CBC 248 Folha Rubrica

CONTRATO DE FORNECIMENTO QUE ENTRE SI CELEBRAM O COMITÊ BRASILEIRO DE CLUBES – CBC E A EMPRESA ALLSEC SERVIÇOS EM TECNOLOGIA DA INFORMAÇÃO LTDA.

Aos 13 dias do mês de abril do ano de 2020, o **Comitê Brasileiro de Clubes** – CBC, sediado à Rua Açaí, 566, Bairro das Palmeiras, CEP: 13092-587, em Campinas/SP, CNPJ 00.172.849/0001-42, neste ato representado nos termos do seu Estatuto Social, doravante denominado **CONTRATANTE**, e a empresa **Allsec Serviços em Tecnologia da Informação LTDA**, localizada na Rua Ribeiro de Brito, n° 830, sala 1.901, Boa Viagem, CEP: 51021-310, Recife/PE, CNPJ: 13.497.079/0001-50, neste ato representada pela sócia Francisca Andrea Caminha Cirino, brasileira, casada em regime de comunhão parcial de bens, administradora, portadora da cédula de identidade RG nº 2001002296402 SSP/CE e devidamente inscrita no CPF nº 824.533.063-91, doravante denominada **CONTRATADA**, do objeto do Processo de Contratação NLP 069/2019, têm entre si justo e contratado, nos termos do que determina o REGULAMENTO DE COMPRAS E CONTRATAÇÕES DO COMITÊ BRASILEIRO DE CLUBES – CBC, o que se segue:

CLÁUSULA PRIMEIRA - DO OBJETO

1.1. É objeto do presente contrato o fornecimento de solução integrada de segurança do tipo endpoint protection (antivírus/antimalware/ransomware), incluindo suporte técnico, repasse de conhecimento hands-on, garantia e atualização, conforme descritivo constante no Termo de Especificações Técnicas (anexo I), Termo de Referência (Anexo II) e na Proposta Comercial da **CONTRATADA** (Anexo III), os quais fazem partes integrantes do presente instrumento e obrigará a **CONTRATADA**, nos seus exatos termos, a cumpri-los rigorosamente.

1.1.1. Detalhamento do objeto:

Item	Especificações	Quantidade	Valor Unitário	Valor Total
1	Solução integrada de segurança do tipo endpoint protection (antivirus/antimalware/ransomware), incluindo suporte técnico, repasse de conhecimento hands-on.	105	R$ 90,10	R$ 9.460,50
2	Licenças para servidores com 02 interfaces de administração.	06	R$ 90,00	R$ 540,00
			Valor Total	10.000,50

Allsec Conferido

1.2. O objeto do presente contrato será executado de forma indireta, por empreitada por preço unitário.

CLÁUSULA SEGUNDA: DO VALOR E DO PAGAMENTO

2.1. O **CONTRATANTE** pagará à **CONTRATADA** o valor total de R$ 10.000,50 (dez mil reais e cinquenta centavos).

2.1.1. 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.

2.1.2. 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.

2.1.3. O pagamento será efetuado por meio de ordem bancária de crédito, mediante depósito em conta - corrente, na agência e estabelecimento bancário indicado pela **CONTRATADA**.

2.1.4. A Fatura correspondente será examinada diretamente pelo Fiscal designado pelo **CONTRATANTE**, o qual somente atestará 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 único - 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.

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

2.3. Para efeito do imposto (ISSQN) incidente sobre a nota fiscal, deverão ser consideradas as seguintes condições:

2.3.1. De acordo com a legislação vigente no município da sede do Comitê Brasileiro de Clubes - CBC, a empresa estabelecida fora deste município deverá se cadastrar no CENE, pois caso o cadastro não seja realizado poderá haver a incidência de ISSQN sobre o pagamento a ser realizado à

CBC 250 Folha Rubrica

CONTRATADA. Os casos de não incidência desse imposto serão apreciados nos termos do artigo 2º da Lei Complementar nº 116/2003.

2.4. No caso de constatação de erros ou irregularidades no documento fiscal comprobatório, o prazo de pagamento será interrompido e reiniciará somente após a apresentação de nova documentação, devidamente corrigida.

2.5. Previamente ao pagamento o **CONTRATANTE** poderá realizar consulta aos órgãos competentes para verificação da situação de regularidade da **CONTRATADA**. Constatada qualquer irregularidade, a **CONTRATADA** será comunicada e o pagamento dos serviços prestados, será realizado após a comprovação da regularização.

CLÁUSULA TERCEIRA - DO REAJUSTE

3.1. Os preços contratados são fixos e irreajustáveis.

CLÁUSULA QUARTA - DO SUPORTE TÉCNICO

4.1. O suporte técnico será fornecido pelo fabricante Bitdefender, sendo este, 8x5 direto com a Securisoft, através dos canais de atendimento, telefone: (11) 3018-1855 – Opção 4, Chat: (Atendimento 08h às 18h) https://www.securisoft.com.br/suporte-tecnico-bitdefender e Ferramenta: https://bitdefenderbrasil.octadesk.com/login.

4.2. Os serviços de suporte técnico e manutenção não incluem, em nenhuma hipótese, a reposição de componentes e fornecimento de softwares necessários aos reparos, ajustes ou configurações, que não estão descritos no termo de referência e na proposta comercial. Ocorrendo a necessidade de aquisição de algum componente ou software que não estão descritos nos documentos acima citados, a **CONTRATADA** apresentará a relação dos itens necessários, para atender as necessidades do **CONTRATANTE**, correndo por conta exclusiva deste último, todas as despesas com a referida aquisição.

4.3. Não estão inclusos nos serviços de suporte técnico e manutenção, a instalação de novos dispositivos no ambiente do **CONTRATANTE**, seja este Software ou Hardware. Caso seja solicitado pelo **CONTRATANTE** à **CONTRATADA**, esta apresentará orçamento para execução de novos serviços.

CLAUSULA QUINTA – DAS CONDIÇÕES DE ENTREGA, RECEBIMENTO E ACEITE

5.1. As condições de entrega, recebimento e aceite do objeto do presente instrumento, deverão cumprir as formalidades estabelecidas no item 06 do Termo de Especificações Técnicas (Anexo I).

Allsec Conferido

CBC Folha Rubrica

CLÁUSULA SEXTA – DAS GARANTIAS E ATUALIZAÇÕES

6.1. As garantias e as atualizações das licenças, objeto do presente instrumento tem o prazo determinado de 4 (quatro) anos, a contar da data de recebimento definitivo do Software, bem como do treinamento de seu uso.

CLÁUSULA SÉTIMA – DOS ENCARGOS

7.1. Os encargos trabalhistas, previdenciários, fiscais, comerciais, de seguro, inclusive aqueles relativos a impostos, 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, sendo que sua inadimplência, com relação a tais encargos, não transfere ao **CONTRATANTE** o ônus pelo seu pagamento, não podendo onerar a presente avença.

CLÁUSULA OITAVA – DAS SANÇÕES PARA O CASO DE INADIMPLEMENTO

8.1. O descumprimento das condições técnicas, comerciais ou jurídicas estabelecidas neste CONTRATO e na proposta comercial caracterizará o descumprimento das obrigações assumidas e poderá acarretar à **CONTRATADA** as seguintes penalidades:

I – glosa;

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.

§ 1º - 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 46 e seguintes do RCC do CBC.

§ 2º - Das Multas:

I- No caso de inexecução parcial, fica estabelecida multa de 10% (dez por cento) sobre o valor total do contrato à **CONTRATADA**, quando esta infringir ou deixar de cumprir quaisquer das obrigações ou Cláusulas Contratuais.

II - A inexecução total do ajuste ensejará a aplicação de multa de 20% (vinte por cento) do valor do ajuste.

Allsec Conferido

CBC Folha Rubrica

III - 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.

8.2. O montante da multa poderá ser retido dos valores de pagamentos devidos à **CONTRATADA**, como garantia, independentemente de qualquer notificação, garantida a prévia defesa.

8.3. Independentemente da apuração de responsabilidade e da incidência da multa previstas acima, o **CONTRATANTE** poderá aplicar as demais penalidades previstas no RCC do CBC, em decorrência de inadimplência contratual e, em especial, nas circunstâncias abaixo:

I - inobservância do(s) prazo(s) estabelecido(s);

II - execução do ajuste em desconformidade com o proposto ou em padrão/qualidade inferior à requerida;

III - não cumprimento de obrigações futuras decorrentes da execução do ajustado.

8.4. A critério do **CONTRATANTE**, as sanções previstas na Cláusula 8.1 poderão ser aplicadas isolada ou conjuntamente, facultada a defesa prévia da **CONTRATADA**, no respectivo processo, no prazo de 05 (cinco) dias úteis.

8.5. Aplicar-se-á advertência por faltas leves, assim entendidas como aquelas que não acarretarem prejuízos significativos ao objeto da contratação.

8.6. 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.

8.7. 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.

8.8. 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**.

8.9. Descumprimentos a quaisquer outros itens estabelecidos neste Contrato serão notificados pelo **CONTRATANTE** à **CONTRATADA** com a informação do prazo para a correção do inadimplemento e a gravidade considerada.

CLÁUSULA NONA – DAS OBRIGAÇÕES DA CONTRATADA

9.1. Cumprir todas as obrigações constantes do presente instrumento, bem como nos anexos I, II e III, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto e, ainda:

Allsec Conferido

9.1.1. Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local, acompanhado da respectiva nota fiscal, na qual constarão as indicações referentes a: marca, modelo, procedência e garantia;

9.1.2. Seguir as instruções e observações efetuadas pelo Fiscal do Contrato, bem como reparar, corrigir, remover, reconstruir ou substituir às suas expensas, no todo ou em parte, serviços efetuados em que se verificarem vícios, defeitos ou incorreções;

9.1.3. Substituir, reparar ou corrigir, às suas expensas, no prazo fixado neste instrumento, o produto com avarias ou defeitos, sem prejuízo da aplicação das penalidades cabíveis, nos termos previstos pelo Regulamento de Compras e Contratações (RCC) do CBC;

9.1.4. Comunicar o **CONTRATANTE**, 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;

9.1.5. Utilizar melhores práticas, capacidade técnica, materiais, equipamentos, recursos humanos e supervisão técnica e administrativa, para garantir a qualidade do(s) serviço(s) e o atendimento às especificações contratuais;

9.1.6. Reportar formal e imediatamente ao Fiscal do Contrato quaisquer problemas, anormalidades, erros e irregularidades que possam comprometer a execução do objeto;

9.1.7. Prestar as informações e os esclarecimentos que venham a ser solicitados pelos técnicos do **CONTRATANTE**, referentes a qualquer problema detectado ou ao andamento de atividades previstas;

9.1.8. Detalhar e repassar, conforme orientação e interesse do **CONTRATANTE**, todo o conhecimento técnico utilizado na execução do objeto;

9.1.9. Indicar preposto e cuidar para que esse mantenha permanente contato com o gestor do contrato e adote as providências requeridas, além de comandar, coordenar e controlar a execução do objeto, inclusive os seus profissionais;

9.1.10. Responsabilizar-se integralmente pela sua equipe técnica, primando pela qualidade, desempenho, eficiência e produtividade, visando à execução dos trabalhos durante todo o contrato, dentro dos prazos estipulados, sob pena de ser considerada infração passível de aplicação de penalidades previstas, caso os prazos, indicadores e condições não sejam cumpridos;

9.1.11. Responder integralmente por quaisquer perdas ou danos causados ao **CONTRATANTE** ou a terceiros em razão de ação ou omissão, dolosa ou culposa, sua ou dos seus profissionais em razão da execução do objeto, independentemente de outras cominações contratuais ou legais a que estiver sujeito;

CBC 154 Folha Rubrica

9.1.12. Manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de que tomar conhecimento em razão da execução do objeto do contrato, respeitando todos os critérios de sigilo, segurança e inviolabilidade, aplicáveis aos dados, informações, regras de negócio, documentos, entre outros;

CLÁUSULA DÉCIMA – DAS OBRIGAÇÕES DO CONTRATANTE

10.1. Receber as licenças no prazo e condições estabelecidas no presente instrumento;

10.2. Verificar minuciosamente, no prazo fixado, a conformidade das licenças recebidas provisoriamente com as especificações constantes no presente instrumento e na proposta comercial, para fins de aceitação dos mesmos.

10.3. Comunicar a **CONTRATADA**, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido.

10.4. Acompanhar e fiscalizar, através da Área de Tecnologia da Informação, o cumprimento das obrigações da **CONTRATADA**.

10.5. Efetuar os pagamentos à **CONTRATADA** no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecida na Cláusula Quarta.

10.6. O **CONTRATANTE** 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.

CLÁUSULA DÉCIMA PRIMEIRA – DA VIGÊNCIA

11.1. O presente contrato terá vigência de 60 (sessenta) dias, contados da data de sua assinatura, ou até a emissão do Termo de Recebimento Definitivo relativo à entrega e treinamento, o que ocorrer primeiro, ressalvado o suporte técnico do objeto, que terá a vigência de 48 (quarenta e oito) meses contados a partir da data de emissão do Termo de Recebimento Definitivo relativa à fase de entrega e treinamento, conforme os termos da Proposta de Preços da CONTRATADA.

CLÁUSULA DÉCIMA SEGUNDA – DA RESCISÃO

12.1. Além das hipóteses de inadimplemento previstas, este Contrato poderá ser rescindido à 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 Federal nº 13.756/18, ressalvando-se, apenas, ao direito do recebimento por parte da **CONTRATADA** das prestações vencidas até a data da rescisão;

Allsec Conferido

CBC Folha 135 Rubrica

12.2. O presente contrato também poderá ser rescindido nas hipóteses previstas no Art. 44 do RCC do CBC.

CLÁUSULA DÉCIMA TERCEIRA - DAS DESPESAS

13.1. As despesas decorrentes da execução deste processo de contratação correrão à conta de recursos oriundos da Lei Federal nº 13.756/18.

CLÁUSULA DÉCIMA QUARTA – DA LEGISLAÇÃO APLICÁVEL

14.1. A execução deste Contrato será disciplinada pela legislação 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.

14.2. Os casos omissos serão resolvidos com base no RCC do CBC.

CLÁUSULA DÉCIMA QUINTA – DO FORO

15.1. Fica eleito o Foro da Comarca de Campinas, Estado de São Paulo, para dirimir dúvidas ou controvérsias do presente instrumento contratual que não puderem ser resolvidas administrativamente pelas partes.

E, por estarem, assim as partes justas e contratadas assinam o presente instrumento, em 02 (duas) vias de igual teor e único efeito, na presença das testemunhas abaixo.

Campinas, 13 de abril de 2020.

Comitê Brasileiro de Clubes – CBC
Jair Alfredo Pereira
CONTRATANTE

Allsec Serviços em Tecnologia da Informação Ltda.
Francisca Andrea Caminha Cirino
CONTRATADA

Testemunhas:

Nome: Jose Murilo Cirino Nogueira Junior
CPF: 648.711.503-72

Nome: Edilson Novais de Souza
CPF: 155.817.278-56

TERMO DE REFERÊNCIA

1. DO OBJETO

1.1. O presente Termo de Referência tem por objeto a contratação de solução integrada de segurança do tipo endpoint protection (antivirus/antimalware/ransomware), incluindo suporte técnico, repasse de conhecimento hands-on, garantia e atualização por 36 (trinta e seis) meses, conforme condições, quantidades, exigências e estimativas, estabelecidas neste Termo de Referência e no Anexo I – A – Especificações.

2. DAS OBRIGAÇÕES DO CBC

2.1. São obrigações do CBC:

2.1.1. Receber os produtos no prazo e condições estabelecidos neste Termo de Referência e no Anexo I – A - Especificações;

2.1.2. Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes deste Termo de Referência, do Anexo I – A e da proposta, para fins de aceitação dos mesmos;

2.1.3. Comunicar à empresa Contratada, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido;

2.1.4. Acompanhar e fiscalizar, através do Departamento de Tecnologia da Informação, o cumprimento das obrigações da Contratada;

2.1.5. Efetuar pagamento à Contratada no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos neste Termo de Referência e seus anexos;

2.1.6. 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.

3. DAS OBRIGAÇÕES DA CONTRATADA

3.1. São obrigações da Contratada:

3.1.1. A contratada deve cumprir todas as obrigações constantes deste Termo de Referência e seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto;

3.1.2. Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes deste Termo de Referência e seus anexos, acompanhado da respectiva nota fiscal, na qual constarão as indicações referentes a: marca, fabricante, modelo, procedência e prazo de garantia ou validade;

3.1.3. Substituir, reparar ou corrigir, às suas expensas, no prazo fixado nesteTermo de Referência e seus anexos, o material com avarias ou defeitos, sem prejuízo da aplicação das penalidades cabíveis, nos termos previstos pelo Regulamento de Compras e Contratações do CBC;

3.1.4. Comunicar o 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;

3.1.5. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas neste Termo de Referência e seus anexos, bem como no instrumento convocatório e seus anexos;

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

3.1.7. A empresa participante do processo de contratação deverá comunicar ao CBC a publicação de eventuais pacotes de correções de bugs ou problemas encontrados nos softwares, os quais deverão ser instalados nos equipamentos que fizerem uso das soluções, bem como disponibilizar plataforma para gerenciar os itens adquiridos com base neste Termo de Referência e seus anexos;

3.1.8. Durante o prazo de vigência do contrato, a empresa participante do processo deverá indicar o canal de atendimento por prestar todo o suporte de utilização da solução em sua totalidade, onde será possível a solicitação de informações, auxilio à correção de problemas, abertura de tickets, acompanhamento de todas as solicitações e também plataforma para gerenciar todas as soluções.

3.1.9. Correrão por conta da contratada todas as despesas com material, instalação, mão-de-obra (com base em salário e outros direitos fixados para cada categoria, através de acordo ou convenção coletiva de trabalho, sentença normativa ou outra forma prevista em lei), auxílio-alimentação, auxílio- transporte, gastos com transporte, tarifas telefônicas e de comunicação, bem como todos os encargos trabalhistas, previdenciários, fiscais e comerciais, prêmios de seguro, taxas e outras despesas de qualquer natureza que se fizerem indispensáveis ao bom funcionamento das licenças.

4. LOCAL E PRAZO DE ENTREGAS

4.1. A entrega das licenças, suas mídias e documentação, deverá ser realizada mediante o fornecimento do Grant Number, com indicação do sítio na internet e dos procedimentos necessários,

viabilizando o recebimento através de download no sítio do fornecedor / fabricante, no prazo máximo de 10 (dez) dias úteis, contados, após o recebimento.

4.2. As mídias e documentações complementares que não puderem seguir por meio eletrônico, sem quaisquer acréscimos no preço constante da proposta, deverão ser entregues no mesmo prazo estabelecido acima, no horário das 8:00 às 18:00 horas, devidamente embaladas, de forma a não ser danificadas durante as operações de transporte, no seguinte local:

Comitê Brasileiro de Clubes – CBC

A/C Departamento de Tecnologia da Informação

R. Açaí nº 492 - Bairro das Palmeiras - CEP: 13.092-587 - Campinas/SP

4.3. Juntamente com a liberação da solução, deverá ser entregue o manual de instruções e demais documentos técnicos pertinentes, em mídia digital. O referido manual e documentos técnicos serão considerados parte integrante da solução e não poderão gerar ônus adicional ao CBC.

5. TREINAMENTO

5.1. No preço da solução deverá estar incluso um treinamento para que o administrador do CBC possa fazer a gestão, configuração e administração das licenças. O treinamento deverá ser ministrado para um grupo de até 03 (três) funcionários do Departamento de Tecnologia da Informação do CBC.

5.1.1. Alternativamente, o treinamento de que trata o item anterior, poderá ser ministrado de forma virtual ou até mesmo com a disponibilização de vídeos tutoriais que atendam às necessidades do CBC.

5.2. O prazo para entrega, ativação do objeto e disponibilização do treinamento à equipe do CBC não poderá ser superior a 10 (dez) dias úteis a contar da data de assinatura do contrato, sendo que o CBC ajustará um cronograma de execução destas etapas com a empresa Contratada, a fim de cumprimento do referido prazo.

6. DO RECEBIMENTO DO OBJETO

6.1. O objeto deste Termo de Referência será recebido conforme as condições estabelecidas no item 6 do Anexo I – A – Especificações.

7. CONDIÇÕES DE PAGAMENTO

7.1. O CBC 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, mensalmente, 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 da data do recebimento do documento.

7.1.1. Junto com a Nota Fiscal, para fins de comprovação fiscal, deverão ser entregues mensalmente os seguintes documentos: Certidão Conjunta de Débitos relativos a Tributos Federais e à Dívida Ativa da União e Certificado de Regularidade do FGTS.

7.1.2. As notas fiscais que apresentarem incorreções serão devolvidas à Contratada e seu vencimento ocorrerá no 15° (décimo quinto) dia corrido da data da apresentação da nota devidamente corrigida, observando o critério estabelecido no item 7.1 deste Termo de Referência.

7.2. O pagamento será feito sempre através de transferência bancária diretamente na conta corrente indicada pela empresa Contratada, que acompanhará a nota fiscal ou fatura.

7.2.1. Ocorrendo atraso no pagamento, e desde que para tal não tenha concorrido de alguma forma por culpa do fornecedor, 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.

8. CARACTERÍSTICAS DE ADMINISTRAÇÃO

8.1. A contratada deverá fornecer um console de administração para gerenciamento.

9. DO SUPORTE TÉCNICO

9.1. A Contratada deverá incluir no custo da solução ofertada o suporte técnico necessário a recolocar o produto em seu perfeito estado de uso, funcionamento e desempenho e demais atividades necessárias de acordo com os manuais de manutenção do fabricante e normas técnicas específicas para cada caso;

9.2. O suporte técnico deverá disponibilizar número telefônico, ou e-mail, com atendimento de segunda-feira a sexta-feira, em dias úteis, no horário comercial (8h às 18h), para resolução de incidentes e esclarecimento de dúvidas sobre a solução fornecida, durante toda a vigência do contrato, e contemplando as seguintes características:

9.2.1. Abertura de chamados através de Internet e/ou e-mail, e Central 0800, com atendimento em português e número ilimitado de chamados;

9.2.2. A cada chamado deve ser atribuído um número para acompanhamento e controle;

9.2.3. O atendimento será realizado de forma remota, eventualmente requerendo conexão via internet aos equipamentos do CBC, e deverá sempre ser acompanhado por um técnico do Departamento de Tecnologia da Informação do CBC,

9.2.4. Ao final de cada chamado deverá ser gerado um documento relatando o problema ocorrido e a solução adotada.

9.3. Em problemas detectados nos produtos ofertados considere-se o seguinte:

9.3.1. Caso haja suspensão total no funcionamento das soluções fornecidas, o atendimento e suporte da Contratada deverão iniciar em até 2 (duas) horas úteis

9.3.2. Caso o problema detectado acarrete em suspensão parcial ou degradação das funcionalidades da solução fornecida, o atendimento e suporte da Contratada deverão iniciar em até 4 (quatro) horas uteis.

10. DA VIGÊNCIA

10.1. A vigência do contrato será de **36 (trinta e seis) meses**, contados a partir da assinatura do contrato e renováveis até o limite previsto no Regulamento de Compras e Contratações do CBC.

11. DA DOCUMENTAÇÃO

A presente contratação está condicionada à comprovação, por parte da empresa participante, da regularidade com o FGTS a Fazenda Federal, Fazendas Estadual/Distrital e Municipal, e da comprovação da inexistência de débitos inadimplidos perante a Justiça do Trabalho.

CBC | COMITÊ BRASILEIRO DE CLUBES

CBC Folha Rubrica

ANEXO I – A – ESPECIFICAÇÕES
Aquisição de solução de Antivírus Corporativo

1. DO OBJETO

1.1. Contratação de solução integrada de segurança do tipo endpoint protection (antivirus/antimalware/ransomware), incluindo suporte técnico, repasse de conhecimento hands-on, garantia e atualização por **36 (trinta e seis) meses**, conforme condições, quantidades, exigências e estimativas, estabelecidas neste documento.

2. RESULTADOS A SEREM ALCANÇADOS

2.1. Garantia da prestação dos serviços de antivírus corporativo, garantindo proteção atual e futura às estações de trabalho e servidores físicos de rede, assegurando a sua continuidade e eficácia com qualidade, confiabilidade e disponibilidade.

2.2. Segurança com a disponibilização das atualizações de arquivos de características de vacinas de vírus (.dat), revisões de mecanismos de varredura e versões de software mais atualizados (manutenção de software).

3. JUSTIFICATIVA E OBJETIVO DA CONTRATAÇÃO

3.1. A pretendida contratação faz-se indispensável, pois visa prover segurança, proteção e automação do monitoramento da rede de computadores do Comitê Brasileiro de Clubes - CBC, de forma a minimizar e, em grande parte, coibir a contaminação dos serviços e sistemas informatizados por programas ou atividades digitais maliciosas, contribuindo para a garantia do nível mínimo adequado e desejado de proteção dos dados e informações da entidade.

3.2. É fundamental manter recursos tecnológicos que garantam a segurança dos dados e informações de propriedade ou sob custódia dos diversos departamentos do CBC, haja vista a necessidade precípua de proteção de tais ativos, de grande valor para o CBC, contra os mais diversos tipos de ameaças, conforme estabelecido nas diretrizes da Política de Segurança da Informação.

3.3. A presente contratação tem como objetivo, mitigar o risco de infecção das estações trabalho e servidores por malwares.

CBC Folha Rubrica

3.4. A aquisição da solução de antivírus centralizada permitirá que o Departamento de Tecnologia da Informação, mantenha os níveis exigidos de segurança das informações trafegadas em rede e os controles e políticas necessárias para certificar que tais informações estão sendo acessadas e manipuladas somente por pessoas autorizadas. Tal fato resulta em otimização da infraestrutura de segurança dos dados armazenados na instituição e, também, provê serviços com confidencialidade para as informações trafegadas e armazenadas nas estações de trabalho e nos mais diversos sistemas corporativos.

4. DESCRIÇÃO DA SOLUÇÃO

4.1. Aquisição de ***105 (cento e cinco)*** novas licenças de antivírus para máquinas e ***06 (seis)*** licenças para servidores com 02 interfaces de administração, em sua versão mais atual, com garantia de atualização de versões e suporte técnico por um período de 36 (trinta e seis) meses.

5. DETALHAMENTO DO OBJETO

5.1. Aquisição de Licenças:

5.1.1. A aquisição de licenças tem como objetivo a implantação da solução de antivírus, mantendo-a atualizada e em perfeitas condições de operação e de uso por 36 (trinta e seis) meses.

5.1.2. Deverá ser fornecido um Grant Number (número de identificação) equivalente à aquisição das licenças, que permita fazer o download da solução antivírus completa, assim como de seus upgrades e updates.

5.1.3. A solução de antivírus, objeto de aquisição, deverá ser fornecida na sua versão original, mais atualizada na época de sua entrega.

5.1.4. As licenças de software fornecidas deverão ser perpétuas, ou seja, com prazo indeterminado para o fim de sua vigência, e, com isso, não poderão ser cobrados quaisquer valores adicionais pelo seu uso, durante ou após o término do contrato.

5.1.5. O CBC poderá executar e transferir os produtos licenciados, sem custo adicional, para qualquer plataforma de hardware, sistema operacional ou banco de dados suportados pelo produto.

5.1.6. O CBC, nos casos de alterações na sua estrutura organizacional, poderá incorporar ou transferir os direitos de uso dos produtos licenciados, mediante comunicação à empresa CONTRATADA e providências para os ajustes contratuais necessários.

5.1.7. Todas as licenças e componentes que compõem a solução deverão ser entregues com todos os impostos, taxas e demais custos inerentes ao fabricante e/ou distribuidor da solução, devidamente quitados.

5.1.8. A CONTRATADA deverá se responsabilizar pelo seguinte fornecimento junto com as licenças adquiridas:

5.1.8.1. Manutenção de software por no mínimo 36 (trinta e seis) meses, prevalecendo a garantia do fabricante, caso seja maior, contada a partir da emissão do Termo de Recebimento Definitivo, garantindo atualização de arquivos de características (.dat), revisões de mecanismos de varredura e novas versões de software, devendo as atualizações serem on-line e atualizadas automaticamente;

5.1.8.2. Suporte técnico por no mínimo 36 (trinta e seis) meses, prevalecendo a garantia do fabricante, caso seja maior, contada a partir da emissão do Termo de Recebimento Definitivo, nas modalidade online, dando acesso às soluções da base de dados de conhecimento, vídeos e guias sobre práticas recomendadas, alertas de malware com análise de correção, serviços de análise de malware e ferramentas de diagnóstico, bem como suporte via atendimento telefônico e/ou e-mail, com disponibilidade em regime 8x5, das 8h às 18h, através de ligação gratuita 0800 e/ou internet;

5.1.8.3. Documentação técnica original, preferencialmente em meio eletrônico, completa e atualizada, contendo os manuais e guias de utilização, não sendo aceitas cópias de qualquer tipo.

5.1.8.4. Documentação, preferencialmente em meio eletrônico, com um descritivo completo do processo de implantação de cada produto ofertado, explicações sobre o registro e uso de licenças de software, forma de acesso ao site do fabricante para download da solução antivírus completa, assim como de seus upgrades e updates.

5.1.9. A CONTRATADA ficará obrigada a substituir, às suas expensas, as licenças que forem recusadas, parcial ou totalmente, sendo que o ato do recebimento não importará a sua aceitação.

6. CONDIÇÕES DE ENTREGA, RECEBIMENTO E ACEITE

6.1. A entrega das licenças, suas mídias e documentação, deverá ser realizada mediante o fornecimento do Grant Number, com indicação do sítio na internet e dos procedimentos necessários, viabilizando o recebimento através de download no sítio do fornecedor / fabricante, no prazo máximo de 10 (dez) dias úteis, contados, após o recebimento.

6.2. As mídias e documentações complementares que não puderem seguir por meio eletrônico, sem quaisquer acréscimos no preço constante da proposta, deverão ser entregues no mesmo prazo estabelecido acima, no horário das 8:00 às 18:00 horas, devidamente embaladas, de forma a não ser danificadas durante as operações de transporte, no seguinte local:

Comitê Brasileiro de Clubes – CBC
A/C Departamento de Tecnologia da Informação
R. Açaí nº 492 - Bairro das Palmeiras - CEP: 13.092-587 - Campinas/SP

6.3. Será considerada como recusa formal a falta de entrega das licenças no prazo estabelecido neste Termo de Referência, salvo motivo de força maior ou caso fortuito, devidamente comprovado pelo CONTRATADO e reconhecido por este Comitê.

6.4. O recibo da solução em questão, dar-se-á nas seguintes condições:

6.4.1. **Provisoriamente**, 05 (cinco) dias úteis após ter sido efetuado a entrega, para comprovação da adequação dos softwares à especificação técnica entregues; e

6.4.2. **Definitivamente**, após 15 (quinze) dias úteis contados do recebimento provisório, para a validação do Grant Number, do sítio na internet e dos procedimentos repassados, viabilizando o download no sítio do fornecedor / fabricante e verificação do cumprimento das demais obrigações estabelecidas neste Termo de Referência.

6.5. Se, após o recebimento, constatar-se que os softwares foram entregues em desacordo com a especificação, com defeitos ou incompletos, a CONTRATANTE notificará o CONTRATADO, por escrito, interrompendo-se os prazos de recebimento até a sua regularização.

6.6. Caso o produto não corresponda ao exigido pelo CONTRATANTE, consoante às especificações contidas neste Termo de Referência, o CONTRATADO deverá providenciar sua correção em até 05 (cinco) dias úteis da notificação do CBC, independentemente da aplicação das penalidades cabíveis.

6.7. Não serão aceitas quaisquer alegações da licitante vencedora, com referência a desconhecimento sobre as especificações estabelecidas neste Termo de Referência.

CBC
Folha 265
Rubrica

7. PROPRIEDADE, SIGILO E RESTRIÇÕES

7.1. Todas as informações obtidas ou extraídas pelo CONTRATADO quando da execução dos serviços deverão ser tratadas como confidenciais, sendo vedada qualquer reprodução, utilização ou divulgação a terceiros, devendo o CONTRATADO zelar por si e por seus sócios e profissionais pela manutenção do sigilo absoluto sobre os dados, informações, documentos, especificações técnicas e comerciais de que eventualmente tenham conhecimento ou acesso em razão dos serviços executados.

7.2. O CONTRATADO obriga-se a dar ciência à CONTRATANTE, imediatamente e por escrito, sobre qualquer anormalidade que verificar na prestação dos serviços.

8. ESPECIFICAÇÕES TÉCNICAS

8.1. REQUISITOS COMUNS:

8.1.1. As soluções devem fazer parte do catálogo de produtos comercializados e não ter sido descontinuados;

8.1.2. A solução fornecida não deve estar relacionada em listas "*end of sale*" e "*end of support*" ou similares do site do fabricante;

8.1.3. Permitir a utilização de todas as funcionalidades, tecnologias e recursos especificados neste termo especificados de maneira ininterrupta, irrestrita e sem necessidade de licenciamentos ou ônus adicionais durante o prazo de vigência do contrato.

8.1.4. Todas as licenças referentes aos sistemas operacionais, bancos de dados e softwares componentes da solução adquirida, inclusive os que forem implantados em ambiente virtualizado, devem estar em nome da CONTRATANTE, legalizado, não sendo admitidas versões "*shareware*" ou "*trial*";

8.1.5. A solução deverá ser composta de todos componentes necessários à sua completa instalação, configuração e operação, bem como a respectiva garantia;

8.1.6. Deverão ser fornecidos todas as documentações e manuais técnicos completos necessários à instalação, configuração e operação da solução; A documentação e manuais técnicos deverão estar em Português. Deverão ser fornecidos materiais técnicos e manuais em formato digital que permitam a importação para base de conhecimento online (Microsoft Word, PDF, HTML, etc.);

8.1.7. A solução deverá ter capacidade para operar com todas as instâncias e funções solicitadas neste termo, inclusive com mais de uma capacidade ou função simultaneamente.

8.2. SOLUÇÃO ANTIVÍRUS:

8.2.1. Deve suportar os seguintes requisitos mínimos:

8.2.1.1. Reputação de Arquivos, tanto locais como no acesso web;

8.2.1.2. IPS de Próxima Geração (*Next Generation IPS*);

8.2.1.3. Proteção de Navegadores (*Browser Protection*);

8.2.1.4. Aprendizado de Máquinas (*Machine Learning*);

8.2.1.5. Análise Comportamental (*Behavioral Analysis*);

8.2.1.6. Mitigação da Exploração de Memória (*Memory Exploit Mitigation*);

8.2.1.7. Controle de Aplicações (*Application Control*);

8.2.1.8. Controle de Dispositivos (*Device Control*);

8.2.1.9. Emulação para Malware (*Emulation for Malware*);

8.2.1.10. Mitigação de Exploração de Vulnerabilidades em aplicações conhecidas (*Exploit Mitigation*).

8.2.2. Deve ter a capacidade de implementar a funcionalidade de "*Machine Learning*" utilizando como fonte de aprendizado a rede de inteligência do fabricante, correlacionando no mínimo as seguintes técnicas de proteção com os vetores de ataques, identificando não somente os aspectos maliciosos, como também as características de boa pontuação:

8.2.2.1. Exploração de navegadores com reputação de URL;

8.2.2.2. Websites infectados com reputação de URL;

8.2.2.3. Office Exploits com reputação de URL;

8.2.2.4. Arquivos anexos com reputação de arquivos;

8.2.2.5. Download de arquivos com reputação de arquivos;

8.2.2.6. Instalação de software com as técnicas de SAPE – *Static Attribute Protection Engine*;

8.2.2.7. Instalação de software com as técnicas de Malheur;

8.2.2.8. Cópia de arquivos com as técnicas de SAPE – *Static Attribute Protection Engine*;

8.2.2.9. Cópia de arquivos com as técnicas de Malheur;

8.2.2.10. Execução do instalador de software com classificação comportamental do instalador (boa e ruim);

8.2.2.11. Execução do malware de software com classificação comportamental do instalador (boa e ruim);

8.2.2.12. A funcionalidade de "*Machine Learning*" deve trabalhar baseado no mínimo nas seguintes premissas:

8.2.2.12.1. Atualização da base de reputação das URL's com a periodicidade mínima de 2,5 horas;

8.2.2.12.2. Bloqueio de URL's de má reputação;

8.2.2.12.3. Bloqueio das instruções de "*Command & Control*";

8.2.2.12.4. Atualização da base de reputação de Arquivos com a periodicidade mínima de 2,5 horas;

8.2.2.12.5. Bloqueio das ameaças polimorfas mesmo que arquivos desconhecidos;

8.2.2.12.6. Prevenção de Falso Positivos;

8.2.2.12.7. Bloqueio de malwares desconhecidos e suas variantes;

8.2.2.12.8. Implementar a classificação comportamental dos arquivos;

8.2.2.12.9. "Aprendizado" a partir dos indicadores de compromisso (IOC).

8.2.3. A funcionalidade de "Machine Learning" deve ter a capacidade de implementar uma análise em tempo real correlacionando entre:

8.2.3.1. Veredicto das análises entre usuários da plataforma de segurança do mesmo fabricante;

8.2.3.2. Arquivos de softwares mundialmente espalhados na rede mundial de computadores;

8.2.3.3. Sites Web mundialmente espalhados pela rede mundial de computadores.

8.2.4. A funcionalidade de emulação para malware deve a partir do software de proteção de endpoint, implementar a emulação em um ambiente virtual (local) possibilitando detectar e impedir as técnicas de evasão de detecção, mesmo que utilizando polimorfismo no seu empacotamento;

8.2.5. A funcionalidade de emulação para malware deve ter suporte para as plataformas Windows (32 e 64 bits) e Linux (64 bits);

8.2.6. O software de proteção dos endpoints deve ter a funcionalidade específica de impedir as técnicas de manipulação e randomização de memória impossibilitando a exploração de vulnerabilidades em aplicações, para no mínimo:

8.2.6.1. Adobe PDF;

8.2.6.2. Flash;

8.2.6.3. Java;

8.2.6.4. Navegadores (Internet Explorer, Microsoft Edge, Chrome e Firefox).

8.2.7. O software de proteção do endpoint deve ter a capacidade de impedir os ataques direcionados mesmo que utilizando as vulnerabilidades de dia zero, mitigando no mínimo os conhecidos comportamentos de exploração de vulnerabilidades:

8.2.7.1. SEHOP - *Structured Exception Handler Overwrite Protection*;

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

8.2.7.3. *Java Exploit Protection*.

8.2.8. O software de proteção do endpoint deve ter a capacidade de bloquear exploits que trabalham em nível de "shell code", assim como, implementar a funcionalidade de "virtual patching" para as aplicações;

8.2.9. O software de proteção do endpoint deve ter a capacidade de implementar integração entre a gerência central com plataformas de terceiros, possibilitando no mínimo:

8.2.9.1. Capturas de Login e Logout na Gerência Central;

8.2.9.2. Captura dos detalhes das máquinas protegidas;

8.2.9.3. Captura dos detalhes de Domínios implementados pelo software;

8.2.9.4. Captura dos detalhes de Grupos implementados pelo software;

8.2.9.5. Captura da lista de "*Fingerprint*" de aplicações (*Blacklisting*);

8.2.9.6. Captura da atualização da lista de "*Fingerprint*" de aplicações (Blacklisting);

8.2.9.7. Captura dos detalhes das políticas aplicadas;

8.2.9.8. Captura das atualizações dos detalhes das políticas aplicadas;

8.2.9.9. Captura da lista dos usuários administradores da solução;

8.2.9.10. Criação de novos administradores da solução;

8.2.9.11. Capacidade de mover clientes de endpoints entre grupos lógicos.

8.2.10. O software de proteção do endpoint deve ter a capacidade de receber instruções de comando e ações diretamente do módulo de proteção contra ataques de APT (*Advanced Persistent Threats*), sem a necessidade de interpretação pelo gerenciador do endpoint, possibilitando ações mais rápidas, assertivas e minimizando falsos positivos;

8.2.11. A solução deve ter capacidade de implementar técnicas de EDR (*Endpoint Detection and Response*), possibilitando detecção e investigação nos endpoints com atividades suspeitas;

8.2.12. Deve possuir Console de Gerenciamento Centralizado:

8.2.12.1. O gerenciamento deve estabelecer uma correlação de eventos entre os softwares gerenciados, possibilitando priorização nas ações a serem tomadas;

8.2.12.2. Administração centralizada por console única de gerenciamento acessível através de tecnologia Web HTTPS;

8.2.12.3. As configurações do Antivírus, AntiSpyware, Firewall, Proteção Contra Intrusos, Controle de Dispositivos e Controle de Aplicações deverão ser realizadas para máquinas físicas e virtuais através da mesma console;

8.2.12.4. A solução que será implantada para prestar os serviços deverá funcionar com agente único a ser instalado em estação de trabalho, servidores físicos e virtuais a fim de diminuir o impacto ao usuário final;

8.2.12.5. Deve possuir mecanismo de comunicação (via *push*) em tempo real entre servidor e clientes, para entrega de configurações e assinaturas;

8.2.12.6. Deve possuir mecanismo de comunicação randômico (via *pull*) em tempo determinado pelo administrador entre o cliente e servidor, para consulta de novas configurações e assinaturas evitando sobrecarga de rede e servidor;

8.2.12.7. Permitir a divisão lógica dos computadores, dentro da estrutura de gerenciamento, em sites, domínios e grupos, com administração individualizada por domínio;

8.2.12.8. O servidor de gerenciamento deverá possuir compatibilidade para instalação nos sistemas operacionais Microsoft Windows Server 2008, 2008 R2 ou superior;

8.2.12.9. O servidor de gerenciamento deverá possuir compatibilidade para instalação em sistemas operacionais 32 bits e 64 bits suportando, no mínimo, ambiente virtual VMware e Microsoft Hyper-V;

8.2.12.10. Possuir integração com LDAP, inclusive com o serviço de diretório Microsoft Active Directory, para importação da estrutura organizacional e autenticação dos Administradores;

8.2.12.11. Possibilidade de aplicar regras diferenciadas baseando-se na localidade lógica da rede;

8.2.12.12. Permitir que a localidade lógica da rede seja definida pelo conjunto dos seguintes itens:

8.2.12.12.1. IP e range de IP;

8.2.12.12.2. Endereço de Servidores de DNS, DHCP e WINS;

8.2.12.12.3. Conexão com o servidor de gerência;

8.2.12.12.4. Conexões de rede como VPN, Ethernet e Wireless.

8.2.12.13. Possibilidade de aplicar regras diferenciadas por grupos de usuários e máquinas;

8.2.12.14. Possuir a funcionalidade e recursos para a criação e agendamento periódicos de backups da base de dados ou fornecer uma ferramenta para tal finalidade;

8.2.12.15. Permitir a instalação de Servidores de Gerenciamento adicionais fornecendo assim a possibilidade de trabalhar em modo de Load Balance e Failover;

8.2.12.16. Possuir na solução replicação nativa do Banco de Dados entre os Servidores de Gerenciamento com opção de customização do conteúdo à ser replicado (Assinaturas, Pacotes de Instalação, Políticas e Logs);

8.2.12.17. Possibilidade de instalação dos clientes em servidores, estações de trabalho e máquinas virtualizadas de forma remota via console de gerenciamento com opção de remoção de soluções previamente instaladas;

8.2.12.18. Permitir a instalação remota do software por Group Policy (GPO), Web e via console de gerenciamento;

8.2.12.19. Descobrir automaticamente as estações da rede que não possuem o cliente instalado;

8.2.12.20. Fornecer ferramenta de pesquisa de estações e servidores da rede que não possuem o cliente instalado com opção de instalação remota;

8.2.12.21. Fornecer atualizações do produto e das definições de vírus e proteção contra intrusos;

8.2.12.22. O console de gerenciamento deve permitir travar as configurações por senha nos clientes, definindo permissões para que somente o administrador possa alterar as configurações, desinstalar ou parar o serviço do cliente;

8.2.12.23. A console de gerenciamento deve permitir ao administrador travar separadamente os itens e cada um dos subitens de acesso as configurações do cliente;

8.2.12.24. Capacidade de criação de contas de usuário com diferentes níveis de acesso de administração e operação;

8.2.12.25. Instalação e atualização do software sem a intervenção do usuário;

8.2.12.26. Possibilidade de configurar o bloqueio da desinstalação, desabilitar o serviço do cliente, importar e exportar configurações e abrir a console do cliente, por senha;

8.2.12.27. Utilizar comunicação segura (criptografada) entre o servidor de gerenciamento e o cliente gerenciado;

8.2.12.28. Deverá fornecer acesso gráfico aos problemas, eventos e alertas detectados, com opção de salvaguardar os logs ou direcioná-los para um servidor syslog, além de oferecer mecanismos de emissão de alarmes via correio eletrônico, syslog e traps SNMPv3;

8.2.12.29. Todos os eventos gerados pela solução devem ser armazenados por um período configurável;

8.2.12.30. Deverá ser possível a criação, edição, habilitação, desativação e deleção de alertas customizados, com emissão via SNMPv3, para integração com outros sistemas de gerenciamento;

8.2.12.31. Deverá possuir integração com sistemas SIEM, para possibilitar coleta de logs de gerenciamento e correlação em "real-time";

8.2.13. Atualização de Vacinas:

8.2.13.1. Atualização incremental, remota e em tempo real das vacinas do Antivírus e mecanismo de verificação (Engine) dos clientes da rede;

8.2.13.2. Permitir criar planos de distribuição das atualizações via comunicação segura entre cliente e Servidores de Gerenciamento, Site do fabricante, Via Servidor de atualização interno e podendo eleger qualquer cliente gerenciado para distribuição das atualizações;

8.2.13.3. Permitir eleger qualquer cliente gerenciado como um servidor de distribuição das atualizações com opção de controle de banda, quantidades de definições espaço em disco utilizado, podendo eleger mais de um cliente para esta função;

8.2.13.4. Atualização remota e incremental da versão do software cliente instalado;

8.2.13.5. Nas atualizações das configurações e das definições de vírus não poderá utilizar scripts de login, agendamentos ou tarefas manuais ou outros módulos adicionais que não sejam parte integrante da solução e sem requerer reinicialização do computador ou serviço para aplicá-la;

8.2.13.6. Atualização automática das assinaturas dos servidores de gerenciamento e clientes via Internet, com periodicidade mínima diária;

8.2.13.7. Capacidade de voltar qualquer vacina e assinatura anterior armazenadas no servidor, utilizando opção e comando do console podendo utilizar a arquitetura de grupos lógicos do console;

8.2.13.8. Possuir um único e mesmo arquivo de vacina de vírus para todas as plataformas Windows e versões do antivírus.

8.2.14. Quarentena:

8.2.14.1. Possuir funcionalidades que permitam o isolamento (área de quarentena) de arquivos contaminados por códigos maliciosos que não sejam conhecidos ou que não possam ser reparados em um servidor central da rede;

8.2.14.2. Possibilidade de adicionar manualmente arquivos na quarentena do cliente com opção de restrições na console de gerenciamento;

8.2.14.3. Envio automático dos arquivos da área de isolamento para o fabricante, via protocolo seguro, onde este será responsável por gerar a vacina, automaticamente, sem qualquer tipo de intervenção do administrador. O recebimento da vacina deverá ocorrer da mesma forma que foi enviada e logo em seguida deverá ser aplicada nas estações de trabalho;

8.2.15. Cliente Gerenciado:

8.2.15.1. Deve ter a capacidade de compor de forma nativa com a solução de APT do mesmo fabricante, sem a necessidade da implementação de scripts, utilizando apenas configurações realizadas no console padrão do produto;

8.2.15.2. Suportar máquinas com arquitetura 32-bit e 64-bit;

8.2.15.3. O cliente para instalação em estações de trabalho deverá possuir compatibilidade com no mínimo os sistemas operacionais:

8.2.15.3.1. Windows 7 ou superior;

8.2.15.3.2. Debian 8.0 ou superior;

8.2.15.3.3. Ubuntu 16.04 LTS ou superior.

8.2.15.4. O cliente para instalação em servidores deverá possuir compatibilidade com os sistemas operacionais:

8.2.15.4.1. Windows 2008 e superiores;

8.2.15.4.2. Debian;

8.2.15.4.3. Ubuntu Server;

8.2.15.4.4. CentOS 6 e superiores.

8.2.16. Deve possuir funcionalidade de Firewall e de Detecção e Proteção de Intrusão (IDS\IPS) com as funcionalidades:

8.2.16.1. Suporte aos protocolos TCP, UDP e ICMP;

8.2.16.2. Reconhecimento dos tráfegos DNS, DHCP e WINS com opção de bloqueio;

8.2.16.3. Possuir proteção contra exploração de buffer overflow;

8.2.16.4. Possuir proteção contra ataques de Denial of Service (DOS), Port-Scan e MAC Spoofing;

8.2.16.5. Possibilidades de criação de assinaturas personalizadas para detecção de novos ataques;

8.2.16.6. Possibilidade de agendar a ativação da regra de Firewall;

8.2.16.7. Possibilidade de criar regras diferenciadas por aplicações;

8.2.16.8. Possibilidade de reconhecer automaticamente as aplicações utilizadas via rede baseado no fingerprint do arquivo;

8.2.16.9. Proteger o computador através da criação de uma impressão digital para cada executável existente no sistema, para que somente as aplicações que possuam essa impressão digital executem no computador;

8.2.16.10. Funcionalidade de Whitelist e Blacklist para o recurso de Impressão digital para os executáveis, possibilitando bloquear todos os executáveis da lista ou só liberar os executáveis da lista;

8.2.16.11. Permitir criação de zona confiável, permitindo que determinados IPs, protocolos ou aplicações se comuniquem na rede;

8.2.16.12. Bloqueio de ataques baseado na exploração da vulnerabilidade;

8.2.16.13. Gerenciamento integrado à console de gerência da solução.

8.2.17. Funcionalidade de Antivírus e AntiSpyware:

8.2.17.1. Proteção em tempo real contra vírus, trojans, worms, cavalos-de-tróia, spyware, adwares e outros tipos de códigos maliciosos;

8.2.17.2. Proteção anti-spyware deverá ser nativa do próprio antivírus, ou seja, não dependente de plugin ou módulo adicional;

8.2.17.3. As configurações do anti-spyware deverão ser realizadas através da mesma console de todos os itens da solução;

8.2.17.4. Permitir a configuração de ações diferenciadas para cada subcategoria de riscos de segurança (Adware, Discadores, Ferramentas de hacker, Programas de brincadeiras, Acesso remoto, Spyware, Trackware e outros);

8.2.17.5. Permitir a configuração de duas ações, primária e secundária, executadas automaticamente para cada ameaça, com as opções de: somente alertar, limpar automaticamente, apagar automaticamente e colocar em quarentena;

8.2.17.6. Permitir a criação de listas de exclusões com informação da severidade, impacto e grau de remoção da ameaça nos níveis baixos, médio e alto, onde os riscos excluídos não serão verificados pelo produto;

8.2.17.7. Permitir configurar a verificação contra ameaças para ser executada de maneira manual, agendada e em Tempo Real detectando ameaças no nível do Kernel do Sistema Operacional fornecendo a possibilidade de detecção de Rootkits;

8.2.17.8. Permitir configurar a verificação contra ameaças com a possibilidade de selecionar uma máquina ou grupo de máquinas para rastrear com periodicidade mínima diária;

8.2.17.9. Permitir configurar a verificação contra ameaças com a possibilidade de selecionar uma máquina ou grupo de máquinas para rastrear;

8.2.17.10. Implementar intervalos de tempo para início de verificações agendadas de forma a reduzir impacto em ambientes virtuais;

8.2.17.11. Verificação de vírus nas mensagens de correio eletrônico, pelo antivírus da estação de trabalho, suportando clientes Outlook e POP3/SMTP;

8.2.17.12. Capacidade de detecção em tempo real de vírus novos, desconhecidos pela vacina com opção da sensibilidade da detecção (baixo, médio e alto);

8.2.17.13. Capacidade de identificação da origem da infecção, para vírus que utilizam compartilhamento de arquivos como forma de propagação informando nome ou IP da origem com opção de bloqueio da comunicação via rede;

8.2.17.14. Possibilidade de bloquear verificação de vírus em recursos mapeados da rede, por senha;

8.2.17.15. Possuir funcionalidades de otimização de verificação (scaneamento) em ambientes virtuais, contemplando, no mínimo, as soluções de virtualização VMWare e Microsoft Hyper-V, para no mínimo:

8.2.17.15.1. Diferenciação automática entre máquinas físicas e virtuais, possibilitando aplicar as funcionalidades específicas para as máquinas virtuais;

8.2.17.15.2. Proteção com as mesmas funcionalidades aplicáveis em máquinas físicas, para no mínimo:

8.2.17.15.2.1. Proteção de Antivírus e AntiSpyware;

8.2.17.15.2.2. Proteção de heurística e reputação de arquivos em tempo real (realtime);

8.2.17.15.2.3. Proteção de IPS de rede e "host";

8.2.17.15.2.4. Controle de dispositivos e aplicações;

8.2.17.15.3. Cache local na reputação de arquivos, possibilitando não varrer arquivos categorizados como não maliciosos e já escaneados anteriormente;

8.2.17.15.4. Capacidade de verificar "templates" de máquinas virtuais, excluindo da operação de varredura todos os arquivos categorizados como confiáveis existentes na máquina virtual utilizada como origem (template);

8.2.17.16. Capacidade de implementar varreduras otimizadas em máquinas físicas e virtuais, onde o arquivo verificado pela varredura uma vez, não será verificado novamente, até que ocorra alguma alteração no mesmo;

8.2.17.17. Capacidade de realizar monitoramento em tempo real (*real-time*) por heurística correlacionando com a reputação de arquivos;

8.2.17.18. Capacidade de verificar a reputação de arquivos, correlacionando no mínimo às seguintes características:

8.2.17.18.1. Origem confiável;

8.2.17.18.2. Origem não confiável;

8.2.17.18.3. Tempo de existência do arquivo na internet;

8.2.17.18.4. Comportamento do arquivo;

8.2.17.18.5. Quantidade mínima de usuários que baixaram o arquivo da internet.

8.2.17.19. Capacidade de implementar regras distintas por grupo (ex. Departamento), a partir do resultado da reputação, em conjunto com o correlacionamento da quantidade de utilizadores do arquivo e tempo de existência do mesmo;

8.2.17.20. Possuir funcionalidades que permitam o isolamento (área de quarentena) de arquivos contaminados por códigos maliciosos que não sejam conhecidos ou que não possam ser reparados no cliente;

8.2.17.21. Possuir funcionalidades que permitam a inclusão manual em isolamento (área de quarentena) de arquivos a serem enviados e vistoriados pelo centro de pesquisa do fabricante;

8.2.17.22. Permitir configurar ações a serem tomadas na ocorrência de ameaças, incluindo Reparar, Deletar, Mover para a Área de Isolamento e Ignorar;

8.2.17.23. Possuir funcionalidades que permitam a detecção e reparo de arquivos contaminados por códigos maliciosos mesmo que sejam compactados nos formatos ZIP, ARJ, LHA, RAR, TAR, GZIP e Microsoft Compress, no mínimo em 10 níveis de compactação;

8.2.17.24. Capacidade de remoção automática total dos danos causados por spyware, adwares e worms, como limpeza do registro e pontos de carregamento, com opção de terminar o processo e terminar o serviço da ameaça no momento de detecção;

8.2.17.25. Criar uma cópia backup do arquivo suspeito antes de limpá-lo;

8.2.17.26. Gerenciamento integrado à console de gerência da solução;

8.2.17.27. Possibilitar a criação de um disco (CD ou DVD) inicializável para verificação e remoção de ameaças sem a necessidade de carregar o Sistema Operacional do cliente;

8.2.17.28. Capacidade de executar varreduras em tempo real (real time) contra-ataques dirigidos a vulnerabilidades do navegador (browser);

8.2.17.29. Detecção e remoção de vírus de macro em tempo real;

8.2.18. Detecção Proativa de reconhecimento de novas ameaças:

8.2.18.1. Funcionalidade de detecção de ameaças desconhecidas que estão em memória por comportamento dos processos e arquivos das aplicações;

8.2.18.2. Não utilizar a assinatura de vírus para esta funcionalidade e fornecer assinatura periódicas da técnica de detecção;

8.2.18.3. Capacidade de detecção de keyloggers, Trojans, spyware e Worms por comportamento dos processos em memória, com opção da sensibilidade distintas da detecção;

8.2.18.4. Reconhecimento comportamento malicioso de modificação da configuração de DNS e arquivo Host;

8.2.18.5. Possuir a funcionalidade de exclusão de detecção diferenciada do recurso de Antivírus;

8.2.18.6. Possibilidade de habilitar o recurso de correlacionamento da funcionalidade de detecção Pró-Ativa com a base de reputação do fabricante;

8.2.18.7. Capacidade de detecção de Trojans e Worms por comportamento dos processos em memória, com opção da sensibilidade distintas da detecção;

8.2.18.8. Possibilidade de agendar o escaneamento da detecção Pró-Ativa com periodicidade mínima por minuto e em todos os novos processos;

8.2.19. Funcionalidade de Controle de Dispositivos e Aplicações:

8.2.19.1. Gerenciar o uso de dispositivos USB e CD/DVD, através de controles de leitura/escrita/execução do conteúdo desses dispositivos e também sobre o tipo de dispositivo permitido (ex: permitir mouse USB e bloquear disco USB);

8.2.19.2. Controlar o uso de dispositivos com comunicação infravermelho, firewire, portas seriais e paralelas, através de mecanismos de permissão e bloqueio identificando pelo "Class ID" e pelo "Device ID" do Dispositivo;

8.2.19.3. Permitir criar políticas de bloqueio de dispositivos baseadas na localização atual da estação;

8.2.19.4. Gerenciamento integrado a console de gerência da solução;

8.2.19.5. Oferecer proteção para o sistema operacional, permitindo a definição de controles de acesso (escrita/leitura) para arquivos, diretórios, chaves de registro e controle de processos;

8.2.19.6. Permitir o bloqueio do uso de aplicações baseado em nome, diretório e hash da aplicação;

8.2.19.7. O software de proteção do endpoint deve ter a capacidade de implementar controle de dispositivos para leitura, escrita e execução em Windows 7 e superiores, para no mínimo:

8.2.19.7.1. USB;

8.2.19.7.2. Firewire;

8.2.19.7.3. CD/DVD/BR;

8.2.19.7.4. SD Card;

8.2.19.7.5. eSATA.

8.2.19.8. O software de proteção do endpoint deve ter a capacidade de implementar controle de dispositivos para Windows 7 e superiores, possibilitando regras de "white list" e "black list" utilizando expressões regulares, assim como, possibilidade de implementar teste de regras sem impactar na produção;

8.2.19.9. O software de proteção do endpoint deve ter a capacidade de implementar controle de dispositivos para Windows 7 e superiores, possibilitando administração por parte dos usuários e administração remota, com a possibilidade de monitoração e relatórios a partir da console de administração;

8.2.20. As funcionalidades de emissão de Relatórios e Monitoramento da solução deve possuir:

8.2.20.1. Pelo menos 25 tipos de relatórios diferentes, permitindo a exportação para os formatos PDF e HTML e visualização em Dashboards;

8.2.20.2. Recursos do relatório e monitoramento deverão ser nativos da própria console central de gerenciamento;

8.2.20.3. A capacidade de exibir a lista de servidores e estações que possuam o antivírus instalado, contendo informações como nome da máquina, usuário logado, versão do antivírus, versão do engine, data da vacina, data da última verificação e status, etc.);

8.2.20.4. A capacidade de Geração de relatórios, estatísticos e gráficos contendo no mínimo os seguintes tipos pré-definidos:

8.2.20.4.1. As 10 máquinas com maior ocorrência de códigos maliciosos;

8.2.20.4.2. Os 10 usuários com maior ocorrência de códigos maliciosos;

8.2.20.4.3. Localização dos códigos maliciosos;

8.2.20.4.4. Sumários das ações realizadas;

8.2.20.4.5. Número de infecções detectadas diário, semanal e mensal;

8.2.20.4.6. Códigos maliciosos detectados.

8.2.21. Console avançada de distribuição e Relatórios

8.2.21.1. Console de gerenciamento via tecnologia Web (HTTP e HTTPS) independente da console central da solução;

8.2.21.2. Possibilidade de executar inventário do ambiente e descobrir os antivírus e respectivas versões;

8.2.21.3. Detectar e desinstalar soluções de antivírus de no mínimo o seguinte fabricante:

8.2.21.3.1. F-Secure;

8.2.21.3.2. Kaspersky;

8.2.21.3.3. McAfee;

8.2.21.3.4. Sophos;

8.2.21.3.5. Symantec;

8.2.21.3.6. Trend Micro.

8.2.21.4. Criar tarefas de migração baseadas no resultado do inventário de antivírus;

8.2.21.5. Permitir agendamento e implementar controle de banda para minimizar impacto na rede durante o processo de instalação em clientes;

8.2.21.6. Possibilidade de recuperar instalação em clientes em caso de falha;

8.2.21.7. Oferecer relatórios avançados através da criação de cubos OLAP e tabelas Pivot;

8.2.21.8. Os seguintes cubos devem ser disponibilizados para criação de relatórios:

8.2.21.8.1. Alertas;

8.2.21.8.2. Clientes;

8.2.21.8.3. Políticas;

8.2.21.8.4. Rastreamento;

8.2.21.9. Exportar os relatórios criados nos formatos PDF e HTML.

8.2.22. Funcionalidades do Controle de Acesso à Rede:

8.2.22.1. Deve possibilitar a colocação dos equipamentos em quarentena, restringindo o acesso à rede para aqueles computadores que não estiverem em conformidade com as políticas, para no mínimo as seguintes premissas:

8.2.22.1.1. Computador deve possuir antivírus, atualizado e ativo;

8.2.22.1.2. Computador deve possuir firewall ativo;

8.2.22.1.3. Computador deve possuir anti-spyware, atualizado e ativo;

8.2.22.1.4. Computador deve possuir patches instalados, ativos e atualizados.

8.2.22.2. Deve ter a capacidade de iniciar à auto remediação do computador que falhou a auditoria, ou seja, corrigir os pontos onde a verificação especificada pelo administrador falhou;

8.2.22.3. Deve ter a capacidade de alterar automaticamente as regras de firewall nos clientes que falharam na política restringindo o acesso à rede;

8.2.22.4. A auto remediação deve suportar download de programas e arquivos por links de HTTP, FTP e UNC;

8.2.22.5. Deve ter a possibilidade de notificação customizada para o usuário com diferentes ícones e como erro, informação e notificação;

8.2.22.6. Deve ter a possibilidade de não aceitar a comunicação ponto a ponto entre máquinas que não utilizam o agente (Máquinas não gerenciadas);

8.2.22.7. Deve ter a possibilidade de não aceitar a comunicação ponto a ponto entre máquinas que não estiverem em conformidade com as políticas do controle de acesso à rede;

8.2.23. Das funcionalidades de proteção contra ransomwares:

a) Para estações de trabalho, dispor de capacidade de proteção contra ransomware não baseada exclusivamente na detecção por assinaturas;

b) Deve possuir proteger endpoints contra-ataques de ransomware;

c) Deve automaticamente reverte alterações de arquivos criptografados;

d) Deve possuir nível forense para identificar e remover malwares;

e) Para estações de trabalho, dispor de capacidade de remediação da ação de criptografia maliciosa dos ransomwares;

f) Para servidores, dispor de capacidade de prevenção contra a ação de criptografia maliciosa executada por ransomwares, possibilitando ainda o bloqueio dos computadores de onde partirem tal ação;

g) Deve bloquear técnicas de explorações de vulnerabilidades conhecidas.

CBC
283
Folha
Rubrica

ALLSEC
IT SECURITY

EMPRESA "VISIONÁRIA"
GARTNER'S
MAGIC QUADRANT

Cliente Final
COMITE BRASILEIRO DE CLUBES - CBC
CNPJ: 00.172.849/0001-42
ENDEREÇO RUA ACAI 566
CIDADE BAIRRO DAS PALMEIRAS, CAMPINAS SP
CEP 13.092-587
TELEFONE (19)3514-6852
EMAIL alcivan.silva@cbclubes.org.br/ adolpho.pires@cbclubes.org.br
RESPONSÁVEL ALCIVAN / ADOLPHO

Revenda Autorizada
Empresa: : ALLSEC
CNPJ: 13.497.079/0001-50
Endereço: RUA RIBEIRO DE BRITO 830, BOA VIAGEM
Cidade/ UF: RECIFE PE
CEP: 51.021-110
Telefone: 81-3224-2267/ 8198718-2172
E-mail: karla.silva@networksecure.com.br
Responsável: Karla Silva

Bitdefender
Empresa: Securisoft do Brasil Ltda
CNPJ: 07.760.258/0001-35
Endereço: Praça das Violetas, 84
Cidade/ UF: Barueri - SP
CEP: 06453-004
Telefone: 11 30181855 ramal 137
E-mail: wagner.santos@bitdefenderbrasil.com.br
Responsável: Wagner Santos

Solução
Advanced Business Security

CBC
084
Folha
Rubrica

ALLSEC
IT SECURITY

Sumário

Rua Agenor Lopes Nº 277 Sala 901 | (81) 3224 4283 | www.allsec.com.br

CBC
Folha
Rubrica

Item	Especificações	Quantidade	Valor Unitário	Valor total
	Solução integrada de segurança do tipo endpoint protection (antivirus/antimalware/ransomware), incluindo suporte técnico, pelo distribuidor e repasse de conhecimento remoto. garantia e atualização por 36 (trinta e seis) meses	**105.00**	**R$90,10**	**R$9.460,50**
	Licenças para servidores com 02 interfaces de administração, conforme especificações apresentadas nos Termos de Referência.	**06**	**R$90.00**	**R$540,00**
	Obs na aquisição de 3 anos, o 4º ano é gratuito.			**R$10.000,50**

Valor por extenso; (Dez mil reais e cinquenta centavos)

Prazo de entrega: Conforme especificado no Termo de Referência Anexo I - A.

Apresentamos a V.S.ª, nossa proposta para fornecimento de solução integrada de segurança do tipo endpoint protection (antivirus/antimalware/ransomware), conforme descritivos constantes no Termo de Referência – Anexo I e no Termo de Referência - Anexo I – A – Especificações.

d) Declaramos que nos preços cotados estão incluídas todas as despesas que, direta ou indiretamente, fazem parte do presente objeto, tais como impostos, seguros, frete, taxas, ou quaisquer outros que possam incidir sobre gastos da empresa.

e) Forma de pagamento: 15 dias corridos após a entrega das licenças, tendo como vencimento um dos dias especificados abaixo:

I - O CBC 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 também o prazo de 15 (quinze) dias corridos ao da apresentação da nota fiscal, contados a partir do primeiro dia útil ao do recebimento do documento.

II - As notas fiscais que apresentarem incorreções serão devolvidas à Contratada e seu vencimento ocorrerá no 15° (décimo quinto) dia corrido da data da apresentação da nota devidamente corrigida, observando o critério acima estabelecido.

Rua Agenor Lopes Nº 277 Sala 901 | (81) 3224 4283 | www.allsec.com.br

CBC
Folha
Rubrica

A contratação está condicionada a regularidade das certidões inerentes ao FGTS e a de Débitos Relativos a Créditos Tributários Federais e à Dívida Ativa da União, as quais são consultadas através da internet.

Dados da Proponente

Produto: GravityZone Advanced Business Security

Prazo de pagamento: 15 dias após a compra

Informações Importantes:

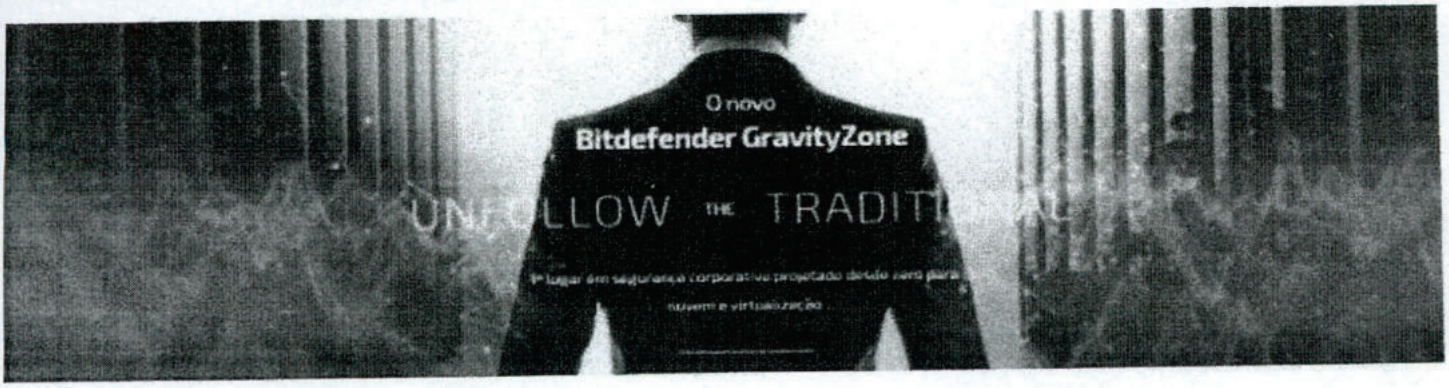
- *Valores FOB na cidade de Barueri: As diferenças de impostos a serem retidos referente ao ajuste do ISS, serão adicionados ao valor final da venda*
- *A partir do segundo boleto bancário gerado em compras parceladas, será cobrado o valor de R$ 4,80 por boleto, isso inclui a remissão de boletos além de impostos e juros.*
- *Estão inclusos nos preços dos bens/serviços acima discriminados: PIS/PASEP-Faturamento, COFINS-Faturamento e ISS-Imposto Sobre Serviços. Quaisquer outros tributos incidentes/exigidos sobre esta operação deverão ser acrescidos aos preços acima.*

- ***Suporte técnico***

- Incluso Suporte técnico 24x7 direto com a Securisoft via:
- **Telefone:** (11) 3018-1855 – Opção 4
- **Chat: (Atendimento 08h30 às 18h)** <https://www.securisoft.com.br/suporte-tecnico-bitdefender >
- **Ferramenta:** <https://bitdefenderbrasil.octadesk.com/login>

- ***Repasse de conhecimento***

Será efetuado remotamente por um analista certificado na solução
Período: 4 horas

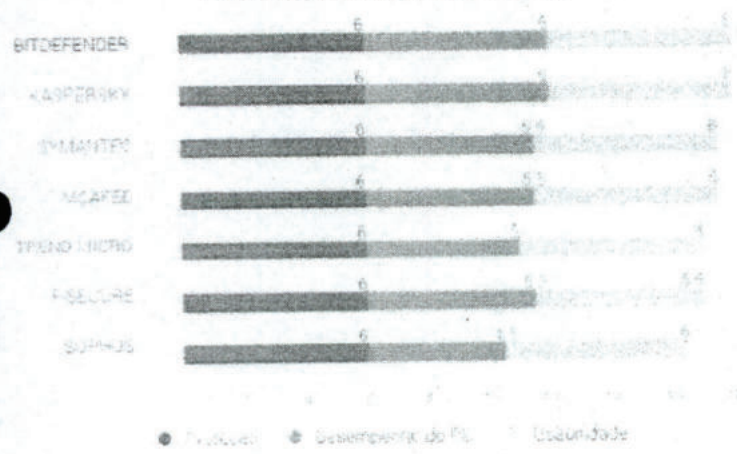


Segurança mais rápida e eficaz para o seu negócio

O Bitdefender GravityZone é uma solução de segurança de ponta no mercado para nuvem e ambientes virtualizados, oferecendo uma proteção mais rápida e uma gestão de forma mais eficiente. Usando uma arquitetura diferente e tecnologias exclusivas, o GravityZone é a solução antimalware classificada em primeiro lugar como melhor proteção e desempenho.

Melhor segurança corporativa em 2015

maior pontuação média para proteção, desempenho e usabilidade



Tecnologias GravityZone

Mantém-se à frente de ameaças avançadas em constante evolução e proporciona a melhor combinação de proteção, desempenho e usabilidade somente e possível inovando-se constantemente.

A arquitetura do GravityZone permite uma instalação de solução para empresas em horas, em vez de dias. **A BRAIN** utiliza mecanismos inteligentes de aprendizado e proporciona inteligência contra ameaças em questão de 3 segundos em qualquer lugar do mundo. **O Bitdefender Endpoint Security Tools** se adapta automaticamente a sistemas virtuais ou físicos, proporcionando o melhor desempenho em todos os ambientes.

Escolha a oferta que melhor atenda às suas necessidades

GravityZone é uma solução empresarial que pode ser instalada de forma local ou hospedada pela Bitdefender. Antivírus, Antimalware com detecção heurística proativa, Firewall, e Controle de Dispositivos são incluídos em cada uma das 3 opções abaixo.

	Bitdefender GravityZone **Segurança corporativa** — Ideal para pequenos negócios buscando segurança simples — Compatível com Windows 10	Bitdefender GravityZone **Segurança empresarial avançada** — Recomendado a empresas de tamanho médio buscando proteção abrangente — Compatível com Windows 10	Bitdefender GravityZone **Segurança Empresarial** — Solução flexível para organizações maiores com centros de dados que utilizam virtualização — Compatível com Windows 10
Opção de console Deixe o Bitdefender hospedar o console ou hospede na infraestrutura local	Console de Nuvem recomendado Console local disponível	Opções disponíveis para nuvem e console local	Console local
Áreas de trabalho físicas Proteção para áreas de trabalho Windows, Mac ou Linux	✔	✔	✔
Servidores físicos Proteção para servidores Windows, Mac ou Linux	✔	✔	✔
Áreas de trabalho virtuais Proteção para áreas de trabalho virtuais Windows, Solaris e Linux	✔	✔	✔
Servidores virtuais Proteção para servidores virtuais Windows, Solaris e Linux	✔	✔	✔
Microsoft Exchange Proteção de servidor e antispam		✔	✔
Dispositivos móveis Controle e proteja dispositivos Android e iOS		✔ Disponível separadamente	✔
Licenciamento de centro de dados Licenciamento de CPU dedicada para servidores virtuais			✔
Varredura inteligente centralizada Capacidade de descarregar a varredura em uma ferramenta central dedicada	Não	Sim	Sim
Licenciamento mensal para provedores de serviços gerenciados Disponível através de solução dedicada para provedores de serviços gerenciados	Adquiridas separadamente		
Instâncias da Amazon Web Services Proteção para instâncias AWS gerenciada a partir do mesmo console em nuvem. Adquirida separadamente.	Adquiridas separadamente	Adquiridas separadamente	

Rua Agenor Lopes Nº 277 Sala 901 | (81) 3224 4283 | www.allsec.com.br

Bitdefender
GravityZone Advanced Business Security

GravityZone Advanced Security Business é uma solução de segurança "tudo em um" que inclui proteção e gerenciamento de segurança unificado para estações de trabalho, servidores, e-mail e dispositivos móveis.

"Durante um ano de difíceis testes na indústria, Bitdefender Endpoint Security superou consistentemente toda a concorrência uma combinação excepcional de eficiência e segurança para usuários corporativos"

Andreas Marx, CEO of AV-TEST

UNFOLLOW THE TRADITIONAL

Ao contrário das soluções tradicionais que combinam patchs baseado em Windows, o Bitdefender GravityZone combina todos os serviços de segurança que uma empresa precisa

em uma única plataforma de entrega e oferece a melhor combinação de proteção e desempenho.

CBC
290
Folha
Rubrica

PRINCIPAIS BENEFICIOS

Proteção abrangente e eficaz em termos de custos X benefícios
Bitdefender GravityZone Business Security oferece às organizações uma proteção eficaz para estações de trabalho, servidores físicos ou virtuais e para dispositivos móveis, com uma licença por dispositivo. Proteção para Exchange sem custos adicionais, o numero de caixas de e-mails protegidas é proporcional ao número de licenças.

Lider em segurança antimalware e antispam
Bitdefender Endpoint Security ganhou com Melhor Perfomance no AV-Test Award 2014 e a melhor pontuação geral para proteção, desempenho e usabilidade. A única solução a ganhar em todas as categorias no VBSpam. O Bitdefender consistentemente registra detecções de spam maiores que os concorrentes.

Gerenciamento de Segurança simplificada
As empresas podem usar o console de gerenciamento hospedado na nuvem ou podem implementar o console localmente. Baseado em um Linux voltado para appliances virtuais, a console local do Bitdefender pode ser configurado e está pronto para uso em menos de 2 horas. Opções granulares e integrações com o Active Directory, Citrix XenServer ou VMware vCenter economizam tempo e agilizam os processos de segurança.

PRINCIPAIS CARACTERISTICAS

• **Um console** de gerenciamento centralizado oferecendo fácil implantação e execução de políticas de segurança para qualquer tipo e número de endpoints em qualquer local;

• **Integração com o Active Directory, VMware e Citrix** *(console on-premise);*

• **Um agente** cobrindo qualquer plataforma de virtualização, provedores de serviço em nuvem, sistemas operacionais e dispositivos físicos;

• **Múltiplas camadas de segurança** para endpoints: antivírus e antimalware com monitoramento comportamental, proteção contra ameaças, controle de aplicativos e sandboxing (criação de uma máquina virtual dentro do antivírus para análise de comportamento do arquivo), firewall, controle de dispositivos e controle de conteúdo com anti-phishing e anti-spam para servidores de email Exchange.

Cobertura Universal
• Qualquer endpoint: Físico, virtuais e em nuvem;
• Qualquer tipo: Estação de trabalho, servidor, sistemas embedded, móvel;
• Qualquer sistema operacional: Windows, Linux, Mac;
• Qualquer plataforma de virtualização: VMware, Citrix, Microsoft Hyper-V, KVM, Oracle;
• Organizações de qualquer porte: Escalas de dezenas a milhões de terminais apenas clonando os appliances virtuais;
• Qualquer ambiente: datacenters, redes locais, redes

8

mistas, nuvem privada, nuvem pública e nuvem híbrida;

• Servidores de segurança centralizados, que "tomam conta" do escaneamento de maquinas fisicas ou virtuais levando cada arquivo para esse servidor escanear ao invés de cada máquina faze-lo

CBC
291
Folha
Rubrica

Rua Agenor Lopes Nº 277 Sala 901 | (81) 3224 4283 | www.allsec.com.br

Requisitos de Sistema

O GravityZone Advanced Business Security é indicado para workstations, laptops e servidores rodando o Microsoft® Windows, Mac e Linux. ***A segurança para todos os sistemas pode ser gerenciada com uma console On-Premises ou através de uma simples abertura de navegador e acesso ao GravityZone Advanced Business Security.***

GBC
292
Folha
Rubrica

Requisitos de Hardware:

Processadores compatíveis com Intel® Pentium:

Sistemas Operacionais de Workstations

1 GHz ou superior em Microsoft Windows XP SP3, Windows XP SP2 64 bit e Windows 7 Enterprise (32/64 bit).

2 GHz ou superior para Microsoft Windows Vista SP1 or higher (32 and 64 bit), Microsoft Windows 7 (32 and 64 bit), Microsoft Windows 7 SP1 (32 and 64bit), Windows 8.

800 MHZ ou superior para Microsoft Windows Embedded Standard 7 SP1, Microsoft Windows POSReady 7, Microsoft Windows POSReady 2009, Microsoft Windows Embedded Standard 2009, Microsoft Windows XP Embedded with Service Pack 2, Microsoft Windows XP Tablet PC Edition

Sistemas Operacionais de Servidor:

Minimo: 2.4 GHz single-core CPU.

Recomendado: 1.86 GHz ou superior em Intel Xeon multi-core CPU.

Memória RAM livre:

	ENGINE ÚNICA					
OS	Escaneamento Local		Escaneamento Híbrido		Escaneamento Centralizado	
	Apenas AV	Todas Opções	Apenas AV	Todas Opções	Apenas AV	Todas Opções
Windows	1024	1200	512	660	256	400
Linux	1024	1024	512	512	256	256
Mac	1024	1024	n/a	n/a	n/a	n/a

Espaço em HD livre:

	ENGINE ÚNICA				ENGINE DUPLA					
OS	Escaneamento Local		Escaneamento Híbrido		Escaneamento Centralizado		Centralizado + Escaneamento Local		Centralizado + Escaneamento Híbrido	
	Apenas AV	Todas Opções	Apenas AV	Todas Opções	Apenas AV	Todas Opções	Apenas AV	Todas Opções	Apenas AV	Todas Opções
Windows	1024	1200	500	700	350	570	1024	1200	500	700
Linux	1024	1024	400	400	250	250	1024	1024	400	400
Mac	1024	1024	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a

Nota: É necessário ao menos 6 GB de espaço livre em disco para maquinas definidas como Relay do Bitdefender Endpoint Security pois ele irá armazenar todas as atualizações e pacotes de instalação.

Sistemas Operacionais Mac e Microsoft Suportados:

Sistemas Operacionais para Desktops	Sistemas Operacionais para Servidores	Sistemas Operacionais para Tablets Microsoft
Windows 8.1	Windows Server 2012 R2	Windows Embedded Standard 7
Windows 8	Windows Server 2012	Windows Embedded Compact 7
Windows 7	Windows SBS 2011	Windows Embedded POSReady 7
Windows Vista SP1	Windows SBS 2008	Windows Embedded Enterprise 7
Windows XP SP3	Windows Server 2008 R2	Windows Embedded POSReady 2009
Mac OS X Lion (10.7.x)	Windows Server 2008	Windows Embedded Standard 2009
Mac OS X Mountain Lion (10.8.x)	Windows SBS 2003	Windows XP Embedded SP2
Mac OS X Mavericks (10.9.x)	Windows Server 2003 R2	Windows XP Tablet PC Edition
Mac OS X Yosemite (10.10.x)	Windows Server 2003 SP1	Windows Embedded 8.1 Industry
	Windows Home Server	Windows Embedded 8.1 Standard

Sistemas Operacionais Linux Suportados:

Red Hat Enterprise Linux / CentOS 5.6 ou superior
Ubuntu 10.04 LTS ou superior
SUSE Linux Enterprise Server 11 ou superior
OpenSUSE 11 ou superior
Fedora 15 ou superior
Debian 5.0 ou superior
Escaneamento em tempo Real está disponível para todos os sistemas operacionais suportados.
Nos sistemas Linux, o acesso será concedido nas seguintes situações:

Versões de Kernel	Distribuições de Linux	Escaneamento em tempo real
2.6.38 ou superior	Todas	Necessita de Bibliotecas Inotify instaladas.
2.6.18 - 2.6.37	Debian 5.0, 6.0 Ubuntu 10.04 LTS CentOS 6.x Red Hat Enterprise Linux 6.x	Bitdefender da suporte via DazukoFS com módulos essenciais

Browsers Suportados:
Internet Explorer 9+, Mozilla Firefox 14+, Google Chrome 15+, Safari 5+
Definição de tela recomendada: 1024x768 ou superior

CBC
294
Folha
Rubrica

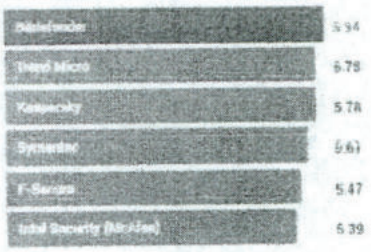
O 1º DO RANKING DE TECNOLOGIA EM ANTIVÍRUS

A melhor combinação de proteção, desempenho e usabilidade.

A pontuação geral mais alta em versões de solução corporativa da Av-Test em 2015

Melhor segurança corporativa em 2015

pontuação média para proteção, desempenho e usabilidade

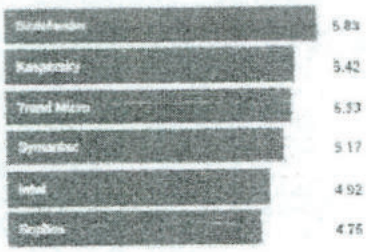


"Empresas que confiam na solução Bitdefender recebem em troca de sua confiança não só uma solução segura, mas também um produto com recursos exemplares em termos de baixo sobrecarregamento do sistema."

Guido Habekh, CEO AV-TEST GmbH

Melhor Desempenho 2015

pontuação média de desempenho em 2015)



"Defesa Impecável e extrema facilidade de uso"

"Bitdefender é uma solução de proteção discreta que, além de fácil manuseio, fornece proteção excelente."

Maik Morgenstern, **CTO AV-TEST GmbH**

CBC
295
Folha
Rubrica

EMPRESA "VISIONÁRIA"
GARTNER'S
MAGIC QUADRANT

"Este prêmio é o reconhecimento que permite a Bitdefender inovar continuamente suas tecnologias em cibersegurança"

vb 100 VIRUS virusbtn.com

LIDER DE RANKING – 54 prêmios VB100

De acordo:

Recife, 19 de Março de 2020

Consultora: Karla Simone da Silva

ATLSEC SERVIÇOS EM TECNOLOGIA DA INFORMAÇÃO
CNPJ: Nº 13.497.079/0001-50

COMITE BRASILEIRO DE CLUBES – CBC

SNPJ: 00.172.849/0001-42