



INSTRUMENTO PARTICULAR DE CONTRATO Nº NLP-119/2017 QUE ENTRE SI CELEBRAM O COMITÊ BRASILEIRO DE CLUBES – CBC E A EMPRESA ALERTA SECURITY SOLUTIONS INFORMÁTICA LTDA, NA FORMA ABAIXO:

Aos vinte e três dias do mês de janeiro do ano de 2018 (dois mil e dezoito), nesta cidade de Campinas, na Rua Açaí, 566, Bairro das Palmeiras, Campinas, S.P., CEP 13092-587, pelo presente instrumento, e na melhor forma de direito, de um lado o **COMITÊ BRASILEIRO DE CLUBES**, associação civil de natureza desportiva, sem fins econômicos, inscrito no CNPJ/MF sob o nº 00.172.849/0001-42, no uso de suas atribuições legais, neste ato representado na forma de seu Estatuto Social, doravante denominado simplesmente **CONTRATANTE**, e, de outro lado, a **ALERTA SECURITY SOLUTIONS INFORMÁTICA LTDA**, sociedade inscrita no CNPJ/MF sob o nº 06.946.041/0001-51, com sede na Rua Boa Vista, 254 – Conjunto 1714, CEP: 01014-000, Centro, São Paulo/SP, neste ato representada na forma de seu Contrato Social por Djeimes Reis Brito, doravante denominada **CONTRATADA**, considerando que esta última sagrou-se vencedora do Pregão Presencial nº NLP-017/2017, nos termos do que determina o Regulamento de Compras e Contratações do CBC ("RCC do CBC") e obedecidas as disposições contidas no Edital e seus Anexos, têm entre si ajustado o fornecimento de Solução de Firewall de Aplicação para no mínimo 100 (cem) usuários, compreendendo hardware e software (appliance), serviços de instalação e configuração, garantia, suporte técnico e treinamentos, destinados atender as unidades do CBC em Campinas/SP e Brasília/DF, mediante as cláusulas e condições seguintes que mutuamente aceitam, outorgam e estipulam:

1 CLÁUSULA PRIMEIRA – DO OBJETO

- 1.1 A **CONTRATADA**, na qualidade de adjudicatária do **PREGÃO PRESENCIAL nº NLP-017/2017**, sob o regime de empreitada por menor preço total por lote, obriga-se a cumprir o estabelecido neste instrumento contratual, o qual tem por objeto a contratação de empresa para o fornecimento de Solução de Firewall de Aplicação para no mínimo 100 (cem) usuários, compreendendo hardware e software (appliance), serviços de instalação e configuração, garantia, suporte técnico e treinamentos, destinados atender as unidades do CBC em Campinas/SP e Brasília/DF, conforme características e descrições informadas no Edital e seu Anexo I – Termo de Referência, bem como as demais disposições da respectiva Proposta Comercial que, para todos os efeitos, ficam fazendo parte integrante deste instrumento contratual, vinculando-se totalmente a este.

2 CLÁUSULA SEGUNDA – DAS OBRIGAÇÕES DA CONTRATADA

- 2.1 São obrigações da **CONTRATADA**, além de outras fixadas neste CONTRATO, no Edital e Anexos, assim como nas leis vigentes ou que entrarem em vigor, as seguintes:
- 2.1.1 Manter, durante todo o prazo de vigência deste CONTRATO, em compatibilidade com as obrigações por ela assumidas, todas as condições de qualificação e habilitação exigidas no respectivo processo de aquisição, comprovando-as quando solicitado pelo CBC;
- 2.1.2 Cumprir o objeto da presente avença de acordo com o Anexo I do Edital (Termo de Referência) e Proposta Comercial, na estrita observância da legislação pertinente em vigor;

**CBC****COMITÊ BRASILEIRO
DE CLUBES**

- 2.1.3 Resguardar o sigilo dos dados e documentos que lhe forem confiados para o desempenho dos serviços ora contratados, ou que vier a ter acesso, direta ou indiretamente, durante a execução do objeto, devendo orientar os seus profissionais envolvidos a cumprir esta obrigação. Não divulgar quaisquer dados, conhecimentos e resultados decorrentes da execução do objeto deste CONTRATO, sem prévia e expressa autorização da **CONTRATANTE**;
- 2.1.4 Fornecer, às suas expensas, todos os materiais, mão-de-obra e equipamentos necessários à execução dos serviços;
- 2.1.5 Comunicar a imposição de qualquer penalidade que acarrete o impedimento de contratar com o CBC, bem como a eventual perda dos pressupostos para o processo de aquisição;
- 2.1.6 Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do CONTRATO em que se verificarem vícios, defeitos ou incorreções decorrentes da execução;
- 2.1.7 Reparar todos os danos e prejuízos causados ao CBC, decorrentes de sua culpa ou dolo, não restando excluída ou reduzida esta responsabilidade pela presença de fiscalização ou pelo acompanhamento da execução por parte do Gestor do CONTRATO;
- 2.1.8 Pagar todos os encargos e tributos, que incidam ou venham a incidir, direta ou indiretamente, sobre o objeto deste CONTRATO, podendo o CBC, a qualquer momento, exigir da CONTRATADA a comprovação de sua regularidade;
- 2.1.9 Designar 01 (um) preposto como responsável pelo CONTRATO firmado com o CBC, para participar de eventuais reuniões e ser o interlocutor da CONTRATADA, zelando pelo fiel cumprimento das obrigações previstas neste Instrumento;
- 2.1.10 Prestar todos os esclarecimentos que lhe forem solicitados pela CONTRATANTE, atendendo prontamente a quaisquer reclamações;
- 2.1.11 Providenciar que seus contratados portem crachá de identificação quando da execução dos serviços à CONTRATANTE;
- 2.1.12 Arcar com os ônus resultantes de quaisquer ações, demandas, custos e despesas decorrentes de contravenção, seja por culpa sua ou de quaisquer de seus empregados ou prepostos, obrigando-se, outrossim, a quaisquer responsabilidades decorrentes de ações judiciais ou extrajudiciais de terceiros, que lhe venham a ser exigidas por força da lei, ligadas ao cumprimento do CONTRATO;
- 2.1.13 Assumir a responsabilidade por todos os encargos previdenciários e obrigações sociais previstos na legislação social e trabalhista em vigor, obrigando-se a saldá-los na época própria, vez que os seus empregados não manterão nenhum vínculo empregatício com a CONTRATANTE;
- 2.1.14 Assumir a responsabilidade por todas as providências e obrigações estabelecidas na legislação específica de acidentes de trabalho, quando, em ocorrência da espécie, forem vítimas os seus empregados quando da prestação dos serviços ou em conexão com eles, ainda que acontecido em dependência da CONTRATANTE, inclusive por danos causados a terceiros;

**CBC****COMITÊ BRASILEIRO
DE CLUBES**

- 2.1.15 Assumir todos os encargos de possível demanda trabalhista, cível ou penal, relacionados a prestação do serviço, originariamente ou vinculada por prevenção, conexão ou contingência;
- 2.1.16 Manter sigilo em relação aos dados, informações ou documentos que tomar conhecimento em decorrência da prestação dos serviços objeto desta contratação, bem como se submeter às orientações e normas internas de segurança da informação vigentes, devendo orientar seus empregados e/ou prepostos nesse sentido, sob pena de responsabilidade civil, penal e administrativa;
- 2.1.17 Prestar todo o suporte técnico necessário ao adequado funcionamento do objeto, de acordo com o estabelecido no Termo de Referência – Anexo I do Edital;
- 2.1.18 Corrigir quaisquer faltas verificadas na execução do objeto, sem qualquer ônus adicional, cumprindo todas as determinações do CBC.
- 2.1.19 Não se valer do CONTRATO para assumir obrigações perante terceiros, dando-o como garantia, nem utilizar os direitos de crédito, a serem auferidos em função dos serviços prestados, em quaisquer operações de desconto bancário, sem a prévia autorização da CONTRATANTE.

Parágrafo Primeiro: É admitida a cessão contratual somente nas hipóteses em que a CONTRATADA realizar as operações societárias de fusão, cisão ou incorporação, condicionada aos seguintes requisitos.

- a) aquiescência prévia do CBC, que analisará eventuais riscos ou prejuízos decorrentes de tal alteração contratual; e
- b) manutenção de todas as condições contratuais e requisitos de habilitação originais.

Parágrafo Segundo: Caso ocorra a cessão contratual admitida no Parágrafo anterior, o cessionário assumirá integralmente a posição do cedente, passando a ser responsável pela execução do presente CONTRATO, fazendo jus, por conseguinte, ao recebimento dos créditos dele decorrentes.

Parágrafo Terceiro: É vedada a transferência e a subcontratação, total ou parcialmente, dos serviços contratados para a execução do objeto deste CONTRATO, sem a prévia e expressa aprovação do CBC.

- 2.1.20 Demonstrar, durante toda a vigência do CONTRATO, a manutenção da qualidade na prestação dos serviços especificados no Termo de Referência – Anexo I e neste CONTRATO.

3 CLÁUSULA TERCEIRA - DAS OBRIGAÇÕES DO CONTRATANTE

- 3.1 São obrigações do **CONTRATANTE**, além de outras fixadas neste instrumento contratual e no respectivo Edital, as seguintes:
- 3.1.1 Assegurar à **CONTRATADA** o recebimento dos créditos decorrentes do adimplemento de suas obrigações;



- 3.1.2 Fornecer todas as informações, esclarecimentos e condições necessárias à plena execução do objeto do presente ajuste.
- 3.1.3 Fiscalizar a observância das disposições deste CONTRATO, a fim de assegurar seu correto e tempestivo cumprimento, sem prejuízo dos procedimentos do controle exercidos pelo **CONTRATADA**.
- 3.1.4 Comunicar por escrito à **CONTRATADA** as deficiências verificadas pela fiscalização, que serão imediatamente corrigidas, sem prejuízo da aplicação das penalidades administrativas previstas.
- 3.1.5 Devolver à **CONTRATADA** a(s) nota(s) fiscal(ais)/fatura(s) contendo incorreções com as razões da devolução, por escrito, para as devidas retificações. A devolução de nota(s) fiscal(ais) fatura(s) não aprovada pelo **CONTRATANTE**, em hipótese alguma servirá de motivo para que a **CONTRATADA** suspenda ou atrase a execução do objeto do contrato.
- 3.1.6 Efetuar o pagamento à **CONTRATADA**, nas condições e dentro do prazo estabelecido neste CONTRATO.
- 3.1.7 Comunicar à **CONTRATADA**, por escrito:
- a) quaisquer instruções ou procedimentos sobre assuntos relacionados ao CONTRATO;
 - b) a abertura de procedimento para a apuração de condutas irregulares da **CONTRATADA**, concedendo-lhe prazo para defesa; e
 - c) a aplicação de eventual penalidade, nos termos deste CONTRATO;
- 3.1.8 Atestar as faturas por intermédio do gestor competente;
- 3.1.9 Permitir o acesso ao local da instalação do objeto contratado do pessoal da **CONTRATADA**, necessários à execução dos serviços de instalação e ativação dos equipamentos a serem fornecidos;

4 **CLÁUSULA QUARTA – DA EXECUÇÃO E RECEBIMENTO DO OBJETO E DA FISCALIZAÇÃO**

- 4.1 Os prazos para a entrega de materiais e execução dos serviços, são aqueles estabelecidos no Termo de Referência - Anexo I do Edital.

Parágrafo Primeiro: A entrega dos equipamentos e execução de serviços de instalação e ativação dos mesmos, objeto do presente Contrato, será acompanhada e fiscalizada por agente do **CONTRATANTE**, devidamente designado para tanto, ao qual competirá velar pela perfeita exação do pactuado, em conformidade com o previsto no edital e na proposta da **CONTRATADA**. Em caso de eventual irregularidade, inexecução ou desconformidade na execução do contrato, o agente fiscalizador dará ciência ao **CONTRATANTE** do sucedido, fazendo-o por escrito, bem assim das providências exigidas da **CONTRATADA** para sanar a falha ou defeito apontado, anotando em registro próprio qualquer ocorrência havida que esteja em desacordo com



os termos do ato convocatório, seus Anexos ou deste instrumento contratual, determinando, em decorrência disto, o que for necessário à regularização das falhas observadas.

Parágrafo Segundo: Uma vez concluídos os serviços de forma satisfatória, o Departamento responsável pela fiscalização atestará o cumprimento da obrigação com o registro na nota fiscal e emitirá o termo de recebimento dos equipamentos e serviços de instalação e ativação dos mesmos.

5 CLÁUSULA QUINTA - DA ALTERAÇÃO CONTRATUAL

- 5.1 Qualquer alteração contratual deverá observar o disposto nos artigos 46 e 47 do Regulamento de Compras e Contratações da COMITÊ BRASILEIRO DE CLUBES - CBC.

6 CLÁUSULA SEXTA - DO PREÇO, DO ELEMENTO ECONÔMICO E DAS CONDIÇÕES DE PAGAMENTO

- 6.1 O preço total do objeto enunciado na Cláusula Primeira deste ajuste é de **R\$ 122.000,00 (cento e vinte e dois mil reais)**, assim compreendido:

- **Lote 1**, destinado à unidade do CBC na cidade de Campinas - SP: valor total de **R\$ 61.000,00 (sessenta e um mil reais)**;
- **Lote 2**, destinado à unidade do CBC na cidade de Brasília - DF: valor total de **R\$ 61.000,00 (sessenta e um mil reais)**.

O **CONTRATANTE** executa os seus pagamentos aos fornecedores nos dias 5, 15 e 25 de cada mês, ou, na coincidência com finais de semana ou feriados, no dia útil imediatamente seguinte. Assim, constatado o cumprimento da obrigação e trâmites internos de aprovação, o pagamento será efetuado em um dos dias mencionados acima, desde que observado, no entanto, o prazo mínimo de 15 (quinze) dias corridos ao da apresentação da nota fiscal, contados a partir do primeiro dia útil ao do recebimento do documento, acompanhado dos documentos de cobrança, das certidões do FGTS e Certidão Negativa de Débitos Relativos aos Tributos Federais e à Dívida Ativa da União atualizadas.

- 6.1.1 Para execução do pagamento, a **CONTRATADA** deverá fazer constar como beneficiário/cliente da Nota Fiscal/Fatura correspondente, emitida sem rasuras, o Comitê Brasileiro de Clubes - CBC.
- 6.1.2 O pagamento será efetuado por meio de ordem bancária de crédito, mediante depósito em conta - corrente, na agência e estabelecimento bancário indicado pela **CONTRATADA**.
- 6.1.3 Na hipótese de a **CONTRATADA** optar pelo pagamento mediante BOLETO BANCÁRIO, deverá emití-lo com vencimento anotado para uma das três datas previstas no item 6.1 desta Cláusula Sexta, obrigando-se, no entanto, a que o BOLETO BANCÁRIO seja apresentado ao CBC com antecedência de 15 (quinze) dias corridos ao da data de seu vencimento, sem prejuízo da apresentação da Nota Fiscal.

**CBC****COMITÊ BRASILEIRO
DE CLUBES**

- 6.1.4 A Fatura correspondente será examinada diretamente pelo Fiscal designado pelo **CONTRATANTE**, o qual somente atestará o recebimento dos equipamentos e a prestação dos serviços e liberará a referida Nota Fiscal/Fatura para pagamento quando cumpridas, pela **CONTRATADA**, todas as condições pactuadas relativas ao objeto do Contrato.

Parágrafo Primeiro: Ocorrendo atraso no pagamento, e desde que para tal não tenha concorrido de alguma forma por culpa da **CONTRATADA**, haverá incidência de atualização monetária sobre o valor devido, pela variação acumulada do Índice Geral de Preços do Mercado - IGP-M, publicado pela Fundação Getúlio Vargas - FGV.

Parágrafo Segundo: O requerimento de pagamento bem como os documentos de cobrança da **CONTRATADA**, deverão ser entregues em um dos endereços estabelecidos na CLÁUSULA QUARTA deste instrumento contratual, considerando, para tanto, o respectivo endereço para o qual o objeto será executado.

- 6.2 No caso de incorreção nos documentos apresentados, inclusive na Nota Fiscal/Fatura, serão estes restituídos à **CONTRATADA** para as correções solicitadas, não respondendo o **CONTRATANTE** por quaisquer encargos resultantes de atrasos na liquidação dos pagamentos correspondentes.

7 CLÁUSULA SÉTIMA – DAS CONDIÇÕES PARA A CONTRATAÇÃO

- 7.1 A **CONTRATADA** exibe, neste ato, as certidões expedidas pelo FGTS e a Certidão Negativa de Débitos Relativos aos Tributos Federais e à Dívida Ativa da União, com prazo de validade em vigor, que demonstrem sua regularidade no cumprimento dos encargos estabelecidos em lei, obrigando-se a atualizá-las sempre que se vencerem no prazo de execução deste CONTRATO, como condição para liberação do respectivo pagamento.

8 CLÁUSULA OITAVA – DOS ENCARGOS

- 8.1 Os encargos trabalhistas, previdenciários, fiscais, comerciais, de transportes e seguro, inclusive aqueles relativos a impostos e taxas, inclusive de administração, são de inteira responsabilidade da **CONTRATADA**, bem como despesas e obrigações financeiras de qualquer natureza, despesas operacionais com frete e entrega, o valor dos materiais, matérias-primas, mão-de-obra, inclusive horas extras e adicionais noturnos de profissionais, auxílio alimentação, auxílio transporte e transporte local, sendo que sua inadimplência, com relação a tais encargos, não transfere ao **CONTRATANTE** o ônus pelo seu pagamento, não podendo onerar a presente avença.

9 CLÁUSULA NONA – DAS PENALIDADES

- 9.1 O descumprimento das condições técnicas, comerciais ou jurídicas estabelecidas no edital, proposta comercial e contrato caracterizará o descumprimento das obrigações assumidas e poderá acarretar ao participante as seguintes penalidades, previstas no instrumento convocatório:



CBC

COMITÊ BRASILEIRO
DE CLUBES



I - glosa correspondente à parcela de materiais não entregues e/ou entregues em desacordo com o objeto deste contrato;

II - advertência;

III - multa;

IV - suspensão temporária para participar dos processos seletivos do CBC e de suas entidades filiadas e, por consequência, de contratar com a mesma, pelo prazo mínimo de 6 (seis) meses e máximo de 24 (vinte e quatro) meses, nas condições estabelecidas no instrumento convocatório.

Parágrafo Primeiro: As penas previstas nos incisos I, II, III e IV desta cláusula poderão ser aplicadas cumulativamente ou não, sem prejuízo da rescisão do ajuste por ato unilateral do CBC ou de sua entidade filiada bem como a aplicação das demais disposições dos artigos 48 e seguintes do RCC do CBC.

Parágrafo Segundo: Das Multas:

I - A recusa injustificada do adjudicatário em assinar, aceitar ou retirar o contrato, dentro do prazo estabelecido pelo **CONTRATANTE**, ensejará a multa correspondente a 30% (trinta por cento) do valor do ajuste ou, a critério do CBC, multa correspondente à diferença do preço resultante de nova Contratação para realização da obrigação não cumprida, prevalecendo a de maior valor.

II - No caso de inexecução parcial, fica estabelecida multa de 20% (vinte por cento) sobre o valor total do contrato à **CONTRATADA**, quando esta infringir ou deixar de cumprir quaisquer das obrigações ou Cláusulas Contratuais.

III - A inexecução total do ajuste ensejará a aplicação de multa de 30% (trinta por cento) do valor do ajuste ou, a critério do CBC, multa correspondente à diferença do preço resultante de nova Contratação para realização da obrigação não cumprida, prevalecendo a de maior valor.

IV - Em caso de rescisão contratual, por culpa da **CONTRATADA**, não terá ela direito à indenização de qualquer espécie, sendo aplicável multa de 30% (trinta por cento) do valor não executado do respectivo contrato, sem prejuízo das sanções anteriores.

9.2 O descumprimento injustificado de prazos fixados no contrato para entrega de materiais e execução de serviços com prazos determinados, ensejará a aplicação das seguintes multas, que incidirão sobre o valor das obrigações não cumpridas:

a) atraso de até 15 dias = 0,2% por dia de atraso;

b) atraso de 16 a 30 dias = 0,3% por dia de atraso;

c) atraso de 31 a 60 dias = 0,4% por dia de atraso.

9.3 O atraso superior a 60 dias será considerado inexecução parcial ou total do ajuste, conforme o caso.

9.4 Nos casos de serviços e/ou produtos não entregues, o atraso será contado a partir do primeiro dia útil subsequente ao término do prazo estabelecido para a entrega.

**CBC****COMITÊ BRASILEIRO
DE CLUBES**

- 9.5 Nos casos de serviços e/ou produtos não entregues e não aceitos, o atraso será contado a partir do 1º dia útil subsequente ao prazo estabelecido para a nova entrega.
- 9.6 Configurado o descumprimento da obrigação contratual, será a **CONTRATADA** notificada da infração e da penalidade correspondente, para apresentar defesa no prazo de 5 (cinco) dias úteis contados do 1º dia útil subsequente ao recebimento da notificação.
- 9.7 Recebida a defesa, a autoridade competente deverá manifestar-se motivadamente sobre o acolhimento ou rejeição das razões apresentadas, para concluir pela imposição ou não da penalidade.
- 9.8 No caso de aplicação de quaisquer das sanções, a(s) mesma(s) deverá(ão) ser publicada(s) no sítio eletrônico do CBC e notificado ao interessado.
- 9.9 O valor correspondente à multa, após o devido procedimento em que tenha sido assegurado o direito da ampla defesa à **CONTRATADA**, será descontado do primeiro pagamento subsequente devido à **CONTRATADA** decorrente de execução contratual e no caso de não haver pagamentos pendentes à **CONTRATADA**, o valor da multa deverá ser recolhido ao CBC, por meio de depósito bancário, no prazo de até 05 dias úteis contados da publicação da multa no sítio eletrônico do CBC e notificação ao interessado ou, caso o contrato tenha exigido garantia, o valor da multa será descontado da garantia prestada.
- 9.10 Aplicar-se-á advertência por faltas leves, assim entendidas como aquelas que não acarretarem prejuízos significativos ao objeto da contratação.
- 9.11 A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa, observando-se o RCC do CBC e os Princípios Gerais da Administração Pública.
- 9.12 As multas devidas e/ou prejuízos causados ao **CONTRATANTE** serão deduzidos dos valores a serem pagos, ou recolhidos em favor do CBC, ou deduzidos da garantia, ou ainda, quando for o caso, serão cobrados judicialmente.
- 9.13 Caso o **CONTRATANTE** determine, a multa deverá ser recolhida no prazo máximo de 05 (cinco) dias, a contar da data do recebimento da comunicação enviada à **CONTRATADA**.
- 9.14 Descumprimentos a quaisquer outros itens estabelecidos no Edital ou neste Contrato serão notificados pelo **CONTRATANTE** à **CONTRATADA** com a informação do prazo para a correção do inadimplemento e a gravidade considerada.

10 CLÁUSULA DÉCIMA – DA RESCISÃO

- 10.1 Além das hipóteses de inadimplemento previstas, este Contrato poderá ser rescindido a critério do **CONTRATANTE** e mediante aviso prévio por escrito, com antecedência de 10 (dez) dias corridos, caso ocorra insuficiência de repasse dos recursos financeiros oriundos da Lei nº



COMITÊ BRASILEIRO
DE CLUBES



9.615/98, ressalvando-se, apenas, ao direito do recebimento por parte da **CONTRATADA** das obrigações cumpridas até a data da rescisão:

- 10.2 As partes estarão eximidas de suas responsabilidades e, consequentemente, da aplicação de quaisquer penalidades, nada podendo pleitear uma da outra, a que título for, em caso de força maior, greves ou atos de terrorismo, casos em que os serviços e/ou produtos eventualmente ainda não prestados e/ou não entregues não serão reembolsados.
- 10.3 Os motivos de força maior que a juízo do **CONTRATANTE** possam justificar a suspensão da contagem de quaisquer prazos ou a prestação do serviço fora do prazo estipulado, somente serão considerados quando apresentados na ocasião das respectivas ocorrências. Não serão consideradas quaisquer alegações baseadas em ocorrências não aceitas pelo **CONTRATANTE** ou apresentadas intempestivamente.
- 10.4 O presente contrato também poderá ser rescindido nas hipóteses previstas no Art. 49 do RCC do CBC.

11 CLÁUSULA DÉCIMA PRIMEIRA – DOS DESCONTOS

- 11.1 Os valores de quaisquer indenizações, bem como das multas aplicadas pelo **CONTRATANTE**, poderão ser descontados do pagamento devido à **CONTRATADA**.

12 CLÁUSULA DÉCIMA SEGUNDA – DA VIGÊNCIA

- 12.1 O prazo de vigência deste Contrato é de 36 (trinta e seis) meses, a contar da data de sua assinatura, compreendendo neste prazo o período de prestação de garantia e assistência técnica referentes ao objeto fornecido pela **CONTRATADA**, podendo ser prorrogado até o limite de sessenta meses.

13 CLÁUSULA DÉCIMA TERCEIRA – DA INTEGRALIDADE DO TERMO

- 13.1 Este instrumento contratual, em conjunto com o Edital, Termo de Referência, Proposta Comercial e o Regulamento de Compras e Contratações do CBC, o **CONTRATANTE**, contém todos os termos e condições acordados pelas partes, sendo superveniente em relação a todos os contratos e entendimentos anteriores, sejam eles verbais ou escritos.
- 13.2 A renúncia a qualquer disposição deste instrumento somente terá validade caso seja feita por escrito, admitindo-se, neste caso, apenas interpretação restritiva.



COMITÊ BRASILEIRO
DE CLUBES



14 CLÁUSULA DÉCIMA QUARTA – DAS COMUNICAÇÕES

- 14.1 Toda e qualquer comunicação entre as partes, relativa ao presente CONTRATO, deverá ser feita por escrito e encaminhada da forma a seguir:

CONTRATANTE

Rua Açai, 566, Bairro das Palmeiras - CEP 13.092-587 - Campinas - S.P.

Tel. nº (19) 3381-3005; e-mail: compras@cbclubes.org.br A/C: Departamento de Compras

CONTRATADA

Rua Boa Vista, nº 254, Conj. 1714 - CEP 01014-000 - São Paulo - SP

Tel. nº (11) 3105-8655; e-mail: adiniz@alertasecurity.com.br; A/C: Sr. Antonio Lino Diniz

- 14.2 As comunicações ou notificações de uma parte a outra, relacionadas com este CONTRATO, serão consideradas efetivadas se:

- a) entregues pessoalmente, contra recibo;
- b) enviadas por carta registrada, com aviso de recepção, ou
- c) enviada por meio eletrônico, desde que comprovado o recebimento pelo CBC;

- 14.2.1 Qualquer alteração nos dados informados nesta cláusula deverá ser informada por escrito à outra parte no prazo máximo de 10 (dez) dias, a contar da sua ocorrência.

15 CLÁUSULA DÉCIMA QUINTA – DA CONFIDENCIALIDADE

- 15.1 A **CONTRATADA**, por si, seus empregados, prepostos, agentes ou representantes, obriga-se a manter em absoluto sigilo sobre as operações, dados, materiais, informações, documentos, especificações comerciais do **CONTRATANTE**, inclusive quaisquer programas, rotinas ou arquivos a que eventualmente tenham ciência ou acesso, ou que lhe venham a ser confiados por qualquer razão.

- 15.2 A **CONTRATADA** se compromete, incondicionalmente, a:

- a) não usar, comercializar, reproduzir ou dar ciência a terceiros, de forma omissa ou mesmo comissivamente, das informações acima referidas;
- b) responder solidariamente, civil e criminalmente, com os seus sócios e/ou administradores, por si, seus funcionários e/ou prepostos, contratados e consultores, pela eventual quebra de sigilo das informações que tenha eventual acesso ou ciência, direta ou indiretamente em qualquer fase da execução do objeto contratado bem como a qualquer tempo após sua conclusão.



COMITÊ BRASILEIRO
DE CLUBES



16 CLÁUSULA DÉCIMA SEXTA – DAS DISPOSIÇÕES GERAIS

- 16.1 Toda e qualquer tolerância quanto ao descumprimento, ou cumprimento irregular, pelas Partes, das condições estabelecidas neste Contrato não significará alteração das disposições pactuadas, mas, tão somente, mera liberalidade.
- 16.2 A CONTRATADA não poderá utilizar o nome e/ou qualquer imagem do CONTRATANTE, sem autorização expressa e por escrito para tanto.
- 16.3 O extrato do presente Contrato será publicado no Site do CBC, no prazo previsto no RCC do CBC.

17 CLÁUSULA DÉCIMA SÉTIMA – DA REPARAÇÃO DOS DANOS

- 17.1 A **CONTRATADA** é responsável direta pela execução do objeto deste contrato e, conseqüentemente, responde, exclusivamente, por danos que, por dolo ou culpa, eventualmente, causar ao **CONTRATANTE**, aos seus funcionários, à coisa ou propriedade de terceiros, em decorrência deste Contrato, correndo as suas expensas os ressarcimentos e indenizações devidos.

18 CLÁUSULA DÉCIMA OITAVA – DA LEGISLAÇÃO APLICÁVEL

- 18.1 A execução deste Contrato será disciplinada pela lei brasileira, pelas Normas do REGULAMENTO DE COMPRAS E CONTRATAÇÕES do CONTRATANTE, o RCC do CBC, sendo regulada por cláusulas e Princípios Gerais da Administração Pública, aplicando-se lhe, supletivamente, os princípios de teoria geral dos contratos e as disposições de direito privado.
- 18.2 Os casos omissos serão resolvidos com base no RCC do CBC.

19 CLÁUSULA DÉCIMA NONA – DA DOTAÇÃO ORÇAMENTÁRIA

- 19.1 As despesas decorrentes da execução deste Contrato correrão à conta de recursos destinados as despesas administrativas, de acordo com a Lei nº 9.615/98.

20 CLÁUSULA VIGÉSIMA – DA FISCALIZAÇÃO

- 20.1 A Fiscalização deste contrato será exercida pelo Departamento de Tecnologia da Informação, do **CONTRATANTE**, na sede em Campinas, SP, especificamente pelo Sr. Adolpho Pires Bognar, ao qual incumbirá acompanhar a execução do contrato, anotando as infrações contratuais constatadas.
- 20.2 A Fiscalização deverá:
- 20.2.1 Atestar a(s) faturas/nota(s) fiscal(is) apondo o seu "aceite" e vistar os demais documentos apresentados pela **CONTRATADA**.

**CBC****COMITÊ BRASILEIRO
DE CLUBES**

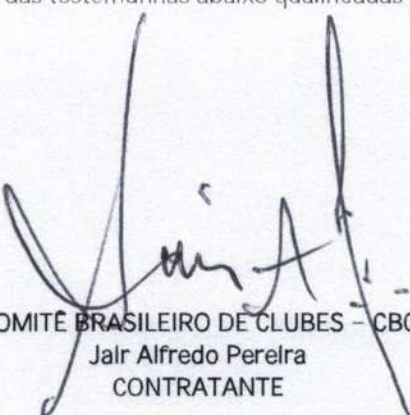
20.2.2 O Departamento responsável pela fiscalização referida anotará, em registro próprio, todas as ocorrências relacionadas com a execução do Contrato, determinando o que for necessário a regularização das faltas ou defeitos observados.

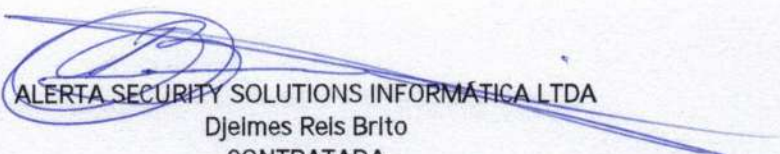
21 CLÁUSULA VIGÉSIMA PRIMEIRA – DO FORO

21.1 As partes estabelecem que o Foro eleito para dirimir quaisquer dúvidas oriundas do presente CONTRATO é o da comarca de Campinas, renunciando as partes a qualquer outro, por mais privilegiado que seja.

E assim, por estarem as partes justas e contratadas, assinam o presente instrumento em 02 (duas) vias de igual forma e teor, na presença das testemunhas abaixo qualificadas para os devidos fins de direito.

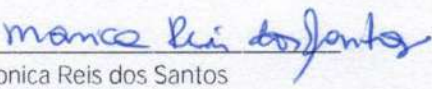
Campinas, 23 de janeiro de 2018.


COMITÊ BRASILEIRO DE CLUBES – CBC
Jair Alfredo Perelra
CONTRATANTE


ALERTA SECURITY SOLUTIONS INFORMÁTICA LTDA
Djelmes Reis Brito
CONTRATADA

Testemunhas:

1. 
Edilson Novais de Souza
RG nº 22.068.302-5 SSP/SP

2. 
Monica Reis dos Santos
RG nº 29.970.734-9

ANEXO I

ANEXO I - TERMO DE REFERÊNCIA

PREGÃO PRESENCIAL N° NLP-017/2017

1 OBJETO

- 1.1 O objeto do presente Termo de Referência consiste na aquisição de Solução de Firewall de Aplicação, compreendendo hardware e software (appliance), serviços de instalação e configuração, garantia, suporte técnico e treinamentos, destinados atender as unidades do CBC em Campinas/SP e Brasília/DF, conforme especificações e condições a seguir estabelecidas.
- 1.2 A solução de firewall descrita neste documento, destina-se a proteger as informações disponíveis na rede de dados do CBC, sendo necessário instalar dois equipamentos de firewalls após os links de internet, funcionando em modo ativo/passivo, onde poderemos através de uma política de segurança controlar o fluxo de entrada e saída de informações e do grau de segurança desejado. Também com a necessidade de integrar as redes da sede e sub sede do CBC (Campinas e Brasília) sendo que, após a contratação desse equipamento, será configurado o serviço de VPN (Rede Virtual Privada) entre as redes, permitindo que o tráfego de dados seja realizado de forma segura, possibilitando o acesso a rede interna da empresa mesmo quando o funcionário estiver trabalhando externamente.
- 1.3 Em síntese, os principais benefícios esperados com a implantação da solução de firewall, objeto deste Termo de Referência são:
 - Garantir acesso aos colaboradores, provendo interligação através de qualquer conexão internet de forma segura;
 - Prover as funcionalidades de VPN (Rede Virtual Privada);
 - Atender às boas práticas, recomendações e normas internacionais de segurança para acessos remotos;
 - Permitir o uso de tecnologia de ponta, conferindo produtividade ao trabalho dos usuários dos serviços de conectividade e de rede corporativa;
 - Permitir o crescimento modular, dando ao CBC a possibilidade de escalabilidade ao longo do tempo.
 - Manter a segurança das informações em trânsito na rede corporativa;
 - Aperfeiçoamento da gestão dos serviços de TI, através da implantação de aplicativos;
 - Permitir atuação proativa e preventiva na identificação, diagnóstico e resolução de falhas e indisponibilidade;
 - Gerenciamento, controle e auditoria do conteúdo navegado na internet pelos usuários;

2 CRITÉRIO DE ADJUDICAÇÃO

- 2.1 O objeto do presente processo de contratação será adjudicado por lote. As empresas participantes poderão apresentar proposta de preços para qualquer um dos lotes estabelecidos, ou para ambos os lotes.

3 DA PROPOSTA DE PREÇOS

- 3.1 A empresa participante deverá elaborar Proposta de Preços no modelo disponibilizado pelo CBC – Anexo II, utilizando como base a quantidade de equipamentos e serviços estabelecidos no presente Termo de Referência.
- 3.2 No julgamento das propostas considerar-se-á o critério do menor preço total de cada lote ofertado, para o fornecimento do objeto deste Termo de Referência.
- 3.3 No preço dos produtos ofertados pela empresa participante deverão estar inclusos todos encargos trabalhistas, previdenciários, fiscais, comerciais, de transportes e seguro, inclusive aqueles relativos a tributos, impostos e taxas, bem como despesas e obrigações financeiras de qualquer natureza, além de despesas operacionais com frete e entrega nos locais estabelecidos neste Termo de Referência

4 REQUISITOS BÁSICOS PARA O FIREWALL

4.1 RELAÇÃO DE LOTES

Abaixo, segue a relação dos LOTES a serem contratados com as suas respectivas quantidades de aquisição:

LOTE 01 (SEDE – CAMPINAS)	
DESCRIÇÃO	QTDE.
Solução de firewall de aplicação para no mínimo 100 usuários, composta por 01 (um) appliances físico (Ativo), fornecendo alta disponibilidade e gerenciamento centralizado, serviços de instalação e configuração, garantia e suporte técnico. Item 05, item 06, item 07 deste Termo de Referência.	01
Solução de firewall de aplicação para no mínimo 100 usuários, composta por 01 (um) appliances físico de contingência (Passivo), serviços de instalação e configuração, garantia e suporte técnico. Item 05, item 06, item 07 deste Termo de Referência.	01
Serviço de treinamento (02 pessoas) - conforme item 08 deste Termo de Referência	01

LOTE 2 (SUB SEDE – BRASÍLIA)	
DESCRIÇÃO	QTDE.
Solução de firewall de aplicação para no mínimo 100 usuários, composta por 01 (um) appliances físico (Ativo), fornecendo alta disponibilidade e gerenciamento centralizado, serviços de instalação e configuração, garantia e suporte técnico. Item 05, item 06, item 07 deste Termo de Referência.	01
Solução de firewall de aplicação para no mínimo 100 usuários, composta por 01 (um) appliances físico de contingência (Passivo), serviços de instalação e configuração, garantia e suporte técnico. Item 05, item 06, item 07 deste Termo de Referência.	01
Serviço de treinamento (02 pessoas) - conforme item 08 deste Termo de Referência	01

5 ESPECIFICAÇÕES TÉCNICAS

5.1 DISPOSIÇÕES GERAIS

- 5.1.1 Fazem parte da presente especificação, no que forem aplicáveis, as normas dos fabricantes, bem como as normas pertinentes da Associação Brasileira de Normas Técnicas (ABNT). Os equipamentos e serviços deverão atender obrigatoriamente a presente especificação, sendo que qualquer solicitação de modificação assim como qualquer esclarecimento adicional sobre os equipamentos/serviços a serem executados, objeto da presente especificação deverá ser feita, por escrito e fundamentada, para análise por parte da equipe do CBC (Comitê Brasileiro de Clubes);
- 5.1.2 Todos os equipamentos a serem fornecidos devem ser necessariamente novos, e os firewalls deverão ser a última versão lançada pelo fabricante;
- 5.1.3 O sistema operacional deverá ser homologado pelo fabricante do equipamento e na última versão disponível;
- 5.1.4 A solução deverá ser provida com 2 (dois) equipamentos por localidade, do tipo appliance, com função de firewall de aplicação (WAF – Web Application Firewall), para serem instalados em rack padrão 19”;
- 5.1.5 Fonte de alimentação com operação automática entre 110 e 220 v;
- 5.1.6 Implementar alta disponibilidade com tolerância a falhas, sendo admitidas as configurações ativo-ativo ou ativo-passivo;

5.2 ESPECIFICAÇÕES TÉCNICAS DO FIREWALL

- 5.2.1 Dispositivo de sistema de segurança de informação perimetral que inclui firewall, administração de largura de banda de serviço de internet (QoS), suporte para conexões VPN IPSec e SSL, proteção contra ameaças de vírus e malware, bem como controle de transmissão de dados e acesso a internet;
- 5.2.2 Deverá incluir um módulo de proteção contra ameaças de rede, bloqueio de vírus, spyware, controle de transferência de arquivos, controle da navegação de internet e bloqueio de arquivos por tipo;
- 5.2.3 Deverá incluir licenças para no mínimo 100 (cem) usuários para as funcionalidades de controle de ameaças, controle de vírus, spyware e filtro de URL;
- 5.2.4 A solução deve ser ofertada em Appliance/hardware específico para o propósito solicitado, não sendo aceitas soluções baseadas em servidores abertos;
- 5.2.5 A solução deve utilizar sistema operacional próprio “hardenizado”, não sendo aceitos sistemas operacionais Linux ou baseados em distribuições abertas;
- 5.2.6 Deverá suportar redes virtuais, vlans 802.1q;
- 5.2.7 Deverá suportar tradução de endereços da rede (NAT) por origem e destino, por endereços IP dinâmicos e pool de portas;
- 5.2.8 Deverá suportar PPPoE, BGP, OSPF e RIP2, DHCP server e DHCP relay;
- 5.2.9 Deverá suportar os protocolos de criptografia IKE, 3DES, AES (com chaves de 128, 192 e 256 bits), SHA1 e MD5;
- 5.2.10 Deverá suportar pelos menos os seguintes protocolos de VOIP: H.323, SIP, SCCP e MGCP;
- 5.2.11 Deverá suportar a detecção de aplicações dinâmicas dentro de sessões de proxy HTTP;
- 5.2.12 Deverá suportar o controle de tráfego IPv4 e IPv6, este último inclui visibilidade e inspeção de ameaças em aplicações e controle de conteúdo;
- 5.2.13 O fornecedor deverá descrever os controles suportados na política de acesso (zonas de segurança, usuários, IP, aplicações, agendamentos, etc.).

5.2.14 REQUERIMENTOS DE HARDWARE E DESEMPENHO

- 5.2.14.1 O equipamento deve possuir no mínimo 8 (oito) interfaces 10/100/1000 Copper Ethernet;
- 5.2.14.2 O equipamento deve possuir interface “Out-Of-Band” dedicada para gerenciamento;
- 5.2.14.3 Suportar pelo menos 500 Mbps de throughput para Firewall;
- 5.2.14.4 Suportar pelo menos 500 Mbps de throughput para controle de aplicações;

- 5.2.14.5 Suportar pelo menos 300 Mbps de throughput para controle de antivírus e antispware;
- 5.2.14.6 Suportar pelo menos 500 Mbps de throughput de IPS;
- 5.2.14.7 Suportar pelo menos 500 Mbps de throughput para VPN IPSec;
- 5.2.14.8 Suportar pelo menos 200 Mbps de throughput para as funcionalidades de firewall, controle de aplicações, IPS, antivírus e antispware habilitados simultaneamente;
- 5.2.14.9 Deve suportar pelo menos 64.000 sessões concorrentes;
- 5.2.14.10 Deve suportar pelo menos 7.000 novas sessões por segundo;
- 5.2.14.11 Deve suportar pelo menos 25 interfaces túnel de VPN IPSec;
- 5.2.14.12 Suportar pelo menos 50 usuários concorrentes de SSL VPN.
- 5.2.15 IDENTIFICAÇÃO, CONTROLE E VISIBILIDADE, SENDO:
 - 5.2.15.1 Identificação e controle para o uso de aplicações por usuário mediante interação com servidores LDAP, Active Directory ou Radius e endereço IP;
 - 5.2.15.2 Identificação deve ser de modo independente à porta lógica e/ou aplicações que utilizam as portas 80 e 443;
 - 5.2.15.3 Visibilidade de aplicações incluindo peer-to-peer, facebook, twitter e web 2.0;
 - 5.2.15.4 Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam métodos de ocultamento via comunicações cifradas, tais como Ultrasurf, Skype e ataques mediante a porta 443;
 - 5.2.15.5 Em caso de protocolos desconhecidos, poderão designar-se assinaturas próprias;
 - 5.2.15.6 Deverá suportar descrição e controle de tráfego SSHv2.
- 5.2.16 CONTROLES POR POLÍTICAS DE FIREWALL
 - 5.2.16.1 Deverá suportar controles por zona de segurança;
 - 5.2.16.2 Controle de políticas por porta e protocolo;
 - 5.2.16.3 Controle de políticas por aplicações e categorias de aplicações;
 - 5.2.16.4 Controle de políticas por usuários, grupos de usuários, endereços IP, redes e zonas de segurança;
 - 5.2.16.5 Controle de inspeção e deciframento do protocolo SSL por política para tráfego de entrada (Inbound) e Saida (Outbound);
 - 5.2.16.6 Controle de inspeção e deciframento do protocolo SSH por política;

- 5.2.16.7 Deverá suportar o bloqueio dos seguintes tipos de arquivos: bat, cab, dll, exe, pif, e reg;
- 5.2.16.8 Deverá suportar aplicação de QoS baseado em políticas para prioridade, garantia de banda e banda máxima;
- 5.2.16.9 Deverá suportar QoS baseado em políticas para marcação de pacotes (diffserv marking);
- 5.2.16.10 Deverá suportar objetos e regras IPV6;
- 5.2.16.11 Deverá suportar objetos e regras multicast;
- 5.2.16.12 Deverá suportar a atribuição de agendamento as políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.
- 5.2.17 **CONTROLE DE APLICAÇÕES**
 - 5.2.17.1 Deverá contar com ferramentas de visibilidade que permitam administrar o tráfego de aplicações, permitindo a execução de aplicações autorizadas e bloqueio de aplicações não autorizadas;
 - 5.2.17.2 O controle de aplicações deve identifica-las independente das portas e protocolos, bem como de técnicas de evasão utilizadas;
 - 5.2.17.3 O fornecedor deverá descrever as técnicas utilizadas pela solução para a detecção das aplicações (Assinaturas, Porta/Protocolo, heurística, etc.) e se as mesmas são baseadas em inspeção IPS ou inspeção profunda de pacotes (Deep Packet Inspection);
 - 5.2.17.4 Deverá suportar múltiplos métodos de identificação e classificação das aplicações.
 - 5.2.17.5 Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;
 - 5.2.17.6 Deverá suportar a criação de aplicações customizadas pela interface gráfica do produto;
 - 5.2.17.7 Deverá incluir a capacidade de atualização para identificar novas aplicações;
 - 5.2.17.8 Deverá atualizar a base de assinaturas de aplicações automaticamente, durante o período de suporte/garantia contratado;
 - 5.2.17.9 O fabricante deve permitir a solicitação de inclusão de aplicações na base padrão de assinaturas;
 - 5.2.17.10 Deverá alertar o usuário quando uma aplicação for bloqueada;
 - 5.2.17.11 Deverá possibilitar que o controle de portas seja aplicado para todas as aplicações;
 - 5.2.17.12 Deverá possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, neonet, etc.) possuindo granularidade de controle/políticas para os mesmos;
 - 5.2.17.13 Deverá possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, YIM, Facebook Chat, etc.) possuindo granularidade de controle/políticas para os mesmos;

- 5.2.17.14 Deverá possibilitar a diferenciação e controle de partes das aplicações como, por exemplo, permitir o chat e bloquear a transferência de arquivos;
- 5.2.17.15 Deverá possibilitar a diferenciação de aplicações Proxies (ultrasurf, ghostsurf, freegate, etc.) possuindo granularidade de controle/políticas para os mesmos;
- 5.2.17.16 Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, Edirectory e base de dados local;
- 5.2.17.17 Deverá incluir a capacidade de criação de políticas baseadas no controle por aplicação, categoria de aplicação, subcategoria, tecnologia e fator de risco;
- 5.2.17.18 Deverá incluir a capacidade de criação de políticas baseadas no controle por usuário, grupos de usuários ou endereço IP;
- 5.2.17.19 Deverá incluir a capacidade de criação de políticas baseadas em “traffic shaping” por aplicação, usuário, origem, destino, túnel vpnipsec-ssl;
- 5.2.17.20 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);
- 5.2.17.21 Deverá suportar autenticação Kerberos;
- 5.2.17.22 Deverá possuir suporte a identificação de usuários em ambiente Citrix e Microsoft terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços.

5.2.18 PREVENÇÃO DE AMEAÇAS

5.2.18.1 IPS

- 5.2.18.1.1 Para proteção do ambiente contra-ataques, deve ser incluído modulo de IPS integrado na própria ferramenta de Firewall ou entregue com composição com outro fabricante;
- 5.2.18.1.2 Deverá suportar granularidade nas políticas de IPS, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
- 5.2.18.1.3 Deverá possibilitar a criação de diferentes perfis de IPS a serem aplicados por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
- 5.2.18.1.4 Deverá permitir o bloqueio de vulnerabilidades;
- 5.2.18.1.5 Deverá permitir o bloqueio de exploits conhecidos;
- 5.2.18.1.6 Deverá incluir proteção contra ataques de negação de serviços;

5.2.18.1.7 Deverá possuir os seguintes mecanismos de inspeção de IPS:

5.2.18.1.7.1 Análise de padrões de estado de conexões;

5.2.18.1.7.2 Análise de decodificação de protocolo;

5.2.18.1.7.3 Análise para detecção de anomalias de protocolo;

5.2.18.1.7.4 Análise heurística;

5.2.18.1.7.5 IP Defragmentation;

5.2.18.1.7.6 Remontagem de pacotes de TCP;

5.2.18.1.7.7 Bloqueio de pacotes malformados;

5.2.18.1.8 Deverá possuir assinaturas para bloqueio de ataques "buffer overflow";

5.2.18.1.9 Deverá possuir assinaturas para auxílio no bloqueio de ataques DoS/DDoS;

5.2.18.1.10 Deverá suportar o reconhecimento de ataques em tráfego IPv6;

5.2.18.1.11 Deverá possuir assinaturas e mecanismos de detecção de anomalias prontas;

5.2.18.1.12 Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

5.2.18.1.13 Deverá ser possível a criação de exceções/exclusões por hosts para determinadas assinaturas;

5.2.18.1.14 Deverá suportar referência cruzada com CVE (Common Vulnerabilities and Exposures);

5.2.18.1.15 Deverá possuir granularidade de ajustes com opções para sobrescrever assinaturas individualmente;

5.2.18.1.16 Deverá suportar atualização automática das assinaturas através de conexão segura;

5.2.18.1.17 Todos os modelos de equipamentos devem utilizar as mesmas assinaturas;

5.2.18.1.18 Deverá suportar várias técnicas de prevenção, incluindo Drop e TCP-RST (Cliente, Servidor e ambos);

5.2.18.1.19 Deverá suportar ações por assinaturas;

5.2.18.1.20 Suportar notificações e alertas via e-mail, SNMP traps e log de pacotes.

5.2.18.2 ANTIVÍRUS / ANTI-SPYWARE

5.2.18.2.1 Para proteção do ambiente contra malware conhecido, deve ser incluído módulo de antivírus e antispysware de gateway integrado na própria ferramenta de Firewall ou entregue com composição com outro fabricante;

- 5.2.18.2.2 Deverá permitir o bloqueio de malwares e spywares;
- 5.2.18.2.3 Deverá ser possível a inspeção de antivírus para pelo menos nos seguintes tipos de tráfegos: HTTP, SMTP, POP3, IMAP e SMB;
- 5.2.18.2.4 Deverá incluir proteção contra vírus, spyware e worms em conteúdo HTML e javascript;
- 5.2.18.2.5 Proteção contra downloads involuntários de arquivos executáveis maliciosos usando HTTP;
- 5.2.18.2.6 Rastreamento de vírus em arquivos pdf;
- 5.2.18.2.7 Deverá realizar a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.);
- 5.2.18.2.8 Deverá suportar bloqueio de arquivos por tipo (pelo menos 50 tipos);
- 5.2.18.2.9 A atualização de assinaturas deverá ser diária, semanal e de emergência;
- 5.2.18.2.10 Deve suportar atualização automática das assinaturas através de conexão segura, até no mínimo o limite do suporte/garantia contratado;
- 5.2.18.2.11 As atualizações de ameaças, antivírus e antispymware não devem depender de reboot do equipamento para efetivação;
- 5.2.18.2.12 Todos os modelos de equipamentos devem utilizar as mesmas assinaturas;
- 5.2.18.2.13 Suportar notificações e alertas via e-mail, SNMP traps e log de pacotes.
- 5.2.18.3 **ANÁLISE DE MALWARE "IN CLOUD"**
 - 5.2.18.3.1 Devido aos malwares hoje em dia serem muito dinâmicos e um antivírus comum reativo não ser capaz de detectar os mesmos com a mesma velocidade que suas variações são criadas, a solução ofertada deve possuir funcionalidades para análise de malwares não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante;
 - 5.2.18.3.2 Para ameaças/malwares não conhecidos, o produto deve ser capaz de enviar o arquivo para análise automática "In Cloud" ou analisa-lo localmente. Onde o arquivo será executado e simulado em ambiente controlado.
 - 5.2.18.3.3 Esse sistema automático de análise "InCloud" deve prover:
 - 5.2.18.3.3.1 Informações sobre as ações do malware na máquina infectada;
 - 5.2.18.3.3.2 Informações sobre quais aplicações são utilizadas para causar/propagar a infecção;
 - 5.2.18.3.3.3 Detectar aplicações não confiáveis utilizadas pelo malware;
 - 5.2.18.3.3.4 Gerar assinaturas de antivírus e antispymware automaticamente;
 - 5.2.18.3.3.5 Definir URLs não confiáveis utilizadas pelo novo malware.

5.2.19 FILTRO DE URL

- 5.2.19.1 Para maior controle e visibilidades dos acessos dos usuários do ambiente, deve ser incluído módulo de filtro de URL integrado na própria ferramenta de Firewall ou entregue com composição com outro fabricante;
- 5.2.19.2 Deve ser possível a criação de políticas por usuário, grupos de usuários, endereços IP, redes e zonas de segurança;
- 5.2.19.3 Deve ser possível definir horários para o funcionamento da política;
- 5.2.19.4 Deverá incluir a 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, Edirectory e base de dados local;
- 5.2.19.5 Deverá incluir a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
- 5.2.19.6 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);
- 5.2.19.7 Deverá possuir suporte a identificação de usuários em ambiente Citrix e Microsoft Terminal Server, permitindo visibilidade e controle sobre o uso das URLs que estão sendo acessadas através destes serviços;
- 5.2.19.8 Deve possibilitar base de URLs local no Appliance, evitando delay de comunicação/validação da URLs;
- 5.2.19.9 Deverá possibilitar a criação de categorias de URLs customizadas;
- 5.2.19.10 Deverá possibilitar a exclusão de URLs do bloqueio por categoria;
- 5.2.19.11 Deve possibilitar a customização da página de bloqueio;
- 5.2.19.12 Deve possibilitar o bloqueio e continuação, possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e a utilização de um botão "Continuar" para possibilitar o usuário continuar acessando o site;
- 5.2.19.13 Os logs do produto devem incluir informações das atividades dos usuários;
- 5.2.19.14 A atualização da base de dados deve ser automática com a opção de ser feita manualmente via TFTP.

5.2.20 FILTRO DE DADOS

- 5.2.20.1 Deve ser possível a criação de filtros para arquivos e dados pré-definidos;
- 5.2.20.2 Os arquivos devem ser identificados por extensão e assinaturas;

- 5.2.20.3 O firewall deve ser capaz de identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (ex. MS Office, PDF, etc.) identificados sobre aplicações (Ex. P2P, IM, SMB, etc.);
- 5.2.20.4 Deve ser possível a identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 5.2.20.5 O firewall deve ser capaz de identificar e opcionalmente prevenir a transferência de informações sensíveis (Ex. Número de cartão de credito, etc.) possibilitando a criação de novos tipos de dados via expressão regular;
- 5.2.20.6 Listar o número de aplicações suportadas para controle de dados;
- 5.2.20.7 Listar o número de tipos de arquivos suportados para controle de dados.
- 5.2.21 QOS
 - 5.2.21.1 Deverá permitir o controle através de políticas de uso com base nas aplicações: permitir, negar, agendar, inspecionar e controlar o consumo da largura de banda que cada aplicação ou usuário utiliza;
 - 5.2.21.2 Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, ustream, etc.) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicação, deva ter a capacidade de controlá-las por políticas de consumo máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;
 - 5.2.21.3 Suportar a criação de políticas de QoS por:
 - 5.2.21.3.1 Endereço de origem;
 - 5.2.21.3.2 Endereço de destino;
 - 5.2.21.3.3 Por usuário ou grupo do AD;
 - 5.2.21.3.4 Por aplicações (como por exemplo: Skype, Bittorrent, YouTube)
 - 5.2.21.3.5 Por aplicações estaticamente ou grupos dinamicamente (como por exemplo, Instant Messaging ou grupo de aplicações P2P);
 - 5.2.21.3.6 Por porta;
 - 5.2.21.4 O QoS deve possibilitar a definição de classes por:
 - 5.2.21.4.1 Banda Garantida;
 - 5.2.21.4.2 Banda Máxima;
 - 5.2.21.4.3 Fila de Prioridade;

- 5.2.21.5 Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;
- 5.2.21.6 Suportar marcação de pacotes Diffserv;
- 5.2.21.7 Disponibilizar estatísticas em tempo real para as classes de QoS;
- 5.2.21.8 Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.
- 5.2.22 **DECIFRAMENTO SSL / SSH**
 - 5.2.22.1 Deve identificar, decifrar e analisar o tráfego SSL em conexões de saída (Outbound);
 - 5.2.22.2 Deve identificar, decifrar e analisar o tráfego SSL em conexões de entrada (Inbound);
 - 5.2.22.3 Deve identificar, decifrar e analisar o tráfego SSH em conexões de saída (Outbound);
 - 5.2.22.4 Deve identificar, decifrar e analisar o tráfego SSH em conexões de entrada (Inbound);
 - 5.2.22.5 A inspeção de SSL deve permitir a diferenciação de conexões pessoais (Bancos, Shopping, etc.) e tráfegos não pessoais;
 - 5.2.22.6 Deve decifrar o tráfego em todos os tipos de implantação suportadas pelo firewall, como:
 - 5.2.22.6.1 Tap mode ou Mirror/Monitor mode;
 - 5.2.22.6.2 Modo Transparente/Bridge;
 - 5.2.22.6.3 Layer 2;
 - 5.2.22.6.4 Layer 3.
- 5.2.23 **IDENTIFICAÇÃO DE USUÁRIOS**
 - 5.2.23.1 Deverá suportar pelo menos os seguintes serviços de autenticação para identificação de usuários:
 - 5.2.23.1.1 Active Directory;
 - 5.2.23.1.2 LDAP;
 - 5.2.23.1.3 eDirectory;
 - 5.2.23.1.4 RADIUS;
 - 5.2.23.1.5 Kerberos;
 - 5.2.23.1.6 Client Certificate;

- 5.2.23.2 Deverá suportar a criação de políticas baseado em Grupos e Usuários do Active Directory adicionalmente a IP Origem / Destino;
- 5.2.23.3 Deverá possibilitar a identificação de usuários sem a necessidade de instalação de agente individualmente em cada equipamento da rede;
- 5.2.23.4 Deverá suportar a identificação de usuários em ambientes Citrix e Terminal server, assim como a utilização dos mesmos nas políticas de acesso;
- 5.2.23.5 Deverá popular todos os logs de tráfego, IPS, URL, Data, Aplicações entre outros com as informações dos usuários;
- 5.2.23.6 Os logs de identificação de usuários deverão ser feitos em tempo real;
- 5.2.23.7 Deverá possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 5.2.23.8 Deverá possuir integração com RADIUS para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 5.2.23.9 Deverá possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários.
- 5.2.24 **FUNCIONALIDADES DE REDE**
 - 5.2.24.1 Suportar funcionamento em Tap Mode (Via porta espelhada, Tap ou SPAN port);
 - 5.2.24.2 Suportar funcionamento em modo transparente (Bridge ou similar);
 - 5.2.24.3 Suportar funcionamento em Layer 2;
 - 5.2.24.4 Suportar funcionamento em Layer 3;
 - 5.2.24.5 Suportar a implementação simultânea em todos os modos descritos acima (Tap, Transparente, Layer2 e Layer3) no mesmo equipamento;
 - 5.2.24.6 Deve suportar Vlan Tagging (802.1Q) em todos os cenários de implementação acima (Transparente, Layer2 e Layer3);
 - 5.2.24.7 Deve suportar controle de aplicações em IPV6 em todos os cenários de implementação acima (Tap, Transparente, Layer2 e Layer3);
 - 5.2.24.8 Suportar sub-interfaces ethernet logicas.
- 5.2.25 **NAT**
 - 5.2.25.1 Deverá suportar:
 - 5.2.25.1.1 Porta/IP Nat dinâmico (Many-to-1 e Many-to-Many);

5.2.25.1.2 IP Nat dinâmico (Many-to-Many);

5.2.25.1.3 IP Nat estático (1-to-1, Many-to-Many);

5.2.25.1.4 Nat estático bidirecional 1-to-1;

5.2.25.2 IP Virtual (VIP);

5.2.25.3 Tradução de porta (PAT);

5.2.25.4 NAT de Origem;

5.2.25.5 NAT de Destino;

5.2.25.6 Suportar NAT de origem e NAT de destino simultaneamente;

5.2.25.7 Prover capacidade de NAT Traversal, suportando aplicações e serviços VoIP.

5.2.26 VPN

5.2.26.1 Suportar VPN Site-to-Site e Cliente-to-Site;

5.2.26.2 Suportar IPSec VPN;

5.2.26.3 Suportar SSL VPN;

5.2.26.4 Suportar atribuição de endereço IP nos clientes remotos de VPN;

5.2.26.5 Suportar atribuição de DNS nos clientes remotos de VPN;

5.2.26.6 Deverá estar licenciada para no mínimo 100 clientes de VPN simultâneos;

5.2.26.7 IPSec VPN deve suportar:

5.2.26.7.1 3DES, AES (chaves de 128, 192 e 256 bits);

5.2.26.7.2 Autenticação MD5 e SHA-1;

5.2.26.7.3 Diffie-Hellman Group 1, Group 2 e Group 5;

5.2.26.7.4 Algoritmo Internet Key Exchange(IKE);

5.2.26.8 Deve possuir interoperabilidade com os seguintes fabricantes:

5.2.26.8.1 Cisco;

5.2.26.8.2 Checkpoint;

5.2.26.8.3 Juniper;

5.2.26.8.4 Fortinet;

5.2.26.8.5 Sonic Wall;

5.2.26.9 O módulo de VPN IPSec deve suportar pelo menos 25 túneis e ter performance de pelo menos 500 Mbps de throughput;

5.2.26.10 Deverá permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulem dentro dos túneis SSL;

5.2.26.11 Deverá contar com um software cliente de VPN-SSL para os sistemas operacionais Windows XP, Vista (32 e 64 bits), Windows 7 (32 e 64 bits), Windows 8 (32 e 64 bits) e Windows 10;

5.2.26.12 Deverá permitir criar políticas para tráfego VPN-SSL;

5.2.26.13 SSL VPN com suporte a proxy arp e uso de interfaces PPPoE;

5.2.26.14 Deverá suportar pelo menos 50 usuários simultâneos via SSL VPN;

5.2.26.15 Suporte para autenticação de VPNs SSL, LDAP, Secure id e base de dados própria;

5.2.26.16 Capacidade de realizar balanceamento de tráfego em VPNs gateway-to-gateway (com equipamentos do mesmo fabricante), quando utilizado 2 (dois) links de acesso WAN, sem a necessidade de implementação de protocolos de roteamento.

5.2.27 ROTEAMENTO

5.2.27.1 Deve suportar as seguintes funcionalidades de roteamento:

5.2.27.1.1 Estático e Dinâmico;

5.2.27.1.2 RIP v2;

5.2.27.1.3 OSPF;

5.2.27.1.4 BGP v4;

5.2.27.2 Suporte a roteamento IPv6;

5.2.27.3 Suporte a roteadores virtuais (Virtual Routers);

5.2.27.4 Suporte a "Policy Based Forwarding" por:

5.2.27.4.1 Zona de segurança;

5.2.27.4.2 Endereço de origem e destino;

5.2.27.4.3 Porta de origem e destino;

5.2.27.4.4 Aplicação;

5.2.27.4.5 Usuários e/ou Grupos da base AD/LDAP;

5.2.27.4.6 Combinação de todos acima.

5.2.28 ALTA DISPONIBILIDADE

5.2.28.1 Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo:

5.2.28.1.1 Em modo Transparente;

5.2.28.1.2 Em layer 2;

5.2.28.1.3 Em layer 3;

5.2.28.2 O sistema de alta disponibilidade deve sincronizar:

5.2.28.2.1 Todas as sessões;

5.2.28.2.2 Certificados decifrados;

5.2.28.2.3 Todas associações de segurança das VPNs;

5.2.28.2.4 Todas as assinaturas de antivírus, antispymware e aplicações;

5.2.28.2.5 Todas as configurações;

5.2.28.2.6 Tabelas FIB;

5.2.28.3 O sistema de alta disponibilidade deve possibilitar o rastreamento (tracking) de IP;

5.2.28.4 Monitoração de falha de link.

5.2.29 GERENCIAMENTO

5.2.29.1 Deve ser suportado o gerenciamento por:

5.2.29.1.1 CLI via SSH;

5.2.29.1.2 WebUI via HTTPS;

5.2.29.1.3 Console;

5.2.29.1.4 API Aberta;

5.2.29.2 O gerenciamento local do equipamento deve permitir/Possuir:

5.2.29.2.1 Criação e administração de políticas;

5.2.29.2.2 Administração de políticas de IPS, antivírus e antispymware;

5.2.29.2.3 Política de filtro de dados e filtro de URLs;

- 5.2.29.2.4 Monitoração de logs;
- 5.2.29.2.5 Ferramentas de investigação de logs;
- 5.2.29.2.6 Debugging;
- 5.2.29.2.7 Captura de pacotes;
- 5.2.29.3 A solução ofertada deverá suportar gerenciamento centralizado através de solução do mesmo fabricante, possibilitando o gerenciamento de diversos equipamentos;
- 5.2.29.4 Deverá possuir relatórios de utilização dos recursos por aplicações, URL e ameaças;
- 5.2.29.5 Prover uma visualização sumarizada de todas as aplicações, ameaças e URLs que passaram pela solução;
- 5.2.29.6 Deverá possuir mecanismo "Drill-Down" para navegação nos relatórios em tempo real;
- 5.2.29.7 Deverá ser possível identificar o usuário que fez determinado acesso nas opções de "Drill Down";
- 5.2.29.8 Deverá ser possível exportar os logs para formato CSV;
- 5.2.29.9 Deverá ser possível acessar o equipamento e aplicar configurações durante momentos onde o tráfego é muito alto e a CPU e memória do equipamento estiverem totalmente utilizadas;
- 5.2.29.10 Deverá ser possível capturar as URLs acessadas para todas as sessões HTTP;
- 5.2.29.11 Deverá possibilitar a criação de diferentes perfis de administração separando pelo menos: leitura, alterações, relatórios e monitoração;
- 5.2.29.12 Deverá ser possível de forma granular, assinar permissões para os administradores criarem outros usuários, alterarem configurações, ler configurações;
- 5.2.29.13 Deverá ser possível administrar o firewall localmente ou remotamente sem causar problemas de sincronismo de configurações;
- 5.2.29.14 Deverá possuir interface ethernet "Out-of-Band" para gerenciamento via SSH e HTTPS;
- 5.2.29.15 Deverá gerar alertas automáticos, via e-mail, SNMP e Syslogs;
- 5.2.29.16 Deverá suportar o upgrade de software via SCP, TFTP e Web-UI;
- 5.2.29.17 Deverá suportar "rollback" de configuração para a última configuração salva;
- 5.2.29.18 Deverá suportar "rollback" de Sistema Operacional para a última versão local;
- 5.2.29.19 Deverá suportar a validação de regras antes da aplicação;

- 5.2.29.20 Deverá possibilitar o bloqueio da interface para alterações, evitando o conflito de configurações entre administradores quando houver mais de um administrador executando alterações simultaneamente;
- 5.2.29.21 Deverá suportar autenticação de administradores usando base de dados local e RADIUS;
- 5.2.29.22 Deverá suportar a geração de relatórios de atividades do usuário;
- 5.2.29.23 Deverá suportar objetos e políticas compartilhadas;
- 5.2.29.24 Deverá suportar relatórios predefinidos e relatórios projetados pelo usuário (custom), sendo que todos os relatórios deverão poder ser exportados em formatos CSV e PDF.

5.2.30 AUTENTICAÇÃO

- 5.2.30.1 Para autenticação dos administradores da solução deve ser suportado:

- 5.2.30.1.1 LDAP;

- 5.2.30.1.2 RADIUS;

- 5.2.30.1.3 Soluções Baseadas em Token (i.e. Secure-ID);

- 5.2.30.2 Para autenticação de VPN SSL deve ser suportado no mínimo por uma das tecnologias listadas:

- 5.2.30.2.1 LDAP;

- 5.2.30.2.2 RADIUS;

- 5.2.30.2.3 Soluções Baseadas em Token (i.e. Secure-ID);

- 5.2.30.2.4 Kerberos.

5.2.31 CAPTURA DE PACOTES

- 5.2.31.1 Deverá ser possível a captura de pacotes por:

- 5.2.31.1.1 Endereço de Origem;

- 5.2.31.1.2 Endereço de destino;

- 5.2.31.1.3 Aplicações;

- 5.2.31.1.4 Aplicações desconhecidas;

- 5.2.31.1.5 Portas;

- 5.2.31.1.6 IPS;

- 5.2.31.1.7 Antivírus;

5.2.31.1.8 Antispyware;

5.2.31.1.9 Filtro de dados;

5.2.31.1.10 Usuário;

5.2.31.1.11 Qualquer combinação acima.

5.2.32 RELATÓRIOS

5.2.32.1 Deverá incluir a capacidade de proporcionar um resumo gráfico de aplicações utilizadas e ameaças encontradas diariamente;

5.2.32.2 Deverá permitir o controle de transferência de dados não autorizados com ferramenta para realizar padrões definidos por usuário;

5.2.32.3 Deverá contar com a funcionalidade para exportação de logs, captura de tráfego URL e ameaças;

5.2.32.4 Deverá permitir a criação de relatórios personalizáveis;

5.2.32.5 Deverá contar com ferramenta para criar filtros de monitoramento das sessões históricas no firewall seja por aplicação, endereço IP de origem e de destino;

5.2.32.6 Deverá ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado.

5.2.32.7 O equipamento deverá proporcionar os seguintes conjuntos de relatórios:

5.2.32.7.1 Utilização de largura de banda de entrada e saída por aplicação;

5.2.32.7.2 Número de sessões por aplicação;

5.2.32.7.3 Taxa de transferência (em bytes) por aplicação;

5.2.32.7.4 Origem e destino do tráfego por aplicação – Usuário;

5.2.32.7.5 Sessões e E-mail público;

5.2.32.7.6 Utilização de navegação;

5.2.32.7.7 Eventos / Ataques por: origem, categoria, ameaça, protocolo;

5.2.32.7.8 Nível de risco da rede;

5.2.32.7.9 Principais protocolos e aplicações que circulam pelo firewall;

5.2.32.7.10 Principais endereços de IP destino por protocolo;

5.2.32.7.11 Os principais endereços IP para cada um dos protocolos e aplicações principais.

5.2.33 INFORMAÇÕES GERAIS

5.2.33.1 Descrever a forma de licenciamento para cada item abaixo:

5.2.33.1.1 Application Detection;

5.2.33.1.2 IPS;

5.2.33.1.3 Antivirus;

5.2.33.1.4 Antispyware;

5.2.33.1.5 Botnet detection;

5.2.33.1.6 URL-Filtering;

5.2.33.1.7 Data Content Filtering;

5.2.33.1.8 IPSec VPN;

5.2.33.1.9 SSL-VPN;

5.2.33.1.10 Clientes de VPN;

5.2.33.1.11 High Availability;

5.2.33.1.12 QoS (marking and/or traffic shaping);

5.2.33.1.13 SSL Decryption;

5.2.33.1.14 SSH Decryption.

6 SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO DO FIREWALL

6.1 A Contratada deverá apresentar previamente à execução dos serviços de instalação, dentro do prazo de 5 (cinco) dias corridos, a contar da assinatura do contrato, um plano de execução desses serviços, detalhando fases e prazos estimados. O plano deverá conter, ainda, a previsão de eventos que afetem outras instalações do CBC ou interajam com outros equipamentos já em operação;

6.2 O item 4 constante neste Termo de Referência, deverá ser entregue em até 60 (sessenta) dias corridos contados da data da assinatura do contrato;

6.3 Os equipamentos devem ser instalados em par de Ativo/Passivo por localidade. Logo, serão instalados 2 (dois) equipamentos: 01 (um) na Sede Campinas (Ativo/Passivo) e 01 (um) na Sub Sede Brasília (Ativo/Passivo) fornecendo alta disponibilidade em ambas as localidades;

- 6.4 A instalação dos equipamentos deverá ser feita por profissionais devidamente qualificados e certificados pelo fabricante contemplando os itens abaixo:
- 6.4.1 Análise da topologia e arquitetura da rede do CBC, considerando os roteadores e switches de backbone instalados, acesso à Internet, sites remotos, serviços de rede oferecidos aos funcionários do CBC, serviços externos, regras de firewall existentes, bem como qualquer outro equipamento ou sistema relevante na segurança do perímetro, sendo então feitas as configurações gerais do sistema de firewall de acordo com a configuração atual;
 - 6.4.2 Para as regras específicas de usuários e aplicações deverá ser repassado o modo de criação do modelo destas regras, ficando a cargo do CBC o desenvolvimento conforme suas políticas;
 - 6.4.3 Durante toda a implantação do projeto, o técnico da Contratada deverá demonstrar aos técnicos do CBC como instalar e configurar o firewall (instalação assistida);
 - 6.4.4 Todo o processo de instalação e configuração do sistema deverá ser documentado pela Contratada sob a forma de relatório ou roteiro, de forma que os técnicos do CBC possam reproduzir a instalação do firewall quando necessário consultando a documentação;
 - 6.4.5 Após a instalação dos equipamentos, a Contratada deverá entregar ao CBC um inventário com todos os equipamentos e componentes instalados em cada unidade;

7 GARANTIA E SUPORTE TECNICO

- 7.1 Garantia de 36 (trinta e seis) meses com atendimento em até 4 horas a partir da abertura do chamado, podendo o atendimento ser feito remotamente, quando possível e reposição de peças e equipamento em até 72 (setenta e duas) horas. Durante este período, deve ser garantida a atualização de firmware e contato de suporte com telefone com o próprio fabricante/fornecedor do equipamento, em português, durante todo o período de garantia, durante o horário comercial.
- 7.2 Os produtos fornecidos deverão estar cobertos por garantia, compreendendo os defeitos decorrentes de projeto, fabricação, construção, montagem ou acondicionamento, pelo período mínimo especificado, a contar da data do recebimento definitivo dos produtos.
- 7.3 Os serviços de garantia aos produtos deverão ser prestados por empresa credenciada pelo fabricante ou pelo próprio fabricante dos produtos fornecidos.
- 7.4 O fabricante/fornecedor deve possuir estrutura de suporte com atendimento em português do Brasil via chamada telefônica, a cobrar ou 0800;
- 7.5 A empresa deve indicar os procedimentos para abertura de suporte técnico, cabendo a este órgão a abertura do chamado com intermediação da empresa fornecedora dos equipamentos ou diretamente com o fabricante dos equipamentos.
- 7.6 A empresa deve possuir, no fornecimento e prestação de serviço, pelo menos 1 (um) profissional com certificação técnica emitida pelo fabricante do equipamento ofertado, capaz de prestar suporte de primeiro nível aos produtos em garantia, e escalar o suporte ao fabricante conforme necessidade.

- 7.7 A empresa Contratada deverá disponibilizar um portal web 24x7 com sistema de help-desk para abertura de chamados de suporte técnico. Mediante login e senha de acesso ao sistema, os membros da equipe técnica do CBC poderão abrir, gerenciar status e conferir todo o histórico de chamados de suporte técnico.
- 7.8 Todo o chamado aberto deverá ter sua resolução técnica registrada no sistema web de help-desk.
- 7.9 O CBC poderá solicitar o escalonamento de incidentes ao fabricante do equipamento quando se tratarem de correções especiais, defeitos nos programas ou defeito em hardware.
- 7.10 A garantia iniciará sua contagem a partir de aceite registrado na NF dos equipamentos, serviços ou licenças.

8 TREINAMENTO

- 8.1 A capacitação deverá ser realizada no idioma português do Brasil;
- 8.2 É desejável que o material didático utilizado na capacitação esteja no idioma português do Brasil;
- 8.3 O instrutor que ministrará a capacitação da solução deve possuir certificação do fabricante da solução ofertada;
- 8.4 A documentação exigida em relação ao instrutor deverá ser apresentada na assinatura do contrato;
- 8.5 A capacitação deverá abordar no mínimo sobre a instalação, configuração, administração e resolução de problemas da solução ofertada;
- 8.6 A capacitação será realizada na cidade de Campinas, podendo ser nas dependências do CBC;
- 8.7 O licitante vencedor irá capacitar 2 (dois) funcionários do CBC;
- 8.8 A capacitação deverá ser realizada em até 30 (trinta) dias corridos, contados a partir da entrega, instalação e ativação do ambiente, e deverá estar prevista no cronograma de implantação do objeto a ser apresentado pela Contratada ao Fiscal do Contrato do CBC.
- 8.9 Na hipótese de uma só empresa participante arrematar ambos os lotes, o CBC dispensará a futura Contratada de promover dois treinamentos. Nesse caso a Contratada deverá faturar o serviço de treinamento apenas uma vez.

9 DOCUMENTAÇÃO TÉCNICA

- 9.1 A empresa deverá fornecer ao CBC (Comitê Brasileiro de Clubes), uma via da documentação técnica necessária à manutenção e operação dos sistemas;
- 9.2 Toda a documentação técnica fornecida pela empresa deverá ser redigida em língua portuguesa;

- 9.3 A documentação a ser fornecida pelo proponente contratado deve permitir a completa e rápida compreensão de todo o sistema, oferecer plenas condições para sua operação/manutenção e proporcionar total autonomia para repará-lo, alterá-lo e adaptá-lo a diferentes configurações;
- 9.4 A documentação deve abranger todos os equipamentos fornecidos;
- 9.5 Toda a documentação técnica deverá ser entregue em mídia CD-ROM ao CBC.

10 PROPOSTA, PREÇO E CONDIÇÕES DE PAGAMENTO

10.1 A Proposta deverá ser elaborada em papel timbrado, considerando o Modelo de Proposta ANEXO II deste edital:

- Razão Social, nome fantasia, endereço e Nº do CNPJ;
- Nome completo, ASSINATURA de próprio punho, função/cargo;
- local (cidade) e data do Orçamento;
- Valor unitário e total por lote;
- Valor Global da Proposta;
- Prazo de pagamento: 15 (quinze) dias, sendo que será realizado ou no dia 5, ou 15, ou 25.
- Prazo de entrega da Solução: 90 (noventa) dias (observar itens 6.2, 8.8 e 11.1)
- Prazo de validade da Proposta: 60 (sessenta) dias
- Garantia e Suporte Técnico: 36 (trinta e seis) meses (observar item 7)
- Frete: CIF – entregas efetuadas Sede CBC - Campinas/SP e Sub sede CBC - Brasília/DF

11 PERÍODO CONTRATUAL, PRAZO E LOCAL DE ENTREGA

- 11.1 O prazo de entrega do objeto deste Termo de Referência é de 90 (noventa) dias corridos, compreendidos neste prazo a entrega de todos os itens que compõem a solução, a instalação e ativação do ambiente e o treinamento, conforme seus respectivos prazos delineados nos itens 6.2 e 8.8 deste Termo de Referência.
- 11.2 A Solução de Firewalls serão instalados no CBC – Comitê Brasileiro de Clubes, conforme item 6.3 deste Termo de Referência, nos seguintes endereços:

UNIDADE CAMPINAS Rua Açai, 492 Bairro das Palmeiras CEP: 13092-587 Campinas SP	UNIDADE BRASÍLIA SBN Quadra 2, Lote 12, Bloco F Edifício Via Capital, Sala 1503. CEP 70.041-906 Brasília DF
--	---

12 DESPESAS E CUSTOS

- 12.1 Correrão por conta da Contratada todas as despesas com material, instalação, configuração, suporte técnico, gastos com transporte de pessoal ou carga, tarifas telefônicas e de comunicação, bem como todos os encargos trabalhistas, previdenciários, fiscais, tributários e comerciais, prêmios de seguro, taxas e outras despesas de qualquer natureza decorrentes da entrega e disponibilidade dos bens e serviços ora contratados.

13 DAS OBRIGAÇÕES DO CBC

13.1 São obrigações do CBC:

- 13.1.1 Receber os materiais no prazo e condições estabelecidas deste Termo de Referência;
- 13.1.2 Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes deste Termo de Referência e da proposta, para fins de aceitação dos mesmos;
- 13.1.3 Comunicar a Contratada, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido;
- 13.1.4 Acompanhar e fiscalizar, através do Departamento Responsável (Fiscalizador), o cumprimento das obrigações da Contratada;
- 13.1.5 Efetuar pagamento à Contratada no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos neste Termo de Referência;
- 13.1.6 O CBC não responderá por quaisquer compromissos assumidos pela Contratada com terceiros, ainda que vinculados ao fornecimento do material, bem como por qualquer dano causado a terceiros em decorrência de ato da Contratada, de seus empregados, prepostos ou subordinados.

14 DAS OBRIGAÇÕES DA CONTRATADA

14.1 São obrigações da Contratada:

- 14.1.1 A Contratada deve cumprir todas as obrigações constantes neste Termo de Referência, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto e, ainda;
- 14.1.2 Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes neste Termo de Referência, acompanhado da respectiva nota fiscal, na qual constarão as indicações referentes à: marca, fabricante, modelo, procedência e prazo de garantia ou validade;
- 14.1.3 Substituir, reparar ou corrigir, às suas expensas, no prazo fixado neste Termo de Referência, o material com avarias ou defeitos, sem prejuízo da aplicação das penalidades cabíveis, nos termos previstos pelo Regulamento de Compras e Contratações do CBC (IN Nº 2-A, DE 28 DE ABRIL DE 2017);
- 14.1.4 Comunicar ao CBC, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;
- 14.1.5 Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas neste processo de contratação;

14.1.6 Não será admitida a subcontratação de fornecimento dos materiais objeto do presente processo de contratação.



Ao
Comitê Brasileiro de Clubes – CBC
CNPJ nº 00.172.849/0001-42
Referente: Pregão Presencial NLP Nº017/2017

Prezados Senhores,

Apresentamos a V.S.^a, nossa proposta para fornecimento de Solução de Firewall de Aplicação, compreendendo hardware e software (appliance), serviços de instalação e configuração, garantia, suporte técnico e treinamentos, conforme Termo de Referência Técnica e condições comerciais abaixo, sendo:

Lote 1 – Solução destinada à sede do CBC em Campinas – SP

DESCRIÇÃO	QTDE.	PREÇO UNITÁRIO
Solução de firewall de aplicação para no mínimo 100 usuários, composta por 01 (um) appliances físico (Ativo), fornecendo alta disponibilidade e gerenciamento centralizado, serviços de instalação e configuração, garantia e suporte técnico. Item 05, item 06, item 07 do Termo de Referência do CBC.	01	34.415,00
Solução de firewall de aplicação para no mínimo 100 usuários, composta por 01 (um) appliances físico de contingência (Passivo), serviços de instalação e configuração, garantia e suporte técnico. Item 05, item 06, item 07 do Termo de Referência do CBC.	01	25.585,00
Serviço de treinamento (02 pessoas) - conforme item 08 do Termo de Referência do CBC.	01	1.000,00
Valor Total Lote 1		61.000,00

Lote 2 – Solução destinada à sub sede do CBC em Brasília - DF

DESCRIÇÃO	QTDE.	PREÇO UNITÁRIO
Solução de firewall de aplicação para no mínimo 100 usuários, composta por 01 (um) appliances físico (Ativo), fornecendo alta disponibilidade e gerenciamento centralizado, serviços de instalação e configuração, garantia e suporte técnico. Item 05, item 06, item 07 do Termo de Referência do CBC.	01	34.915,00



Solução de firewall de aplicação para no mínimo 100 usuários, composta por 01 (um) appliances físico de contingência (Passivo), serviços de instalação e configuração, garantia e suporte técnico. Item 05, item 06, item 07 do Termo de Referência do CBC.	01	26.085,00
Valor Total Lote 2		61.000,00

Valores, despesas e prazos:

- Valor Global da Proposta: R\$ 122.000,00 (Cento e vinte e dois mil reais)
- Prazo de pagamento: 15 (quinze) dias, sendo que será realizado ou no dia 5, ou 15, ou 25.
- Prazo de entrega da Solução: 90 (noventa) dias (observar itens 6.2, 8.8 e 11.1)
- Prazo de validade da Proposta: 60 (Sessenta) dias
- Garantia e Suporte Técnico: 36 (trinta e seis) meses (observar item 7)
- Frete: CIF – entregas efetuadas Sede CBC - Campinas/SP e Sub sede CBC - Brasília/DF

Banco: 341 – Itaú
Agência: 8499
Conta Corrente: 09236-2

- A) Declaramos que no Valor Global da proposta estão inclusos, todas as despesas relativas aos serviços de instalação, configuração, garantia, suporte técnico e treinamento, respectivamente, itens 06, 07 e 08 do Termo de Referência.
- B) Declaramos, também, que o(s) item(ns) constante(s) desta proposta corresponde(m) exatamente às especificações técnicas descritas no item 05 Termo de Referência, às quais aderimos formalmente.
- C) Declaramos, ainda, que disponibilizaremos equipamentos e pessoal técnico adequados para realização do objeto do presente processo de aquisição.
- D) Em todos os preços cotados estão incluídas todas as despesas que, direta ou indiretamente, fazem parte do presente objeto, tais como impostos, seguros, taxas, ou quaisquer outros que possam incidir sobre gastos da empresa.

Dados da Proponente:

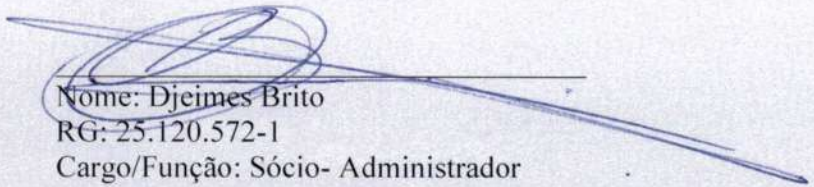
Razão Social: ALERTA SECURITY SOLUTIONS INFORMÁTICA LTDA - CNPJ: 06.946.041-0001/51
Endereço: Rua Boa Vista, 254- Tel./Fax (11) 3105-8655
CEP: 01014-000 Cidade: São Paulo UF: SP

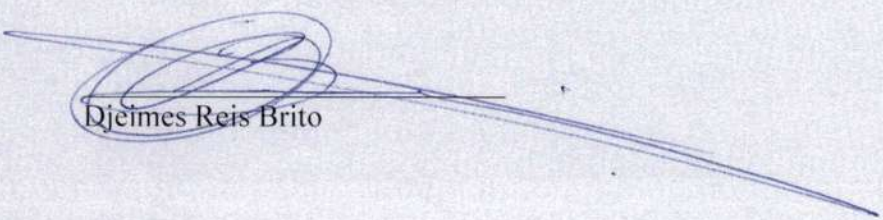


Dados da Proponente:

Razão Social: ALERTA SECURITY SOLUTIONS INFORMÁTICA LTDA - CNPJ: 06.946.041-0001/51
Endereço: Rua Boa Vista, 254- Tel./Fax (11) 3105-8655
CEP: 01014-000 Cidade: São Paulo UF: SP

São Paulo, 10 de Janeiro de 2018


Nome: Djeimes Brito
RG: 25.120.572-1
Cargo/Função: Sócio- Administrador


Djeimes Reis Brito