

Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do firewall e a remoção de qualquer uma destas sessões ou conexões;

Permitir a geração de gráficos em tempo real, representando os serviços mais utilizados e as máquinas mais acessadas em um dado momento;

Permitir a visualização de estatísticas do uso de CPU, memória da máquina onde o firewall está rodando e tráfego de rede em todas as interfaces do Firewall através da interface gráfica remota, em tempo real e em forma tabular e gráfica;

Permitir a conexão simultânea de vários administradores, sendo um deles com poderes de alteração de configurações e os demais apenas de visualização das mesmas. Permitir que o segundo ao se conectar possa enviar uma mensagem ao primeiro através da interface de administração.

Possibilitar o registro de toda a comunicação realizada através do firewall, e de todas as tentativas de abertura de sessões ou conexões que forem recusadas pelo mesmo;
Possuir interface orientada a linha de comando para a administração do firewall a partir do console ou conexão SSH sendo está múltiplas sessões simultâneas.

Possuir mecanismo que permita inspecionar o tráfego de rede em tempo real (sniffer) via interface gráfica, podendo opcionalmente exportar os dados visualizados para arquivo formato PCAP e permitindo a filtragem dos pacotes por protocolo, endereço IP origem e/ou destino e porta IP origem e/ou destino, usando uma linguagem textual;

Permitir a visualização do tráfego de rede em tempo real tanto nas interfaces de rede do Firewall quando nos pontos internos do mesmo: anterior e posterior à filtragem de pacotes, onde o efeito do NAT (tradução de endereços) é eliminado;

Possuir sistema de respostas automáticas que possibilite alertar imediatamente o administrador através de e-mails, janelas de alerta na interface gráfica, execução de programas e envio de Traps SNMP;

Relatórios

Ser capaz de visualizar, de forma direta no appliance e em tempo real, as aplicações mais utilizadas, os usuários que mais estão utilizando estes recursos informando sua sessão, total de pacotes enviados, total de bytes enviados e média de utilização em Kbps, URLs acessadas e ameaças identificadas.

Possibilitar a geração de pelo menos os seguintes tipos de relatório com cruzamento de informações, mostrados em formato HTML: máquinas acessadas X serviços bloqueados, usuários X URLs acessadas, usuários X categorias Web bloqueadas (em caso de utilização de um filtro de conteúdo Web);

Possibilitar a geração de pelo menos os seguintes tipos de relatório, mostrados em formato HTML: máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas, ou categorias Web mais acessadas (em

caso de existência de um filtro de conteúdo Web), maiores emissores e receptores de e-mail;

Permitir o envio dos relatórios, através de email para usuários prédefinidos;

Possuir relatórios pré-definidos na solução e permitir a criação de relatórios customizados;

Possibilitar a geração dos relatórios sob demanda e através de agendamento diário, semanal e mensal. No caso de agendamento, os relatórios deverão ser publicados de forma automática.

Disponibilizar download dos relatórios gerados;

Garantia, Suporte e Licenciamento

O licenciamento para todos os serviços de Next Generation Firewall deverá ser de 36 meses.

A garantia deverá ser de 36 meses.

Deve contemplar suporte do Fabricante pelo período vigente. Com no mínimo, as seguintes características:

a. O suporte do fabricante deve ter um sistema de abertura de chamados para acompanhamento – funcionando 24 horas por dia e 7 dias por semana. Para atendimento telefônico, deve operar em língua Portuguesa pelo menos em regime 8x5.

b. Deve assegurar a utilização de novas versões de software da solução sem ônus a Licitante, sempre que esta estiver disponível a qualquer cliente

c. Deve permitir o acesso à base de conhecimento da solução.

Conformidade

a)O Fabricante deve comprovar participação no MAPP da Microsoft;

b)A tecnologia deve possuir pelo menos uma certificação da ICSA Labs, ICSA Firewall ou Antivirus;

c)O fabricante da solução deverá ser avaliado pela NSS Labs (Network Security Services) no desempenho do Next Generation Firewall Comparative Analysis mais recente, estando no "Security Value Map" acima de 90% (noventa por cento) da avaliação de segurança efetiva.

d) A Empresa arrematante/vencedora deverá enviar juntamente com toda a documentação exigida, declaração do(s) fabricante(s), em papel timbrado com firma reconhecida dos produtos ofertados em proposta comercial, declarando que a proponente possui credenciamento do mesmo nas áreas de Consultoria Técnica, Venda, Suporte/Instalação e Manutenção dos referidos produtos Sonicwall;

e) Deve ser homologado pela ANATEL.

LOTE 2 - SOFTWARE – LICENCIAMENTO PERPÉTUO MICROSOFT SQL SERVER 2017 GOVERNO POR PROCESSADOR.

ITEM	QTD	DESCRIÇÃO
01	02	SQLSRVSTDCORE 2017 SNGL OLP 2LIC NL GOV CORELIC QLFD-7QN-0183G BRL.

IV - DO PAGAMENTO

O pagamento será efetuado pelo Conselho Regional de Economia – 2ª Região - SP, em até 21 (vinte e um) dias corridos, contados a partir da entrega dos objetos, mediante apresentação da Nota Fiscal/Fatura, sendo efetuada a retenção de tributos e contribuições sobre o pagamento a ser realizado, conforme determina a legislação vigente.

V - DOTAÇÃO ORÇAMENTÁRIA

As despesas decorrentes desta licitação correrão pela seguinte dotação orçamentária:

LOTES 1 e 2: 3.1.30.02.20 Serviços de Informática

PREGÃO ELETRÔNICO Nº 07/2018

PROCESSO Nº L-07/2018

A N E X O II

MODELO DE DECLARAÇÃO DE ME-EPP

DECLARAÇÃO

Em atendimento ao previsto na Condição 11, Item 11.8 do Pregão Eletrônico nº 07/2018, a empresa....., inscrita no CNPJ nº ....., por intermédio de seu representante legal o(a) Sr(a)....., portador(a) da Carteira de Identidade nº ..... e do CPF nº....., DECLARA, sob as penas da lei, ser microempresa ou empresa de pequeno porte nos termos da legislação vigente, estando apta a usufruir o tratamento favorecido estabelecido na Lei Complementar nº 123/2006.

Local e Data

_____
assinatura e carimbo
(representante legal)

OBS.: Emitir em papel que identifique a **licitante**.

PREGÃO ELETRÔNICO Nº 07/2018

PROCESSO Nº L-07/2018

A N E X O III

MODELO DE SUPERVENIENCIA DE FATO IMPEDITIVO DE HABILITAÇÃO

_____*(nome da empresa),* CNPJ/MF n.º_____, sediada à _____, declara sob as penas da lei, que até a presente data inexistem fatos impeditivos de sua habilitação no presente processo licitatório, ciente da obrigatoriedade de declarar ocorrências posteriores.

(local e data) _____.

_____
(assinatura autorizada, devidamente identificada)

Obs.: Emitir em papel que identifique a licitante e apresentar no original.

PREGÃO ELETRÔNICO Nº 07/2018

PROCESSO Nº L-07/2018

A N E X O IV

MODELO DE DECLARAÇÃO DE CUMPRIMENTO DO DISPOSTO NO INCISO XXXIII DO ART. 7º DA CONSTITUIÇÃO FEDERAL

_____*(nome da empresa),* CNPJ/MF n.º_____, sediada à _____, declara sob as penas da lei, que cumprimos o disposto no inciso XXXIII do art. 7º da Constituição Federal, que estabelece a proibição de trabalho noturno, perigoso ou insalubre a menores de dezoito anos e de qualquer trabalho a menores de dezesseis anos, salvo na condição de aprendiz, a partir de quatorze anos.

(local e data) _____.

_____
(assinatura autorizada, devidamente identificada)

OBS.: Emitir em papel que identifique a **licitante**.

PREGÃO ELETRÔNICO Nº 07/2018

PROCESSO Nº L-07/2018

A N E X O V

MINUTA DE CONTRATO

CONTRATO QUE ENTRE SI FORMALIZAM, DE UM LADO O CONSELHO REGIONAL DE ECONOMIA – 2ª REGIÃO - SP E, DE OUTRO, A EMPRESA _____ PARA O FIM QUE NELE SE DECLARA.

O **Conselho Regional de Economia – 2ª Região - SP**, com sede na Rua Líbero Badaró, 425, 14º andar, nesta Capital, inscrita no CNPJ sob o nº 62.144.084/0001-94, neste ato representado por seu Presidente, Econ. Manuel Enriquez Garcia, portador do CPF nº XXX.XXX.XXX-XX e RG nº X.XXX.XXX, doravante denominado **CONTRATANTE** e, de outro, a empresa _____, pessoa jurídica de direito _____ estabelecida na Rua/Av _____, inscrita no CNPJ sob o nº _____ e Inscrição Estadual nº _____, adiante denominada **CONTRATADA**, tendo como representante legal o Sr(a). _____, portador do CPF nº _____ e RG. nº _____, resolvem firmar o presente contrato, com fundamento no art. 22, inciso II, da Lei 8.666/93 e alterações subsequentes, e ainda, em conformidade com o Decreto 1.070/94, combinada com as demais normas de direito aplicáveis à espécie e no que consta no processo administrativo de Pregão Eletrônico, tipo Menor Preço nº 07/2018 - CORECON-SP, mediante as condições constantes das seguintes cláusulas, que ambas as partes aceitam, ratificam e outorgam, por si e seus sucessores.

CLÁUSULA PRIMEIRA – DO OBJETO

1.1. O objeto da presente licitação consiste em manter ativo o Suporte Técnico e Atualização dos Produtos DELL SONICWALL CGSS Comprehensive Gateway Security Suite for the NSA 2400 Series por 36 meses, para AGSS Advanced Gateway Security Suíte for the NSA 2400 Series por 36 meses, conforme especificações constantes do Termo de Referência (Anexo I).

1.1.1. A CONTRATADA se obriga a aceitar acréscimos ou supressões, mediante comunicação por escrito do CONTRATANTE, nas mesmas condições deste contrato, até o limite de 25% (vinte e cinco por cento) do seu valor inicial atualizado, conforme previsto no Parágrafo 1º do Art. 65 da Lei nº 8.666/93.

CLÁUSULA SEGUNDA - DAS OBRIGAÇÕES DA CONTRATADA

2.1. Constituem obrigações da CONTRATADA:

a) Responsabilizar-se integralmente pela entrega do objeto e/ou execução dos serviços, no Departamento de Informática do Conselho Regional de Economia – 2ª Região - SP, situado na Rua Líbero Badaró, 425, 14º andar, Centro, São Paulo - SP, de acordo com as especificações e demais normas pertinentes, em data e horário previamente agendados;

b) Apresentar Nota Fiscal/Fatura, discriminando necessariamente todos os artigos ofertados, bem como o valor de cada item, observando também as

Instruções Normativas da Secretaria da Fazenda nº 480, de 15 de dezembro de 2004 e nº 539 de 25 de abril de 2005 que trata da retenção na fonte do Imposto Sobre a Renda da Pessoa Jurídica (IRPJ), da Contribuição Social Sobre o Lucro Líquido (CSLL), da Contribuição Para o Financiamento da Seguridade Social (COFINS) e da Contribuição para o PIS/PASEP. Em obediência às normas legais e tributárias, o Conselho Regional de Economia – 2ª Região – SP, por ser autarquia federal, está sujeita a reter na fonte e recolher os impostos mencionados, independentes do valor da nota ou documento fiscal, conforme a natureza do bem fornecido ou do serviço prestado conforme o Anexo I – Tabela de Retenções da IN SRF nº. 539;

c) Disponibilizar para o CONTRATANTE todos os documentos, informações e esclarecimentos, quando solicitados;

d) Responder financeiramente, sem prejuízo de outras medidas que possam ser adotadas, por quaisquer danos de sua responsabilidade para com a União, o Estado, o Município ou terceiros;

e) Efetuar pontualmente o pagamento de todos os impostos, taxas e tributos devidos à União, ao Estado e ao Município relacionados com a execução do presente contrato, apresentando, quando solicitado pelo CONTRATANTE, comprovante de regularidade;

f) Responder, em relação aos seus empregados, por todas as despesas decorrentes do fornecimento dos equipamentos, tais como: salários, seguros de acidentes, taxas, impostos e contribuições; indenizações; benefícios e outras que porventura venham a ser criadas e exigidas pelo Poder Público;

g) Assumir a responsabilidade por todas as providências e obrigações estabelecidas na legislação específica de acidentes de trabalho, quando ocorrerem e forem vítimas seus empregados ou representantes no desempenho de atividade pertinente ao objeto do contrato, inclusive se o sinistro se der nas dependências do CONTRATANTE;

h) Responder pelos danos causados diretamente ao CONTRATANTE ou a terceiros, decorrente de culpa ou dolo da CONTRATADA, quando da entrega do objeto, não ficando reduzida essa responsabilidade pela fiscalização ou acompanhamento do CONTRATANTE;

i) Responder por quaisquer danos causados diretamente aos equipamentos, quando estes tenham sido ocasionados por funcionários da CONTRATADA, quando do manuseio ou transporte incorretos;

j) Reparar, corrigir, remover, reconstituir ou substituir, a expensas da CONTRATADA, no total ou em parte, os objetos apresentados com vícios, defeitos ou incorreções decorrentes de imperfeições de fabricação ou manuseamento incorreto por parte da CONTRATADA;

k) Manter os seus funcionários identificados quando da entrega ou suporte dos equipamentos;

l) É expressamente proibida, à CONTRATADA, a veiculação de publicidade acerca deste Contrato, salvo se houver prévia autorização da Administração da CONTRATANTE.

CLÁUSULA TERCEIRA – DAS OBRIGAÇÕES DA CONTRATANTE

3.1. Constituem obrigações do CONTRATANTE:

a) Acompanhar, fiscalizar e dar recibo da entrega do objeto;

b) Indicar um funcionário lotado no Departamento de Informática para o acompanhamento do trabalho. O funcionário designado registrará todas as ocorrências relacionadas com o objeto deste Contrato, determinando o que for necessário para a regularização das faltas ou defeitos observados;

c) Efetuar o pagamento nas condições pactuadas;

d) Assumir a responsabilidade pelos prejuízos causados ao objeto, em decorrência de defeitos provenientes de operação imprópria em manuseio, uso e/ou intervenção indevidos, negligência, imprudência ou imperícia dos prepostos do CONTRATANTE, bem como de terceiros;

e) Suspender o recebimento do objeto, ao constatar incompatibilidade com as especificações descritas no Anexo I- Termo de Referência;

f) Solicitar a substituição do objeto se, no decorrer de 30 (trinta) dias consecutivos após o recebimento definitivo, apresentar defeitos sistemáticos de fabricação, devidamente comprovada pelas reiteradas manutenções corretivas.

CLÁUSULA QUARTA – DO PRAZO DE ENTREGA

4.1. A licitante vencedora terá até 20 (vinte) dias corridos para a entrega e/ou execução do objeto deste certame, a contar da data de assinatura do contrato.

CLÁUSULA QUINTA – DA EXECUÇÃO DOS SERVIÇOS

5.1. A entrega dos produtos e a prestação dos serviços se dará preponderantemente em dias úteis, horário comercial, podendo, todavia, serem estipulados outros horários ou dias de fins de semana, a critério do CORECON-SP, sem custos adicionais de qualquer natureza, desde que se entenda que tal estipulação permita maior eficiência e melhores resultados na execução deste contrato.

5.2. O objeto desta licitação será entregue na sede do CORECON-SP, na Rua Líbero Badaró, 425, 14º andar, Centro, São Paulo SP, Departamento de Informática.

CLÁUSULA SEXTA – DOS PREÇOS E CONDIÇÕES DE PAGAMENTO

6.1. O valor total da aquisição do lote é de R$ xx.xxx,xx (xxxxx xxxxxx xxxxxx xxxxx).

6.2. O pagamento será efetuado em até 21 (vinte e um) dias corridos, contados a partir da entrega do objeto, contra apresentação da nota fiscal/ fatura respectiva, ficando ainda condicionado ao aceite definitivo do objeto, atestado este emitido pelo Setor competente.

6.3. A CONTRATANTE deduzirá das faturas à serem pagas à CONTRATADA:

a) As quantias a ele devidas, a qualquer título;

b) O valor das multas porventura aplicadas à CONTRATADA, conforme previsto neste contrato;

c) O valor dos prejuízos causados pela CONTRATADA, em decorrência deste contrato;

d) O valor dos pagamentos porventura efetuados pelo CONTRATANTE a terceiros, por quaisquer prejuízos causados pela CONTRATADA, relacionados a execução do objeto deste contrato.

6.4. No preço previsto nesta Cláusula estão inclusos todos os custos decorrentes do perfeito cumprimento do presente contrato, inclusive os relacionados a pessoal, materiais e supervisão para a execução dos serviços, impostos, taxas, seguros, transportes, contribuições sociais e trabalhistas e quaisquer outras despesas diretas ou indiretamente incidentes, além do valor pago pelos bens adquiridos.

6.5. As despesas decorrentes do presente Processo Licitatório, e deste exercício, correrão pela seguinte dotação orçamentária:

LOTES 1 e 2: 3.1.30.02.20 – Serviços de Informática.

CLÁUSULA SÉTIMA – DA EXISTÊNCIA DOS BENS COMPRADOS

7.1. A CONTRATADA garante a existência dos bens comprados pelo CONTRATANTE, conforme previsto no objeto do Edital, sob pena de rescisão contratual e aplicação das penalidades cabíveis.

CLÁUSULA OITAVA - DA AQUISIÇÃO DA PROPRIEDADE

8.1. Após o pagamento, o CONTRATANTE adquirirá plena propriedade de todos os objetos comprados e, em consequência, poderá usar, transferir, vender, alienar, doar, gravar com qualquer ônus, sem necessidade de qualquer autorização da CONTRATADA para esses procedimentos e outros que julgarem necessários.

CLÁUSULA NONA – DA VIGÊNCIA

9.1. Este Contrato tem vigência a partir da sua assinatura até o término da garantia do objeto.

CLÁUSULA DÉCIMA – DAS SANÇÕES CONTRATUAIS

10.1. A CONTRATADA sujeitar-se-á, em caso de inadimplemento das suas obrigações, além de outras responsabilidades de natureza civil e penal, sanções previstas no art. 7º, da Lei nº 10.520/02, bem como aos arts. 86 e 87 da Lei nº 8.666/93, sem prejuízo da reparação dos danos causados ao CONSELHO.

10.2. A CONTRATADA ficará sujeita, em caso de atraso injustificado na execução do contrato, sem prejuízo da rescisão unilateral e de outras sanções previstas na Lei Nº 8.666/93, a multa nos seguintes limites:

a) 20% (vinte por cento) sobre o valor da Proposta, em caso de recusa da CONTRATADA em assinar o Contrato dentro de 05 (cinco) dias úteis, contados da data de sua convocação;

b) 0,3% (três décimos por cento) ao dia, até o trigésimo dia de atraso na entrega dos produtos, sobre o valor do contrato não realizado;
c) 20% (vinte por cento) sobre o valor do Contrato não realizado, no caso de:

- Atraso superior a 30 (trinta) dias, na entrega dos produtos;
- Desistência da entrega dos bens;

d) A suspensão temporária de participação em licitação e impedimento em contratar com a Administração Pública, pelo prazo de 01 (um) ano;

e) A Declaração de Inidoneidade para licitar e contratar com a Administração será aplicada à CONTRATADA que der causa, por duas vezes, à suspensão prevista no item anterior;

f) As multas referidas nesta Cláusula serão descontadas, "ex-offício", de qualquer fatura ou crédito existente no CONTRATANTE em favor da CONTRATADA.

CLÁUSULA DÉCIMA PRIMEIRA – DA RESPONSABILIDADE DA CONTRATADA

11.1. Fica expressamente excluída qualquer responsabilidade da CONTRATANTE, na hipótese da CONTRATADA infringir, em decorrência da execução do objeto deste contrato, quaisquer leis.

11.2. Caso a CONTRATANTE, por qualquer motivo, venha a ser judicialmente processada por infringir patentes, marcas, direitos autorais, direitos exclusivos de representação, relacionados com o fornecimento dos bens comprados a CONTRATADA responsabilizar-se-á pelos prejuízos decorrentes da ação judicial, inclusive honorários advocatícios, custas e despesas processuais, perdas e danos, lucros cessantes, juros moratórios ou quaisquer outras despesas aqui não expressamente relacionadas, devendo a CONTRATADA ser denunciada à lide.

11.3. Fica, ainda, expressamente excluída qualquer responsabilidade da CONTRATANTE por eventuais contratações que a CONTRATADA venha a efetivar para cumprimento das obrigações assumidas neste contrato.

CLÁUSULA DÉCIMA SEGUNDA - DA RESCISÃO

12.1. A rescisão do presente contrato subordinar-se-á às disposições estabelecidas no Capítulo III, Seção V, da Lei Federal Nº 8.666/93, e suas alterações posteriores, nas hipóteses e com as consequências ali prescritas.

12.2. É vedado o direito à CONTRATADA de rescindir, unilateralmente, o presente contrato.

CLÁUSULA DÉCIMA TERCEIRA – DA VINCULAÇÃO AO EDITAL E À PROPOSTA DA CONTRATADA

13.1. Serão partes integrantes deste Contrato o Edital e seus anexos e a proposta apresentada pela CONTRATADA.

CLÁUSULA DÉCIMA QUARTA - DO FORO

14.1. Para dirimir as questões oriundas do presente contrato, as partes elegem o Foro da Justiça Federal da Comarca desta Cidade de São Paulo, Capital do Estado de São Paulo, com renúncia de qualquer outro, por mais privilegiado que seja.

14.2. E, por estarem, assim, justas e acordadas, assinam o presente instrumento em 02 (duas) vias de igual teor e valor, para todos os efeitos jurídicos, na presença das testemunhas abaixo assinadas.

São Paulo, _____ de _____ de 2018.

CONTRATANTE	CONTRATADA

Testemunhas:

Nome:	Nome:

PREGÃO ELETRÔNICO Nº 07/2018
PROCESSO Nº L- 07/2018

ANEXO VI

MODELO DE PROPOSTA COMERCIAL

São Paulo, _____ de _____de 2018.

AO CONSELHO REGIONAL DE ECONOMIA – 2ª REGIÃO – SÃO PAULO

Ref.: Manter ativo o Suporte Técnico e Atualização dos Produtos DELL SONICWALL CGSS Comprehensive Gateway Security Suite for the NSA 2400 Series por 36 meses, para AGSS Advanced Gateway Security Suíte for the NSA 2400 Series por 36 meses.

LOTE 1 - SOFTWARE - RENOVAÇÃO CGSS SONICWALL COM ATUALIZAÇÃO PARA AGSS SONICWALL E SUPORTE TÉCNICO PARA EQUIPAMENTO NSA 2400 EM HA PARA 36 MESES.

ITEM	QTD	DESCRIÇÃO
01	**01**	**DELL SONICWALL CGSS (Comprehensive Gateway Security Suite Bundle for the NSA 2400 Series (3Year) com atualização para AGSS (Advanced Gateway Security Suite) 3 Year.**

LOTE 2 - SOFTWARE – LICENCIAMENTO PERPÉTUO MICROSOFT SQL SERVER 2017 GOVERNO POR PROCESSADOR.

ITEM	QTD	DESCRIÇÃO
01	**02**	**SQLSRVSTDCORE 2017 SNGL OLP 2LIC NL GOV CORELIC QLFD-7QN-0183G BRL.**

VALOR
Item 1:
Item 2:

Nome:		Nacionalidade:
Profissão:		Cargo:
RG:	CPF:	Estado Civil:
Razão Social da Empresa:		
Endereço completo:		
CNPJ-MF:	Inscrição Estadual:	

_____

Assinatura do Representante Legal da Licitante