EDITAL DE LICITAÇÃO

LICITAÇÃO EXCLUSIVA PARA MICROEMPRESAS (ME) E EMPRESAS DE PEQUENO PORTE (EPP)

PREGÃO ELETRÔNICO Nº 007/2018

TIPO: MENOR PREÇO POR LOTE

OBJETO: CONTRATAÇÃO DE EMPRESA PARA FORNECIMENTO DE SOLUÇÃO DE PROTEÇÃO ENDPOINT (ANTIVIRUS), SERVIÇO DE IMPLANTAÇÃO E TREINAMENTO VISANDO ATENDER AS NECESSIDADES DA AGEHAB, DE ACORDO COM AS DESCRIÇÕES CONTIDAS NO ANEXO I – TERMO DE REFERÊNCIA, PARTE INTEGRANTE DESTE EDITAL.

ABERTURA: 20/04/2018 às 09:00 horas
Obs.: Horário de Brasília

Agência Goiana de Habitação S/A
Rua 18-A nº 541, Setor Aeroporto - Goiânia - Goiás - 74.070-060 - (62) 3096-5000
Ouvidoria Agehab 3096-5049
Internet: www.agehab.go.gov.br
e-mail ouvidoria@agehab.go.gov.br

AVISO DE LICITAÇÃO

LICITAÇÃO EXCLUSIVA PARA MICROEMPRESAS (ME) E EMPRESAS DE PEQUENO PORTE (EPP)

PREGÃO ELETRÔNICO Nº 007/2018

A Agência Goiana de Habitação S/A – AGEHAB, por intermédio de seu Pregoeiro e Equipe de Apoio designados pela Portaria nº 200/2017, de 20/09/2017, torna público que fará realizar licitação na modalidade **Pregão** (eletrônico), tipo **Menor Preço por Lote,** destinada à **CONTRATAÇÃO DE EMPRESA PARA FORNECIMENTO DE SOLUÇÃO DE PROTEÇÃO ENDPOINT (ANTIVIRUS), SERVIÇO DE IMPLANTAÇÃO E TREINAMENTO VISANDO ATENDER AS NECESSIDADES DA AGEHAB, DE ACORDO COM AS DESCRIÇÕES CONTIDAS NO ANEXO I – TERMO DE REFERÊNCIA, PARTE INTEGRANTE DESTE EDITAL,** relativo ao Processo Administrativo nº 2017.01031.006807-53, SEI nº 201700031000181, nos termos da Lei Federal nº 10.520, de 17 de julho de 2002, Lei Complementar nº 123, de 14 de dezembro de 2006, Decreto Estadual nº 7.468, de 20 de outubro de 2011, Decreto Estadual nº 7.466 de 18 de outubro de 2011, Lei Estadual nº 17.928/2012, Lei Complementar 117/2015, aplicando-se subsidiariamente, no que couberem, as disposições da Lei Federal nº 8.666, de 23 de junho de 1993, e demais normas regulamentares aplicáveis à espécie. O edital alterado e seus anexos encontram-se disponíveis no endereço: Rua 18-A, nº 541, 2º andar, coordenação de licitações, Setor Aeroporto, Goiânia – Goiás, fone (62) 3096-5041 ou nos sites www.comprasnet.go.gov.br e www.agehab.go.gov.br. A licitação será realizada em sessão pública, com **RECURSOS PRÓPRIOS,** através do Sistema Eletrônico de Gestão de Compras – COMPRASNET.GO, por meio do *site* **www.comprasnet.go.gov.br** no dia **20/04/2018 a partir das 09h00min (horário de Brasília-DF)**.

Aquilino Alves de Macedo
Pregoeiro

Agência Goiana de Habitação S/A
Rua 18-A nº 541, Setor Aeroporto - Goiânia - Goiás - 74.070-060 - (62) 3096-5000
Ouvidoria Agehab 3096-5049
Internet: www.agehab.go.gov.br
e-mail ouvidoria@agehab.go.gov.br

EDITAL DE LICITAÇÃO

PREGÃO ELETRÔNICO Nº 007/2018

PROCESSO Nº 2017.01031.006807-53

1 - PREÂMBULO

A Agência Goiana de Habitação S/A – AGEHAB, por intermédio de seu Pregoeiro e Equipe de Apoio designados pela Portaria nº 200/2017, de 20/09/2017, torna público que se encontra aberta, nesta unidade, licitação na modalidade **Pregão Eletrônico**, tipo **Menor Preço por Lote,** a ser realizada em sessão pública pelo Pregoeiro **Aquilino Alves de Macedo** e equipe de apoio, através do Sistema Eletrônico de Gestão de Compras – COMPRASNET.GO, por meio do *site* www.comprasnet.go.gov.br, conforme as disposições da Lei Federal nº 10.520, de 17 de julho de 2002, Lei Complementar nº 123, de 14 de dezembro de 2006, Decreto Estadual nº 7.468, de 20 de outubro de 2011, Decreto Estadual nº 7.466 de 18 de outubro de 2011, Lei Estadual nº 17.928/2012, Lei Complementar 117/2015, aplicando-se subsidiariamente, no que couberem, as disposições da Lei Federal nº 8.666, de 23 de junho de 1993, e demais normas regulamentares aplicáveis à espécie, bem como as condições estabelecidas neste Edital e seus anexos.

2 – DO OBJETO

2.1. Constituem objeto da presente licitação a **CONTRATAÇÃO DE EMPRESA PARA FORNECIMENTO DE SOLUÇÃO DE PROTEÇÃO ENDPOINT (ANTIVIRUS), SERVIÇO DE IMPLANTAÇÃO E TREINAMENTO VISANDO ATENDER AS NECESSIDADES DA AGEHAB, DE ACORDO COM AS DESCRIÇÕES CONTIDAS NO ANEXO I – TERMO DE REFERÊNCIA, PARTE INTEGRANTE DESTE EDITAL.**

3 – DO LOCAL, DATA E HORA

3.1. O Pregão Eletrônico será realizado em sessão pública, através do site www.comprasnet.go.gov.br no dia **20/04/2018** a partir das **09h00min**, mediante condições de segurança, criptografia e autenticação, em todas as suas fases.

3.2. As Propostas Comerciais deverão ser encaminhadas, através do site www.comprasnet.go.gov.br no período compreendido entre as **09h00min e 10h00min horas** do dia **20 de abril de 2018.**

3.3. A fase competitiva (lances) terá início previsto às **10h10min do dia 20/04/2018.**

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

3.5. Todas as referências de tempo contidas neste Edital, no Aviso e durante a Sessão

Agência Goiana de Habitação S/A
Rua 18-A nº 541, Setor Aeroporto - Goiânia - Goiás - 74.070-060 - (62) 3096-5000
Ouvidoria Agehab 3096-5049
Internet: www.agehab.go.gov.br
e-mail ouvidoria@agehab.go.gov.br

Pública observarão, obrigatoriamente, o horário de Brasília – DF e, dessa forma, serão registradas no sistema eletrônico e na documentação relativa ao certame.

4 – DAS CONDIÇÕES DE PARTICIPAÇÃO

4.1. Poderão participar deste Pregão as empresas:

a) Do ramo pertinente ao seu objeto, legalmente constituídas;

b) Que atendam as condições estabelecidas neste edital e seus anexos;

c) Que possuam o Certificado de Registro Cadastral – CRC emitido pelo Cadastro Unificado de Fornecedores do Estado – CADFOR ou outro certificado de registro cadastral que atenda aos requisitos previstos na legislação geral;

d) Que estejam previamente credenciadas no ComprasNet.Go; e

e) Que se enquadrem na condição de Microempresa ou Empresa de Pequeno Porte, nos termos da Lei Complementar nº 117/2015;

4.1.1. O CRC, emitido pelo CADFOR, poderá ser impresso pelo pregoeiro para averiguação da sua conformidade com as exigências do edital e caso ele apresente *"status* irregular" será assegurado à licitante o direito de apresentar a documentação atualizada e regular na própria sessão.

4.2. Como requisito para participação neste Pregão, a licitante deverá manifestar, em campo próprio do sistema eletrônico www.comprasnet.go.gov.br o pleno conhecimento e atendimento às exigências de habilitação previstas no Edital.

4.3. As licitantes arcarão com todos os custos decorrentes da elaboração e apresentação de suas propostas. A AGEHAB não será, em nenhuma hipótese, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

4.4. A participação neste certame implica na aceitação de todas as condições estabelecidas neste instrumento convocatório.

4.5. Não poderão participar deste Pregão:

a) Empresa suspensa perante o CADFOR, durante o prazo da sanção aplicada;

b) Empresa declarada inidônea para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação;

c) Empresa impedida de licitar e contratar com o Estado de Goiás, durante o prazo da sanção aplicada;

d) Empresa proibida de contratar com o Poder Público, em razão do disposto no art. 72, § 8º, V, da Lei nº 9.605,98;

Agência Goiana de Habitação S/A
Rua 18-A nº 541, Setor Aeroporto - Goiânia - Goiás - 74.070-060 - (62) 3096-5000
Ouvidoria Agehab 3096-5049
Internet: www.agehab.go.gov.br
e-mail ouvidoria@agehab.go.gov.br

e) Empresa proibida de contratar com o Poder Público, nos termos do art. 12 da Lei nº 8.429/92;

f) Sociedade estrangeira não autorizada a funcionar no País;

g) Empresa cujo estatuto ou contrato social não seja pertinente e compatível com o objeto deste Pregão;

h) Empresa que se encontre em processo de dissolução, recuperação judicial, recuperação extrajudicial, falência, concordata, fusão, cisão, incorporação, concurso de credores ou em liquidação;

i) Empresa cujos sócios ou diretores pertençam, simultaneamente, a mais de uma empresa licitante;

j) Empresas cujos sócios tenham vínculos de parentesco com servidores ou dirigentes da AGEHAB, em observância ao disposto no art. 9º, inciso III, da Lei nº 8.666/93.

4.5.1. Não será permitida neste certame a participação de empresa não enquadrada como Microempresa ou Empresa de Pequeno Porte.

4.5.2. Também não poderá participar direta ou indiretamente da licitação, da execução dos serviços e do fornecimento de bens a eles necessários, conforme o artigo 9º da Lei Federal nº 8.666/93:

a) O autor do Termo de Referência, pessoa física ou jurídica; e

b) Servidor ou dirigente de órgão ou entidade Contratante ou responsável pela licitação.

4.5.2.1. Considera-se participação indireta, para fins do disposto no subitem 4.5.2, a existência de qualquer vínculo de natureza técnica, comercial, econômica, financeira ou trabalhista entre o autor do Termo de Referência e a Licitante, incluindo-se os fornecimentos de bens e serviços a estes necessários.

4.5.2.2. O disposto no item 4.5.2 aplica-se também aos membros da Comissão de Licitação, ao Pregoeiro e à Equipe de Apoio.

5 – DO CREDENCIAMENTO

5.1. O acesso ao credenciamento se dará somente às licitantes com cadastro homologado pelo Cadastro Unificado de Fornecedores do Estado – CADFOR da Superintendência de Suprimentos e Logística da SEGPLAN ou àquelas que atendam às condições do item 5.1.5. abaixo.

5.1.1. Para cadastramento, renovação cadastral e regularização, o interessado deverá atender a todas as exigências do cadastro Unificado de Fornecedores do Estado – CADFOR da Superintendência de Suprimentos e Logística da SEGPLAN até o 5º (quinto) dia útil anterior à data de registro das propostas. A relação de documentos para cadastramento está disponível no site www.comprasnet.go.gov.br.

5.1.2. Não havendo pendências documentais será emitido o CRC – Certificado de Registro Cadastral pelo CADFOR, no prazo de 04 (quatro) dias úteis contados do recebimento da documentação.

5.1.3. A simples inscrição do pré-cadastro no sistema Comprasnet.go, não dará direito à licitante de credenciar-se para participar deste Pregão, em razão do bloqueio inicial da sua senha.

5.1.4. O desbloqueio do login e da senha do fornecedor será realizado após a homologação do cadastro da licitante.

5.1.5. Conforme Instrução Normativa nº 004/2011 – SEGPLAN, em caso do licitante pretender utilizar-se de outros cadastros que atendam a legislação pertinente para participar do pregão eletrônico, efetuará seu credenciamento de forma simplificada junto ao CADFOR, caso em que ficará dispensado de apresentar toda a documentação abrangida pelo referido cadastro, mediante a apresentação do mesmo ao CADFOR e terá registrado apenas a condição de "credenciado".

5.2. Os interessados que estiverem com o cadastro homologado ou "credenciados" (conforme item 5.1.5.), deverão credenciar-se pelo *site* www.comprasnet.go.gov.br, opção "login do FORNECEDOR", conforme instruções nele contidas.

5.3. O credenciamento dar-se-á de forma eletrônica por meio da atribuição de chave de identificação ou senha individual.

5.4. O credenciamento do usuário será pessoal e intransferível para acesso ao sistema, sendo o mesmo responsável por todos os atos praticados nos limites de suas atribuições e competências.

5.5. O credenciamento do usuário implica sua responsabilidade legal e a presunção de sua capacidade técnica para realização das transações inerentes ao pregão eletrônico.

5.6. O uso da senha de acesso pelo licitante é de sua exclusiva responsabilidade, incluindo qualquer transação efetuada diretamente ou por seu representante, não cabendo ao provedor do sistema ou a AGEHAB, promotora da licitação, responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.

5.7. As informações complementares para cadastro e credenciamento poderão ser obtidas pelos telefones (62) 3096-5041 e 3096-5003, e para operação no sistema Comprasnet.go pelo telefone (62) 3201-6515 e 3201-6516.

6 – DAS PROPOSTAS COMERCIAIS

6.1. Concluída a fase de credenciamento, as licitantes registrarão suas propostas. Só será aceita uma proposta por lote para cada licitante e, ao término do prazo estipulado para a fase de registro de propostas, o sistema automaticamente bloqueará o envio de novas propostas.

6.2. As propostas comerciais deverão ser enviadas através do site

www.comprasnet.go.gov.br na data e hora estabelecidas neste edital, após o preenchimento do formulário eletrônico, com manifestação em campo próprio do sistema de que tem pleno conhecimento e que atende às exigências de habilitação e demais condições da proposta comercial previstas no edital e seus anexos.

6.3. A proposta comercial deverá ser formulada e enviada, exclusivamente por meio do Sistema Eletrônico, **indicando o valor unitário do item,** e o ônus de comprovação de sua exequibilidade caberá exclusivamente à licitante, caso solicitado pelo pregoeiro.

6.3.1. O sistema Comprasnet.go possibilita à licitante a exclusão/alteração da proposta dentro do prazo estipulado no edital para registro de propostas. Ao término desse prazo, definido no item 3.2, não haverá possibilidade de exclusão/alteração das propostas, as quais serão analisadas conforme definido no edital.

6.4. A licitante se responsabilizará por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras suas propostas, assim como os lances inseridos durante a sessão pública.

6.5. O licitante é responsável pelo ônus da perda de negócios resultante da inobservância de quaisquer mensagens emitidas pelo Pregoeiro ou pelo sistema, ainda que ocorra sua desconexão.

6.6. As propostas deverão atender as especificações contidas no Termo de Referência, Anexo I deste Edital.

6.7. Todas as empresas deverão cotar seus preços com todos os tributos cabíveis inclusos, bem como todos os demais custos diretos e indiretos necessários ao atendimento das exigências do Edital e seus anexos.

6.8. Quaisquer tributos, custos e despesas diretas ou indiretas omitidos na proposta ou incorretamente cotados, serão considerados como inclusos nos preços, não sendo aceitos pleitos de acréscimos, a esse ou qualquer outro título.

6.9. A licitante detentora da melhor oferta, após a fase de lances, deverá enviar Proposta Comercial, por fax ou e-mail, devendo a mesma conter, obrigatoriamente, ainda:

a) Nome da Empresa, CNPJ, endereço, fone/fax, nº da conta corrente, Banco, nº da agência, nome do responsável;
b) Nº do Pregão;
c) Preço em Real, unitário e total com no máximo duas casas decimais, onde deverá estar inclusas todas as despesas que influam nos custos, tais como: encargos sociais, trabalhistas, previdenciários, fiscais e comerciais, impostos, taxas, assim como outros de qualquer natureza que se fizerem indispensáveis ao cumprimento integral do objeto do presente edital;
d) Objeto ofertado, consoante exigências editalícias e com a quantidade licitada;
e) Prazo de validade da proposta de **60 (sessenta) dias,** a contar da data da sessão deste Pregão Eletrônico. Caso não apresente prazo de validade será este considerado;
f) Data e assinatura do responsável;
g) Deverá ser apresentado junto com a proposta de preço:

*** Portifólio do produto ofertado;**

Agência Goiana de Habitação S/A
Rua 18-A nº 541, Setor Aeroporto - Goiânia - Goiás - 74.070-060 - (62) 3096-5000
Ouvidoria Agehab 3096-5049
Internet: www.agehab.go.gov.br
e-mail ouvidoria@agehab.go.gov.br

*** Part Numbers (P/N) e fabricante da solução ofertada.**

6.10. – Critério de Julgamento e estimativa de preços:

6.10.1. O critério de julgamento e seleção da proposta mais vantajosa para a **AGEHAB** será a que oferecer o **menor preço do lote**.

6.10.2. O valor estimado é de **R$ 73.001,70 (setenta e três mil, um real e setenta centavos),** para um período de 12 (doze) meses.

7 – DA SESSÃO DO PREGÃO ELETRÔNICO

7.1. A partir das **09h00min, do dia 20 de abril de 2018,** data e horário previstos neste Edital, terá início à sessão pública do **Pregão Eletrônico nº 007/2018**, com a divulgação das Propostas de Preços recebidas.

7.2. Após a abertura da sessão pública deste Pregão Eletrônico não serão permitidos quaisquer adendos, complementações, acréscimos ou retificações às Propostas de Preços apresentadas.

7.3. Após a abertura da sessão pública deste Pregão Eletrônico não caberá desistência da Proposta de Preços apresentada, salvo por motivo justo, decorrente de fato superveniente e aceito pelo Pregoeiro.

7.4. O Pregoeiro verificará as propostas apresentadas, desclassificando aquelas que não estiverem em conformidade com os requisitos estabelecidos no Edital, em decisão fundamentada e registrada no sistema, com acompanhamento em tempo real por todos os participantes.

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

7.6. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os Licitantes, permitindo que durante o transcurso da sessão pública eletrônica, haja a divulgação, em tempo real, de todas as mensagens trocadas no *chat* do sistema, inclusive valor e horário do menor lance registrado e apresentado pelas Licitantes, vedada a identificação do fornecedor.

8 – DOS LANCES

8.1. Após a análise e classificação das propostas, o Pregoeiro dará início à fase competitiva, quando então as Licitantes poderão encaminhar lances exclusivamente por meio do sistema eletrônico, observado o horário estabelecido e as regras de aceitação dos mesmos, sendo imediatamente informados do seu recebimento e respectivo horário de registro e valor.

8.2. Os licitantes poderão oferecer lances sucessivos, **MENOR PREÇO,** sempre inferior ao último por ele ofertado e registrado pelo sistema, obedecendo, quando o Pregoeiro fixar, ao percentual ou valor mínimo exigido entre os lances.

8.2.1. O sistema eletrônico rejeitará automaticamente os lances em valores superiores aos anteriormente apresentados pelo mesmo licitante.

8.3. Não serão aceitos dois ou mais lances iguais, **para a mesma proposta,** prevalecendo aquele que for recebido e registrado no sistema em primeiro lugar.

8.4. Caso a licitante não realize lances, permanecerá o valor inicial de sua proposta eletrônica, que será incluída na classificação final.

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

8.6. A fase de lances terá duas etapas: a primeira, com tempo de duração de **15 minutos,** após a abertura da fase de lances e será encerrada mediante aviso de fechamento iminente dos lances, emitido pelo sistema às Licitantes. A segunda transcorrerá com abertura de prazo de até 30 (trinta) minutos, aleatoriamente determinado também pelo sistema eletrônico, findo o qual será automaticamente encerrada a recepção de lances.

8.7. Após o encerramento da etapa de lances da sessão pública, o Pregoeiro poderá encaminhar, pelo sistema eletrônico, contraproposta ao licitante que tenha apresentado lance mais vantajoso, para que seja obtida melhor proposta, observado o critério de julgamento, não se admitindo negociar condições diferentes das previstas no edital.

8.8. A negociação será realizada por meio do sistema eletrônico, podendo ser acompanhada pelas demais licitantes.

8.9. No caso de desconexão com o pregoeiro, no decorrer da etapa competitiva do pregão, se o sistema eletrônico permanecer acessível às licitantes para a recepção dos lances, estes continuarão sendo recebidos, sem prejuízo dos atos realizados.

8.10. Quando a desconexão persistir por tempo superior a 10 (dez) minutos, a sessão do pregão será suspensa e reiniciada somente após comunicação aos participantes, no endereço eletrônico utilizado para divulgação.

9 – DO JULGAMENTO DAS PROPOSTAS DE PREÇOS

9.1. O julgamento das propostas será objetivo, tendo seu critério baseado no ***MENOR PREÇO DO LOTE*****,** não se admitindo, sob pena de responsabilidade, reformulação dos critérios de julgamento previstos no ato convocatório.

9.2. Considerar-se-á **vencedora do certame** aquela proposta que, tendo sido aceita, estiver de acordo com os termos deste Edital e seus Anexos, ofertar o menor preço, após a fase de lances e for devidamente habilitada após apreciação da documentação.

9.2.1. Na análise da Proposta de Preços, fica facultado ao Pregoeiro, se necessário, solicitar parecer técnico para subsidiar sua análise, podendo suspender temporariamente a sessão pública do pregão, informando através do *chat* de comunicação o horário de reabertura dos trabalhos.

Agência Goiana de Habitação S/A
Rua 18-A nº 541, Setor Aeroporto - Goiânia - Goiás - 74.070-060 - (62) 3096-5000
Ouvidoria Agehab 3096-5049
Internet: www.agehab.go.gov.br
e-mail ouvidoria@agehab.go.gov.br

9.3. Havendo apenas uma proposta de preços, desde que atenda a todas as condições do edital e estando o seu valor compatível com os praticados no mercado, poderá ser aceita, devendo o Pregoeiro negociar, visando a obter melhor preço.

9.4. Encerrada a etapa de lances da sessão pública ou, quando for o caso, após a negociação e decisão acerca da aceitação do lance de menor valor, a proposta de preços que, em consequência com as especificações contidas no Termo de Referência, tenha apresentado menor valor, o sistema informará a Licitante detentora da melhor oferta, e esta deverá encaminhar de imediato, nova proposta com valores (unitários e total) readequados ao valor ofertado e registrado como de menor lance, bem como a documentação de habilitação para as exigências não contempladas no CRC e todos os documentos exigidos neste Edital e seus Anexos. Esta comprovação se dará mediante encaminhamento da documentação *via fax: (62) 3096-5041 ou e-mail:* cpl@agehab.go.gov.br.

9.4.1. Posteriormente deverá ser encaminhada, no prazo máximo de 05 (cinco) dias úteis contados da data de encerramento do Pregão Eletrônico, via correio ou por representante, a proposta de preços em original, assinada e atualizada com os valores, unitários e global, informando todas as características do objeto e demais exigências descritas neste Edital e seus Anexos. Deverão ser enviadas, no mesmo prazo, as demais documentações exigidas para habilitação, estas em original ou por cópia autenticada, sendo inclusive condição indispensável para a contratação.

9.4.2. O pregoeiro verificará a regularidade cadastral da Licitante que apresentou a melhor oferta junto ao CADFOR, e em caso de irregularidade, será assegurado o direito de apresentar a documentação atualizada, ao final da sessão em até 02 (duas) horas, via fax ou pelo e-mail: cpl@agehab.go.gov.br, devendo a documentação original ou cópia autenticada ser encaminhada no prazo máximo de 05 (cinco) dias úteis contados da data de encerramento do Pregão Eletrônico.

9.4.3. O CRC, emitido pelo CADFOR, poderá ser impresso pelo Pregoeiro para averiguação da sua conformidade com as exigências do Edital e apresentando *"status irregular",* será assegurada à Licitante o direito de apresentar a documentação atualizada e regular na própria sessão.

9.4.4. Para fins de habilitação a verificação, pela Equipe de Apoio do certame, nos sítios oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova.

9.5. Constatado, que a Licitante que apresentou proposta de menor preço final atende às exigências editalícias, será ela declarada vencedora.

9.6. Na hipótese da Licitante detentora da melhor oferta desatender às exigências habilitatórias, o Pregoeiro deverá restabelecer a etapa competitiva de lances entre os licitantes. **(Lei Estadual nº 18.989, 27/08/2015).**

9.7. Da sessão pública do Pregão Eletrônico, o sistema gerará ata circunstanciada, na qual estarão registrados todos os atos do procedimento e as ocorrências relevantes, que estará disponível para consulta no site www.comprasnet.go.gov.br.

9.8. O resultado final será disponibilizado no site: www.comprasnet.go.gov.br.

10 – DOS DOCUMENTOS DE HABILITAÇÃO

10.1. A habilitação da Licitante detentora da melhor oferta será verificada ao final da etapa de lances.

10.1.1. A Licitante deverá estar cadastrada no CADFOR – Cadastro de Fornecedor da SUPRILOG – Superintendência de Suprimentos e Logística da Secretaria de Estado de Gestão e Planejamento do Estado de Goiás, com o seu Certificado de Regularidade de Registro Cadastral – CRRC em vigência, compatível com o objeto licitado ou deverá apresentar toda a documentação jurídica e fiscal atualizada e regularizada na própria sessão.

10.2. A Licitante regularmente cadastrada na Superintendência de Suprimentos e Logística da Secretaria de Estado da Gestão e Planejamento – SUPRILOG/SEGPLAN-GO, que apresentar o Certificado de Regularidade de Registro Cadastral – CRRC, devidamente atualizado, fica desobrigada de apresentar os documentos relativos à habilitação jurídica (item 10.3.1), regularidade fiscal (item 10.3.2) e qualificação econômico-financeira (item 10.3.3), desde que os referidos documentos integrantes do Certificado estejam atualizados e em vigência, sendo assegurado o direito de apresentar a documentação que estiver vencida no CRC, atualizada e regularizada na própria sessão.

10.2.1. No caso de não constar no CRC apresentado pela Licitante os respectivos índices de Liquidez Corrente, Liquidez Geral e Solvência Geral, a mesma deverá apresentar a documentação especificada na alínea "a", do item 10.3.3.

10.3. As Licitantes deverão atender obrigatoriamente, quando for o caso, às seguintes exigências:

10.3.1. Habilitação Jurídica

a) Cédula de Identidade e CPF dos sócios, administradores e/proprietários;

b) Registro Comercial, no caso de empresa individual; ou

c) Ato Constitutivo, estatuto ou **contrato social** e suas respectivas alterações (endereço, razão social, etc) devidamente registrados na junta comercial do domicílio da empresa;

d) Certidão expedida pela Junta Comercial comprovando a condição de ME ou EPP (conforme artigo 1º e 8º da Instrução Normativa nº 103 de 30/04/2007 do Departamento Nacional de Registro do Comércio – DNRC):

10.3.2. Regularidade Fiscal e Trabalhista

a) Comprovante de inscrição do CNPJ;

b) Prova de Inscrição no Cadastro de Contribuintes Estadual ou Municipal, se houver relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

c) Prova de quitação com a Fazenda Estadual: Certidão Negativa de Tributos Estaduais, expedida pela Secretaria da Fazenda do Estado de Goiás;

d) Prova de Regularidade com a Fazenda Estadual do domicílio da empresa, na forma da lei;

e) Prova de quitação com a Fazenda Municipal: Apresentar Certidão Negativa de Tributos Mobiliários, expedida pela Secretaria de Finanças Municipal;

f) Prova de Regularidade para com a Fazenda Nacional/Receita Federal: apresentar Certificado Conjunta Negativa de Débitos relativos a Tributos Federais e à Dívida Ativa da União; Certidão Negativa de Débito relativo às contribuições sociais (INSS);

g) Prova de Regularidade de Situação com o Fundo de Garantia por Tempo de Serviço – FGTS;

h) Certidão Negativa de Débitos Trabalhistas – CNDT, junto à Justiça do Trabalho.

10.3.3. Qualificação Econômico-Financeiro

a) Certidão Negativa de Falência e Recuperação judicial, emitida pelo distribuidor da sede da pessoa jurídica, com data de emissão não superior a 60 (sessenta) dias.

b) Qualificação Patrimonial e Demonstrações Contábeis do último exercício social, já exigíveis e apresentados na forma da Lei, que comprovem a boa situação financeira da empresa, vedada sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrados há mais de 03 (três) meses da data de apresentação da proposta;

c) Comprovação de boa situação financeira da empresa através de no mínimo um doa seguintes índices contábeis, o qual deverá ser maior ou igual a 1:

- ILC – Índice de Liquidez Corrente ou,
- ILG – Índice de Liquidez Geral ou,
- GS – Grau de Solvência

ILC =	$\frac{AC}{PC}$	$\frac{\text{Ativo Circulante}}{\text{Passivo Circulante}}$
ILG =	$\frac{AC+RLP}{PC+PNC}$	$\frac{\text{Ativo Circulante+Realizável a Longo Prazo}}{\text{Passivo Circulante+Passivo Não Circulante}}$
GS =	$\frac{AT}{PC+PNC}$	$\frac{\text{Ativo Circulante}}{\text{Passivo Circulante+Passivo Não Circulante}}$

10.3.4. Qualificação Técnica e das Declarações

a) Apresentar atestado de capacidade técnica, fornecido por pessoa jurídica de direito público ou privado, identificação e telefone do emitente, que comprovem o fornecimento e treinamento nos produtos ofertados, conforme termos do Termo de Referência, dos produtos e serviços compatíveis com o objeto desta licitação, devendo

constar o seguinte: fornecimento mínimo de 50% (cinquenta por cento) de unidades de licenças; experiência no fornecimento de serviço de instalação, configuração e treinamento da solução adquirida.

Obs.: O atestado de capacidade técnica fornecido por pessoa jurídica de direito privado deverá ter firma reconhecida, nome completo do signatário e número do cadastro de Pessoa Física, estando as informações ali contidas sujeitas à verificação da sua veracidade.

b) Da Capacitação técnico-profissional:

b.1) O serviço deverá ser prestado por técnicos devidamente qualificados e certificados pelo fabricante dos produtos para executar as atividades compatíveis com as exigências deste edital.

b.2) A licitante deverá comprovar que possui equipe técnica certificada na solução pelo FABRICANTE no momento da apresentação do cronograma de execução dos serviços, para prestação dos serviços de implantação e treinamento.

b.3) A comprovação do vínculo empregatício do Responsável Técnico será feita mediante cópia do Contrato de Trabalho com a empresa, constante da Carteira Profissional ou da Ficha de Registro de Empregados (FRE) ou contrato de Prestação de Serviços.

c) Declaração de que a empresa não se acha declarada inidônea para licitar e contratar com o Poder Público ou suspensa do direito de licitar ou contratar com a Administração Estadual (**Anexo III**);

d) Declaração de que não emprega menor de 18 anos (**Anexo IV**);

e) Declaração I de pleno conhecimento e atendimento aos requisitos exigidos no Edital (**Anexo V**);

f) Declaração II de pleno conhecimento e atendimento aos requisitos exigidos no Edital (**Anexo VI**);

g) Declaração de enquadramento na LC nº 117/2015 (**Anexo VII**).

h) Declaração de Inexistência de Sócios comuns, endereços coincidentes e/ou indícios de parentesco com os licitantes participantes deste procedimento. (**Anexo VIII**).

10.4. Os documentos exigidos para habilitação não contemplados pelo CRRC, bem como a Proposta de Preços atualizada após a fase de lances, deverão ser encaminhados pela Licitante detentora da melhor oferta, de imediato, após a solicitação feita pelo Pregoeiro por fax: (62) 3096-5041 ou e-mail: cpl@agehab.go.gov.br, com posterior encaminhamento do original ou cópia autenticada dos documentos, no prazo máximo de até 05 (cinco) dias úteis após a data de encerramento do Pregão Eletrônico.

10.5. Os documentos extraídos via INTERNET poderão ter seus dados conferidos perante o site correspondente.

10.6. Para microempresa e empresa de pequeno porte, em cumprimento a Lei Complementar nº 147/2014, caso haja alguma restrição na comprovação da regularidade fiscal, será assegurado o prazo de **5 (cinco) dias úteis,** cujo termo inicial corresponderá ao momento em que o proponente for declarado o vencedor do certame, **prorrogável por igual período,** para a regularização da documentação, pagamento ou parcelamento do débito, e emissão de eventuais certidões negativas ou positivas com efeito de certidão negativa.(art. 43, § 1º da LC nº 147/2014)

10.6.1. O tratamento favorecido previsto no item 10.6 somente será concedido se as microempresas e empresas de pequeno porte apresentarem no certame toda a documentação fiscal exigida, mesmo que esta contenha alguma restrição.

10.6.2. O motivo da irregularidade fiscal pendente ficará registrado em ata, bem como a indicação do documento necessário para comprovar a regularização.

10.6.3. A não-regularização da documentação, no prazo previsto no item anterior, implicará decadência do direito à contratação, sem prejuízo das sanções previstas no Artigo 81 da Lei nº 8.666/93, sendo facultado à Administração convocar as Licitantes remanescentes, na ordem de classificação, verificado o atendimento das condições de sua habilitação, para a assinatura do contrato ou revogar a licitação.

10.7. As certidões que não possuírem prazo de validade, somente serão aceitas com data de emissão não superior a 30 (trinta) dias contados da data da emissão do documento.

10.8. Os documentos originais exigidos neste Edital deverão ser enviados em envelope fechado e lacrado contendo os dizeres abaixo descritos no seguinte endereço: RUA 18-A Nº 541, SETOR AEROPORTO, GOIANIA – GOIÁS – CEP: 74.070-060:

Envelope nº 01 – PROPOSTA
Pregão Eletrônico nº 007/2018
Processo nº 2017.01031.006807-53

Envelope nº 02 – DOCUMENTAÇÃO
Pregão Eletrônico nº 007/2018
Processo nº 2017.01031.006807-53

10.9. Os prazos de envio da documentação deverão ser respeitados, sob pena de enquadramento nas sanções previstas no Artigo 7º, da Lei Federal nº 10.520/2002.

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

10.11. O resultado final será disponibilizado nos sites: www.comprasnet.go.gov.br e www.agehab.go.gov.br para intimação e conhecimento dos interessados.

11. DOS PEDIDOS DE ESCLARECIMENTO, PROVIDÊNCIAS E IMPUGNAÇÃO DO ATO CONVOCATÓRIO

11.1. Até 2 (dois) dias úteis antes da data fixada para a abertura da sessão pública, qualquer cidadão ou licitante poderá solicitar esclarecimentos, providências ou impugnar o ato convocatório deste Pregão Eletrônico.

11.2. Os pedidos de esclarecimentos, providências ou impugnação do edital e seus anexos deverão ser encaminhados por escrito ao Pregoeiro na Rua 18-A nº 541, Setor Aeroporto, Goiânia – Goiás, Fone: (62) 3096-5003, Fax: (62) 3096-5003, e-mail: aquilino.macedo@agehab.go.gov.br.

11.2.1. Nos pedidos de esclarecimentos, providências ou impugnação do edital, remetidos ao Pregoeiro, deverá constar, obrigatoriamente, o e-mail do peticionante.

11.2.2. Caberá ao Pregoeiro decidir sobre os pedidos no prazo de 24 (vinte e quatro) horas e encaminhar a resposta ao peticionante por e-mail.

11.3. Acolhida a impugnação do ato convocatório, o Pregoeiro procederá à retificação do edital, e republicação, com devolução dos prazos quando a alteração afetar a formulação das propostas.

12. DOS RECURSOS

12.1. Declarado o vencedor, ao final da sessão, qualquer licitante poderá manifestar, no prazo de até 10 (dez) minutos, a intenção motivada de recorrer da decisão do Pregoeiro, com o registro da síntese de suas razões no campo próprio definido no sistema eletrônico, sendo que a falta de manifestação no prazo concedido importará na decadência do direito de recurso e, consequentemente, na adjudicação do objeto da licitação ao licitante vencedor.

12.2. A intenção motivada de recorrer é aquela que identifica, objetivamente, os fatos e o direito que a licitante pretende que sejam revistos pelo Pregoeiro.

12.3. Ao licitante que manifestar intenção de interpor recurso será concedido o prazo de 03 (três) dias, contados de sua manifestação, para apresentação das razões do recurso, através de formulário próprio do Sistema Eletrônico, ficando as demais licitantes desde logo intimados para apresentar, através de formulário próprio do sistema eletrônico, contrarrazões em igual prazo, que terá inicio no primeiro dia útil subsequente ao do término do prazo do recorrente.

12.4. Somente serão conhecidos os recursos, suas razões e, consequentemente, as contrarrazões, quando interpostos tempestivamente e encaminhados através do sistema eletrônico.

12.5. Caberá ao pregoeiro receber, examinar, instruir e decidir sobre os recursos e, quando mantida a sua decisão, encaminhar os autos ao Presidente da AGEHAB para deliberação.

12.5.1. O exame, a instrução e, em caso de manutenção de sua decisão, o encaminhamento dos recursos ao Presidente da AGEHAB, autoridade competente, para nesse caso, apreciá-los, serão realizados pelo Pregoeiro no prazo de até 3 (três) dias

úteis, podendo este prazo ser dilatado até o dobro, por motivo justo.

12.6. O Presidente da AGEHAB terá prazo de 3 (três) dias úteis para decidir sobre os recursos interpostos, podendo este prazo ser dilatado até o dobro, por motivo justo, devidamente comprovado.

12.7. O acolhimento do recurso pelo Pregoeiro ou pela autoridade competente importará a invalidação apenas dos atos insuscetíveis de aproveitamento.

12.8. A decisão em grau de recurso será definitiva e dela dar-se-á conhecimento às interessadas, através de comunicação por escrito via fax e divulgação nos "sites" pertinentes.

13. DA ADJUDICAÇÃO E DA HOMLOGAÇÃO

13.1. Inexistindo manifestação recursal, o Pregoeiro adjudicará o objeto da licitação ao licitante vencedor, com a posterior homologação do resultado pelo Presidente da AGEHAB.

13.2. Havendo manifestação recursal, após decididos os recursos, o Presidente da AGEHAB adjudicará o objeto ao licitante vencedor e homologará a licitação.

14. DAS CONDIÇÕES DE ASSINATURA, VIGÊNCIA, ALTERAÇÃO E RESCISÃO DO CONTRATO

14.1. Findo o processo licitatório, o licitante vencedor será convocado a assinar o contrato relativo ao objeto do Pregão Eletrônico.

14.2. O não comparecimento do licitante vencedor, injustificadamente, dentro do prazo de 10 (dez) dias após regularmente convocado para assinatura do termo contratual, ensejará, garantido o direito prévio ao contraditório e à ampla defesa.

14.2.1. O impedimento de licitar e contratar com a Administração e descredenciamento junto ao Cadastro de Fornecedores – CADFOR, pelo prazo de até 05 (cinco) anos, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação;

14.2.2. A aplicação de multa de até 10% (dez por cento) sobre o valor do contrato.

14.3. O prazo de convocação poderá ser prorrogado uma vez, por igual período, quando solicitado pela parte durante o seu transcurso e desde que ocorra motivo justificado aceito pela Administração.

14.4. Se o licitante vencedor não apresentar situação regular no ato da assinatura do contrato, ou recursar-se a assiná-lo, o Pregoeiro convocará os licitantes remanescentes, na ordem de classificação, para negociar diretamente com a proponente melhor classificada e, respeitados os procedimentos já definidos neste edital, será declarada a nova adjudicatária do objeto deste Pregão Eletrônico.

14.5. Até a efetiva assinatura do contrato, a proposta do licitante vencedor poderá ser

desclassificada caso da AGEHAB venha ter conhecimento de fato que desabone sua habilitação, conhecido após o julgamento.

14.6. O contrato terá vigência de 12 (doze) meses, a contar da data de sua assinatura.

14.7. O contrato poderá ser rescindido a qualquer tempo, com base nos motivos previstos no art. 77 e 78, na forma dos arts. 79 e 80, da Lei Federal nº 8.666/93, assegurado à **CONTRATADA** o direito ao contraditório e à ampla defesa.

14.8. O contrato poderá ser alterado, com as devidas justificativas, nos casos previstos no art. 65 da Lei Federal nº 8.666/93, sempre por meio de termos aditivos.

14.9. A **CONTRATADA** é obrigada a aceitar nas mesmas condições da licitação, os acréscimos ou supressões que se fizerem no objeto licitado, de até 25% (vinte e cinco por cento) sobre o valor inicial atualizado do contrato, nos termos do § 1º, do art. 65, da Lei Federal nº 8.666/93.

15. DO PRAZO, LOCAL DE ENTREGA E FORMA DE RECEBIMENTO

15.1. Todas as licenças deverão ser registradas em nome da Agência Goiana de Habitação S/A, CNPJ nº 01.274.240/0001-47, tendo como sede a localização na Rua 18-A nº 541, Setor Aeroporto, Goiânia – Goiás, CEP nº 74.070-060.

15.2. A data para efetivo início da execução dos serviços não poderá exceder 15 (quinze) dias depois da publicação do Contrato.

15.3. A entrega será feita de forma única contemplando Licenciamento dos objetos e entrega da documentação.

15.4. Os equipamentos deverão ser entregues até 30 (trinta) dias a contar da publicação do contrato ou instrumento equivalente, à sede da Agência Goiana de Habitação S/A Rua 18 A nº 541, Setor Aeroporto, Goiânia-GO, CEP 74070-060;

15.5. O prazo máximo para entrega do serviço, incluindo licenciamento, instalação, treinamento e Entrega da Documentação, será de no máximo 30 (trinta) dias, contados a partir da data de publicação do contrato.

16. DOS RECURSOS FINANCEIROS, LOCAL DE ENTREGA E PAGAMENTO

16.1. As despesas decorrentes da presente licitação correrá à conta de **Recursos Próprios da AGEHAB.**

16.2. O local de entrega e a forma de pagamento estão definidos no termo de referência e Minuta Contratual.

17. DAS SANÇÕES ADMINISTRATIVAS

17.1. O licitante que, convocado dentro do prazo de validade de sua proposta, não celebrar o contrato, deixar de entregar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução do seu objeto, não mantiver a proposta,

falhar ou fraudar na execução do contrato, comportar-se de modo inidôneo ou cometer fraude fiscal, garantido o direito prévio da ampla defesa, ficará impedido de licitar e contratar com a Administração e será descredenciado junto ao CADFOR, pelo prazo de até 05 (cinco) anos, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, sem prejuízo das multas previstas neste edital e demais cominações legais inclusive advertência.

17.2. A inexecução contratual, inclusive por atraso injustificado na execução do contrato, sujeitará a **CONTRATADA,** além das cominações legais cabíveis, à multa de mora, graduada de acordo com a gravidade de infração obedecidos os seguintes limites máximos:

17.2.1. 10% (dez por cento) sobre o valor do contrato, em caso de descumprimento total da obrigação, inclusive no caso de recusa do adjudicatório em firmar o contrato ou retirar a nota de empenho, dentro de 10 (dez) dias contados da data de sua convocação;

17.2.2. 0,3% (três décimos por cento) ao dia, até o trigésimo dia de atraso, sobre o valor da parte do fornecimento não realizado;

17.2.3. 0,7% (sete décimos por cento) sobre o valor da parte do fornecimento não realizado, por cada dia subsequente ao trigésimo;

17.2.4. O valor da multa será descontado quando dos próximos pagamentos devidos pela AGEHAB em razão da execução do contrato, ou, ainda, quando for o caso, cobrada judicialmente.

17.7. Antes da aplicação de qualquer penalidade, será garantido à **CONTRATADA** a ampla defesa e o contraditório.

18. DA GARANTIA CONTRATUAL

18.1. A CONTRATADA deverá apresentar à AGEHAB, no prazo máximo de até 15 (quinze) dias uteis, contado da data de assinatura do CONTRATO, comprovante de prestação de garantia correspondente ao percentual de 5% (cinco por cento) do valor atualizado do total do contrato, nos termos do art. 56, da Lei nº 8.666, de 1993 e instruções complementares definidas no Edital.

18.2. Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Fazenda.

18.3. Não serão admitidos, como garantia, os títulos da dívida pública, emitidos por pessoas jurídicas de direito público no período de 1850 a 1930, assim como aqueles de duvidosa liquidez, ao critério do CONTRATANTE, além de pedras preciosas, ainda que portadoras de certificado de conformação geológica.

18.4. A garantia, se prestada na forma de fiança bancária ou seguro-garantia, deverá ter validade durante a vigência do contrato.

Agência Goiana de Habitação S/A
Rua 18-A nº 541, Setor Aeroporto - Goiânia - Goiás - 74.070-060 - (62) 3096-5000
Ouvidoria Agehab 3096-5049
Internet: www.agehab.go.gov.br
e-mail ouvidoria@agehab.go.gov.br

18.5. Em se tratando de garantia prestada através de caução em dinheiro, o depósito deverá ser feito obrigatoriamente na Caixa Econômica Federal - CEF, conforme determina o art. 82 do Decreto nº 93872, de 23 de dezembro de 1986, sendo esta devolvida atualizada monetariamente, nos termo do §§ 4º, art. 56, da Lei nº 8.666/93.

18.6. No caso de garantia na modalidade de fiança bancária, deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

18.7. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser readequada nas mesmas condições.

18.8. Se o valor da garantia for utilizado, total ou parcialmente, pela CONTRATANTE, para compensação de prejuízo causado no decorrer da execução contratual por conduta da CONTRATADA, esta deverá proceder à respectiva reposição no prazo de 10 (dez) dias úteis, contados da data em que tiver sido notificada.

18.9. A garantia prestada pela CONTRATADA será liberada, após o término da vigência do Contrato, depois de certificado pelo Gestor deste Contrato que o mesmo foi Totalmente realizado a contento, dentro do prazo de 10 (dez) dias úteis.

19. DAS DISPOSIÇÕES FINAIS

19.1. Este Edital deverá ser lido e interpretado na integra. Após o registro da proposta no sistema, não serão aceitas alegações de desconhecimento.

19.2. A AGEHAB poderá revogar a licitação em face de razões de interesse público, derivadas de fato superveniente devidamente comprovado, pertinente e suficiente para justificar tal conduta, devendo anulá-la por ilegalidade, de oficio ou por provocação de qualquer pessoa, mediante ato escrito e fundamentado.

19.2.1. Da decisão que anular ou revogar a licitação caberá recurso, no prazo de 05 (cinco) dias úteis contados da intimação do ato ou lavratura da ata garantindo aos licitantes o contraditório e a ampla defesa.

19.2.2. A anulação do procedimento licitatório induz à do contrato.

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

19.3. É facultado ao Pregoeiro ou ao Senhor Presidente da AGEHAB, ou autoridade por ele delegada, a promoção de diligência destinada a esclarecer ou complementar a instrução do processo, vedada a inclusão posterior de documento ou informação que deveria constar no ato da Sessão Pública.

19.4. Os licitantes são responsáveis pela fidelidade e legitimidade das informações e dos documentos apresentados em qualquer fase da licitação.

19.5. É vedada a subcontratação, cessão ou transferência no todo ou em parte do objeto

Agência Goiana de Habitação S/A
Rua 18-A nº 541, Setor Aeroporto - Goiânia - Goiás - 74.070-060 - (62) 3096-5000
Ouvidoria Agehab 3096-5049
Internet: www.agehab.go.gov.br
e-mail ouvidoria@agehab.go.gov.br

ora licitado.

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

19.7. Na contagem dos prazos estabelecidos neste Edital e seus anexos, excluir-se-á o dia do inicio e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dia de expediente regular e integral na AGEHAB.

19.8. O desatendimento de exigências formais não essenciais não importará no afastamento do Licitante, desde que seja possível a aferição da sua qualificação e a exata compreensão da sua proposta.

19.8.1. Exigências formais não essenciais são aquelas cujo descumprimento não acarretam irregularidades no procedimento, bem como não importam em vantagens a um ou mais Licitantes em detrimento dos demais.

19.9. As normas que disciplinam este Pregão Eletrônico serão sempre interpretadas em favor da ampliação da disputa entre os interessados, sem comprometimento da segurança do futuro contrato ou instrumento equivalente.

19.10. Havendo divergência entre a descrição do objeto constante no Edital e seus anexos e a descrição do objeto constante nos sites www.comprasnet.go.gov.br e www.agehab.go.gov.br, **prevalecerá, sempre, a descrição deste Edital e seus anexos**.

19.11. É de responsabilidade do licitante o acompanhamento do processo pelos sites www.comprasnet.go.gov.br ou www.agehab.go.gov.br até a data da realização da sessão pública.

20. DO FORO

20.1. O foro para solucionar os litígios decorrentes do presente edital é o da Comarca de Goiânia, Capital do Estado de Goiás, excluído qualquer outro.

21. DOS ANEXOS

ANEXO I - Termo de Referência

ANEXO II – Modelo de carta proposta

ANEXO III – Modelo de Declaração de Inexistência de Fato Superveniente

ANEXO IV – Declaração de Inexistência de Menor Trabalhador

ANEXO V – Declaração I de pleno atendimento aos requisitos de habilitação

ANEXO VI – Declaração II de pleno atendimento aos requisitos de habilitação

ANEXO VII – Declaração de Enquadramento na Lei Complementar nº 117/2015

ANEXO VIII – Declaração de inexistência de sócios comuns.

ANEXO IX – Minuta do Contrato

Goiânia, 06 de abril de 2018.

Aquilino Alves de Macêdo
Pregoeiro

Agência Goiana de Habitação S/A
Rua 18-A nº 541, Setor Aeroporto - Goiânia - Goiás - 74.070-060 - (62) 3096-5000
Ouvidoria Agehab 3096-5049
Internet: www.agehab.go.gov.br
e-mail ouvidoria@agehab.go.gov.br

ANEXO I

TERMO DE REFERÊNCIA

1. OBJETO

1.1. Aquisição de Solução de Proteção ENDPOINT (Antivírus), serviço de implantação e treinamento visando atender as necessidades da AGEHAB, conforme descrição contida no Termo de Referência.

1.2. A licitação deverá ser adjudicada com menor preço GLOBAL

2. JUSTIFICATIVA

2.1. As ameaças virtuais vêm de vários lugares: e-mails, websites suspeitos, pendrives e até mesmo de programas baixados ilegalmente, que muitas vezes trazem consigo malwares, worms, rootkits ou até mesmo os chamados cavalos de troia, que deixam os sistemas da AGEHAB totalmente vulnerável. Quando os computadores corporativos são infectados, isso causa uma grande lentidão da rede, o que diminui a produtividade dos funcionários e abre brechas para o vazamento de informações confidenciais e até mesmo perda de dados.

2.2. A crescente difusão de ameaças tecnológicas tais como vírus de computador e outros malwares, tem causado diversos prejuízos financeiros e a proteção das informações, o bem mais valioso da instituição. Dentre essas ameaças mais recentes temos o **Ransomware**, um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (ransom) para restabelecer o acesso ao usuário. O ransomware pode se propagar de diversas formas, embora as mais comuns sejam através de e-mails com o código malicioso em anexo ou que induzam o usuário a seguir um link ou explorando vulnerabilidades em sistemas que não tenham recebido as devidas atualizações de segurança.

2.3. Antivírus ENDPOINT têm proteção múltipla em vários pontos da rede. Apresentam proteção para desktops, notebooks, smartphones, servidores de arquivos, servidores de e-mail e gateway. Em cada ponto pode haver proteção em vários níveis: para arquivos, e-mail, web, anti-spam, registry, anti-spyware, anti-adware, firewall, controle de aplicações; intrusion detection e controle de portas.

2.4. Antivírus ENDPOINT, consegue realizar intervenção automática para aumentar o rigor das políticas a fim de evitar a disseminação de vírus pela rede.

2.5. Os antivírus ENDPOINT são projetados com o objetivo de proteger as corporações e são, dessa forma, mais adequados para as suas necessidades específicas. Dentre os benefícios que a adoção de tal recurso traz, podemos citar:

2.5.1. Maior rapidez na detecção de vírus e de ameaças virtuais;

2.5.2. Não há sobrecarga dos computadores da empresa por serem mais leves, evitando a lentidão do sistema;

2.5.3. Gestão de processos mais simplificada, já que, a partir de uma mesma tela, é possível proteger todos os computadores, dispositivos móveis e servidores de uma só vez;

2.5.4. Avisos e atualizações automáticas dos programas usados na empresa.

2.5.5. Controle de sites suspeitos, para evitar que sejam acessados e infectem o sistema da empresa;

2.5.6. Restrição do uso de dispositivos móveis (como, por exemplo, pendrives), que podem ser usados nas máquinas e infectar diversos computadores ao mesmo tempo;

2.5.7. Auxílio de suporte técnico em eventuais problemas ou dúvidas que possam aparecer durante o uso do programa.

2.5.8. O parque computacional da AGEHAB é composto aproximadamente por 270 ativos como DeskTop, servidores de rede, Notebook, Tablets e SmartPhones.

2.5.9. Para que sejamos exitosos no combate as ameaças cibernéticas, um fator determinante é a aquisição de uma solução de segurança robusta que atenda todas as exigências essenciais para um ambiente seguro, confiável e com gerenciamento centralizado (ENDPOINT) a todos os ativos da instituição, sejam eles: Servidores de Dados, DeskTop, Notebook, Tablets ou SmartPhones, visto que cada um corresponde a uma porta de entrada de ameaças em potencial.

3. DO LOTE ÚNICO

3.1. A aquisição será realizada em LOTE único, visto que todos os itens compõem uma solução de antivírus com instalação e treinamento tornando-se indivisíveis, sendo de mesma natureza e do mesmo fabricante, constituindo uma solução única e integrada. A licitação em lote único não representa qualquer restrição ou prejuízo a ampla concorrência, uma vez que os canais de vendas autorizados pelos fabricantes de antivírus poderão fornecer todos os itens.

3.2. Considerando a complexidade no gerenciamento e na quantidade de ferramentas necessárias para proteção de segurança da rede de computadores, a contratação dos serviços de treinamento da solução, visa à transferência de conhecimento e/ou uso da solução e na disseminação das ações adotadas por esta instituição. Faz-se necessário por tratar-se de um projeto de padronização amplo e irrestrito.

4. DA QUALIFICAÇÃO TÉCNICA

4.1. O licitante deverá apresentar atestados de capacidade técnica fornecidos por pessoa jurídica de direito público ou privado, identificação e telefone do emitente, que comprovem o fornecimento e treinamento nos produtos ofertados, conforme termos do Termo de Referência, dos produtos e serviços compatíveis com o objeto desta licitação.

4.1.1. Consta no atestado o mínimo de 50% (135) unidade do objeto licitado

4.1.2. Experiência no fornecimento de serviço de instalação, configuração e treinamento da solução adquirida.

4.1.3. O atestado de capacidade técnica fornecidos por pessoa jurídica de direito privado deverá ter firma reconhecida, nome completo do signatário e número do cadastro de Pessoa Física, estando as informações ali contidas sujeitas à verificação da sua veracidade.

4.2. **CAPACITAÇÃO TÉCNICO-PROFISSIONAL**

4.2.1. O serviço deverá ser prestado por técnicos devidamente qualificados e certificados pelo fabricante dos produtos para executar as atividades compatíveis com as exigidas no edital.

Agência Goiana de Habitação S/A
Rua 18-A nº 541, Setor Aeroporto - Goiânia - Goiás - 74.070-060 - (62) 3096-5000
Ouvidoria Agehab 3096-5049
Internet: www.agehab.go.gov.br
e-mail ouvidoria@agehab.go.gov.br

4.2.2. A CONTRATADA deverá comprovar que possui equipe técnica certificada na solução pelo FABRICANTE no momento da apresentação do cronograma de execução dos serviços, para prestação dos serviços de implantação e treinamento.

4.2.3. A comprovação do vínculo empregatício do Responsável Técnico será feita mediante cópia do Contrato de Trabalho com a empresa, constante da Carteira Profissional ou da Ficha de Registro de Empregados (FRE) ou contrato de Prestação de Serviços.

5. DA PROPOSTA DE PREÇO

5.1. A licitante deverá apresentar junto com a proposta de preço:

5.1.1. Portfólio do produto ofertado;

5.1.2. A licitante deverá apresentar Part Numbers (P/N) e Fabricante da solução ofertada, juntamente com sua proposta devidamente assinada.

6. DA DESCRIÇÃO DO OBJETO

Todos os requisitos do objeto licitado descritos nesse item são requisitos mínimos exigidos.

LOTE ÚNICO	
ITEM 01	Licenciamento, manutenção e suporte de Solução de Proteção ENDPOINT (ANTIVIRUS) - por 36 meseS
ITEM 02	Instalação de Solução de Proteção ENDPOINT (ANTIVIRUS)
ITEM 03	Treinamento de Solução de Proteção ENDPOINT (ANTIVIRUS)

6.1.

6.2. Todas as funcionalidades solicitadas deverão ser atendidas por uma única solução/produto, não sendo aceitas composições de soluções;

6.3. As Licenças deverão ser fornecidas através de Download

6.4. Os preços cotados do objeto da presente licitação deverão ser expressos em moeda corrente nacional, neles inclusos os acréscimos e despesas, como impostos, sem inclusão de qualquer encargo financeiro ou previsão inflacionária, sem que sofra correção ou reajuste durante o período licitatório.

6.5. A solução ofertada após a assinatura do contrato, deverá ser a versão mais atual das ferramentas descritas nesse Termo de Refrência;

6.6. **SERVIDOR DE ADMINISTRAÇÃO E CONSOLE ADMINISTRATIVA (COMPATIBILIDADE)**

6.6.1. Microsoft Windows Server 2008 x64 e R2;

6.6.2. Microsoft Windows Small Business Server 2008 (Todas edições);

6.6.3. Microsoft Windows Server 2012 e R2 (Todas edições);

6.6.4. Microsoft Windows Server 2016 R2 (Todas edições);

6.6.5. Microsoft Windows XP Professional SP3 ou superior;

6.6.6. Microsoft Windows XP Professional x64 SP2 ou superior;

6.6.7. Microsoft Windows Vista Business / Enterprise / Ultimate SP1 ou posterior;

6.6.8. Microsoft Windows VistaBusiness / Enterprise / Ultimate SP1 x64 ou posterior

Agência Goiana de Habitação S/A
Rua 18-A nº 541, Setor Aeroporto - Goiânia - Goiás - 74.070-060 - (62) 3096-5000
Ouvidoria Agehab 3096-5049
Internet: www.agehab.go.gov.br
e-mail ouvidoria@agehab.go.gov.br

6.6.9. Microsoft Windows 7 Professional / Enterprise / Ultimate;
6.6.10. Microsoft Windows 7 Professional / Enterprise / Ultimate x64;
6.6.11. Microsoft Windows 8 Professional / Enterprise;
6.6.12. Microsoft Windows 8 Professional / Enterprise x64;
6.6.13. Microsoft Windows 8.1 Professional / Enterprise;
6.6.14. Microsoft Windows 8.1 Professional / Enterprise x64.
6.6.15. Microsoft Windows 10 Professional / Enterprise x64

6.7. **SUPORTA AS SEGUINTES PLATAFORMAS VIRTUAIS:**

6.7.1. VMware: Workstation 9.x, Workstation 10.x, ESXi 5.5, ESXi 6.0 e superior;
6.7.2. Microsoft Hyper-V: 2008, 2008 R2, 2012, 2012 R2 e 2016;
6.7.3. Oracle VM VirtualBox 4.0.4 e Superior (Somente logon como convidado);
6.7.4. Citrix XenServer 6.0 e Superior

6.8. **CARACTERÍSTICAS**

6.8.1. A console deve ser acessada via WEB (HTTPS) ou MMC;

6.8.2. Console deve ser baseada no modelo cliente/servidor;

6.8.3. Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;

6.8.4. Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus;

6.8.5. Console deve ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch management e MDM;

6.8.6. As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração da licença;

6.8.7. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;

6.8.8. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory;

6.8.9. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;

6.8.10. A solução de gerencia deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;

6.8.11. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;

6.8.12. Capacidade de instalar remotamente a solução de segurança em smartphones e tablets de sistema iOS, Android e Windows;

6.8.13. Capacidade de instalar remotamente qualquer “app” em smartphones e tablets de sistema iOS;

Agência Goiana de Habitação S/A
Rua 18-A nº 541, Setor Aeroporto - Goiânia - Goiás - 74.070-060 - (62) 3096-5000
Ouvidoria Agehab 3096-5049
Internet: www.agehab.go.gov.br
e-mail ouvidoria@agehab.go.gov.br

6.8.14. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;

6.8.15. Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os seguintes parâmetros: KB/s e horário;

6.8.16. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus;

6.8.17. Capacidade de gerenciar smartphones e tablets (Windows Phone, Android e iOS) protegidos pela solução de segurança;

6.8.18. Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença econfigurações do produto;

6.8.19. Capacidade de atualizar os pacotes de instalação com as últimas vacinas;

6.8.20. Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes;

6.8.21. A comunicação entre o cliente e o servidor de administração deve ser criptografada;

6.8.22. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;

6.8.23. Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou ENDPOINT instalado utilizando os seguintes parâmetros:

6.8.23.1. Nome do computador;

6.8.23.2. Nome do domínio;

6.8.23.3. Range de IP;

6.8.23.4. Sistema Operacional;

6.8.23.5. Máquina virtual

6.8.24. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;

6.8.25. Deve permitir, por meio da console de gerenciamento, extrair um artefato em quarentena de um cliente sem a necessidade de um servidor ou console de quarentena adicional;

6.8.26. Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção;

6.8.27. Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção;

6.8.28. Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente;

Agência Goiana de Habitação S/A
Rua 18-A nº 541, Setor Aeroporto - Goiânia - Goiás - 74.070-060 - (62) 3096-5000
Ouvidoria Agehab 3096-5049
Internet: www.agehab.go.gov.br
e-mail ouvidoria@agehab.go.gov.br

6.8.29. Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivírus instalado, agrupar todas as máquinas que não receberam atualização nos últimos X dias, etc.;

6.8.30. Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos;

6.8.31. Deve fornecer as seguintes informações dos computadores:

6.8.31.1. Deve fornecer as seguintes informações dos computadores:

6.8.31.2. Se o antivírus está instalado;

6.8.31.3. Se o antivírus está iniciado;

6.8.31.4. Se o antivírus está atualizado;

6.8.31.5. Minutos/horas desde a última conexão da máquina com o servidor administrativo;

6.8.31.6. Minutos/horas desde a última atualização de vacinas;

6.8.31.7. Data e horário da última verificação executada na máquina;

6.8.31.8. Versão do antivírus instalado na máquina;

6.8.31.9. Se é necessário reiniciar o computador para aplicar mudanças;

6.8.31.10. Data e horário de quando a máquina foi ligada;

6.8.31.11. Quantidade de vírus encontrados (contador) na máquina;

6.8.31.12. Nome do computador;

6.8.31.13. Domínio ou grupo de trabalho do computador;

6.8.31.14. Data e horário da última atualização de vacinas;

6.8.31.15. Sistema operacional com Service Pack;

6.8.31.16. Quantidade de processadores;

6.8.31.17. Quantidade de memória RAM;

6.8.31.18. Usuário(s) logado(s) naquele momento, com informações de contato (caso disponível no Active Directory);

6.8.31.19. Endereço IP;

6.8.31.20. Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido;

6.8.31.21. Atualizações do Windows Updates instaladas;

6.8.31.22. Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD;

6.8.31.23. Vulnerabilidades de aplicativos instalados na máquina;

Agência Goiana de Habitação S/A
Rua 18-A nº 541, Setor Aeroporto - Goiânia - Goiás - 74.070-060 - (62) 3096-5000
Ouvidoria Agehab 3096-5049
Internet: www.agehab.go.gov.br
e-mail ouvidoria@agehab.go.gov.br

6.8.32. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;

6.8.33. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:

6.8.33.1. Alteração de Gateway Padrão;

6.8.33.2. Alteração de subrede;

6.8.33.3. Alteração de domínio;

6.8.33.4. Alteração de servidor DHCP;

6.8.33.5. Alteração de servidor DNS;

6.8.33.6. Alteração de servidor WINS;

6.8.33.7. Alteração de subrede;

6.8.33.8. Resolução de Nome;

6.8.33.9. Disponibilidade de endereço de conexão SSL;

6.8.34. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;

6.8.35. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;

6.8.36. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;

6.8.37. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;

6.8.38. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;

6.8.39. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo

6.8.40. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML;

6.8.41. Capacidade de gerar traps SNMP para monitoramento de eventos;

6.8.42. Capacidade de enviar e-mails para contas específicas em caso de algum evento;

6.8.43. Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server;

6.8.44. Deve possuir compatibilidade com Cisco Network AdmissionControl (NAC);

6.8.45. Deve possuir documentação da estrutura do banco de dados para geração de relatórios a partir de ferramentas específicas de consulta (Crystal Reports, por exemplo).

6.8.46. Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação, etc), inclusive de máquinas que estejam em subnets diferentes do servidor;

6.8.47. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);

6.8.48. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;

6.8.49. Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:

6.8.49.1. Nome do vírus;

6.8.49.2. Nome do arquivo infectado;

6.8.49.3. Data e hora da detecção;

6.8.49.4. Nome da máquina ou endereço IP;

6.8.49.5. Ação realizada

6.8.50. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;

6.8.51. Capacidade de realizar inventário de hardware de todas as máquinas clientes;

6.8.52. Capacidade de realizar inventário de aplicativos de todas as máquinas clientes;

6.8.53. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

6.9. **ESTAÇÕES WINDOWS – COMPATIBILIDADE**

6.9.1. Microsoft Windows Embedded 8.0 Standard x64;

6.9.2. Microsoft Windows Embedded 8.1 Industry Pro x64;

6.9.3. Microsoft Windows Embedded Standard 7 x86 / x64 SP1;

6.9.4. Microsoft Windows XP Professional x86 SP3 e superior;

6.9.5. Microsoft Windows Vista x86 / x64SP2 e posterior;

6.9.6. Microsoft Windows 7 Professional/Enterprise/Ultimate x86 / x64 e posterior;

6.9.7. Microsoft Windows 8 Professional/Enterprise x86 / x64;

6.9.8. Microsoft Windows 8.1 Pro / Enterprise x86 / x64 (Todas as Versões);

6.9.9. Microsoft Windows 10 Pro / Enterprise x86 / x64 (Todas as Versões)

6.9.10. **CARACTERÍSTICAS**

6.9.10.1. Deve prover as seguintes proteções:

6.9.10.1.1.1. Deve prover as seguintes proteções:

6.9.10.1.1.2. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc.) que verifique qualquer arquivo criado, acessado ou modificado;

6.9.10.1.1.3. Antivírus de Web (módulo para verificação de sites e downloads contra vírus);

6.9.10.1.1.4. Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);

6.9.10.1.1.5. Antivírus de Mensagens Instantâneas (módulo para verificação de mensagens instantâneas, MSN, por exemplo);

6.9.10.1.1.6. O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;

6.9.10.1.1.7. Firewall com IDS;

6.9.10.1.1.8. Autoproteção (contra-ataques aos serviços/processos do antivírus);

6.9.10.1.1.9. Controle de dispositivos externos;

6.9.10.1.1.10. Controle de acesso a sites por categoria;

6.9.10.1.1.11. Controle de acesso a sites por horário;

6.9.10.1.1.12. Controle de acesso a sites por usuários;

6.9.10.1.1.13. Controle de execução de aplicativos;

6.9.10.1.1.14. Controle de vulnerabilidades do Windows e dos aplicativos instalados;

6.9.10.1.1.15. Controle de vulnerabilidades do Windows e dos aplicativos instalados;

6.9.10.1.1.16. Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

6.9.10.1.1.17. As vacinas devem ser atualizadas pelo fabricante e disponibilizadas aos usuários em no máximo, 02 (duas) em 02 (duas) horas independentemente do nível das ameaças encontradas no período (alta, média ou baixa);

6.9.10.1.1.18. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;

6.9.10.1.1.19. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado

6.9.10.1.1.20. Capacidade de adicionar aplicativos a uma lista de “aplicativos confiáveis”, onde as atividades de rede,

atividades de disco e acesso ao registro do Windows não serão monitoradas;

6.9.10.1.1.21. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);

6.9.10.1.1.22. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

6.9.10.1.1.23. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

6.9.10.1.1.24. Capacidade de verificar somente arquivos novos e alterados;

6.9.10.1.1.25. Capacidade de verificar objetos usando heurística;

6.9.10.1.1.26. Capacidade de agendar uma pausa na verificação;

6.9.10.1.1.27. Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias;

6.9.10.1.1.28. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;

6.9.10.1.1.29. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

6.9.10.1.1.29.1. Perguntar o que fazer, ou bloquear acesso ao objeto;

6.9.10.1.1.30. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

6.9.10.1.1.31. Caso positivo de desinfecção: Restaurar o objeto para uso;

6.9.10.1.1.32. Caso negativo de desinfecção: Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

6.9.10.1.1.33. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;

6.9.10.1.1.34. Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, IMAP, NNTP, SMTP e MAPI, assim como conexões criptografadas (SSL) para POP3 e IMAP (SSL);

6.9.10.1.1.35. Capacidade de verificar tráfego de ICQ, MSN, AIM e IRC contra vírus e links phishings;

6.9.10.1.1.36. Capacidade de verificar links inseridos em e-mails contra phishings;

6.9.10.1.1.37. Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox e Google Chrome, Opera, etc.;

6.9.10.1.1.38. Capacidade de verificação de corpo e anexos de e-mails usando heurística;

6.9.10.1.1.39. O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:

6.9.10.1.1.39.1. Perguntar o que fazer, ou bloquear o e-mail;

6.9.10.1.1.40. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

6.9.10.1.1.41. Caso positivo de desinfecção: Restaurar o e-mail para o usuário;

6.9.10.1.1.42. Caso negativo de desinfecção: Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);

6.9.10.1.1.43. Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena;

6.9.10.1.1.44. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados;

6.9.10.1.1.45. Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador;

6.9.10.1.1.46. Capacidade de verificação de tráfego HTTP e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc.), usando heurísticas;

6.9.10.1.1.47. Deve ter suporte total ao protocolo IPv6;

6.9.10.1.1.48. Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail;

6.9.10.1.1.49. Na verificação de tráfego web, caso encontrado código malicioso o programa deve:

6.9.10.1.1.49.1. Perguntar o que fazer, ou bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;

6.9.10.1.1.49.2. Permitir acesso ao objeto;

6.9.10.1.1.50. O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:

6.9.10.1.1.50.1. Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em temporeal, ou;

6.9.10.1.1.50.2. Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação;

6.9.10.1.1.51. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web;

6.9.10.1.1.52. Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas;

6.9.10.1.1.53. Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa

6.9.10.1.2. Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas;

6.9.10.1.3. Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-PhishingWorkingGroup (http://www.antiphishing.org/);

6.9.10.1.4. Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;

6.9.10.1.5. Deve possuir módulo IDS (IntrusionDetection System) para proteção contra portscans e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas;

6.9.10.1.6. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

6.9.10.1.6.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;

6.9.10.1.6.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo deaplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, coma possibilidade de escolher quais portas e protocolos poderão ser utilizados.

6.9.10.1.7. Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:

6.9.10.1.7.1. Discos de armazenamento locais;

6.9.10.1.7.2. Armazenamento removível;

6.9.10.1.7.3. Impressoras;

6.9.10.1.7.4. CD/DVD;

6.9.10.1.7.5. Drives de disquete;

6.9.10.1.7.6. Modems;

6.9.10.1.7.7. Dispositivos de fita;

Agência Goiana de Habitação S/A
Rua 18-A nº 541, Setor Aeroporto - Goiânia - Goiás - 74.070-060 - (62) 3096-5000
Ouvidoria Agehab 3096-5049
Internet: www.agehab.go.gov.br
e-mail ouvidoria@agehab.go.gov.br

6.9.10.1.7.8. Dispositivos multifuncionais;

6.9.10.1.7.9. Leitores de smartcard;

6.9.10.1.7.10. Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc);

6.9.10.1.7.11. Wi-Fi;

6.9.10.1.7.12. Adaptadores de rede externos;

6.9.10.1.7.13. Dispositivos MP3 ou smartphones;

6.9.10.1.7.14. Dispositivos Bluetooth;

6.9.10.1.7.15. Câmeras e Scanners

6.9.10.1.8. Capacidade de liberar acesso a um dispositivo e usuários por um período de tempo específico, sem a necessidade de desabilitar a proteção e o gerenciamento central ou de intervenção local do administrador na máquina do usuário;

6.9.10.1.9. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário;

6.9.10.1.10. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento;

6.9.10.1.11. Capacidade de configurar novos dispositivos por Class ID/Hardware ID;

6.9.10.1.12. Capacidade de limitar o acesso a sites da internet por categoria, por conteúdo (vídeo, áudio, etc.), com possibilidade de configuração por usuário ou grupos de usuários e agendamento;

6.9.10.1.13. Capacidade de limitar a execução de aplicativos por hash MD5, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto, etc.);

6.9.10.1.14. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;

6.9.10.1.15. Capacidade de limitar o acesso dos aplicativos a recursos do sistema, como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo;

6.9.10.1.16. Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web;

6.9.10.1.17. Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.

6.9.11. **ESTAÇÕES MAC OS X - COMPATIBILIDADE:**

6.9.11.1. Mac OS X 10.11 (El Capitan);

6.9.11.2. Mac OS X 10.10 (Yosemite);

6.9.11.3. Mac OS X 10.9 (Mavericks).

6.9.11.4. Mac OS X 10.8 (Mountain Lion)

6.9.11.5. Mac OS X 10.7 (Lion)

6.9.12. **CARACTERÍSTICAS:**

6.9.12.1. Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware, etc.) que verifique qualquer arquivo criado, acessado ou modificado;

6.9.12.2. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

6.9.12.3. A instalação e primeira execução do produto deve ser feita sem necessidade de reinicialização do computador, de modo que o produto funcione com toda sua capacidade;

6.9.12.4. Deve possuir suportes a notificações utilizando o Growl;

6.9.12.5. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);

6.9.12.6. Capacidade de voltar para a base de dados de vacina anterior;

6.9.12.7. Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas;

6.9.12.8. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da erificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

6.9.12.9. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);

6.9.12.10. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

6.9.12.11. Capacidade de verificar somente arquivos novos e alterados;

6.9.12.12. Capacidade de verificar objetos usando heurística;

6.9.12.13. Capacidade de agendar uma pausa na verificação;

6.9.12.14. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

6.9.12.14.1. Perguntar o que fazer, ou bloquear acesso ao objeto;

6.9.12.15. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

6.9.12.15.1. Caso positivo de desinfecção: Restaurar o objeto para uso;

6.9.12.15.2. Caso negativo de desinfecção: Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

6.9.12.16. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;

6.9.12.17. Capacidade de verificar arquivos de formato de email;

6.9.12.18. Possibilidade de trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, para o antivírus e iniciar o antivírus pela linha de comando;

6.9.12.19. Capacidade de ser instalado, removido e administrado pela mesma console central de gerenciamento.

6.9.13. **ESTAÇÕES DE TRABALHO LINUX - COMPATIBILIDADE (PLATAFORMA 32 E 64 BITS):**

6.9.13.1. Red Hat Enterprise Linux 6.2 Desktop e Superiores;

6.9.13.2. Fedora 16 e Superiores;

6.9.13.3. CentOS-6.2 e Superiores;

6.9.13.4. SUSE Linux Enterprise Desktop 10 SP4 e Superiores;

6.9.13.5. openSUSE Linux 12.2 e Superiores;

6.9.13.6. Debian GNU/Linux 6.0.5 e Superiores;

6.9.13.7. Mandriva Linux 2011 e Superiores;

6.9.13.8. Ubuntu 10.04 LTS e Superiores;

6.9.13.9. CARACTERÍSTICAS - DEVE PROVER AS SEGUINTES PROTEÇÕES:

6.9.13.9.1. Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware, etc.) que verifique qualquer arquivo criado, acessado ou modificado;

6.9.13.9.2. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

6.9.13.9.3. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

6.9.13.9.3.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

6.9.13.9.3.2. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;

6.9.13.9.3.3. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;

6.9.13.9.3.4. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.

6.9.13.9.4. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;

6.9.13.9.5. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

6.9.13.9.6. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

6.9.13.9.7. Capacidade de verificar objetos usando heurística;

6.9.13.9.8. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;

6.9.13.9.9. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

6.9.13.9.10. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux

6.9.14. **SERVIDORES WINDOWS**

6.9.14.1. COMPATIBILIDADE COM PLATAFORMA 32-BITS:

6.9.14.1.1. Microsoft Windows Server 2008 Standard / Enterprise / DataCenter (SP1 ou posterior);

6.9.14.1.2. Microsoft Windows Server 2008 Core Standard / Enterprise / DataCenter (SP1 ou posterior).

6.9.14.2. COMPATIBILIDADE COM PLATAFORMA 64-BITS:

6.9.14.2.1. Microsoft Windows Server 2008 Standard / Enterprise / DataCenter (SP1 ou posterior);

6.9.14.2.2. Microsoft Windows Server 2008 Core Standard / Enterprise / DataCenter (SP1 ou posterior);

6.9.14.2.3. Microsoft Windows Server 2008 R2 Standard / Enterprise / DataCenter (SP1 ou posterior);

6.9.14.2.4. Microsoft Windows Server 2008 R2 Core Standard / Enterprise / DataCenter (SP1 ou posterior);

6.9.14.2.5. Microsoft Windows Storage Server 2008 R2;

6.9.14.2.6. Microsoft Windows Hyper-V Server 2008 R2 (SP1 ou posterior);

6.9.14.2.7. Microsoft Windows Server 2012 Essentials / Standard / Foundation / Datacenter;

6.9.14.2.8. Microsoft Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter;

6.9.14.2.9. Microsoft Windows Server 2012 Core Essentials / Standard / Foundation / Datacenter;

6.9.14.2.10. Microsoft Windows Server 2012 R2 Core Essentials / Standard / Foundation / Datacenter;

6.9.14.2.11. Microsoft Windows Storage Server 2012 (Todas edições);

6.9.14.2.12. Microsoft Windows Storage Server 2012 R2 (Todas edições);

6.9.14.2.13. Microsoft Windows Storage Server 2016 (Todas edições);

6.9.14.2.14. Microsoft Windows Hyper-V Server 2012;

6.9.14.2.15. Microsoft Windows Hyper-V Server 2012 R2

6.9.14.2.16. Microsoft Windows Hyper-V Server 2016

6.9.15. **CARACTERÍSTICAS - DEVE PROVER AS SEGUINTES PROTEÇÕES:**

6.9.15.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc.) que verifique qualquer arquivo criado, acessado ou modificado;

6.9.15.2. Auto-proteção contra-ataques aos serviços/processos do antivírus;

6.9.15.3. Firewall com IDS;

6.9.15.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados;

6.9.15.5. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

6.9.15.6. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

6.9.15.7. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

6.9.15.7.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

6.9.15.7.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação);

6.9.15.7.3. Leitura de configurações;

6.9.15.7.4. Modificação de configurações;

6.9.15.7.5. Gerenciamento de Backup e Quarentena;

6.9.15.7.6. Visualização de relatórios;

6.9.15.7.7. Gerenciamento de relatórios;

6.9.15.7.8. Gerenciamento de chaves de licença;

6.9.15.7.9. Gerenciamento de permissões (adicionar/excluir permissões acima);

6.9.15.8. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

6.9.15.8.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;

6.9.15.9. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;

6.9.15.10. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

6.9.15.11. Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total;

6.9.15.12. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc.);

6.9.15.13. Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (uninterruptible Power supply – UPS);

6.9.15.14. Em caso de erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares;

6.9.15.15. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor;

6.9.15.16. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;

6.9.15.17. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas;

6.9.15.18. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;

6.9.15.19. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

6.9.15.20. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

6.9.15.21. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

6.9.15.22. Capacidade de verificar somente arquivos novos e alterados;

6.9.15.23. Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários, etc.);

6.9.15.24. Capacidade de verificar objetos usando heurística;

6.9.15.25. Capacidade de configurar diferentes ações para diferentes tipos de ameaças;

6.9.15.26. Capacidade de agendar uma pausa na verificação;

6.9.15.27. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;

6.9.15.28. 3.2.5.3.23. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

6.9.15.28.1. Perguntar o que fazer, ou boquear acesso ao objeto;

6.9.15.29. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

6.9.15.30. Caso positivo de desinfecção: Restaurar o objeto para uso;

6.9.15.31. Caso negativo de desinfecção: Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

6.9.15.32. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;

6.9.15.33. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;

6.9.15.34. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

6.9.15.35. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.

6.9.16. **SERVIDORES LINUX**

6.9.16.1. COMPATIBILIDADE PLATAFORMA 64-BITS:

6.9.16.1.1. Red Hat Enterprise Linux Server 7 e Superiores;

6.9.16.1.2. CentOS-7.0 e Superiores;

6.9.16.1.3. SUSE Linux Enterprise Server 12 e Superiores;

6.9.16.1.4. Novell Open Enterprise Server 11 SP2 e Superiores;

6.9.16.1.5. Ubuntu Server 14.04 LTS e Superiores;

6.9.16.1.6. Ubuntu Server 14.10 e Superiores;

6.9.16.1.7. Oracle Linux 6.5 e Superiores;

6.9.16.1.8. Debian GNU/Linux 7.5, 7.6, 7.7 e Superiores;

6.9.16.1.9. openSUSE® 13.1 e Superiores

6.9.16.2. CARACTERÍSTICAS - DEVE PROVER AS SEGUINTES PROTEÇÕES:

6.9.16.2.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique ualquer arquivo criado, acessado ou modificado;

6.9.16.2.2. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

6.9.16.2.3. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

6.9.16.2.3.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

6.9.16.2.3.2. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;

6.9.16.2.3.3. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;

6.9.16.2.3.4. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados;

6.9.16.2.3.5. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;

6.9.16.2.3.6. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento

6.9.16.2.3.7. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se fo passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

6.9.16.2.3.8. Capacidade de verificar objetos usando heurística;

6.9.16.2.3.9. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;

6.9.16.2.3.10. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados

6.9.16.2.3.11. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux)

6.9.17. **SMARTPHONES E TABLETS – COMPATIBILIDADE**

6.9.17.1. Apple iOS 7.0 – 8.X;

6.9.17.2. Windows Phone 8.1;

6.9.17.3. Android OS 2.3 – 5.1

6.9.17.4. CARACTERÍSTICAS - DEVE PROVER AS SEGUINTES PROTEÇÕES:

6.9.17.4.1. Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:

6.9.17.4.1.1. Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:

6.9.17.4.2. Deverá isolar em área de quarentena os arquivos infectados;

6.9.17.4.3. Deverá atualizar as bases de vacinas de modo agendado;

6.9.17.4.4. Deverá bloquear spams de SMS através de Black lists;

6.9.17.4.5. Deverá ter função de bloqueio do aparelho caso o SIM CARD for trocado para outro não autorizado;

6.9.17.4.6. Capacidade de desativar por política: Wi-fi, Câmera, Bluetooth.

6.9.17.4.7. Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo;

6.9.17.4.8. Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha;

6.9.17.4.9. Deverá ter firewall pessoal (Android);

6.9.17.4.10. Capacidade de tirar fotos quando a senha for inserida incorretamente;

6.9.17.4.11. Possibilidade de instalação remota utilizando o Microsoft System Center Mobile Device Manager 2008 SP1;

6.9.17.4.12. Capacidade de enviar comandos remotamente de:

6.9.17.4.12.1. Localizar;

6.9.17.4.12.2. Bloquear.

6.9.17.4.13. Capacidade de detectar Jailbreak em dispositivos iOS;

6.9.17.4.14. Capacidade de bloquear o acesso a site por categoria em dispositivos;

6.9.17.4.15. Capacidade de bloquear o acesso a sites phishing ou malicioso;

6.9.17.4.16. Capacidade de criar containers de aplicativos, separando dados corporativos de dadospessoais;

6.9.17.4.17. Capacidade de bloquear o dispositivo quando o cartão "SIM" for substituído;

6.9.17.4.18. Capacidade de configurar White e blacklist de aplicativos;

6.9.17.4.19. Capacidade de localizar o dispositivo quando necessário;

6.9.17.4.20. Permitir atualização das definições quando estiver em "roaming";

6.9.17.4.21. Capacidade de selecionar endereço do servidor para buscar a definição de vírus

6.9.17.4.22. Capacidade de enviar URL de instalação por e-mail;

6.9.17.4.23. Capacidade de fazer a instalação através de um link QRCode;

6.9.17.4.24. Capacidade de executar as seguintes ações caso a desinfecção falhe:

6.9.17.4.24.1. Deletar;

6.9.17.4.24.2. Ignorar;

6.9.17.4.24.3. Quarentenar;

6.9.17.4.24.4. Perguntar ao usuário

6.9.17.5. GERENCIAMENTO DE DISPOSITIVOS MÓVEIS (MDM) - COMPATIBILIDADE:

6.9.17.5.1. Dispositivos conectados através do Microsoft Exchange ActiveSync:

6.9.17.5.2. Apple iOS;

6.9.17.5.3. Windows Phone;

6.9.17.5.4. Android.

6.9.17.5.5. Dispositivos com suporte ao Apple PushNotification (APNs).

6.9.17.5.6. Apple iOS 3.0 ou superior.

6.9.17.5.7. CARACTERÍSTICAS:

6.9.17.5.7.1. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange;

6.9.17.5.7.2. Capacidade de ajustar as configurações de:

6.9.17.5.7.3. Sincronização de e-mail;

6.9.17.5.7.4. Uso de aplicativos;

6.9.17.5.7.5. Senha do usuário;

6.9.17.5.7.6. Criptografia de dados;

6.9.17.5.7.7. Conexão de mídia removível.

6.9.17.5.7.8. Capacidade de instalar certificados digitais em dispositivos móveis;

6.9.17.5.7.9. Capacidade de, remotamente, resetar a senha de dispositivos iOS;

6.9.17.5.7.10. Capacidade de, remotamente, apagar todos os dados de dispositivos iOS;

6.9.17.5.7.11. Capacidade de, remotamente, bloquear um dispositivo iOS.

6.9.18. **CRIPTOGRAFIA - COMPATIBILIDADE:**

6.9.18.1. Microsoft Windows Vista Business/Enterprise/ultimate sp2;

6.9.18.2. Microsoft Windows Vista Business/Enterprise/ultimate x64 sp2;

6.9.18.3. Microsoft Windows 7 Professional/Enterprise/ultimate;

6.9.18.4. Microsoft Windows 7 Professional/Enterprise/ultimate x64;

6.9.18.5. Microsoft Windows 8 Professional/Enterprise;

6.9.18.6. Microsoft Windows 8 Professional/Enterprise x64;

6.9.18.7. Microsoft Windows 8.1 Professional / Enterprise;

6.9.18.8. Microsoft Windows 8.1 Professional / Enterprise x64;

6.9.18.9. Microsoft Windows 10 Pro x86 / x64;

6.9.18.10. Microsoft Windows 10 Enterprise x86 /x64

6.9.18.11. CARACTERÍSTICAS:

6.9.18.11.1. O acesso ao recurso criptografado (arquivo, pasta ou disco) deve ser garantido mesmo em caso o usuário tenha esquecido a senha, através de procedimentos de recuperação;

6.9.18.11.2. Utilizar, no mínimo, algoritmo AES com chave de 256 bits;

6.9.18.11.3. Deve ter a capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário;

6.9.18.11.4. Deve ter a capacidade de utilizar single sign-on para a autenticação de pré-boot;

6.9.18.11.5. Permitir criar vários usuários de autenticação pré-boot;

6.9.18.11.6. Deve ter a capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento;

6.9.18.11.7. Deve ter a capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:

6.9.18.11.7.1. Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;

6.9.18.11.7.2. Criptografar todos os arquivos individualmente;

6.9.18.11.7.3. Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;

6.9.18.11.7.4. Criptografar o dispositivo removível, em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;

6.9.18.11.8. Deve ter a capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente. Nesta modalidade, os arquivos devem estar acessíveis para todas as máquinas gerenciadas pela mesma console de maneira transparente para os usuários;

6.9.18.11.9. Deve ter a capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;

6.9.18.11.10. Deve ter a capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados;

6.9.18.11.11. Verificar compatibilidade de hardware antes de aplicar a criptografia;

6.9.18.11.12. Deve ter a capacidade de estabelecer parâmetros para a senha de criptografia;

6.9.18.11.13. Bloquear o reuso de senhas;

6.9.18.11.14. Bloquear a senha após um número de tentativas pré-estabelecidas;

6.9.18.11.15. Deve ter a capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;

6.9.18.11.16. Permitir criar exclusões para não criptografar determinados “discos rígidos” através de uma busca por nome do computador ou nome do dispositivo;

6.9.18.11.17. Permitir criptografar as seguintes pastas pré-definidas: “meus documentos”, “favoritos”, “desktop”, “arquivos temporários” e “arquivos do outlook”;

6.9.18.11.18. Permitir utilizar variáveis de ambiente para criptografar pastas customizadas;

6.9.18.11.19. Deve ter a capacidade de criptografar arquivos por grupos de extensão, tais como: documentos do office, documentos .txt, arquivos de áudio, etc.;

6.9.18.11.20. Permitir criar um grupo de extensões de arquivos a serem criptografados;

6.9.18.11.21. Deve ter a capacidade de criar regra de criptografia para arquivos gerados por aplicações;

6.9.18.11.22. Permitir criptografia de dispositivos móveis mesmo quando o Endpoint não possuir comunicação com a console de gerenciamento

6.9.19. Gerenciamento de Sistemas

6.9.19.1. Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis;

6.9.19.2. Capacidade de corrigir as vulnerabilidades de softwares, fazendo o download centralizado da correção ou atualização e aplicando essa correção ou atualização nas máquinas gerenciadas de maneira transparente para os usuários;

6.9.19.3. Capacidade de gerenciar licenças de softwares de terceiros;

6.9.19.4. Capacidade de registrar mudanças de hardware nas máquinas gerenciadas;

6.9.19.5. Capacidade de gerenciar um inventário de hardware, com a possibilidade de cadastro de dispositivos (ex: router, switch, projetor, acessório, etc), informando data de compra, local onde se encontra, servicetag, número de identificação e outros;

6.9.19.6. Possibilita fazer distribuição de software de forma manual e agendada;

6.9.19.7. Suporta modo de instalação silenciosa;

6.9.19.8. Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;

6.9.19.9. Possibilita fazer a distribuição através de agentes de atualização;

6.9.19.10. Utiliza tecnologia multicast para evitar tráfego na rede;

6.9.19.11. Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;

6.9.19.12. Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no c

6.9.19.13. Capacidade de gerar relatórios de vulnerabilidades e patches;

6.9.19.14. Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administraçã

6.9.19.15. Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;

6.9.19.16. Permite baixar atualizações para o computador sem efetuar a instalação

6.9.19.17. Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atua

6.9.19.18. Capacidade de instalar correções de vulnerabilidades de acordo com a severidade;

6.9.19.19. Permite selecionar produtos a serem atualizados pela console de gerenciamento;

6.9.19.20. Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc.

7. DA GARANTIA

7.1. GARANTIA TÉCNICA

7.1.1. Os objetos deverão possuir garantia técnica mínima de 36 meses, sob a responsabilidade do fornecedor. O fornecedor deverá disponibilizar assistência técnica no período da garantia técnica.

7.2. ASSISTÊNCIA TÉCNICA

7.2.1. Todas as licenças de software utilizadas para atender o objeto deverão possuir garantia de 36 (trinta e seis) meses.

7.2.2. A LICITANTE vencedora deverá prestar suporte técnico e operacional durante o período de vigência da licença, com atendimento através do serviço telefônico, acesso remoto, e-mail ou WEB, para esclarecimento de dúvidas, abertura de chamados, e envio de arquivos para análise (Zero-day).

7.2.3. Os prazos relativos aos chamados deverão obedecer ao seguinte nível mínimo de serviço: 8 x 5 (oito horas por dia, cinco dias por semana em dias úteis e no horário comercial).

7.2.4. **O SERVIÇO DE SUPORTE TÉCNICO GARANTE:**

7.2.4.1. Reinstalação, reconfiguração, e auxilio na utilização de recursos ou solução de problemas relacionados aos sistemas ofertados

7.2.4.2. O direito de receber toda e qualquer atualização de todos os softwares ou patches corretivos de componentes adquiridas após a assinatura do contrato, para a versão mais atual das ferramentas.

7.2.4.3. A CONTRATADA deverá prestar atendimento técnico em regime de garantia.

8. DO PRAZO, LOCAL DE ENTREGA E FORMA DE RECEBIMENTO

8.1. Todas as licenças deverão ser registradas em nome do Agência Goiana de Habitação S/A, CNPJ: 01.274.240/0001-47, tendo como sede a localização na Rua 18 A nº 541 – Setor Aeroporto – Goiânia-GO, CEP: 74.070-060.

8.2. A data para efetivo início da execução dos serviços não poderá exceder 15 (quinze) dias depois de publicação do Contrato.

8.3. A entrega será feita de forma única contemplando Licenciamento dos objetos e Entrega da Documentação.

8.4. Os equipamentos deverão ser entregues em até 30 (trinta) dias a contar da publicação do contrato ou instrumento equivalente, à cede da Agência Goiana de Habitação S/A Rua 18 A nº 541, Setor Aeroporto, Goiânia-GO, CEP 74070-060;

8.5. O prazo máximo para entrega do serviço, incluindo licenciamento, instalação, treinamento e Entrega da Documentação, será de no máximo 30 (trinta) dias, contados a partir da data de publicação do contrato.

9. DA EXECUÇÃO

9.1. Licenciamento e Instalação da solução:

9.1.1. A instalação e configuração deve ser implementada On-site conforme cenário fornecido pela Agência Goiana de Habitação S/A após a emissão e recebimento da assinatura do contrato.

9.1.2. A empresa CONTRATADA deverá realizar toda a instalação da solução adquirida e quaisquer outras providências que tenham relação direta com a instalação do serviço em questão.

9.1.3. Criar senha de acesso com privilégio administrativo para a AGEHAB.

9.1.4. Após a assinatura do contrato, a CONTRATADA deverá apresentar, no prazo máximo de 10 (dez) dias, os requisitos de infraestrutura para instalação da solução, o Plano de instalação, testes e ativação incluindo o Cronograma Detalhado de Execução dos Serviços, prevendo as datas de início e término da instalação de todos os licenciamentos.

9.1.5. O Cronograma da CONTRATADA deverá ser submetido à Gerência de Tecnologia da Informação (GETI) da AGEHAB, observado o respectivo serviço e somente será válido após aprovação. Depois de validado, a Contratada será notificada para dar início à execução do cronograma aprovado pela GETI - AGEHAB.

9.1.6. O fornecedor deverá entregar a solução instalada e customizada de acordo com os padrões fornecidos pela equipe técnica da Gerência de Tecnologia da Informação (GETI).

9.2. **TREINAMENTO (REPASSE TECNOLÓGICO)**

9.2.1. O treinamento abordará no mínimo: o uso da ferramenta, instalação, configuração, backup e restauração de configuração, gerenciamento, resolução de problemas e procedimentos de isolamento de rede em caso de infecção.

9.2.2. O treinamento deverá contemplar todos os recursos e configurações existentes na solução ofertada.

9.2.3. A AGEHAB se encarregará de disponibilizar as instalações físicas para a realização do treinamento, tais como: projetores, tela para apresentação, computador, mesas e poltronas.

9.2.4. É de responsabilidade da CONTRATADA todo material audiovisual, didático e eletrônico para a realização dos treinamentos, além de impressos e quaisquer outras despesas diretas ou indiretas.

9.2.5. O treinamento será com uma turma de até 05 (cinco) alunos e o treinamento será realizado nas dependências da AGÊNCIA GOIANA DE HABITAÇÃO S/A, que irá ceder uma sala para sua realização.

Agência Goiana de Habitação S/A
Rua 18-A nº 541, Setor Aeroporto - Goiânia - Goiás - 74.070-060 - (62) 3096-5000

9.2.6. O treinamento deverá ser organizado em módulos e suas ementas e conteúdos programáticos devem ser previamente disponibilizados a AGEHAB para aprovação.

9.2.7. O material didático será fornecido em português, pela contratada, abordando todos os tópicos do curso;

9.2.8. Os treinamentos deverão ser realizados em dias úteis e não poderão exceder carga horária diária de 8 (oito) horas. Os horários e datas dos treinamentos serão definidos pela equipe técnica da AGEHAB e comunicados a contratada com antecedência de 10 (dez) dias consecutivos.

10. DAS OBRIGAÇÕES DA CONTRATADA

10.1. Além das resultantes da Lei 8.666/93 a adjudicatária se obriga, nos termos deste Termo de Referência, a:

10.1.1. Prestar todos os esclarecimentos que forem solicitados pela fiscalização da contratante;

10.1.2. Manter durante toda a execução do termo respectivo, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na contratação;

10.2. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com os artigos 14 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);

10.3. Manter atualizados, durante a vigência do contrato, para fins de pagamento, a Certidão Negativa de Débito – CND de Débito Trabalhista-CNDT, o Certificado de Regularidade - CRF do FGTS e certidão de regularidade junto à Fazenda Federal e municipal;

10.4. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do Contrato, observando o preconizado neste Termo de Referência.

10.5. **São expressamente vedadas à CONTRATADA**:

10.5.1. Ceder, sob qualquer forma, os créditos oriundos deste contrato a terceiros;

10.6. Os funcionários da CONTRATADA, responsáveis pela instalação do serviço e treinamento aos colaboradores da Gerência de Tecnologia da Informação - GETI, deverão estar devidamente identificados com crachá e/ou outros identificadores quando nas instalações da AGEHAB.

10.7. Ficarão por conta da Contratada as possíveis despesas de transporte e hospedagem necessárias à execução do objeto

10.8. Refazer, às suas expensas, todo e qualquer trabalho realizado em desconformidade com as determinações da AGEHAB ou, ainda, os que apresentarem defeitos, vícios ou incorreções.

10.9. Manter, durante a vigência do Contrato, todas as condições de habilitação e qualificação técnica apresentadas no processo licitatório, compatíveis com as obrigações assumidas neste Contrato.

10.10. Utilizar empregados habilitados e com conhecimentos compatíveis com os necessários para executar os serviços que lhes forem atribuídos, em conformidade com as normas e determinações em vigor.

10.11. Responder inteiramente por todos os encargos trabalhistas, previdenciários, fiscais, comerciais, seguro de acidentes, impostos e quaisquer outros que forem devidos e referentes aos serviços oriundos da contratação

Agência Goiana de Habitação S/A
Rua 18-A nº 541, Setor Aeroporto - Goiânia - Goiás - 74.070-060 - (62) 3096-5000

Internet: www.agehab.go.gov.br
e-mail ouvidoria@agehab.go.gov.br

10.12. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do Contrato, observando o preconizado neste Termo de Referência.

11. DAS OBRIGAÇÕES DA CONTRATANTE

11.1. Prestar as informações e os esclarecimentos pertinentes que venham a ser solicitados pelos empregados da contratada ou por seu preposto;
11.2. Fornecer de toda a infraestrutura necessária para instalação e funcionamento dos equipamentos, como local físico, tomadas elétricas, pontos de acesso à rede, etc.
11.3. Efetuar o pagamento conforme execução dos serviços/produtos, desde que cumpridas todas as formalidades e exigências do contrato;
11.4. Exercer a fiscalização do contrato;
11.5. Comunicar oficialmente à contratada quaisquer falhas verificadas no cumprimento do contrato;
11.6. Convocar reunião inicial, quando necessário, com todos os envolvidos na contratação; e acompanhar e monitorar toda a execução dos serviços.

12. DO LOCAL DE ENTREGA

12.1. Todos produtos licitados serão entregues na sede da Agência Goiana de Habitação S/A - AGEHAB, situadas na Rua 18 A nº 541 – Setor Aeroporto – Goiânia – GO – CEP 74070-060.
12.2. A proposta comercial deverá considerar todos os custos relativos a logística e entrega dos equipamentos na cidade de Goiânia – GO.

13. DA VIGÊNCIA

13.1. O contrato terá um prazo de 12 (doze) meses.
13.2. Na hipótese da adjudicatária não comparecer para assinar o Contrato no prazo estipulado, sem prejuízo das sanções previstas neste Edital, será convocada licitante remanescente, na ordem de classificação, para fazê-lo em igual prazo e nas mesmas condições da sua proposta.

14. DO PAGAMENTO

14.1. O pagamento do item licitado será procedido mediante a apresentação da Nota Fiscal/Fatura, após o fechamento do mês e a quitação até o 10 (décimo) dia útil do mês seguinte.
14.2. As nota(s) fiscal (is)/faturas deverão conter no mínimo os seguintes dados:
14.3. Data de emissão
14.4. Estar endereçada a Agência Goiana de Habitação - AGEHAB, situada a Rua 18-A nº 541, Setor Aeroporto - Goiânia/GO, CNPJ nº 01.274.240/0001-47;
14.5. Preços unitários;
14.6. Descrição do item licitado conforme **ANEXO I - MODELO DE CARTA PROPOSTA**
14.7. O pagamento será efetuado após atesta pela autoridade competente assim como das respectivas requisições da AGEHAB, desde que a Certidão Negativa de Débito – CND, o Certificado de Regularidade do FGTS – CRF, a prova de regularidade para com a Fazenda Federal e municipal

14.8. Na ocorrência da rejeição de nota fiscal/fatura, motivada por erro ou incorreções, o prazo estipulado no subitem 12.1 passará a ser contado a partir da data da sua reapresentação, examinadas as causas da recusa;

15. DA GARANTIA DO CONTRATO

15.1. A CONTRATADA deverá apresentar à AGEHAB, no prazo máximo de até 15 (quinze) dias uteis, contado da data de assinatura do CONTRATO, comprovante de prestação de garantia correspondente ao percentual de 5% (cinco por cento) do valor atualizado do total do contrato, nos termos do art. 56, da Lei nº 8.666, de 1993 e instruções complementares definidas no Edital.

15.2. Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Fazenda.

15.3. Não serão admitidos, como garantia, os títulos da dívida pública, emitidos por pessoas jurídicas de direito público no período de 1850 a 1930, assim como aqueles de duvidosa liquidez, ao critério do CONTRATANTE, além de pedras preciosas, ainda que portadoras de certificado de conformação geológica;

15.4. A garantia, se prestada na forma de fiança bancária ou seguro-garantia, deverá ter validade durante a vigência do contrato.

15.5. Em se tratando de garantia prestada através de caução em dinheiro, o depósito deverá ser feito obrigatoriamente na Caixa Econômica Federal - CEF, conforme determina o art. 82 do Decreto nº 93872, de 23 de dezembro de 1986, sendo esta devolvida atualizada monetariamente, nos termo do §§ 4º, art. 56, da Lei nº 8.666/93.

15.6. No caso de garantia na modalidade de fiança bancária, deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

15.7. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser readequada nas mesmas condições.

15.8. Se o valor da garantia for utilizado, total ou parcialmente, pela CONTRATANTE, para compensação de prejuízo causado no decorrer da execução contratual por conduta da CONTRATADA, esta deverá proceder à respectiva reposição no prazo de 10 (dez) dias úteis, contados da data em que tiver sido notificada.

15.9. A garantia prestada pela CONTRATADA será liberada, após o término da vigência do Contrato, depois de certificado pelo Gestor deste Contrato que o mesmo foi Totalmente realizado a contento, dentro do prazo de 10 (dez) dias úteis.

16. DA ESTIMATIVA DE PREÇOS

16.1. Os respectivos valores unitários de referência para cada item constam do quadro abaixo e foram extraídos da pesquisa mercadológica.

ITEM	DESCRIÇÃO	UND.	QTD	PREÇO UNIT	PREÇO TOTAL
1	Licenciamento, manutenção e suporte da Solução de Proteção ENDPOINT (ANTIVIRUS) - por 36 meses.	UND	270	R$ 242,70	R$ 65.358,90

2	Instalação de Solução de Proteção ENDPOINT (ANTIVIRUS)	UST	20	R$ 191,07	R$ 3.821,40
3	Treinamento de Solução de Proteção ENDPOINT (ANTIVIRUS)	UST	20	R$ 191,07	R$ 3.821,40
		TOTAL ESTIMADO			**73.001,70**

Agência Goiana de Habitação S/A
Rua 18-A nº 541, Setor Aeroporto - Goiânia - Goiás - 74.070-060 - (62) 3096-5000
Ouvidoria Agehab 3096-5049
Internet: www.agehab.go.gov.br
e-mail ouvidoria@agehab.go.gov.br

ANEXO II

MODELO DE CARTA PROPOSTA

Dados da empresa:
Razão Social: CNPJ: Endereço completo: Fone/Fax:
E-mail:

Proposta que faz a empresa _____, CNPJ nº_____, aquisição do produto conforme as especificações contidas no edital nº 007/2018.

LOTE ÚNICO

ITEM	DESCRIÇÃO	UND.	QTD	PREÇO UNIT	PREÇO TOTAL
1	Licenciamento, manutenção e suprote de Solulção de Proteção ENDPOINT (ANTIVIRUS) - por 36 meses.	UND	270	R$ -	R$ -
2	Instalçao de Solução de Proteção ENDPOINT (ANTIVIRUS)	UST	20	R$ -	R$ -
3	Treinamento de Solução de Proteção ENDPOINT (ANTIVIRUS)	UST	20	R$ -	R$ -
		VALOR TOTAL			

Condições gerais da Proposta:
Validade da Proposta:
Prazo e Local de entrega: Rua 18-A n541 Setor Aeroporto – Goiãnia-GO CEP 74.070-060
Condições de pagamento:
Das Declarações:
→ Declaração expressa, de que seus empregados são regidos pela legislação trabalhista vigente (consolidação das Leis de Trabalho - CLT), em cumprimento ao Termo de Conciliação Judicial;
→ Declaração expressa de estarem incluídos nos preços propostos todos os, Impostos e encargos devidos, bem como, quaisquer outras despesas, diretas e indiretas, incidentes no fornecimento do material/serviço.

....., ... de ..... 2018.

_____
assinatura e carimbo
(Representante Legal)

ANEXO III

MODELO DE DECLARAÇÃO DE INEXISTÊNCIA DE FATO SUPERVENIENTE

À
COMISSÃO PERMANENTE DE LICITAÇÃO DA
AGÊNCIA GOIANA DE HABITAÇÃO S/A – AGEHAB
REFERENTE: PREGÃO ELETRÔNICO Nº 007/2018

_____, CNPJ _____(Nome e CNPJ da empresa), sediada na _____**(endereço completo)** declara, sob as penas da lei, que até a presente data inexistam fatos impeditivos para sua habilitação no presente processo licitatório, ciente da obrigatoriedade de declarar ocorrências posteriores.

_____, _____ de _____ de 2018.

_____
(Nome completo do declarante)
(Nº da CI do declarante)

ANEXO IV

MODELO DE DECLARAÇÃO DE INEXISTÊNCIA DE MENOR TRABALHADOR

À
COMISSÃO PERMANENTE DE LICITAÇÃO DA
AGÊNCIA GOIANA DE HABITAÇÃO S/A – AGEHAB
REFERENTE: PREGÃO ELETRÔNICO Nº 007/2018

(Nome da Empresa) _____, **(CNPJ da empresa)** _____, sediada na _____ (endereço completo) por intermédio de seu representante legal o (a) Sr(a) _____ portador(a) da carteira de identidade nº _____ e do CPF nº _____, DECLARA, para fins do disposto no inciso V do art. 27 da Lei nº 8.666, de 21 de junho de 1993, acrescido pela Lei nº 9.854/99, regulamentada pelo Decreto nº 4.358/202, que não emprega menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 (dezesseis) anos.

Ressalva: emprega menor, a partir de 14 (quatorze) anos na condição de aprendiz:
SIM ( ) NÃO ( )

_____, _____ de _____ de 2018.

_____
(Nome e nº da Identidade do declarante)

ANEXO V

DECLARAÇÃO DE PLENO ATENDIMENTO AOS REQUISITOS DE HABILITAÇÃO

A
AGÊNCIA GOIANA DE HABITAÇÃO S/A
Rua 18-A nº 541, Setor Aeroporto
Goiânia - GO

Declaramos, sob as penas da Lei, conhecer e aceitar as condições constantes do Pregão Eletrônico nº 007/2018 e seus anexos e que atendemos plenamente aos requisitos necessários para a habilitação.

....., ... de ..... 2018.

_____

Nome / Assinatura do Representante Legal

Cargo:

PREENCHIDA EM PAPEL TIMBRADO DA EMPRESA E ASSINADA POR SEUS REPRESENTANTES LEGAIS OU PROCURADOR (es) DEVIDAMENTE HABILITADO (s)

ANEXO VI

DECLARAÇÃO DE PLENO ATENDIMENTO AOS REQUISITOS DE HABILITAÇÃO

Ref: Pregão Eletrônico nº 007/2018

.....,inscrito no CNPJ n.º....., por intermédio de seu representante legal o(a) Sr. (a)....., portador da Carteira de Identidade n.º ..... DECLARA, sob as penas da lei, em especial o art. 299 do código penal brasileiro, que é fornecedora de bens e serviço de informática .

Declara, ainda, que apresentará os documentos comprobatórios do disposto acima na etapa de habilitação da empresa.

_____

(Data)

_____

(Representante Legal)

Agência Goiana de Habitação S/A
Rua 18-A nº 541, Setor Aeroporto - Goiânia - Goiás - 74.070-060 - (62) 3096-5000
Ouvidoria Agehab 3096-5049
Internet: www.agehab.go.gov.br
e-mail ouvidoria@agehab.go.gov.br

ANEXO VII

MODELO DE DECLARAÇÃO DE ENQUADRAMENTO NA LEI COMPLEMENTAR Nº 117/2015
(deverá ser entregue, após a fase de lances, junto com a proposta comercial)

PREGÃO ELETRÔNICO Nº 007/2018

A (nome/razão social) _____, inscrita no CNPJ nº _____, por intermédio de seu representante legal o(a) Sr.(a) _____, portador(a) da Carteira de Identidade nº _____ e do CPF nº _____, DECLARA, sob as penas da lei, que cumpre os requisitos legais para a qualificação como microempresa ou empresa de pequeno porte, e atesta a aptidão para usufruir do tratamento favorecido estabelecido nos arts. 42 a 49 da Lei Complementar Federal nº 117/15, não possuindo nenhum dos impedimentos previstos no § 4º do artigo 3º da referida lei.

Local e data.

_____
Representante legal

Nota: A falsidade desta DECLARAÇÃO, objetivando os benefícios da Lei Complementar nº 117/2015, caracterizará crime de que trata o Art. 299 do Código Penal, sem prejuízo do enquadramento em outras figuras penais e das penalidades previstas neste Edital.

Agência Goiana de Habitação S/A
Rua 18-A nº 541, Setor Aeroporto - Goiânia - Goiás - 74.070-060 - (62) 3096-5000
Ouvidoria Agehab 3096-5049
Internet: www.agehab.go.gov.br
e-mail ouvidoria@agehab.go.gov.br

ANEXO VIII

Declaração de Inexistência de Sócios comuns, endereços coincidentes e/ou indícios de parentesco

À CPL/AGEHAB

Ref.: **Pregão Eletrônico nº 007/2018**

_____(RAZÃO SOCIAL DA LICITANTE), _____(CNPJ Nº), sediada no (a)_____ (ENDEREÇO COMPLETO), **DECLARA**, sob as penas da lei, que cumpre, plenamente, os requisitos exigidos no procedimento licitatório referenciado.

Igualmente, **DECLARA** sob as penas da lei, em especial para atender à orientação do TCU – Acórdão 2136/2006/TCU/1ª Câmara, de 01/08/2006, ata nº 27/2006, que nossa Empresa não possui sócios em comum, endereços idênticos e/ou indícios de parentesco, com as demais licitantes presentes, ou das que se fazem representar no momento do credenciamento.

Finalizando, declaramos que temos pleno conhecimento de todos os aspectos relativos à licitação em causa e nossa plena concordância com as condições estabelecidas no Edital da licitação e seus anexos.

Local e Data

Atenciosamente,

_____

FIRMA LICITANTE/CNPJ

ASSINATURA DO REPRESENTANTE LEGAL

Agência Goiana de Habitação S/A
Rua 18-A nº 541, Setor Aeroporto - Goiânia - Goiás - 74.070-060 - (62) 3096-5000
Ouvidoria Agehab 3096-5049
Internet: www.agehab.go.gov.br
e-mail ouvidoria@agehab.go.gov.br

ANEXO IX

MINUTA DO CONTRATO

CONTRATO DE FORNECIMENTO QUE ENTRE SI FAZEM, DE UM LADO, COMO CONTRATANTE, A AGÊNCIA GOIANA DE HABITAÇÃO S/A – AGEHAB, E DE OUTRO LADO, COMO CONTRATADA, A EMPRESA ……., EM CONFORMIDADE COM O PROCESSO N° 2017.01031.006807-53 – SEI 201700031000181.

Por este instrumento particular, as partes abaixo mencionadas e qualificadas, acordam entre si firmar o presente Contrato de fornecimento, conforme as cláusulas e condições a seguir elencadas:

1 – Qualificação das Partes

AGÊNCIA GOIANA DE HABITAÇÃO S/A – AGEHAB *, sociedade de economia mista, portadora do CNPJ nº 01.274.240/0001-47, com sede na Rua 18-A nº 541, Setor Aeroporto, Goiânia – GO, neste ato representada por seu Presidente* ***Cleomar Dutra Ferreira****, brasileiro, casado, portador da Carteira de Identidade nº 1716672 – SSP GO, e do CPF nº 349.423.431-00, residente e domiciliado em Anápolis – Go, por seu Diretor Administrativo* ***Joel Gomes Ribeiro****, brasileiro, casado, portador da Carteira de Identidade nº 224015 – 2ª via – DGPC – GO e do CPF nº 067.834.301-20, residente e domiciliado em Anápolis e por seu Diretor Financeiro* ***Amauri Batista Regis****, brasileiro, casado, portador da Carteira de Identidade nº M 1.464.004- MG e do CPF nº 326.720.476-34, residente e domiciliado em Aparecida de Goiânia - GO, doravante designada simplesmente* ***CONTRATANTE.***

_____, pessoa jurídica de direito privado, situada na _____, _____, inscrita no CNPJ sob o nº _____, neste ato representada por seu representante legal o(a) Sr.(a) _____, brasileiro(a),_____, _____, residente e domiciliado em _____, doravante designada simplesmente ***CONTRATADA****.*

DO FUNDAMENTO LEGAL

Este contrato decorre da licitação realizada na modalidade Pregão Eletrônico nº 007/2018, de acordo com a Lei Federal nº 10.520, de 17 de julho de 2002, Lei Complementar nº 123, de 14 de dezembro de 2006, Decreto Estadual nº 7.468, de 20 de outubro de 2011, Decreto Estadual nº 7.466 de 18 de outubro de 2011, Lei Estadual nº 17.928/2012, Lei Complementar 117/2015, aplicando-se subsidiariamente, no que couberem, as disposições da Lei Federal nº 8.666, de 23 de junho de 1993, e demais normas regulamentares aplicáveis à espécie, conforme termo de Homologação e processo administrativo nº 2017.01031.006807-53, regendo-o no que for omisso.

CLÁUSULA PRIMEIRA – DO OBJETO E SUA DESCRIÇÃO

1.1. O presente contrato tem por finalidade o fornecimento de solução de proteção Endpoint (Antivírus), serviço de implantação e treinamento visando atender as necessidades da AGEHAB, conforme descrições contidas no Termo de Referência e Proposta da Contratada, conforme quadro abaixo:

ITEM 01	Licenciamento, manutenção e suporte de Solução de Proteção ENDPOINT (ANTIVIRUS) - por 36 meses
ITEM 02	Instalação de Solução de Proteção ENDPOINT (ANTIVIRUS)
ITEM 03	Treinamento de Solução de Proteção ENDPOINT (ANTIVIRUS)

1.2. Todas as funcionalidades solicitadas deverão ser atendidas por uma única solução/produto, não sendo aceitas composições de soluções;

1.3. As Licenças deverão ser fornecidas através de Download;

1.4. Os preços cotados do objeto da presente licitação deverão ser expressos em moeda corrente nacional, neles inclusos os acréscimos e despesas, como impostos, sem inclusão de qualquer encargo financeiro ou previsão inflacionária, sem que sofra correção ou reajuste durante o período de execução;

1.5. A solução ofertada após a assinatura do contrato, deverá ser a versão mais atual das ferramentas descritas no Termo de Referência;

1.6. SERVIDOR DE ADMINISTRAÇÃO E CONSOLE ADMINISTRATIVA (COMPATIBILIDADE)
1.6.1. Microsoft Windows Server 2008 x64 e R2;
1.6.2. Microsoft Windows Small Business Server 2008 (Todas edições);
1.6.3. Microsoft Windows Server 2012 e R2 (Todas edições);
1.6.4. Microsoft Windows Server 2016 R2 (Todas edições);
1.6.5. Microsoft Windows XP Professional SP3 ou superior;
1.6.6. Microsoft Windows XP Professional x64 SP2 ou superior;
1.6.7. Microsoft Windows Vista Business / Enterprise / Ultimate SP1 ou posterior;
1.6.8. Microsoft Windows VistaBusiness / Enterprise / Ultimate SP1 x64 ou posterior;
1.6.9. Microsoft Windows 7 Professional / Enterprise / Ultimate;
1.6.10. Microsoft Windows 7 Professional / Enterprise / Ultimate x64;
1.6.11. Microsoft Windows 8 Professional / Enterprise;
1.6.12. Microsoft Windows 8 Professional / Enterprise x64;
1.6.13. Microsoft Windows 8.1 Professional / Enterprise;
1.6.14. Microsoft Windows 8.1 Professional / Enterprise x64;
1.6.15. Microsoft Windows 10 Professional / Enterprise x64.

1.7. SUPORTA AS SEGUINTES PLATAFORMAS VIRTUAIS:
1.7.1. VMware: Workstation 9.x, Workstation 10.x, ESXi 5.5, ESXi 6.0 e superior;
1.7.2. Microsoft Hyper-V: 2008, 2008 R2, 2012, 2012 R2 e 2016;
1.7.3. Oracle VM VirtualBox 4.0.4 e Superior (Somente logon como convidado);
1.7.4. Citrix XenServer 6.0 e Superior.

1.8. CARACTERÍSTICAS:

1.8.1. A console deve ser acessada via WEB (HTTPS) ou MMC;

1.8.2. Console deve ser baseada no modelo cliente/servidor;

1.8.3. Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;

1.8.4. Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus;

1.8.5. Console deve ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch management e MDM;

1.8.6. As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração da licença;

1.8.7. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;

1.8.8. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory;

1.8.9. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;

1.8.10. A solução de gerencia deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;

1.8.11. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;

1.8.12. Capacidade de instalar remotamente a solução de segurança em smartphones e tablets de sistema iOS, Android e Windows;

1.8.13. Capacidade de instalar remotamente qualquer “app” em smartphones e tablets de sistema iOS;

1.8.14. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;

1.8.15. Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os seguintes parâmetros: KB/s e horário;

1.8.16. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus;

1.8.17. Capacidade de gerenciar smartphones e tablets (Windows Phone, Android e iOS) protegidos pela solução de segurança;

1.8.18. Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença econfigurações do produto;

1.8.19. Capacidade de atualizar os pacotes de instalação com as últimas vacinas;

1.8.20. Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes;

1.8.21. A comunicação entre o cliente e o servidor de administração deve ser criptografada;

1.8.22. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;

1.8.23. Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou ENDPOINT instalado utilizando os seguintes parâmetros:

1.8.23.1. Nome do computador;

1.8.23.2. Nome do domínio;

1.8.23.3. Range de IP;
1.8.23.4. Sistema Operacional;
1.8.23.5. Máquina virtual.

1.8.24. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;

1.8.25. Deve permitir, por meio da console de gerenciamento, extrair um artefato em quarentena de um cliente sem a necessidade de um servidor ou console de quarentena adicional;

1.8.26. Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção;

1.8.27. Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção;

1.8.28. Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente;

1.8.29. Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivírus instalado, agrupar todas as máquinas que não receberam atualização nos últimos X dias, etc.;

1.8.30. Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos;

1.8.31. Deve fornecer as seguintes informações dos computadores:

1.8.31.1. Deve fornecer as seguintes informações dos computadores:

a) Se o antivírus está instalado;
b) Se o antivírus está iniciado;
c) Se o antivírus está atualizado;
d) Minutos/horas desde a última conexão da máquina com o servidor administrativo;
e) Minutos/horas desde a última atualização de vacinas;
f) Data e horário da última verificação executada na máquina;
g) Versão do antivírus instalado na máquina;
h) Se é necessário reiniciar o computador para aplicar mudanças;
i) Data e horário de quando a máquina foi ligada;
j) Quantidade de vírus encontrados (contador) na máquina;
k) Nome do computador;
l) Domínio ou grupo de trabalho do computador;
m) Data e horário da última atualização de vacinas;
n) Sistema operacional com Service Pack;
o) Quantidade de processadores;
p) Quantidade de memória RAM;
q) Usuário(s) logado(s) naquele momento, com informações de contato (caso disponível no Active Directory);
r) Endereço IP;
s) Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido;
t) Atualizações do Windows Updates instaladas;

Agência Goiana de Habitação S/A
Rua 18-A nº 541, Setor Aeroporto - Goiânia - Goiás - 74.070-060 - (62) 3096-5000
Ouvidoria Agehab 3096-5049
Internet: www.agehab.go.gov.br
e-mail ouvidoria@agehab.go.gov.br

v) Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD;

w) Vulnerabilidades de aplicativos instalados na máquina.

1.8.32. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;

1.8.33. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:

1.8.33.1. Alteração de Gateway Padrão;

1.8.33.2. Alteração de subrede;

1.8.33.3. Alteração de domínio;

1.8.33.4. Alteração de servidor DHCP;

1.8.33.5. Alteração de servidor DNS;

1.8.33.6. Alteração de servidor WINS;

1.8.33.7. Alteração de subrede;

1.8.33.8. Resolução de Nome;

1.8.33.9. Disponibilidade de endereço de conexão SSL.

1.8.34. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;

1.8.35. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;

1.8.36. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;

1.8.37. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;

1.8.38. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;

1.8.39. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo;

1.8.40. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML;

1.8.41. Capacidade de gerar traps SNMP para monitoramento de eventos;

1.8.42. Capacidade de enviar e-mails para contas específicas em caso de algum evento;

1.8.43. Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server;

1.8.44. Deve possuir compatibilidade com Cisco Network AdmissionControl (NAC);

1.8.45. Deve possuir documentação da estrutura do banco de dados para geração de relatórios a partir de ferramentas específicas de consulta (Crystal Reports, por exemplo);

1.8.46. Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação, etc), inclusive de máquinas que estejam em subnets diferentes do servidor;

1.8.47. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);

1.8.48. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;

1.8.49. Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:

1.8.49.1. Nome do vírus;
1.8.49.2. Nome do arquivo infectado;
1.8.49.3. Data e hora da detecção;
1.8.49.4. Nome da máquina ou endereço IP;
1.8.49.5. Ação realizada.

1.8.50. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;
1.8.51. Capacidade de realizar inventário de hardware de todas as máquinas clientes;
1.8.52. Capacidade de realizar inventário de aplicativos de todas as máquinas clientes;
1.8.53. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

1.9. ESTAÇÕES WINDOWS – COMPATIBILIDADE:
1.9.1. Microsoft Windows Embedded 8.0 Standard x64;
1.9.2. Microsoft Windows Embedded 8.1 Industry Pro x64;
1.9.3. Microsoft Windows Embedded Standard 7 x86 / x64 SP1;
1.9.4. Microsoft Windows XP Professional x86 SP3 e superior;
1.9.5. Microsoft Windows Vista x86 / x64SP2 e posterior;
1.9.6. Microsoft Windows 7 Professional/Enterprise/Ultimate x86 / x64 e posterior;
1.9.7. Microsoft Windows 8 Professional/Enterprise x86 / x64;
1.9.8. Microsoft Windows 8.1 Pro / Enterprise x86 / x64 (Todas as Versões);
1.9.9. Microsoft Windows 10 Pro / Enterprise x86 / x64 (Todas as Versões).

1.10. CARACTERÍSTICAS:
1.10.1. Deve prover as seguintes proteções:

1.10.1.1. Deve prover as seguintes proteções:

* Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc.) que verifique qualquer arquivo criado, acessado ou modificado;
* Antivírus de Web (módulo para verificação de sites e downloads contra vírus);
* Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);
* Antivírus de Mensagens Instantâneas (módulo para verificação de mensagens instantâneas, MSN, por exemplo);
* O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;
* Firewall com IDS;
* Autoproteção (contra-ataques aos serviços/processos do antivírus);
* Controle de dispositivos externos;
* Controle de acesso a sites por categoria;
* Controle de acesso a sites por horário;
* Controle de acesso a sites por usuários;
* Controle de execução de aplicativos;
* Controle de vulnerabilidades do Windows e dos aplicativos instalados;
* Controle de vulnerabilidades do Windows e dos aplicativos instalados;
* Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
* As vacinas devem ser atualizadas pelo fabricante e disponibilizadas aos usuários em no máximo, 02 (duas) em 02 (duas) horas independentemente do nível das ameaças encontradas no período (alta, média ou baixa);

* Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;

* Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

* Capacidade de adicionar aplicativos a uma lista de "aplicativos confiáveis", onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas;

* Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);

* Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

* Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

* Capacidade de verificar somente arquivos novos e alterados;

* Capacidade de verificar objetos usando heurística;

* Capacidade de agendar uma pausa na verificação;

* Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias;

* Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;

* O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

a) Perguntar o que fazer, ou bloquear acesso ao objeto.

* Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

* Caso positivo de desinfecção: Restaurar o objeto para uso;

* Caso negativo de desinfecção: Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

* Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;

* Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, IMAP, NNTP, SMTP e MAPI, assim como conexões criptografadas (SSL) para POP3 e IMAP (SSL);

* Capacidade de verificar tráfego de ICQ, MSN, AIM e IRC contra vírus e links phishings;

* Capacidade de verificar links inseridos em e-mails contra phishings;

* Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox e Google Chrome, Opera, etc.;

* Capacidade de verificação de corpo e anexos de e-mails usando heurística;

* O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:

a) Perguntar o que fazer, ou bloquear o e-mail.

* Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

* Caso positivo de desinfecção: Restaurar o e-mail para o usuário;

* Caso negativo de desinfecção: Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);

Agência Goiana de Habitação S/A
Rua 18-A nº 541, Setor Aeroporto - Goiânia - Goiás - 74.070-060 - (62) 3096-5000
Ouvidoria Agehab 3096-5049
Internet: www.agehab.go.gov.br
e-mail ouvidoria@agehab.go.gov.br

* Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena;

* Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados;

* Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador;

* Capacidade de verificação de tráfego HTTP e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc.), usando heurísticas;

* Deve ter suporte total ao protocolo IPv6;

* Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail;

* Na verificação de tráfego web, caso encontrado código malicioso o programa deve:

a) Perguntar o que fazer, ou bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;

b) Permitir acesso ao objeto.

* O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:

a) Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em temporeal, ou;

b) Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação.

* Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web;

* Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas;

* Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa.

1.10.1.2. Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas;

1.10.1.3. Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-PhishingWorkingGroup (http://www.antiphishing.org/);

1.10.1.4. Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;

1.10.1.5. Deve possuir módulo IDS (IntrusionDetection System) para proteção contra portscans e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas;

1.10.1.6. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

* Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;

* Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, coma possibilidade de escolher quais portas e protocolos poderão ser utilizados.

1.10.1.7. Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:

* Discos de armazenamento locais;
* Armazenamento removível;
* Impressoras;
* CD/DVD;
* Drives de disquete;
* Modems;
* Dispositivos de fita;
* Dispositivos multifuncionais;
* Leitores de smartcard;
* Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc);
* Wi-Fi;
* Adaptadores de rede externos;
* Dispositivos MP3 ou smartphones;
* Dispositivos Bluetooth;
* Câmeras e Scanners.

1.10.1.8. Capacidade de liberar acesso a um dispositivo e usuários por um período de tempo específico, sem a necessidade de desabilitar a proteção e o gerenciamento central ou de intervenção local do administrador na máquina do usuário;

1.10.1.9. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário;

1.10.1.10. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento;

1.10.1.11. Capacidade de configurar novos dispositivos por Class ID/Hardware ID;

1.10.1.12. Capacidade de limitar o acesso a sites da internet por categoria, por conteúdo (vídeo, áudio, etc.), com possibilidade de configuração por usuário ou grupos de usuários e agendamento;

1.10.1.13. Capacidade de limitar a execução de aplicativos por hash MD5, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto, etc.);

1.10.1.14. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;

1.10.1.15. Capacidade de limitar o acesso dos aplicativos a recursos do sistema, como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo;

1.10.1.16. Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web;

1.10.1.17. Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.

1.11. ESTAÇÕES MAC OS X - COMPATIBILIDADE:

1.11.1. Mac OS X 10.11 (El Capitan);
1.11.2. Mac OS X 10.10 (Yosemite);
1.11.3. Mac OS X 10.9 (Mavericks);
1.11.4. Mac OS X 10.8 (Mountain Lion);

1.11.5. Mac OS X 10.7 (Lion).

1.12. CARACTERÍSTICAS:
1.12.1. Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware, etc.) que verifique qualquer arquivo criado, acessado ou modificado;
1.12.2. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
1.12.3. A instalação e primeira execução do produto deve ser feita sem necessidade de reinicialização do computador, de modo que o produto funcione com toda sua capacidade;
1.12.4. Deve possuir suportes a notificações utilizando o Growl;
1.12.5. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);
1.12.6. Capacidade de voltar para a base de dados de vacina anterior;
1.12.7. Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas;
1.12.8. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
1.12.9. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
1.12.10. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
1.12.11. Capacidade de verificar somente arquivos novos e alterados;
1.12.12. Capacidade de verificar objetos usando heurística;
1.12.13. Capacidade de agendar uma pausa na verificação;
1.12.14. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
1.12.14.1. Perguntar o que fazer, ou bloquear acesso ao objeto;
1.12.15. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador):
1.12.15.1. Caso positivo de desinfecção: Restaurar o objeto para uso;
1.12.15.2. Caso negativo de desinfecção: Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
1.12.16. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
1.12.17. Capacidade de verificar arquivos de formato de email;
1.12.18. Possibilidade de trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, para o antivírus e iniciar o antivírus pela linha de comando;
1.12.19. Capacidade de ser instalado, removido e administrado pela mesma console central de gerenciamento.

1.13. ESTAÇÕES DE TRABALHO LINUX - COMPATIBILIDADE (PLATAFORMA 32 E 64 BITS):
1.13.1. Red Hat Enterprise Linux 6.2 Desktop e Superiores;
1.13.2. Fedora 16 e Superiores;
1.13.3. CentOS-6.2 e Superiores;

Agência Goiana de Habitação S/A
Rua 18-A nº 541, Setor Aeroporto - Goiânia - Goiás - 74.070-060 - (62) 3096-5000
Ouvidoria Agehab 3096-5049
Internet: www.agehab.go.gov.br
e-mail ouvidoria@agehab.go.gov.br

1.13.4. SUSE Linux Enterprise Desktop 10 SP4 e Superiores;
1.13.5. OpenSUSE Linux 12.2 e Superiores;
1.13.6. Debian GNU/Linux 6.0.5 e Superiores;
1.13.7. Mandriva Linux 2011 e Superiores;
1.13.8. Ubuntu 10.04 LTS e Superiores;
1.13.9. CARACTERÍSTICAS - DEVE PROVER AS SEGUINTES PROTEÇÕES:

1.13.9.1. Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware, etc.) que verifique qualquer arquivo criado, acessado ou modificado;

1.13.9.2. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

1.13.9.3. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

a) Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

b) Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;

c) Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;

d) Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.

1.13.9.4. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;

1.13.9.5. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

1.13.9.6. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

1.13.9.7. Capacidade de verificar objetos usando heurística;

1.13.9.8. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;

1.13.9.9. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

1.13.9.10. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux.

1.14. SERVIDORES WINDOWS
1.14.1. COMPATIBILIDADE COM PLATAFORMA 32-BITS:

1.14.1.1. Microsoft Windows Server 2008 Standard / Enterprise / DataCenter (SP1 ou posterior);

1.14.1.2. Microsoft Windows Server 2008 Core Standard / Enterprise / DataCenter (SP1 ou posterior).

1.14.2. COMPATIBILIDADE COM PLATAFORMA 64-BITS:

1.14.2.1. Microsoft Windows Server 2008 Standard / Enterprise / DataCenter (SP1 ou posterior);

1.14.2.2. Microsoft Windows Server 2008 Core Standard / Enterprise / DataCenter (SP1 ou posterior);

1.14.2.3. Microsoft Windows Server 2008 R2 Standard / Enterprise / DataCenter (SP1 ou posterior);

1.14.2.4. Microsoft Windows Server 2008 R2 Core Standard / Enterprise / DataCenter (SP1 ou posterior);

1.14.2.5. Microsoft Windows Storage Server 2008 R2;

1.14.2.6. Microsoft Windows Hyper-V Server 2008 R2 (SP1 ou posterior);

1.14.2.7. Microsoft Windows Server 2012 Essentials / Standard / Foundation / Datacenter;

1.14.2.8. Microsoft Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter;

1.14.2.9. Microsoft Windows Server 2012 Core Essentials / Standard / Foundation / Datacenter;

1.14.2.10. Microsoft Windows Server 2012 R2 Core Essentials / Standard / Foundation / Datacenter;

1.14.2.11. Microsoft Windows Storage Server 2012 (Todas edições);

1.14.2.12. Microsoft Windows Storage Server 2012 R2 (Todas edições);

1.14.2.13. Microsoft Windows Storage Server 2016 (Todas edições);

1.14.2.14. Microsoft Windows Hyper-V Server 2012;

1.14.2.15. Microsoft Windows Hyper-V Server 2012 R2;

1.14.2.16. Microsoft Windows Hyper-V Server 2016.

1.15. CARACTERÍSTICAS - DEVE PROVER AS SEGUINTES PROTEÇÕES:

1.15.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc.) que verifique qualquer arquivo criado, acessado ou modificado;

1.15.2. Auto-proteção contra-ataques aos serviços/processos do antivírus;

1.15.3. Firewall com IDS;

1.15.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados;

1.15.5. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

1.15.6. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

1.15.7. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

a) Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

b) Gerenciamento de tarefa (criar ou excluir tarefas de verificação);

c) Leitura de configurações;

d) Modificação de configurações;

e) Gerenciamento de Backup e Quarentena;

f) Visualização de relatórios;

g) Gerenciamento de relatórios;

h) Gerenciamento de chaves de licença;

i) Gerenciamento de permissões (adicionar/excluir permissões acima);

1.15.8. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

a) Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;

1.15.9. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;

1.15.10. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo

terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados;

1.15.11. Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total;

1.15.12. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc.);

1.15.13. Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (uninterruptible Power supply – UPS);

1.15.14. Em caso de erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares;

1.15.15. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor;

1.15.16. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;

1.15.17. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas;

1.15.18. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;

1.15.19. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

1.15.20. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

1.15.21. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

1.15.22. Capacidade de verificar somente arquivos novos e alterados;

1.15.23. Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários, etc.);

1.15.24. Capacidade de verificar objetos usando heurística;

1.15.25. Capacidade de configurar diferentes ações para diferentes tipos de ameaças;

1.15.26. Capacidade de agendar uma pausa na verificação;

1.15.27. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;

1.15.28 O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

a) Perguntar o que fazer, ou boquear acesso ao objeto;

1.15.29. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

1.15.30. Caso positivo de desinfecção: Restaurar o objeto para uso;

1.15.31. Caso negativo de desinfecção: Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

1.15.32. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;

1.15.33. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;

1.15.34. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
1.15.35. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.

1.16. SERVIDORES LINUX
1.16.1. COMPATIBILIDADE PLATAFORMA 64-BITS:

a) Red Hat Enterprise Linux Server 7 e Superiores;
b) CentOS-7.0 e Superiores;
c) SUSE Linux Enterprise Server 12 e Superiores;
d) Novell Open Enterprise Server 11 SP2 e Superiores;
e) Ubuntu Server 14.04 LTS e Superiores;
f) Ubuntu Server 14.10 e Superiores;
g) Oracle Linux 6.5 e Superiores;
h) Debian GNU/Linux 7.5, 7.6, 7.7 e Superiores;
i) openSUSE® 13.1 e Superiores.

1.16.2. CARACTERÍSTICAS - DEVE PROVER AS SEGUINTES PROTEÇÕES:

a) Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

b) As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

c) Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

* Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

* Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;

* Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;

* Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados;

* Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;

* Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

* Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

* Capacidade de verificar objetos usando heurística;

* Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;

* Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

* Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux)

1.17. SMARTPHONES E TABLETS – COMPATIBILIDADE
1.17.1. Apple iOS 7.0 – 8.X;
1.17.2. Windows Phone 8.1;

1.17.3. Android OS 2.3 – 5.1;

1.17.4. CARACTERÍSTICAS - DEVE PROVER AS SEGUINTES PROTEÇÕES:

a) Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:

* Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:

b) Deverá isolar em área de quarentena os arquivos infectados;

c) Deverá atualizar as bases de vacinas de modo agendado;

d) Deverá bloquear spams de SMS através de Black lists;

e) Deverá ter função de bloqueio do aparelho caso o SIM CARD for trocado para outro não autorizado;

f) Capacidade de desativar por política: Wi-fi, Câmera, Bluetooth;

g) Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo;

h) Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha;

i) Deverá ter firewall pessoal (Android);

j) Capacidade de tirar fotos quando a senha for inserida incorretamente;

k) Possibilidade de instalação remota utilizando o Microsoft System Center Mobile Device Manager 2008 SP1;

l) Capacidade de enviar comandos remotamente de:

* Localizar;

* Bloquear;

m) Capacidade de detectar Jailbreak em dispositivos iOS;

n) Capacidade de bloquear o acesso a site por categoria em dispositivos;

o) Capacidade de bloquear o acesso a sites phishing ou malicioso;

p) Capacidade de criar containers de aplicativos, separando dados corporativos de dados pessoais;

q) Capacidade de bloquear o dispositivo quando o cartão "SIM" for substituído;

r) Capacidade de configurar White e blacklist de aplicativos;

s) Capacidade de localizar o dispositivo quando necessário;

t) Permitir atualização das definições quando estiver em "roaming";

u) Capacidade de selecionar endereço do servidor para buscar a definição de vírus;

v) Capacidade de enviar URL de instalação por e-mail;

w) Capacidade de fazer a instalação através de um link QRCode;

x) Capacidade de executar as seguintes ações caso a desinfecção falhe:

* Deletar;

* Ignorar;

* Quarentenar;

* Perguntar ao usuário.

1.18. GERENCIAMENTO DE DISPOSITIVOS MÓVEIS (MDM) - COMPATIBILIDADE:

1.18.1. Dispositivos conectados através do Microsoft Exchange ActiveSync:

a) Apple iOS;

b) Windows Phone;

c) Android;

d) Dispositivos com suporte ao Apple PushNotification (APNs);

e) Apple iOS 3.0 ou superior.

1.18.2. CARACTERÍSTICAS:

a) Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange;

b) Capacidade de ajustar as configurações de:

* Sincronização de e-mail;
* Uso de aplicativos;
* Senha do usuário;
* Criptografia de dados;
* Conexão de mídia removível.
* Capacidade de instalar certificados digitais em dispositivos móveis;
* Capacidade de, remotamente, resetar a senha de dispositivos iOS;
* Capacidade de, remotamente, apagar todos os dados de dispositivos iOS;
* Capacidade de, remotamente, bloquear um dispositivo iOS.

1.19. CRIPTOGRAFIA - COMPATIBILIDADE:

1.19.1. Microsoft Windows Vista Business/Enterprise/ultimate sp2;
1.19.2. Microsoft Windows Vista Business/Enterprise/ultimate x64 sp2;
1.19.3. Microsoft Windows 7 Professional/Enterprise/ultimate;
1.19.4. Microsoft Windows 7 Professional/Enterprise/ultimate x64;
1.19.5. Microsoft Windows 8 Professional/Enterprise;
1.19.6. Microsoft Windows 8 Professional/Enterprise x64;
1.19.7. Microsoft Windows 8.1 Professional / Enterprise;
1.19.8. Microsoft Windows 8.1 Professional / Enterprise x64;
1.19.9. Microsoft Windows 10 Pro x86 / x64;
1.19.10. Microsoft Windows 10 Enterprise x86 /x64.

1.20. CARACTERÍSTICAS:

1.20.1. O acesso ao recurso criptografado (arquivo, pasta ou disco) deve ser garantido mesmo em caso o usuário tenha esquecido a senha, através de procedimentos de recuperação;
1.20.2. Utilizar, no mínimo, algoritmo AES com chave de 256 bits;
1.20.3. Deve ter a capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário;
1.20.4. Deve ter a capacidade de utilizar single sign-on para a autenticação de pré-boot;
1.20.5. Permitir criar vários usuários de autenticação pré-boot;
1.20.6. Deve ter a capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento;
1.20.7. Deve ter a capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:

* Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;
* Criptografar todos os arquivos individualmente;
* Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;
* Criptografar o dispositivo removível, em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;

1.20.8. Deve ter a capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente. Nesta modalidade, os arquivos devem estar acessíveis para todas as máquinas gerenciadas pela mesma console de maneira transparente para os usuários;

1.20.9. Deve ter a capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;
1.20.10. Deve ter a capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados;
1.20.11. Verificar compatibilidade de hardware antes de aplicar a criptografia;
1.20.12. Deve ter a capacidade de estabelecer parâmetros para a senha de criptografia;
1.20.13. Bloquear o reuso de senhas;
1.20.14. Bloquear a senha após um número de tentativas pré-estabelecidas;
1.20.15. Deve ter a capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;
1.20.16. Permitir criar exclusões para não criptografar determinados "discos rígidos" através de uma busca por nome do computador ou nome do dispositivo;
1.20.17. Permitir criptografar as seguintes pastas pré-definidas: "meus documentos", "favoritos", "desktop", "arquivos temporários" e "arquivos do outlook";
1.20.18. Permitir utilizar variáveis de ambiente para criptografar pastas customizadas;
1.20.19. Deve ter a capacidade de criptografar arquivos por grupos de extensão, tais como: documentos do office, documentos .txt, arquivos de áudio, etc.;
1.20.20. Permitir criar um grupo de extensões de arquivos a serem criptografados;
1.20.21. Deve ter a capacidade de criar regra de criptografia para arquivos gerados por aplicações;
1.20.22. Permitir criptografia de dispositivos móveis mesmo quando o Endpoint não possuir comunicação com a console de gerenciamento.

1.21. Gerenciamento de Sistemas
1.21.1. Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis;
1.21.2. Capacidade de corrigir as vulnerabilidades de softwares, fazendo o download centralizado da correção ou atualização e aplicando essa correção ou atualização nas máquinas gerenciadas de maneira transparente para os usuários;
1.21.3. Capacidade de gerenciar licenças de softwares de terceiros;
1.21.4. Capacidade de registrar mudanças de hardware nas máquinas gerenciadas;
1.21.5. Capacidade de gerenciar um inventário de hardware, com a possibilidade de cadastro de dispositivos (ex: router, switch, projetor, acessório, etc), informando data de compra, local onde se encontra, servicetag, número de identificação e outros;
1.21.6. Possibilita fazer distribuição de software de forma manual e agendada;
1.21.7. Suporta modo de instalação silenciosa;
1.21.8. Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;
1.21.9. Possibilita fazer a distribuição através de agentes de atualização;
1.21.10. Utiliza tecnologia multicast para evitar tráfego na rede;
1.21.11. Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;
1.21.12. Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no c;
1.21.13. Capacidade de gerar relatórios de vulnerabilidades e patches;
1.21.14. Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração;
1.21.15. Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;
1.21.16. Permite baixar atualizações para o computador sem efetuar a instalação;

1.21.17. Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atua;
1.21.18. Capacidade de instalar correções de vulnerabilidades de acordo com a severidade;
1.21.19. Permite selecionar produtos a serem atualizados pela console de gerenciamento;
1.21.20. Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc.

CLÁUSULA SEGUNDA – DA GARANTIA

2.1. GARANTIA TÉCNICA

2.1.1. Os objetos deverão possuir garantia técnica mínima de 36 meses, sob a responsabilidade do fornecedor. O fornecedor deverá disponibilizar assistência técnica no período da garantia técnica.

2.2. ASSISTÊNCIA TÉCNICA

2.2.1. Todas as licenças de software utilizadas para atender o objeto deverão possuir garantia de 36 (trinta e seis) meses.

2.2.2. A CONTRATADA deverá prestar suporte técnico e operacional durante o período de vigência da licença, com atendimento através do serviço telefônico, acesso remoto, e-mail ou WEB, para esclarecimento de dúvidas, abertura de chamados, e envio de arquivos para análise (Zero-day).

2.2.3. Os prazos relativos aos chamados deverão obedecer ao seguinte nível mínimo de serviço: 8 x 5 (oito horas por dia, cinco dias por semana em dias úteis e no horário comercial).

2.3. O SERVIÇO DE SUPORTE TÉCNICO GARANTE:

2.3.1. Reinstalação, reconfiguração, e auxilio na utilização de recursos ou solução de problemas relacionados aos sistemas ofertados.

2.3.2. O direito de receber toda e qualquer atualização de todos os softwares ou patches corretivos de componentes adquiridas após a assinatura do contrato, para a versão mais atual das ferramentas.

2.3.3. A CONTRATADA deverá prestar atendimento técnico em regime de garantia.

CLÁUSULA TERCEIRA – DO PRAZO, LOCAL DE ENTREGA E FORMA DE RECEBIMENTO

3.1. Todas as licenças deverão ser registradas em nome do Agência Goiana de Habitação S/A, CNPJ: 01.274.240/0001-47, tendo como sede a localização na Rua 18 A nº 541 – Setor Aeroporto – Goiânia-GO, CEP: 74.070-060.

3.2. A data para efetivo início da execução dos serviços não poderá exceder 15 (quinze) dias depois da publicação do Contrato.

3.3. A entrega será feita de forma única contemplando Licenciamento dos objetos e Entrega da Documentação.

3.4. Os equipamentos deverão ser entregues em até 30 (trinta) dias a contar da publicação do contrato ou instrumento equivalente, à sede da Agência Goiana de Habitação S/A Rua 18 A nº 541, Setor Aeroporto, Goiânia-GO, CEP 74070-060.

3.5. O prazo máximo para entrega do serviço, incluindo licenciamento, instalação, treinamento e Entrega da Documentação, será de no máximo 30 (trinta) dias, contados a partir da data de publicação do contrato.

CLÁUSULA QUARTA – DA EXECUÇÃO

4.1. Licenciamento e Instalação da solução:

4.1.1. A instalação e configuração deve ser implementada On-site conforme cenário fornecido pela Agência Goiana de Habitação S/A após a emissão e recebimento da assinatura do contrato.

4.1.2. A empresa CONTRATADA deverá realizar toda a instalação da solução adquirida e quaisquer outras providências que tenham relação direta com a instalação do serviço em questão.

4.1.3. Criar senha de acesso com privilégio administrativo para a AGEHAB.

4.1.4. Após a assinatura do contrato, a CONTRATADA deverá apresentar, no prazo máximo de 10 (dez) dias, os requisitos de infraestrutura para instalação da solução, o Plano de instalação, testes e ativação incluindo o Cronograma Detalhado de Execução dos Serviços, prevendo as datas de início e término da instalação de todos os licenciamentos.

4.1.5. O Cronograma da CONTRATADA deverá ser submetido à Gerência de Tecnologia da Informação (GETI) da AGEHAB, observado o respectivo serviço e somente será válido após aprovação. Depois de validado, a Contratada será notificada para dar início à execução do cronograma aprovado pela GETI - AGEHAB.

4.1.6. O fornecedor deverá entregar a solução instalada e customizada de acordo com os padrões fornecidos pela equipe técnica da Gerência de Tecnologia da Informação (GETI).

4.2. TREINAMENTO (REPASSE TECNOLÓGICO)

4.2.1. O treinamento abordará no mínimo: o uso da ferramenta, instalação, configuração, backup e restauração de configuração, gerenciamento, resolução de problemas e procedimentos de isolamento de rede em caso de infecção.

4.2.2. O treinamento deverá contemplar todos os recursos e configurações existentes na solução ofertada.

4.2.3. A AGEHAB se encarregará de disponibilizar as instalações físicas para a realização do treinamento, tais como: projetores, tela para apresentação, computador, mesas e poltronas.

4.2.4. É de responsabilidade da CONTRATADA todo material audiovisual, didático e eletrônico para a realização dos treinamentos, além de impressos e quaisquer outras despesas diretas ou indiretas.

4.2.5. O treinamento será com uma turma de até 05 (cinco) alunos e o treinamento será realizado nas dependências da AGÊNCIA GOIANA DE HABITAÇÃO S/A, que irá ceder uma sala para sua realização.

4.2.6. O treinamento deverá ser organizado em módulos e suas ementas e conteúdos programáticos devem ser previamente disponibilizados a AGEHAB para aprovação.

4.2.7. O material didático será fornecido em português, pela contratada, abordando todos os tópicos do curso.

4.2.8. Os treinamentos deverão ser realizados em dias úteis e não poderão exceder carga horária diária de 8 (oito) horas. Os horários e datas dos treinamentos serão definidos pela equipe técnica da AGEHAB e comunicados a contratada com antecedência de 10 (dez) dias consecutivos.

CLÁUSULA QUINTA – DAS OBRIGAÇÕES DA CONTRATADA

5.1. Além das resultantes da Lei 8.666/93 a adjudicatária se obriga, nos termos do Termo de Referência, a:
5.1.1. Prestar todos os esclarecimentos que forem solicitados pela fiscalização da contratante;
5.1.2. Manter durante toda a execução do termo respectivo, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na contratação;
5.2. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com os artigos 14 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);
5.3. Manter atualizados, durante a vigência do contrato, para fins de pagamento, a Certidão Negativa de Débito – CND de Débito Trabalhista-CNDT, o Certificado de Regularidade - CRF do FGTS e certidão de regularidade junto à Fazenda Federal e municipal;
5.4. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do Contrato, observando o preconizado no Termo de Referência.
5.5. São expressamente vedadas à CONTRATADA, Ceder, sob qualquer forma, os créditos oriundos deste contrato a terceiros;
5.6. Os funcionários da CONTRATADA, responsáveis pela instalação do serviço e treinamento aos colaboradores da Gerência de Tecnologia da Informação - GETI, deverão estar devidamente identificados com crachá e/ou outros identificadores quando nas instalações da AGEHAB;
5.7. Ficarão por conta da Contratada as possíveis despesas de transporte e hospedagem necessárias à execução do objeto;
5.8. Refazer, às suas expensas, todo e qualquer trabalho realizado em desconformidade com as determinações da AGEHAB ou, ainda, os que apresentarem defeitos, vícios ou incorreções;
5.9. Manter, durante a vigência do Contrato, todas as condições de habilitação e qualificação técnica apresentadas no processo licitatório, compatíveis com as obrigações assumidas neste Contrato;
5.10. Utilizar empregados habilitados e com conhecimentos compatíveis com os necessários para executar os serviços que lhes forem atribuídos, em conformidade com as normas e determinações em vigor;
5.11. Responder inteiramente por todos os encargos trabalhistas, previdenciários, fiscais, comerciais, seguro de acidentes, impostos e quaisquer outros que forem devidos e referentes aos serviços oriundos da contratação;
5.12. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do Contrato, observando o preconizado no Termo de Referência;
5.13. Executar os serviços de acordo com as condições, especificações, quantidades e demais detalhamentos no Termo de Referência – Anexo I.

CLÁUSULA SEXTA – DAS OBRIGAÇÕES DA CONTRATANTE

6.1. Prestar as informações e os esclarecimentos pertinentes que venham a ser solicitados pelos empregados da contratada ou por seu preposto;
6.2. Fornecer de toda a infraestrutura necessária para instalação e funcionamento dos equipamentos, como local físico, tomadas elétricas, pontos de acesso à rede, etc.
6.3. Efetuar o pagamento conforme execução dos serviços/produtos, desde que cumpridas todas as formalidades e exigências do contrato;
6.4. Exercer a fiscalização do contrato;
6.5. Comunicar oficialmente à contratada quaisquer falhas verificadas no cumprimento do contrato;
6.6. Convocar reunião inicial, quando necessário, com todos os envolvidos na contratação; e acompanhar e monitorar toda a execução dos serviços.

CLÁUSULA SÉTIMA – DO LOCAL DE ENTREGA

7.1. Todos os produtos licitados serão entregues na sede da Agência Goiana de Habitação S/A - AGEHAB, situadas na Rua 18 A nº 541 – Setor Aeroporto – Goiânia – GO – CEP 74070-060.
7.2. A proposta comercial deverá considerar todos os custos relativos a logística e entrega dos equipamentos na cidade de Goiânia – GO.

CLÁUSULA OITAVA – DA VIGÊNCIA

8.1. O prazo de vigência do contrato é de 12 (doze) meses, contados da assinatura deste contrato, sendo que sua eficácia, se dará a partir da publicação na imprensa oficial.

CLÁUSULA NONA – DO VALOR E DA FORMA DE PAGAMENTO

9.1. O valor global do presente contrato é de R$ _____(_____).
9.2. O pagamento será procedido mediante a apresentação da Nota Fiscal/Fatura, que deverá ser eletrônica em original ou a primeira via e original atestada, com a data e contendo a identificação do gestor do contrato que a atestou, após o fechamento do mês e a quitação até o 10º (décimo) dia útil do mês seguinte.
9.3. As nota(s) fiscal (is)/faturas deverão conter no mínimo os seguintes dados:
a) Data de emissão;
b) Estar endereçada a Agência Goiana de Habitação - AGEHAB, situada a Rua 18-A nº 541, Setor Aeroporto - Goiânia/GO, CNPJ nº 01.274.240/0001-47;
c) Preços unitários;
d) Descrição dos serviços;
9.4. O pagamento será efetuado após atesta pela autoridade competente assim como das respectivas requisições da AGEHAB, desde que a Certidão Negativa de Débito – CND, o Certificado de Regularidade do FGTS – CRF, a prova de regularidade para com a Fazenda Federal e municipal.
9.5. Na ocorrência da rejeição de nota fiscal/fatura, motivada por erro ou incorreções, o prazo estipulado no subitem 9.2 passará a ser contado a partir da data da sua reapresentação, examinadas as causas da recusa.
9.6. Se houver treinamento na sede da AGEHAB, deverá a Contratada apresentar, cópias legíveis pagas das guias de recolhimento do INSS, do FGTS com cópia do arquivo da SEFIP dos funcionários que tiveram o referido recolhimento e dos contracheques ou da folha de pagamento dos funcionários, que prestarem serviços para a Contratante, devidamente quitados e assinados, referente ao mês anterior

ao do pagamento, além das Certidões Negativas de Débitos, do INSS, da Prefeitura Municipal, Trabalhista e do CRF do FGTS.

CLÁUSULA DÉCIMA – DA GARANTIA DO CONTRATO

10.1. A CONTRATADA deverá apresentar à AGEHAB, no prazo máximo de até 15 (quinze) dias uteis, contado da data de assinatura do CONTRATO, comprovante de prestação de garantia correspondente ao percentual de 5% (cinco por cento) do valor atualizado do total do contrato, nos termos do art. 56, da Lei nº 8.666, de 1993 e instruções complementares definidas no Edital.

10.2. Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Fazenda.

10.3. Não serão admitidos, como garantia, os títulos da dívida pública, emitidos por pessoas jurídicas de direito público no período de 1850 a 1930, assim como aqueles de duvidosa liquidez, ao critério do CONTRATANTE, além de pedras preciosas, ainda que portadoras de certificado de conformação geológica.

10.4. A garantia, se prestada na forma de fiança bancária ou seguro-garantia, deverá ter validade durante a vigência do contrato.

10.5. Em se tratando de garantia prestada através de caução em dinheiro, o depósito deverá ser feito obrigatoriamente na Caixa Econômica Federal - CEF, conforme determina o art. 82 do Decreto nº 93872, de 23 de dezembro de 1986, sendo esta devolvida atualizada monetariamente, nos termo do §§ 4º, art. 56, da Lei nº 8.666/93.

10.6. No caso de garantia na modalidade de fiança bancária, deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

10.7. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser readequada nas mesmas condições.

10.8. Se o valor da garantia for utilizado, total ou parcialmente, pela CONTRATANTE, para compensação de prejuízo causado no decorrer da execução contratual por conduta da CONTRATADA, esta deverá proceder à respectiva reposição no prazo de 10 (dez) dias úteis, contados da data em que tiver sido notificada.

10.9. A garantia prestada pela CONTRATADA será liberada, após o término da vigência do Contrato, depois de certificado pelo Gestor deste Contrato que o mesmo foi Totalmente realizado a contento, dentro do prazo de 10 (dez) dias úteis.

CLÁUSULA DÉCIMA PRIMEIRA – DA FISCALIZAÇÃO DO CONTRATO

11.1. Será gestor deste contrato o empregado Sr. SAULO DE TARSO GARCIA VITOY. Este ficará responsável pelo acompanhamento da execução bem como pela fiscalização do presente instrumento, por meio de relatórios, inspeções, visitas, atestado da satisfatória realização do objeto e outros procedimentos que julgar necessário.

Agência Goiana de Habitação S/A
Rua 18-A nº 541, Setor Aeroporto - Goiânia - Goiás - 74.070-060 - (62) 3096-5000
Ouvidoria Agehab 3096-5049
Internet: www.agehab.go.gov.br
e-mail ouvidoria@agehab.go.gov.br

CLÁUSULA DÉCIMA SEGUNDA – DOS RECURSOS FINANCEIROS

12.1. As despesas decorrentes do presente contrato correrão à conta de **Recursos Próprios da AGEHAB.**

CLÁUSULA DÉCIMA TERCEIRA – DAS PENALIDADES E MULTAS

13.1. Pela inexecução contratual, atraso injustificado na execução do contrato, sujeitará a Contratada, além das cominações legais cabíveis, à multa de mora, graduada de acordo com a gravidade da infração, obedecida os seguintes limites máximos:

1) 10% (dez por cento) sobre o valor do contrato em caso de descumprimento total da obrigação;

a) Multa de até 0,1% (um décimo por cento) por semana de atraso, calculado sobre a respectiva etapa do serviço de implantação;

b) No caso de atraso superior a 90 (noventa) dias, será aplicada penalidade adicional de até (um por cento) sobre a respectiva etapa do serviço de implantação, por mês, até o limite de 10 (dez) meses;

c) No caso do não cumprimento ou cumprimento irregular dos serviços de Manutenção e Evolução Tecnológica dos Softwares ERPI; Suporte Técnico das Soluções Implementadas ERP; Treinamento nos softwares ERP será aplicada multa de até 0,2% (dois décimos por cento) sobre o valor total do Contrato, por dia de atraso, até o limite de 5% (cinco por cento);

2) 0,3% (três décimos por cento) ao dia, até o trigésimo dia de atraso, sobre o valor da parte do fornecimento não realizado;

3) 0,7% (sete décimos por cento) sobre o valor do fornecimento não realizado, por cada dia subseqüente ao trigésimo.

4) suspensão temporária do direito de participar em licitação e impedimento de contratar com a Administração Pública, por prazo não superior a 05 (cinco) anos;

5) declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação, perante a própria autoridade que aplicou a penalidade, que será concedida sempre que o contratado ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso anterior.

13.2. A multa será descontada dos pagamentos eventualmente devidos, ou ainda, quando for o caso, cobrada judicialmente.

13.3. Qualquer das penalidades aqui previstas e aplicadas será registrada junto ao

Agência Goiana de Habitação S/A
Rua 18-A nº 541, Setor Aeroporto - Goiânia - Goiás - 74.070-060 - (62) 3096-5000
Ouvidoria Agehab 3096-5049
Internet: www.agehab.go.gov.br
e-mail ouvidoria@agehab.go.gov.br

CADFOR.

CLÁUSULA DÉCIMA QUARTA – DA RESCISÃO

14.1. A rescisão do presente contrato poderá ser:

14.1.1. Determinada por ato motivado da Administração, após processo regular, assegurado o contraditório e a ampla defesa, nos casos do artigo 78, incisos I a XII, XVII e parágrafo único e inciso XVIII, da Lei Federal n° 8.666 de 21/06/1993.

14.1.2. Amigável, por acordo entre as partes, reduzida a termo, desde que haja conveniência para a Contratante.

14.1.3. Judicial, nos termos da legislação.

CLÁUSULA DÉCIMA QUINTA – DAS DISPOSIÇÕES GERAIS

15.1. O presente contrato reger-se-á pelas suas cláusulas e normas consubstanciadas na Lei Federal n° 8.666/93.

15.2. Fica declarado competente o foro da Comarca de Goiânia, para dirimir quaisquer dúvidas referentes a este contrato.

15.3. Os casos omissos serão resolvidos de acordo com a Lei nº 8.666/93, e demais normas aplicáveis.

E por estarem justos e contratados, os representantes das partes assinam o presente instrumento, na presença de testemunhas conforme abaixo, em 03(três) vias de igual teor e forma, para um só efeito.

Goiânia,_____ de _____ de 2018.

CLEOMAR DUTRA FERREIRA
Presidente

JOEL GOMES RIBEIRO
Diretor Administrativo

AMAURI BATISTA REGIS
Diretor Financeiro

_____
Representante Legal

Contratada

Testemunhas:

1 - _____

CPF:_____

2 - _____

CPF: _____

Agência Goiana de Habitação S/A
Rua 18-A nº 541, Setor Aeroporto - Goiânia - Goiás - 74.070-060 - (62) 3096-5000
Ouvidoria Agehab 3096-5049
Internet: www.agehab.go.gov.br
e-mail ouvidoria@agehab.go.gov.br