EDITAL DE LICITAÇÃO

PREGÃO ELETRÔNICO Nº 003/2017 AGR

TIPO: MENOR PREÇO GLOBAL

OBJETO: CONTRATAÇÃO DE EMPRESA ESPECIALIZA PARA FORNECIMENTO DE SOLUÇÕES DE SISTEMA DE ANTIVIRUS.

ABERTURA: 13/07/2017 - às 10:00horas

AVISO DE LICITAÇÃO

PREGÃO ELETRÔNICO Nº 003/2017
PROCESSO Nº 201700029000979 de 23/02/2017

A Agência Goiana de Regulação, Controle e Fiscalização de Serviços Públicos - AGR, por intermédio de seu Pregoeiro e Equipe de Apoio designados pela Portaria nº 007/2017 – GAB, torna público, para conhecimento dos interessados, que realizará licitação, na modalidade **Pregão (Eletrônico)**, tipo MENOR PREÇO GLOBAL, em sessão pública eletrônica a partir **10:00 horas** (horário de Brasília-DF) do dia **13/07/2017**, através do *site* www.comprasnet.go.gov.br, destinado à **CONTRATAÇÃO DE EMPRESA ESPECIALIZA PARA FORNECIMENTO DE SOLUÇÕES DE SISTEMA DE ANTIVIRUS,** nos termos da Lei Federal nº 10.520/2002, Lei Federal 8.666/1993 e suas alterações posteriores, Lei Estadual n° 17.928/2012, Decreto Estadual nº 7.468 de 20 de outubro de 2011; Decreto Estadual nº 7.466 de 18 de outubro de 2011, Decreto Estadual 7.600/2012, Lei Complementar nº 123, de 14 de dezembro de 2006 e demais normas regulamentares aplicáveis à espécie. O Edital e seus anexos encontram-se disponíveis no endereço citado abaixo ou nos *sites* www.comprasnet.go.gov.br e www.agr.go.gov.br.

Comissão Permanente de Licitação da AGR, localizada na Avenida Goiás, nº 305, Edifício Visconde de Mauá, 4º andar, Centro, CEP 74005-010 – Goiânia/GO.

Adv. Milton Elizeu da Silva
Pregoeiro

RECIBO DE EDITAL

PREGÃO ELETRÔNICO Nº 003/2017
PROCESSO Nº 201700029000979 de 23/02/2017

NOME DA LICITANTE: _____

CNPJ/MF: _____

ENDEREÇO: _____

CEP: _____ **CIDADE:** _____**ESTADO:**_____

TELEFONES: _____

FAX: _____

E-MAIL: _____

PESSOA PARA CONTATO: _____

_____, aos _____ /_____ / _____

_____
(Assinatura)

1 - ESTE RECIBO DEVERÁ SER DEVIDAMENTE PREENCHIDO E REMETIDO À GERÊNCIA DE LICITAÇÕES PARA EVENTUAIS COMUNICAÇÕES AOS INTERESSADOS, ATRAVÉS DO E-MAIL licitacaoagr@gmail.com.

2 - TODA INFORMAÇÃO ADICIONAL DESTE CERTAME SERÁ DIVULGADA CONFORME EXIGÊNCIA EM LEI. O NÃO ENVIO DESTE DOCUMENTO OU PREENCHIMENTO INCORRETO EXIME A ADMINISTRAÇÃO DA OBRIGAÇÃO DE ENVIAR DIRETAMENTE À LICITANTE EVENTUAIS INFORMAÇÕES SOBRE ESTE PREGÃO.

EDITAL DE LICITAÇÃO

PREGÃO ELETRÔNICO Nº 003/2017
PROCESSO Nº 201700029000979 de 23/02/2017

A Agência Goiana de Regulação, Controle e Fiscalização de Serviços Públicos - AGR, por intermédio de seu Pregoeiro e Equipe de Apoio designados pela Portaria nº 007/2017 – GAB, torna público para conhecimento dos interessados, que realizará licitação na modalidade **Pregão (Eletrônico)**, tipo **MENOR PREÇO GLOBAL**, em sessão pública eletrônica, através do *site* www.comprasnet.go.gov.br, nos termos da Lei Federal nº 10.520/2002, Lei Federal 8.666/1993 e suas alterações posteriores, Lei Estadual n° 17.928/2012, Decreto Estadual nº 7.468 de 20 de outubro de 2011, Decreto Estadual nº 7.466 de 18 de outubro de 2011, Decreto Estadual 7.600/2012, Lei Complementar nº 123, de 14 de dezembro de 2006 e demais normas regulamentares aplicáveis à espécie, bem como as condições estabelecidas neste Edital e seus anexos.

1 – DO OBJETO

O presente Pregão tem por objeto a **CONTRATAÇÃO DE EMPRESA ESPECIALIZA PARA FORNECIMENTO DE SOLUÇÕES DE SISTEMA DE ANTIVIRUS,** de acordo com as condições e especificações constantes no Termo de Referência, Anexo I e demais disposições fixadas neste Edital e seus Anexos.

2 – DO LOCAL, DATA E HORA

2.1 O Pregão Eletrônico será realizado em sessão pública, através do site www.comprasnet.go.gov.br, no dia **13/07/2017** a partir das **10:00 horas**, mediante condições de segurança, criptografia e autenticação, em todas as suas fases.

2.2 As Propostas Comerciais deverão ser encaminhadas, através do site www.comprasnet.go.gov.br, no período compreendido entre às**10:00 e 11:00 horas** do dia **13 de julho de 2017.**

2.3 A fase competitiva (lances) terá início, às**11:30 h** do dia **13/07/2017**, sendo iniciado procedimento de encerramento (conforme estabelecido no item 6.8) as **12:00h.**

2.4 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.

2.5 Todas as referências de tempo contidas neste Edital, no Aviso e durante a Sessão Pública observarão, obrigatoriamente, o horário de Brasília – DF e, dessa forma, serão registradas no sistema eletrônico e na documentação relativa ao certame.

3 – DAS CONDIÇÕES DE PARTICIPAÇÃO E DO TRATAMENTO DIFERENCIADO CONCEDIDO ÀS MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE

3.1 Poderão participar deste Pregão as empresas:

a) do ramo pertinente ao seu objeto, legalmente constituídos;
b) que atendam as condições estabelecidas neste Edital e seus anexos;
c) que possuam cadastro obrigatório (certificado de registro cadastral – CRC emitido pelo CADFOR ou certificado de registro cadastral que atenda aos requisitos previstos na legislação geral). O certificado de registro cadastral deverá estar homologado e válido na data de realização do Pregão. Caso o certificado de registro cadastral apresente *"status* irregular*"*, será assegurado à licitante o direito de apresentar, por e-mail, a documentação atualizada e regular na própria sessão. O licitante vencedor que se valer de outros cadastros para participar de pregão por meio eletrônico deverá providenciar sua inscrição junto ao CADFOR, como condição obrigatória para a sua contratação;
d) que, previamente, realizem o credenciamento junto ao ComprasNet.GO.

3.2 A participação neste pregão eletrônico dar-se-á por meio da digitação de login e senha privativa da licitante e subsequente encaminhamento da Proposta Comercial em data e horário previstos neste Edital, exclusivamente por meio eletrônico.

3.3 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 das exigências de habilitação previstas no Edital.

3.4 É vedada a participação de empresa:

3.4.1 Em recuperação judicial ou em processo de falência, sob concurso de credores, em dissolução ou em liquidação.

3.4.2 Que tenha sido declarada inidônea pela Administração Pública e, caso participe do processo licitatório, estará sujeita às penalidades previstas no Art. 97, parágrafo Único da Lei Federal 8.666/93.

3.4.3 Que esteja suspensa de licitar junto ao Cadastro Unificado de Fornecedores do Estado – CADFOR.

3.5 As licitantes arcarão com todos os custos decorrentes da elaboração e apresentação de suas propostas, sendo que a AGR não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

3.6 Não poderão se beneficiar do regime diferenciado e favorecido em licitações concedido às microempresas e empresas de pequeno porte pela Lei Complementar nº 123, de 14 de dezembro de 2006, licitantes que se enquadrem em qualquer das exclusões relacionadas no artigo terceiro da referida Lei.

3.7 Conforme estabelecido na Lei Estadual n° 17.928/2012 e no Decreto Estadual nº 7.466/2011, será assegurada preferência de contratação para as microempresas e empresas de pequeno porte.

3.7.1 Para usufruir dos benefícios estabelecidos na Lei Estadual n° 17.928/2012, no Decreto Estadual nº 7.466/2011 e na Lei Complementar n° 123/2006, a licitante que se enquadrar como microempresa ou empresa de pequeno porte, deverá declarar-se como tal, devendo apresentar

certidão que ateste o enquadramento, expedida pela Junta Comercial ou, alternativamente, documento gerado pela Receita Federal, por intermédio de consulta realizada no sítio www.receita.fazenda.gov.br/simplesnacional, podendo ser confrontado com as peças contábeis apresentadas ao certame licitatório.

3.7.2 O próprio sistema disponibilizará à licitante a opção de declarar-se como microempresa ou empresa de pequeno porte. A não manifestação de enquadramento, quando indagado pelo sistema eletrônico, implicará no decaimento do direito de reclamar, posteriormente, essa condição, no intuito de usufruir dos benefícios estabelecidos na Lei supramencionada.

3.7.3 Será assegurado, como critério de desempate, preferência de contratação para as microempresas e empresas de pequeno porte.

3.7.3.1 Entende-se por empate aquelas situações em que as ofertas apresentadas pelas microempresas e empresas de pequeno porte sejam iguais ou até 5% (cinco por cento) superiores ao menor preço registrado.

3.7.3.2 O critério de desempate, preferência de contratação, aqui disposto somente se aplicará quando a melhor oferta válida não tiver sido apresentada por microempresa, empresa de pequeno porte ou equiparada.

3.7.3.3 A preferência aqui tratada será concedida da seguinte forma:

I - ocorrendo empate, a microempresa, empresa de pequeno porte ou equiparada melhor classificada poderá apresentar proposta de preço inferior àquela considerada vencedora do certame, situação em que será adjudicado o objeto licitado em seu favor;

II – o direito de preferência previsto no item I será exercido, sob pena de preclusão, após o encerramento da rodada de lances, devendo ser apresentada nova proposta no prazo máximo de 05 (cinco) minutos para o lote em situação de empate;

III - no caso de igualdade dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem em situação de empate, será realizado sorteio entre elas para que se identifique aquela que poderá exercer o direito de preferência previsto no item I;

IV - na hipótese da não contratação da microempresa, empresa de pequeno porte ou equiparada com base no item I, serão convocadas as remanescentes que porventura se enquadrem em situação de empate, na ordem classificatória, para o exercício do mesmo direito.

3.7.3.4 Na hipótese da não-contratação nos termos previstos no item **3.7.3.3**, o objeto licitado será adjudicado em favor da proposta originalmente vencedora do certame.

4 – DO CREDENCIAMENTO

4.1 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 3.1.5 abaixo.

4.1.1 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.

4.1.2 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.

4.1.3 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.

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

4.1.5 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".

4.2 Os interessados que estiverem com o cadastro homologado ou "credenciados" (conforme item 3.1.5), deverão credenciar-se pelo *site* www.comprasnet.go.gov.br, opção "login do FORNECEDOR", conforme instruções nele contidas.

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

4.4 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;

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

4.6 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 AGR, promotora da licitação, responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.

4.7 As informações complementares para cadastro e credenciamento poderão ser obtidas pelos telefones **(62) 3201-6629 e 3201-6625** e para operação no sistema ComprasNet.GO pelo telefone **(62)3201-6515.**

5 – DAS PROPOSTAS COMERCIAIS

5.1 Concluída a fase de credenciamento, as licitantes registrarão suas propostas e ao término do prazo estipulado para a fase de registro de propostas, o sistema automaticamente bloqueará o envio de novas propostas.

5.2 As propostas comerciais deverão ser enviadas através do *site* http://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 previstas no Edital.

5.3 A Proposta Comercial deverá ser formulada e enviada, exclusivamente por meio do Sistema Eletrônico, **indicando o valor unitário do(s) item(s), entretanto, a disputa na fase de lances será feita pelo valor total do lote.** O ônus de comprovação de sua exequibilidade caberá exclusivamente à licitante, caso solicitado pelo pregoeiro.

5.3.1 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 2.2, não haverá possibilidade de exclusão/alteração das propostas, as quais serão analisadas conforme definido no edital.

5.4 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.

5.5 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.

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

5.7 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. **Entretanto, as empresas enquadradas no regime normal de tributação (empresas não optantes do simples), estabelecidas em Goiás, deverão registrar a proposta com preços desonerados do ICMS** conforme disposições do Art. 6º, Inc. XCI do Regulamento do Código Tributário do Estado de Goiás - RCTE, que concede isenção de ICMS nas operações e prestação internas, relativas à aquisição de bem, mercadoria e serviço por órgãos da Administração Pública Estadual Direta e suas fundações e autarquias, ficando mantido o crédito, observado, dentre outras coisas, à transferência do valor correspondente ao ICMS ao adquirente mediante a redução do preço do bem, mercadoria e serviço, devendo a redução ser demonstrada no documento fiscal.

5.7.1 Por determinação da Procuradoria-Geral do Estado através de seu Despacho "AG" nº 00123/2013, para as empresas estabelecidas em Goiás, isentas do ICMS, conforme item 4.7 acima, as propostas comerciais, enviadas pelas empresas detentoras das melhores ofertas após a fase de lances, deverão conter, obrigatoriamente, além do preço normal de mercado dos produtos ou serviços ofertados (valor bruto), o preço resultante da isenção do ICMS conferida (valor líquido), que deverá ser o preço considerado como base de julgamento. **O valor líquido será aquele registrado no sistema comprasnet.go, de acordo com determinação do item 2.2 deste edital**, e será considerado como base para etapa de lances. O valor bruto (com ICMS) servirá

apenas para efeito de análise do desconto concedido e para que as ordens de fornecimento possam apresentar os dois valores, facilitando a execução do contrato ou instrumento equivalente.

5.8 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.

5.9 A licitante detentora da melhor oferta, após a fase de lances, deverá enviar Proposta Comercial, por e-mail (documentos assinados e escaneados), devendo a mesma conter, obrigatoriamente:

a) Nome da Empresa, CNPJ, endereço, fone, 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: transporte, frete, tributos (impostos, taxas, emolumentos, contribuições fiscais e parafiscais), obrigações sociais, trabalhistas, fiscais, encargos comerciais ou de qualquer natureza, e todos os demais custos diretos e indiretos. O preço apresentado deverá ser aquele resultante da fase de lances e/ou negociação com o Pregoeiro;
d) Objeto ofertado, consoante exigências editalícias, com a quantidade licitada e o número do lote;
e) Marca do produto;
f) Prazo de validade da proposta de no **mínimo 90 (noventa) dias**, a contar da data da sessão deste Pregão Eletrônico. Caso não apresente prazo de validade será este considerado;
g) Data e assinatura do responsável;
h) A Microempresa e Empresa de Pequeno Porte detentora da melhor oferta, deverá apresentar também, conforme exigência do art. 10 do Decreto Estadual nº 7.466/2011:

h1) Certidão que ateste o enquadramento expedido pela Junta Comercial ou, alternativamente, documento gerado pela Receita Federal, por intermédio de consulta realizada no sítio www.receita.fazenda.gov.br/simplesnacional, podendo ser confrontado com as peças contábeis apresentadas ao certame licitatório;

h2) Declaração de Enquadramento na Lei Complementar nº 123/06 (conforme **Anexo III**).

6 – DA SESSÃO DO PREGÃO

6.1 O Pregoeiro via sistema eletrônico, dará início à Sessão Pública, na data e horário previstos neste Edital.

6.2 Iniciada a sessão pública do pregão eletrônico, não cabe desistência da proposta, salvo por motivo justo, decorrente de fato superveniente e aceito pelo Pregoeiro.

6.3 O Pregoeiro realizará a análise preliminar das propostas registradas conforme item 5.2 acima.

6.3.1 O Pregoeiro verificará as propostas apresentadas, desclassificando aquelas que não estejam em conformidade com os requisitos estabelecidos no edital.

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

6.3.3 Em seguida, no horário marcado será dado início à fase de lances através do sistema eletrônico, observada as regras de aceitação dos mesmos. Todos os licitantes poderão encaminhar lances exclusivamente por meio do sistema eletrônico, sendo imediatamente informados do seu recebimento e respectivo horário de registro e valor.

6.4 Durante o transcurso da sessão pública eletrônica, os licitantes serão informados, em tempo real, as mensagens trocadas no *chat* do sistema, inclusive valor e horário do menor lance registrado apresentado pelas licitantes, vedada a identificação do detentor do lance.

6.5 As licitantes poderão oferecer lances sucessivos, **pelo valor global**, observando o horário fixado e as regras de aceitação dos mesmos.

6.5.1 A licitante somente poderá oferecer lance inferior ao último por ela ofertado e registrado pelo sistema, obedecendo, quando houver, ao percentual ou valor mínimo exigido entre os lances.

6.5.2 O sistema eletrônico rejeitará automaticamente os lances em valores superiores aos anteriormente apresentados pela mesma licitante.

6.6 Não serão aceitos 02 (dois) ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado no sistema em primeiro lugar.

6.7 Caso a licitante não realize lances, permanecerá o valor da proposta eletrônica apresentada para efeito da classificação final.

6.8 A fase de lances terá duas etapas:

6.8.1 A primeira, com tempo de duração definido no item 2.3 será encerrada mediante aviso de fechamento iminente dos lances, emitido pelo sistema aos licitantes.

6.8.2 Na segunda etapa será adotada a seguinte metodologia: após transcorrido o prazo definido no referido aviso de fechamento iminente dos lances, transcorrerá o tempo de 1 (um) minuto, prorrogado sempre que houver novo lance, contado mais 1 (um) minuto a partir de cada lance, findo o qual será automaticamente encerrada a recepção de lances.

6.9 Após encerradas as operações referidas no item acima, o sistema ficará impedido de receber novos lances.

6.10 Encerrada a etapa competitiva, o Pregoeiro poderá encaminhar, pelo sistema eletrônico, contraproposta diretamente ao licitante que tenha apresentado o lance de menor valor, bem assim decidir sua aceitação, não se admitindo negociar condições diferentes daquelas previstas no edital.

6.11 O Pregoeiro sempre poderá negociar diretamente com o proponente para que seja obtido preço melhor.

7. DO JULGAMENTO DAS PROPOSTAS

7.1 O critério de julgamento é baseado no **MENOR PREÇO GLOBAL.**

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

7.3 Declarado o encerramento da etapa competitiva, o Pregoeiro examinará a aceitabilidade da primeira oferta classificada, quanto ao objeto e valor, decidindo motivadamente a respeito.

7.4 Caso não se realizem lances, será verificada a conformidade da proposta de menor preço com as exigências do Edital.

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

7.6 Sendo aceitável a oferta de menor preço, o sistema informará quem é a licitante detentora da melhor oferta. Essa licitante deverá enviar, por e-mail, a nova proposta comercial com valores readequados ao valor ofertado e registrado como de menor preço e todos os documentos exigidos no Edital e seus anexos.

7.6.1 Posteriormente deverá ser encaminhado, via correio ou representante, os memoriais originais da Proposta Comercial, conforme item 5.9, e a documentação exigida para habilitação, no original ou cópia autenticada.

7.7 Constatado o atendimento das exigências fixadas no edital, a licitante será declarada vencedora.

7.8 Se a oferta não for aceita ou se o licitante desatender às exigências habilitatórias. Pregoeiro examinará as ofertas subsequentes e a qualificação dos licitantes na ordem de classificação, e assim sucessivamente, até a apuração de uma que atenda ao edital, sendo o respectivo licitante declarado vencedor. O pregoeiro poderá negociar diretamente com o proponente para que seja obtido preço melhor (Lei Federal nº 10.520/2002 e Despacho "AG. nº 00123/2013 da Procuradoria-Geral do Estado).

7.9 Serão desclassificadas as propostas que:

a) Forem elaboradas em desacordo com as exigências do Edital e seus Anexos;
b) Apresentarem preços irrisórios, simbólicos ou abusivos, ou seja, as que apresentarem preços manifestamente inexequíveis ou superiores ao preço de mercado, de conformidade, subsidiariamente com os Arts.43, inciso IV, 44, parágrafo 3º e 48, incisos I e II da Lei 8.666/93;
c) Apresentarem propostas alternativas tendo como opção de preço ou marca, ou oferta de vantagem baseada nas propostas das demais licitantes;

7.10 Caso ocorrer desclassificação ou inabilitação por responsabilidade exclusiva da licitante, a mesma poderá sofrer as sanções previstas neste edital.

7.11 Da sessão pública do Pregão, 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.

7.12 Havendo empate, no caso de todas licitantes desistirem da fase de lances e se negarem a negociar com o Pregoeiro, serão utilizados para fins de desempate os seguintes critérios:

1º) o disposto no § 2º do Art. 3º da Lei Federal nº 8.666/93;
2º) sorteio, em ato público, para o qual todas as licitantes serão convocadas.

8 – DA HABILITAÇÃO

8.1 A habilitação da licitante detentora da melhor oferta será verificada ao final da etapa de lances.

8.2 A licitante detentora da melhor oferta, deverá atender, obrigatoriamente, às seguintes exigências, sob pena de inabilitação:

a) Encaminhar de imediato (máximo de **2 (duas) horas** ao final da fase de lances) para análise, pelo e-mail (**licitacaoagr@gmail.com**), a documentação de habilitação para as exigências não contempladas no cadastro obrigatório. Os documentos cuja regularidade deverá ser comprovada por meio de cadastro obrigatório (certificado de registro cadastral emitido pelo CADFOR ou por certificado de registro cadastral que atenda aos requisitos previstos na legislação geral) estão elencados no **Anexo II** deste Edital e dizem respeito à habilitação jurídica, regularidade fiscal e a qualificação econômico-financeira. O Certificado de Registro Cadastral – CRC, emitido pelo Cadastro Unificado de Fornecedores do Estado – CADFOR da Superintendência de Suprimentos e Logística da SEGPLAN, poderá ser impresso pelo Pregoeiro para averiguação da conformidade exigida. Caso o CRC apresente *"status* irregular*"*, será assegurado a licitante o direito de apresentar, por e-mail, a documentação atualizada e regular na própria sessão. O licitante vencedor que se valer de outros cadastros para participar de pregão por meio eletrônico deverá providenciar sua inscrição junto ao CADFOR, como condição obrigatória para a sua contratação.

b) Apresentar para fins de qualificação técnica, no mínimo 01 (um) atestado/declaração fornecido por pessoa jurídica de direito público ou privado, comprovando que a licitante já forneceu, satisfatoriamente, serviços relativo ao objeto. O atestado/declaração deverá conter, no mínimo, o nome da empresa/órgão contratante e o nome do responsável pelo mesmo.

c) Apresentar **DECLARAÇÃO**, juntamente com as demais documentações, declarando que atende plenamente ao que dispõe o Inciso XXXIII do Artigo 7º da Constituição Federal, em cumprimento ao Inciso V do Artigo 27 da Lei nº 8666/93, atestando que não possui em seu quadro, funcionários menores de 18 anos que exerçam trabalho noturno, perigoso ou insalubre, bem como que não possui nenhum funcionário menor de 16 anos, salvo na condição de aprendiz, a partir de 14 anos.

d) Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa de débitos trabalhistas (CNDT), nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei no 5.452, de 1o de maio de 1943. (Incluído pela Lei nº 12.440, de 2011).
Nota: Caso o CRC traga informação a respeito da regularidade para com a justiça do trabalho (CNDT), este será aceito em substituição à apresentação da certidão exigida nesta alínea.

8.3 A licitante detentora da melhor oferta deverá encaminhar de imediato (máximo de 02 (duas) horas ao final da fase de lances) para análise, por e-mail **(licitacaoagr@gmail.com)**, nova proposta com valores readequados ao valor ofertado e registrado como de menor lance, bem como a documentação de habilitação para as exigências não contempladas no cadastro obrigatório.

8.4 Os originais ou cópias autenticadas da documentação e proposta deverão ser encaminhados ao Pregoeiro, em no máximo de 05 (cinco) dias úteis após a da data do encerramento do Pregão, como condição indispensável para a contratação.

8.5 Os documentos extraídos via INTERNET terão seus dados conferidos pela Equipe de Apoio perante o site correspondente.

8.6 Não serão aceitos protocolos de entrega ou solicitação de documento em substituição aos documentos requeridos no presente Edital e seus Anexos.

8.7 Se a documentação de habilitação não atender às exigências deste Edital, o Pregoeiro considerará a licitante inabilitada, estando a licitante sujeita às penalidades cabíveis.

8.8 Para as **microempresas e empresas de pequeno porte**, em cumprimento Caput do Artigo 5° da Lei Estadual n° 17.928/2012, havendo alguma restrição na comprovação da regularidade fiscal das microempresas e empresas de pequeno porte, será assegurado o prazo de até 04 (quatro) dias úteis para a regularização da documentação, contados do momento em que o proponente for declarado o vencedor do certame.

8.8.1 O tratamento favorecido previsto no item 8.8 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.

8.8 O motivo da irregularidade fiscal pendente será registrado pelo Pregoeiro em ata, com a indicação do documento necessário para comprovar a regularização.

8.8.1 A não-regularização da documentação no prazo estabelecido implicará decadência do direito à contratação, sem prejuízo das sanções previstas no art. 81 da Lei n. 8.666, de 21 de junho de 1993, sendo facultado à Administração convocar os licitantes remanescentes, na ordem de classificação, para a assinatura do contrato ou instrumento equivalente, ou revogar a licitação.

8.9 A critério do Pregoeiro, os prazos constantes do item 8.6 poderão ser prorrogados.

8.10 Os documentos originais da Proposta Comercial e dos Documentos de Habilitação deverão ser enviados em envelope fechado e lacrado contendo os dizeres abaixo descritos no seguinte endereço:. Avenida Goiás, nº 305, Edifício Visconde de Mauá, 4º andar, Centro, CEP 74005-010 – Goiânia/GO.

9 – DOS RECURSOS

9.1 Declarada a vencedora, ao final da sessão, qualquer licitante poderá manifestar, motivadamente, no prazo de até **10 (dez) minutos**, a intenção de recorrer da decisão do Pregoeiro, com o registro da síntese de suas razões em campo próprio definido pelo Sistema Eletrônico.

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

9.3 A falta de manifestação imediata e motivada da licitante importará na decadência do direito de recurso.

9.4 À licitante que manifestar intenção de interpor recurso será concedido o prazo de 03 (três) dias para apresentação das razões do mesmo, através de formulário próprio do Sistema Eletrônico, ficando as demais licitantes, desde logo, intimadas a apresentar contrarrazões, se quiserem, através de formulário próprio do Sistema Eletrônico, em igual prazo, cuja contagem terá início no primeiro dia útil subsequente ao do término do prazo da recorrente.

9.5 **Não serão conhecidos** os recursos interpostos após os respectivos prazos legais, bem como os que forem enviados pelo ***chat,*** **correios ou entregue pessoalmente**.

9.6 O exame, a instrução e o encaminhamento dos recursos à autoridade competente para apreciá-los serão realizados pelo pregoeiro no prazo de até 03 (três) dias úteis, podendo este prazo ser dilatado até o dobro, por motivo justo. O encaminhamento à autoridade superior se dará apenas se o pregoeiro, justificadamente, não reformar sua decisão. A autoridade competente terá o prazo de até 03 (três) dias úteis para decidir o recurso, podendo este prazo ser dilatado até o dobro, por motivo justo, devidamente comprovado.

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

9.8 A decisão do recurso será postada nos *sites* www.comprasnet.go.gov.br e www.agr.go.gov.br.

10 – DA ADJUDICAÇÃO E DA HOMOLOGAÇÃO

10.1 Inexistindo manifestação recursal, o Pregoeiro adjudicará o objeto à licitante vencedora. Decididos os recursos, a autoridade superior fará a adjudicação do objeto da licitação.

10.2 A homologação da presente licitação compete ao Conselheiro Presidente da AGR.

11 – DO PEDIDO DE ESCLARECIMENTO E DA IMPUGNAÇÃO DO EDITAL

11.1 Qualquer cidadão ou licitante poderá solicitar esclarecimentos, providências ou impugnar o ato convocatório em até 02 (dois) dias úteis antes da data fixada para a realização da sessão pública do pregão.

11.2 Caberá ao pregoeiro decidir sobre a petição no prazo de 24 (vinte e quatro) horas.

11.3 Se reconhecida a procedência das impugnações ao instrumento convocatório, a administração procederá à sua retificação e republicação com devolução dos prazos.

11.4 Os pedidos de impugnação ou esclarecimentos ao Edital deverão ser encaminhados por escrito, ao Pregoeiro e protocolizados na Agência Goiana de Regulação, Controle e Fiscalização de Serviços Públicos - AGR, no seguinte endereço: Avenida Goiás, nº 305, Edifício Visconde de Mauá, 3º andar, Centro, CEP 74005-010 – Goiânia/GO, ou por meio do email: licitacaoagr@gmail.com.

12 – DO PAGAMENTO, DO FATURAMENTO E DO REAJUSTE

12.1 Após a homologação da licitação será emitida Nota de Empenho a favor da Adjudicatária, que após a realização dos serviços, conforme estabelecido no Termo de Referência, Anexo I, deverá protocolizar na Supervisão de Protocolo da AGR, a Nota Fiscal/Fatura correspondente.

12.2 Os pagamentos serão efetuados em até 20 (vinte) dias após protocolização e aceitação pela Contratante das Notas Fiscais/Faturas correspondentes, devidamente atestadas pela área competente da AGR. O pagamento da Nota Fiscal/Fatura fica condicionado ao cumprimento dos critérios de recebimento.

12.3 Para efetivação do pagamento, a regularidade fiscal e trabalhista deverá ser comprovada pelos documentos hábeis ou por meio do Certificado de Registro Cadastral – CRC, e outros documentos que possam ser considerados pertinentes pelo setor responsável pelo pagamento da AGR, devendo a contratada manter todas as condições de habilitação exigidas pela Lei.

12.4 Na ocorrência de rejeição da Nota Fiscal/Fatura, motivada por erro ou incorreções, o prazo para pagamento estipulado no item 12.2, passará a ser contado a partir da data da sua reapresentação.

12.5 Ocorrendo atraso no pagamento em que a contratada não tenha concorrido de alguma forma para o mesmo, a contratada fará jus a compensação financeira devida, desde a data limite fixada para pagamento até a data correspondente ao efetivo pagamento da parcela. Os encargos moratórios pelo atraso no pagamento serão calculados pela seguinte fórmula:

EM = N x Vp x (I / 365) onde:

EM = Encargos moratórios a serem pagos pelo atraso de pagamento;
N = Números de dias em atraso, contados da data limite fixada para pagamento e a data do efetivo pagamento;
Vp = Valor da parcela em atraso;
I = IPCA anual acumulado (Índice de Preços ao Consumidor Ampliado do IBGE)/100.

12.6 Para efeito de emissão da Nota Fiscal, o número do CNPJ da AGR é nº 03.537.650/0001- 69.

13 – DOS RECURSOS FINANCEIROS E DA DOTAÇÃO ORÇAMENTÁRIA

A despesa decorrente da presente licitação correrá à conta da Dotação Orçamentária nº 2017.5702.04.122.4001.4001.03 e 2017.5702.04.122.4001.4001.04 (Fonte 220).

14 – DAS PENALIDADES

14.1 Constituem ilícitos administrativos, a serem considerados em todas as modalidades licitatórias, sem prejuízo das sanções penais cabíveis, além da prática dos atos previstos nos arts. 81, 86, 87 e 88 da Lei federal nº 8.666, de 21 de junho de 1993, a prática dos atos previstos no art. 7º da Lei federal nº 10.520, de 17 de julho de 2002, ou em dispositivos de normas que vierem a substituí-los.

14.2 Ao candidato a cadastramento, ao licitante e ao contratado, que incorram nas faltas referidas no art. 77 da Lei Estadual 17.928/12, aplicam-se, segundo a natureza e a gravidade da falta, assegurados a ampla defesa e o contraditório, as sanções previstas nos arts. 86 a 88 da Lei federal nº 8.666, de 21 de junho de 1993, e no art. 7º da Lei federal nº 10.520, de 17 de julho de 2002.

14.3 Nas hipóteses previstas no art. 77 da Lei Estadual 17.928/12, o interessado poderá apresentar sua defesa no prazo de 10 (dez) dias úteis, contado da notificação do ato, sendo facultada a produção de todas as provas admitidas em direito, por iniciativa e a expensas daquele que as indicou, conforme previsto no art. 79 §§ 1º e 2º da Lei Estadual 17.928/12.

14.4 Sem prejuízo das demais sanções legais cabíveis, pelo não cumprimento dos compromissos acordados poderão ser aplicadas, a critério da AGR, as penalidades previstas nos arts. 80 a 82 da Lei Estadual 17.928/2012.

a) Aquele que, convocado dentro do prazo de validade de sua proposta, não celebrar o contrato ou instrumento equivalente, 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 ou instrumento equivalente, comportar-se de modo inidôneo ou cometer fraude fiscal, garantido o direito à ampla defesa, ficará impedido de licitar e de contratar com a Administração e será descredenciado do 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 nesse Edital e das demais cominações legais;

b) O atraso injustificado na execução do contrato ou instrumento equivalente, sujeitará a contratada, além das penalidades referidas no art. 78 da Lei Estadual 17.928/12, a multa de mora, graduada de acordo com a gravidade da infração, obedecidos os seguintes limites máximos:

I – 10% (dez por cento) sobre o valor do contrato ou instrumento equivalente, em caso de descumprimento total da obrigação, inclusive no caso de recusa do adjudicatário em retirar a nota de empenho, dentro de 10 (dez) dias contados da data de sua convocação;
II – 0,3% (três décimos por cento) ao dia, até o trigésimo dia de atraso, sobre o valor da parte do fornecimento/serviço não realizado;

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

c) Advertência;

d) A suspensão de participação em licitação e o impedimento de contratar com a Administração serão graduados pelos seguintes prazos:

I – 6 (seis) meses, nos casos de:

a) aplicação de duas penas de advertência, no prazo de 12 (doze) meses, sem que o fornecedor tenha adotado as medidas corretivas no prazo determinado pela Administração;

b) alteração da quantidade ou qualidade da mercadoria fornecida;

II – 12 (doze) meses, no caso de retardamento imotivado da execução de obra, de serviço, de suas parcelas ou do fornecimento de bens;

III – 24 (vinte e quatro) meses, nos casos de;

a) entregar como verdadeira mercadoria falsificada, adulterada, deteriorada ou danificada;

b) paralisação de serviço, de obra ou de fornecimento de bens sem justa fundamentação e prévia comunicação à Administração;

c) praticar ato ilícito visando frustrar os objetivos de licitação no âmbito da administração estadual;

d) sofrer condenação definitiva por praticar, por meio doloso, fraude fiscal no recolhimento de qualquer tributo.

e) Declaração de inidoneidade para licitar e contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação, na forma da lei, perante AGR;

f) As sanções previstas nas alíneas a), c), d) e e) poderão ser aplicadas juntamente com a da alínea b).

14.5 Antes da aplicação de qualquer penalidade será garantido à contratada direito ao contraditório e a ampla defesa. A multa poderá ser descontada dos pagamentos eventualmente devidos pela AGR ou ainda, quando for o caso, cobrada judicialmente.

14.6 As penalidades serão obrigatoriamente registradas junto ao CADFOR.

15 – DAS CONDIÇÕES PARA CONTRATAÇÃO

15.1 Após a homologação será emitida Nota de Empenho em favor da licitante vencedora. O ajuste firmado entre as partes será formalizado através da Nota de Empenho, conforme faculta

o § 4º do Art. 62 da Lei nº 8.666/93, na qual será registrado, no que couber, o disposto no Art. 55 da referida Lei.

15.2 A recusa injustificada da adjudicatária caracteriza o descumprimento total da obrigação assumida, sujeitando-a as penalidades previstas em lei, exceção feita às licitantes que se negarem a aceitar a contratação, fora da validade de suas propostas.

15.3 A rescisão das obrigações decorrentes do presente Pregão se processará de acordo com o que estabelecem os artigos 77 a 80 da Lei nº 8.666/93.

15.4 As exigências dos serviços/fornecimento, as quantidades, os prazos, bem como as demais condições constam no Termo de Referência, Anexo I deste Edital.

15.5 Caberá à contratante indicar o gestor do contrato ou instrumento equivalente, que deverá observar as disposições do Art. 67 da Lei Federal nº 8.666/93.

15.6 Como condição para celebração do contrato ou instrumento equivalente, o licitante vencedor deverá manter as condições de habilitação.

a) Se o licitante vencedor não celebrar o contrato/instrumento equivalente ou não apresentar situação regular, é facultado à Administração examinar e verificar a aceitabilidade das propostas subsequentes, na ordem de classificação, procedendo à contratação, sem prejuízo da aplicação das sanções previstas neste edital.

b) Quando da contratação com autor de proposta subsequente àquela melhor classificada, deverá a Administração negociar o valor, procurando aproximá-lo daquele ofertado inicialmente.

16 – DAS DISPOSIÇÕES GERAIS

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

16.3 A autoridade competente para determinar a contratação 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 ofício ou por provocação de qualquer pessoa, mediante ato escrito e fundamentado, conforme determinação do Art. 18 do Decreto Estadual nº 7.468/2011.

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

16.5 Na contagem dos prazos previstos neste Edital excluir-se-á o dia do início e incluir-se-á o do vencimento, considerando-se os dias consecutivos, exceto quando houver disposição em contrário. Somente se iniciam e vencem os prazos em dia de expediente regular e integral na AGR.

16.6 As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, a finalidade e segurança da contratação.

16.7 A contratada é obrigada a aceitar, nas mesmas condições da licitação, os acréscimos ou supressões, nos termos do § 1º do Artigo 65 da Lei Federal nº 8.666/93.

16.8 As informações e/ou esclarecimentos serão prestados pelo Pregoeiro através dos sites www.comprasnet.go.gov.br e www.agr.go.gov.br ficando todos os Licitantes obrigados a acessá-los para obtenção das informações prestadas pelo Pregoeiro.

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

16.10 Havendo divergências entre a descrição do objeto constante no Edital e a descrição do objeto constante nos *sites* www.comprasnet.go.gov.br e www.agr.go.gov.br e nota de empenho, prevalecerá, sempre, a descrição deste Edital.

16.11 Em qualquer fase da licitação, o Pregoeiro poderá promover diligência destinada a esclarecer ou complementar a instrução do processo, bem como sanear os erros de pequena relevância, mediante ato devidamente motivado.

16.12 Em conformidade com o art. 3º do Decreto nº 7.569/2012, serão isentas do ICMS, as operações e prestação internas, relativas à aquisição de bem, mercadoria e serviço por órgãos da Administração Pública Estadual Direta e suas Fundações e Autarquias, ficando mantido o crédito, observado o seguinte (Convênio ICMS 26/03).

16.13 Para dirimir as questões relativas ao presente Edital elege-se como foro competente o de Goiânia – GO, com exclusão de qualquer outro.

17 – DOS ANEXOS

Constituem Anexos do Edital e dele fazem parte integrante:

ANEXO I – Termo de Referência
ANEXO II – Relação de Documentos que deverão ser substituídos pela apresentação do Certificado de Registro Cadastral – CRC
ANEXO III – Declaração de Enquadramento na Lei Complementar nº 123/06

Goiânia, 10 de abril de 2017.

Adv. Milton Elizeu da Silva
Pregoeiro

ANEXO I

TERMO DE REFERÊNCIA

PREGÃO ELETRÔNICO Nº 003/2017

1. Objeto

Aquisição de solução de segurança integrada para estação de trabalho e ambiente corporativo, baseado nas soluções de mercado com foco na monitoração e proteção da segurança tecnológica, por conseguinte em sua implantação, configuração, garantia, suporte e transferência de conhecimento.

2. Justificativa

Aquisição de solução de antivírus para proteger os computadores e equipamentos servidores da Agência Goiana de Regulação, Controle e Fiscalização de Serviços Públicos - AGR de diferentes tipos de softwares maliciosos (trojans, worms, etc.). A solução de antivírus da AGR contemplava 251 licenças do fabricante adquiridas no ano de 2014 e as mesmas venceram em março/2017. Com o aumento do número de estações de trabalho desktop, a AGR necessita de ao todo 300 licenças de antivírus.

A contratação justifica-se para integrar o conjunto de soluções que compõem o sistema de segurança computacional do órgão e salvaguarda dos serviços de TI proporcionando condições de continuidade dos trabalhos internos e externos da AGR quanto ao fornecimento de serviços obrigatórios desta Agência. A escolha do fabricante Symantec deve-se à padronização da solução junto aos outros órgãos do estado de Goiás.

3. Quantitativos

3.1. Fazem parte da contratação, para a qual se destina este edital, visando a efetiva operacionalização e funcionamento da solução por completo os seguintes itens:

3.1.1. Implantação da solução;
3.1.2. Configuração;
3.1.3. Garantia;
3.1.4. Transferência de conhecimento;

Quantidade	Descrição	Período Licença	Preço Unitário	Preço Total
300	Aquisição de Solução de Proteção de Estação de Trabalho, Servidores, mensageria e segurança correio eletrônico. Symantec Protection Suite – Enterprise Edition 12 meses.	12 meses	R$ 303,72	R$ 91.117,00
1	Serviço de instalação presencial para 300 licenças	n/a	R$ 15.547,26	R$ 15.547,26
Total Geral				**R$ 106.664,26**

4. Especificações da Solução de Proteção de Estação de Trabalho e Equipamentos Servidores

4.1. Solução para "Proteção de Estação de Trabalho e Equipamentos Servidores", deve combinar Antivírus com uma prevenção avançada contra ameaças, IPS / IDS, Firewall, Reputação, visando fornecer uma defesa contra malware para laptops, desktops e equipamentos servidores. Integrando tecnologias de segurança essenciais em um único agente e console de gerenciamento, acarretando no aumento da proteção.

4.2. Software de proteção do endpoint deve ter a capacidade de implementar, no mínimo, as seguintes funcionalidade:

4.2.1. Reputação de Arquivos sejam locais como no acesso web;

4.2.2. IPS de Próxima Geração (Next Generation IPS);

4.2.3. Proteção de Navegadores (Browser Protection);

4.2.4. Aprendizado de Máquinas (Machine Learning);

4.2.5. Análise Comportamental (Behavioral Analysis);

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

4.2.7. Controle de Aplicações (Application Control);

4.2.8. Controle de Dispositivos (Device Control);

4.2.9. Emulação para Malware (Emulation for Malware);

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

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

4.3.1. Exploração de navegadores com reputação de URL;

4.3.2. Websites infectados com reputação de URL;

4.3.3. Office Exploits com reputação de URL;

4.3.4. Arquivos anexos com reputação de arquivos;

4.3.5. Download de arquivos com reputação de arquivos;

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

4.3.7. Instalação de software com as técnicas de Malheur;

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

4.3.9. Cópia de arquivos com as técnicas de Malheur;

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

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

4.3.12. A funcionalidade de “Machine Learning” deve trabalhar baseado no mínimo nas seguintes premissas:

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

4.3.14. Bloqueio de URL’s de má reputação;

4.3.15. Bloqueio das instruções de “Command & Control”;

4.3.16. Atualização da base de reputação de Arquivos com a periodicidade mínima de 2,5 horas;
4.3.17. Bloqueio das ameaças polimorfas mesmo que arquivos desconhecidos;
4.3.18. Prevenção de Falso Positivos;
4.3.19. Bloqueio de malwares desconhecidos e suas variantes;
4.3.20. Implementar a classificação comportamental dos arquivos;
4.3.21. "Aprendizado" a partir dos indicadores de compromisso (IoC);

4.4. A funcionalidade de "Machine Learning" deve ter a capacidade de implementar uma análise em tempo real correlacionando entre:
4.4.1. Veredicto das análises entre usuários da plataforma de segurança do mesmo fabricante;
4.4.2. Arquivos de softwares mundialmente espalhados na rede mundial de computadores;
4.4.3. Sites Web mundialmente espalhados pela rede mundial de computadores;

4.5. A funcionalidade de emulação para malware deve a partir do software de proteção de endpoint, implementar a emulação em um ambiente virtual (local) possibilitando detectar e impedir as técnicas de evasão de detecção, mesmo que utilizando polimorfismo no seu empacotamento;
4.6. A funcionalidade de emulação para malware de ser suportada para as plataformas Windows (32 e 64 bits), Linux (64 bit) e Mac (64 bit);
4.7. O software de proteção dos endpoints deve ter a funcionalidade específica de impedir as técnicas de manipulação e randomização de memória impossibilitando a exploração de vulnerabilidades em aplicações, para no mínimo:
4.7.1. Adobe PDF;
4.7.2. Flash;
4.7.3. Java;
4.7.4. Navegadores (Internet Explorer, Chorme e Firefox);
4.8. O software de proteção do endpoint deve ter a capacidade de impedir os ataques direcionados mesmo que utilizando as vulnerabilidades de dia zero, mitigando no mínimo os conhecidos comportamentos de exploração de vulnerabilidades:
4.8.1. SEHOP - Structured Exception Handler Overwrite Protection;
4.8.2. Heap Spray (Exploits que iniciam através do HEAP);
4.8.3. Java Exploit Protection;
4.9. O software de proteção do endpoint deve ter a capacidade de bloquear exploits que trabalham em nível de "shell code", assim como, implementar a funcionalidade de "virtual patching" para as aplicações;
4.10. O software de proteção do endpoint deve ter a capacidade de implementar integração entre a gerência central com plataformas de terceiros, possibilitando no mínimo:
4.10.1. Capturas de Login e Logout na Gerência Central
4.10.2. Captura dos detalhes das máquinas protegidas
4.10.3. Captura dos detalhes de Domínios implementados pelo software
4.10.4. Captura dos detalhes de Grupos implementados pelo software
4.10.5. Captura da lista de "Fingerprint" de aplicações (Blacklisting)
4.10.6. Captura da atualização da lista de "Fingerprint" de aplicações (Blacklisting)
4.10.7. Captura dos detalhes das políticas aplicadas

4.10.8. Captura das atualizações dos detalhes das políticas aplicadas
4.10.9. Captura da lista dos usuários administradores da solução
4.10.10. Criação de novos administradores da solução
4.10.11. Capacidade de mover clientes de endpoints entre grupos lógicos
4.11. O software de proteção do endpoint deve ter a capacidade de receber instruções de comando e ações diretamente do módulo de proteção contra ataques de APT (Advanced Persistent Threats), sem a necessidade de interpretação pelo gerenciador do endpoint, possibilitando ações mais rápidas, assertivas e minimizando falsos positivos;
4.12. A solução deve ter as capacidade de implementar técnicas de EDR (Endpoint Detection and Response), possibilitando detecção e investigação nos endpoints com atividades suspeitas;
4.13. Gerenciamento
4.13.1. Deve ter administração centralizada por console único de gerenciamento;
4.13.2. Deve ter acesso a console de gerenciamento via tecnologia Web (HTTP e HTTPS);
4.13.3. Deve estabelecer uma correlação de eventos entre os softwares gerenciados, possibilitando priorização nas ações tomadas;
4.14. Console de Gerenciamento
4.14.1. Administração centralizada por console único de gerenciamento;
4.14.2. As configurações do Antivírus, AntiSpyware, Firewall, Proteção Contra Intrusos, controle de Dispositivos e Controle de Aplicações deverão ser realizadas para máquinas físicas e virtuais através da mesma console;
4.14.3. Toda a solução deverá funcionar com agente único na estação de trabalho e servidores físicos e virtuais a fim de diminuir o impacto ao usuário final;
4.14.4. Mecanismo de comunicação (via push) em tempo real entre servidor e clientes, para entrega de configurações e assinaturas;
4.14.5. Mecanismo de comunicação randômico (via pull) em tempo determinado pelo administrador entre o cliente e servidor, para consulta de novas configurações e assinaturas evitando sobrecarga de rede e servidor;
4.14.6. Permitir a divisão lógica dos computadores, dentro da estrutura de gerenciamento, em sites, domínios e grupos, com administração individualizada por domínio;
4.14.7. O servidor de gerenciamento deverá possuir compatibilidade para instalação nos sistemas operacionais Microsoft Windows Server 2008, 2008 R2 ou superior;
4.14.8. O servidor de gerenciamento deverá possuir compatibilidade para instalação em sistemas operacionais 32-bit e 64-bit suportando ambiente virtual XEN, VMWARE e Microsoft;
4.14.9. Possuir integração com LDAP, para importação da estrutura organizacional e autenticação dos Administradores;
4.14.10. Possibilidade de aplicar regras diferenciadas baseando na localidade lógica da rede;
4.14.11. Permitir que a localidade lógica da rede seja definida pelo conjunto dos seguintes itens:
4.14.11.1. IP e range de IP
4.14.11.2. Endereço de Servidores de DNS, DHCP e WINS
4.14.11.3. Conexão com o servidor de gerência
4.14.11.4. Conexões de rede como VPN, Ethernet, Wireless e Modem

4.14.12. Possibilidade de aplicar regras diferenciadas por grupos de usuários e máquinas;
4.14.13. O servidor de gerenciamento deverá permitir o uso de banco de dados relacional Microsoft SQL Server nas versões 2008, 2012 e 2014;
4.14.14. Possuir a funcionalidade e recursos para a criação e agendamento periódicos de backups da base de dados ou fornecer uma ferramenta para tal finalidade;
4.14.15. Permitir a opção instalação de Servidores de Gerenciamento adicionais fornecendo assim a possibilidade de trabalhar em modo de Load Balance e Failover.
4.14.16. Possuir na solução replicação nativa do Banco de Dados entre os Servidores de Gerenciamento com opção de customização do conteúdo à ser replicado (Assinaturas, Pacotes de Instalação, Políticas e Logs);
4.14.17. Possibilidade de instalação dos clientes em servidores, estações de trabalho e máquinas virtualizadas de forma remota via console de gerenciamento com opção de remoção de soluções previamente instaladas;
4.14.18. Permitir a instalação remota do software por Group Policy (GPO), Web e via console de gerenciamento;
4.14.19. Descobrir automaticamente as estações da rede que não possuem o cliente instalado;
4.14.20. Fornecer ferramenta de pesquisa de estações e servidores da rede que não possuem o cliente instalado com opção de instalação remota;
4.14.21. Fornecer atualizações do produto e das definições de vírus e proteção contra intrusos;
4.14.22. A console de gerenciamento deve permitir travar as configurações por senha nos clientes servidores e estações físicos e virtuais definindo permissões para que somente o administrador possa alterar as configurações, desinstalar ou parar o serviço do cliente;
4.14.23. A console de gerenciamento deve permitir ao administrador travar separadamente os itens e cada subitens de acesso às configurações do cliente;
4.14.24. Capacidade de criação de contas de usuário com diferentes níveis de acesso de administração e operação;
4.14.25. Instalação e atualização do software sem a intervenção do usuário;
4.14.26. Possibilidade de configurar o bloqueio da desinstalação, desabilitar o serviço do cliente, importar e exportar configurações e abrir a console do cliente, por senha;
4.14.27. Suportar redirecionamentos dos logs para um servidor de Syslog;
4.14.28. Utilizar os protocolos HTTP e HTTPS para comunicação entre console de gerenciamento e o cliente gerenciado;
4.15. Atualização de Vacinas
4.15.1. Atualização incremental, remota e em tempo-real, da vacina dos Antivírus mecanismo de verificação (Engine) dos clientes da rede;
4.15.2. Permitir criar planos de distribuição das atualizações via comunicação segura entre cliente e Servidores de Gerenciamento, Site do fabricante, Via Servidor de atualização interno e podendo eleger qualquer cliente gerenciado para distribuição das atualizações;
4.15.3. Permitir eleger qualquer cliente gerenciado como um servidor de distribuição das atualizações com opção de controle de banda, quantidades de definições e espaço em disco utilizado, podendo eleger mais de um cliente para esta função;

4.15.4. Atualização remota e incremental da versão do software cliente instalado;
4.15.5. Nas atualizações das configurações e das definições de vírus não poderá utilizar login scripts, agendamentos ou tarefas manuais ou outros módulos adicionais que não sejam parte integrante da solução e sem requerer reinicialização do computador ou serviço para aplicá-la.
4.15.6. Atualização automática das assinaturas do servidores de gerenciamento e clientes via Internet, com periodicidade mínima diária;
4.15.7. Capacidade de voltar qualquer vacina e assinatura anterior armazenadas no servidor, utilizando opção e comando do Console podendo utilizar a arquitetura de grupos lógicos da console;
4.15.8. Um único e mesmo arquivo de vacina de Vírus para todas as plataformas Windows e versões do antivírus.
4.16. Quarentena
4.16.1. Possuir funcionalidades que permitam o isolamento (área de quarentena) de arquivos contaminados por códigos maliciosos que não sejam conhecidos ou que não possam ser reparados em um servidor central da rede;
4.16.2. Forma automática de envio dos arquivos da área de isolamento central para o fabricante, via protocolo seguro, onde este será responsável por gerar a vacina, automaticamente, sem qualquer tipo de intervenção do administrador. Recebimento utilizando o mesmo método e aplicação da vacina recém criada nas estações infectadas.
4.16.3. Possibilidade de adicionar manualmente arquivos na quarentena do cliente com opção de restrições na console de gerenciamento;
4.16.4. Rastreamento agendado contra vírus com a possibilidade de selecionar uma máquina ou grupo de máquinas para rastrear com periodicidade mínima diária;
4.16.5. Rastreamento remoto contra vírus com a possibilidade de selecionar uma máquina ou grupo de máquinas para rastrear;
4.17. Cliente Gerenciado
4.17.1. Deve ter a capacidade de compor de forma nativa com a solução de APT do mesmo fabricante, sem a necessidade da implementação de scripts, utilizando apenas configurações realizadas na console padrão do produto;
4.17.2. Suportar máquinas com arquitetura 32-bit e 64-bit;
4.17.3. O cliente para instalação em estações de trabalho deverá possuir compatibilidade com no mínimo os sistemas operacionais:
4.17.3.1. Windows 2008, 2008 R2;
4.17.3.2. Windows 2012;
4.17.3.3. Windows 7;
4.17.3.4. Windows 8;
4.17.3.5. Windows 10;
4.17.3.6. Mac OS X Server 10.6, 10.7, 10.8, 10.9;
4.17.3.7. Mac OS X 10.6.8, 10.7, 10.8, 10.9, 10.10;
4.17.3.8. Red Hat Enterprise Linux;
4.17.3.9. Debian;
4.17.3.10. Oracle Linux;
4.17.3.11. Novell Open Enterprise Server;
4.17.3.12. SUSE Linux Enterprise (server e desktop);
4.17.3.13. Fedora;
4.17.3.14. Ubuntu;

4.17.4. O cliente para instalação em servidores deverá possuir compatibilidade com no mínimo os sistemas operacionais:
4.17.4.1. Windows 2008, 2008 R2;
4.17.4.2. Windows Small Business Server 2011 (64-bit);
4.17.4.3. Windows Server 2012, 2012 R2;
4.17.4.4. Windows 7;
4.17.5. Possuir certificação FIPS 140-2;
4.18. Funcionalidade de Firewall e Detecção e Proteção de Intrusão (IDS\IPS) com as funcionalidades
4.18.1. Suporte aos protocolos TCP, UDP e ICMP;
4.18.2. Reconhecimento dos tráficos DNS, DHCP e WINS com opção de bloqueio;
4.18.3. Possuir proteção contra exploração de buffer overflow;
4.18.4. Possuir proteção contra ataques de Denial of Service (DoS), Port-Scan Mac Spoofing;
4.18.5. Possibilidades de criação de assinaturas personalizadas para detecção de novos ataques;
4.18.6. Possibilidade de agendar a ativação da regra de Firewall;
4.18.7. Possibilidade de criar regras diferenciadas por aplicações;
4.18.8. Possibilidade de reconhecer automaticamente as aplicações utilizadas via rede baseado no fingerprint do arquivo;
4.18.9. Proteger o computador através da criação de uma impressão digital para cada executável existente no sistema, para que somente as aplicações que possuam essa impressão digital executem no computador;
4.18.10. Funcionalidade de Whitelist e Blacklist para o recurso de Impressão digital para os executáveis, possibilitando bloquear todos os executáveis da lista ou só liberar os executáveis da lista;
4.18.11. Permitir criação de zona confiável, permitindo que determinados IPs, protocolos ou aplicações se comuniquem na rede;
4.18.12. Bloqueio de ataques baseado na exploração da vulnerabilidade;
4.18.13. Gerenciamento integrado à console de gerência da solução;
4.19. Funcionalidade de Antivírus e AntiSpyware as funcionalidades:
4.19.1. Proteção em tempo real contra vírus, trojans, worms, cavalos-de-tróia, spyware, adwares e outros tipos de códigos maliciosos.
4.19.2. Proteção anti-spyware deverá ser nativa do próprio antivírus, ou seja, não dependente de plugin ou módulo adicional;
4.19.3. As configurações do anti-spyware deverão ser realizadas através da mesma console de todos os itens da solução;
4.19.4. Permitir a configuração de ações diferenciadas para cada subcategoria de riscos de segurança (Adware, Discadores, Ferramentas de hacker, Programas de brincadeiras, Acesso remoto, Spyware, Trackware e outros);
4.19.5. Permitir a configuração de duas ações, primária e secundária, executadas automaticamente para cada ameaça, com as opções de: somente alertar, limpar automaticamente, apagar automaticamente e colocar em quarentena;
4.19.6. Permitir a criação de listas de exclusões com informação da severidade, impacto e grau de remoção da ameaça nos níveis baixo, médio ou alto, onde os riscos excluídos não serão verificados pelo produto;
4.19.7. Permitir que verificação das ameaças da maneira manual, agendada e em Tempo-Real detectando ameaças no nível do Kernel do Sistema Operacional fornecendo a possibilidade de detecção de Rootkits;

4.19.8. Implementar intervalos de tempo para início de verificações agendadas de forma a reduzir impacto em ambientes virtuais.
4.19.9. Possuir funcionalidades que permitam o isolamento (área de quarentena) de arquivos contaminados por códigos maliciosos que não sejam conhecidos ou que não possa ser reparados no cliente;
4.19.10. Possuir funcionalidades que permitam a inclusão manual em isolamento (área de quarentena) de arquivos a serem enviados e vistoriados pelo centro de pesquisa do fabricante.
4.19.11. Permitir configurar ações a serem tomadas na ocorrência de ameaças, incluindo Reparar, Deletar, Mover para a Área de Isolamento e Ignorar;
4.19.12. Verificação de vírus nas mensagens de correio eletrônico, pelo antivírus da estação de trabalho, suportando clientes Outlook, Notes e POP3/SMTP;
4.19.13. Possuir funcionalidades que permitam a detecção e reparo de arquivos contaminados por códigos maliciosos mesmo que sejam compactados por ZIP, LHA e ARJ, tendo como abrangência até o 10º (décimo) nível de compactação;
4.19.14. Capacidade de detecção em tempo real de vírus novos, desconhecidos pela vacina com opção da sensibilidade da detecção (baixo, médio e alto);
4.19.15. Capacidade de remoção automática total dos danos causados por spyware, adwares e worms, como limpeza do registro e pontos de carregamento, com opção de terminar o processo e terminar o serviço da ameaça no momento de detecção;
4.19.16. A remoção automática dos danos causados deverá ser nativa do próprio antivírus, ou seja, não dependente de plugin, execução de arquivo ou módulo adicional;
4.19.17. Capacidade de identificação da origem da infecção por vírus que utilizam compartilhamento de arquivos como forma de propagação informando nome ou IP da origem com opção de bloqueio da comunicação via rede;
4.19.18. Possibilidade de bloquear verificação de vírus em recursos mapeados da rede, por senha;
4.19.19. Criar uma cópia backup do arquivo suspeito antes de limpá-lo;
4.19.20. Gerenciamento integrado à console de gerência da solução;
4.19.21. Possibilitar a criação de um disco (CD ou DVD) inicializável para verificação e remoção de ameaças sem a necessidade de carregar o Sistema Operacional do cliente.
4.19.22. Capacidade de executar varreduras em tempo real (real-time) contra ataques dirigidos à vulnerabilidades do navegador (browser);
4.19.23. Possuir funcionalidades de otimização de scans em ambientes virtuais, contemplando os virtualizadores VMWare, Citrix e Microsoft, para no mínimo:
4.19.23.1. Diferenciação automática entre máquinas físicas e virtuais, possibilitando aplicar as funcionalidades específicas para as máquinas virtuais;
4.19.23.2. Proteção com as mesmas funcionalidades aplicáveis em máquinas físicas, para no mínimo:
4.19.23.2.1. Proteção de antivírus e antispyware;
4.19.23.2.2. Proteção de heurística e reputação de arquivos em tempo real (real-time);
4.19.23.2.3. Proteção de IPS de rede e “host”;
4.19.23.2.4. Controle de dispositivos e aplicações;

4.19.23.3. Cache local na reputação de arquivos, possibilitando não varrer arquivos categorizados como não maliciosos e já escaneados anteriormente;
4.19.23.4. Capacidade de verificar "templates" de máquinas virtuais, excluindo da operação de varredura todos os arquivos categorizados como confiáveis, existentes na máquina virtual utilizada como origem (template);

4.19.24. Capacidade de implementar varreduras otimizadas em máquinas físicas e virtuais, onde o arquivo verificado pela varredura uma vez, não será verificado novamente, até que ocorra alguma alteração no mesmo;
4.19.25. Capacidade de realizar monitoramento em tempo real (real-time) por heurística correlacionando com a reputação de arquivos;
4.19.26. Capacidade de verificar a reputação de arquivos, correlacionando no mínimo as seguintes características:
4.19.26.1. Origem confiável;
4.19.26.2. Origem não confiável;
4.19.26.3. Tempo de existência do arquivo na internet;
4.19.26.4. Comportamento do arquivo;
4.19.26.5. Quantidade mínima de usuários que baixaram o arquivo da internet;
4.19.27. Capacidade de implementar regras distintas por grupo (ex. Departamentalmente), a partir do resultado da reputação, em conjunto com o correlacionamento da quantidade de utilizadores do arquivo e tempo de existência do mesmo;
4.20. Funcionalidade de detecção Proativa de reconhecimento de novas ameaças com as funcionalidades
4.20.1. Funcionalidade de detecção de ameaças desconhecidas que estão em memória por comportamento dos processos e arquivos das aplicações;
4.20.2. Não utilizar a assinatura de vírus para esta funcionalidade e fornecer assinatura periódicas da técnica de detecção;
4.20.3. Capacidade de detecção keyloggers, Trojans, spyware e Worms por comportamento dos processos em memória, com opção da sensibilidade distintas da detecção;
4.20.4. Reconhecimento comportamento malicioso de modificação da configuração de DNS e arquivo Host;
4.20.5. Possuir a funcionalidade de exclusão de detecção diferenciada do recurso de Antivírus;
4.20.6. Possibilidade de habilitar o recurso de correlacionamento da funcionalidade de detecção Proativa com a base de reputação do fabricante;
4.20.7. Capacidade de detecção de Trojans e Worms por comportamento dos processos em memória, com opção da sensibilidade distintas da detecção;
4.20.8. Possibilidade de agendar o escaneamento da detecção Proativa com periodicidade mínima por minuto e em todos os novos processos;
4.20.9. Possibilidade de agendar o escaneamento da detecção Proativa com periodicidade mínima por minuto e em todos os novos processos;
4.21. Funcionalidade de Controle de Dispositivos e Aplicações
4.21.1. Gerenciar o uso de dispositivos USB e CD/DVD, através de controles de leitura/escrita/execução do conteúdo desses dispositivos e também sobre o tipo de dispositivo permitido (ex: permitir mouse USB e bloquear disco USB);

4.21.2. Controlar o uso de dispositivos com comunicação infra-vermelho, firewire, PCMCIA, portas seriais e paralelas, através de mecanismos de permissão e bloqueio identificando pelo "Class ID" e pelo "Device ID" do Dispositivo;
4.21.3. Permitir criar políticas de bloqueio de dispositivos baseadas na localização atual da estação;
4.21.4. Gerenciamento integrado à console de gerência da solução;
4.21.5. Oferecer proteção para o sistema operacional, permitindo a definição de controles de acesso (escrita/leitura) para arquivos, diretórios, chaves de registro e controle de processos;
4.21.6. Permitir o bloqueio do uso de aplicações baseada em nome, diretório e hash da aplicação;
4.21.7. O software de proteção do endpoint deve ter a capacidade de implementar controle de dispositivos para leitura, escrita e execução em MAC OSx, para no mínimo:
4.21.7.1. USB;
4.21.7.2. Firewire;
4.21.7.3. Thunderbolt;
4.21.7.4. CD/DVD/BR;
4.21.7.5. SD Card;
4.21.7.6. eSATA;
4.21.8. O software de proteção do endpoint deve ter a capacidade de implementar controle de dispositivos para MAC OSx, possibilitando regras de “white list” e “black list” utilizando expressões regulares, assim como, possibilidade de implementar teste de regras sem impactar na produção;
4.21.9. O software de proteção do endpoint deve ter a capacidade de implementar controle de dispositivos para MAC OSx, possibilitando administração por parte do usuários e administração remota, com a possibilidade de monitoração e relatórios a partir da console de administração;
4.22. Relatórios e Monitoramentos com as funcionalidades
4.22.1. Possuir, pelo menos, 25 tipos de relatórios diferentes, permitindo a exportação para o formato HTML;
4.22.2. Recursos do relatório e monitoramento deverão ser nativos da própria console central de gerenciamento;
4.22.3. Possibilidade de exibir a lista de servidores e estações que possuam o antivírus instalado, contendo informações como nome da máquina, usuário logado, versão do antivírus, versão do engine, data da vacina, data da última verificação e status (com vírus, desatualizada etc.);
4.22.4. Capacidade de Geração de relatórios, estatísticos e gráficos contendo no mínimo os seguintes tipos pré-definidos:
4.22.4.1. As 10 máquinas com maior ocorrência de códigos maliciosos;
4.22.4.2. Os 10 usuários com maior ocorrência de códigos maliciosos;
4.22.4.3. Localização dos códigos maliciosos;
4.22.4.4. Sumários das ações realizadas;
4.22.4.5. Número de infecções detectadas diário, semanal e mensal;
4.22.4.6. Códigos maliciosos detectados.
4.23. Suporte a clientes Mac OS X
4.23.1. O cliente para instalação em estações de trabalho e servidores deverá possuir compatibilidade com o sistema operacional Mac OS X para as funcionalidades de antivírus e antispyware.

4.23.2. O cliente para instalação deverá possuir compatibilidade com os sistemas operacionais Apple Mac OS X 10.5 (Leopard) e 10.6 (Snow Leopard), Mac Os X Server 10.5 e 10.6 em processadores 32 e 64 bits;
4.23.3. Suporte ao Apple Remote Desktop para instalação e atualização remota da solução;
4.23.4. Gerenciamento integrado à console de gerência da solução;
4.23.5. Proteção em tempo real contra vírus, trojans, worms, cavalos-de-tróia, spyware, adwares e outros tipos de códigos maliciosos.
4.23.6. Permitir que verificação das ameaças da maneira manual e agendada;
4.23.7. Permitir a criação de listas de exclusões para pastas e arquivos que não serão verificados pelo antivírus;
4.23.8. Permitir a ações de reparar arquivo ou quarentenar em caso de infeções a arquivos;
4.24. Console avançada de distribuição e relatórios
4.24.1. Console de gerenciamento via tecnologia Web (HTTP e HTTPS) independente da console central da solução;
4.24.2. Possibilidade de executar inventário do ambiente e descobrir os antivírus e respectivas versões;
4.24.3. Detectar e desinstalar soluções de antivírus dos seguintes fabricantes:
4.24.3.1. CA
4.24.3.2. ESET
4.24.3.3. F-Secure
4.24.3.4. Kaspersky
4.24.3.5. McAfee
4.24.3.6. Sophos
4.24.3.7. Symantec
4.24.3.8. Trend Micro
4.24.4. Permitir a remoção de outros softwares não desejados;
4.24.5. Criar tarefas de migração baseadas no resultado do inventário de antivírus;
4.24.6. Permitir agendamento e implementar controle de banda para minimizar impacto na rede durante o processo de instalação em clientes;
4.24.7. Possibilidade de recuperar instalação em clientes em caso de falha;
4.24.8. Oferecer relatórios avançados através da criação de cubos OLAP e tabelas Pivot;
4.24.9. Os seguintes cubos devem ser disponibilizados para criação de relatórios:
4.24.9.1. Alertas;
4.24.9.2. Clientes;
4.24.9.3. Políticas;
4.24.9.4. Rastreamento;
4.24.10. Possibilidade de criação de indicadores de performance para medir eficácia da solução de segurança;
4.24.11. Exportar os relatórios criados nos formados xls, pdf e html;
4.25. Funcionalidades do Controle de Acesso à Rede
4.25.1. Deve possibilitar a colocação dos equipamentos em quarentena, restringindo o acesso à rede para aqueles computadores que não estiverem em conformidade com as políticas, para no mínimo as seguintes premissas:
4.25.1.1. Computador deve possuir antivírus, atualizados e ativo;
4.25.1.2. Computador deve possuir firewall ativo;
4.25.1.3. Computador deve possuir antispyware, atualizado e ativo;
4.25.1.4. Computador deve possuir patches instalados, ativos e atualizados;

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

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

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

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

4.26. Ponto de Reforço no Próprio Agente

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

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

5. Especificações da Solução de Segurança de Mensageria

5.1. A solução de "Segurança de Mensageria" deve integrar a captura eficiente de spams com baixa taxa de categorização das mensagens como falsos positivos. Implementado como gateway de e-mails, deve proteger e-mails e mensagens instantâneas contra vírus, spams, phishing, botnets e outros e-mails indesejados. Deve incorporar recursos flexíveis para o gerenciamento de spams e atualizações automatizadas de filtros.

5.2. Características Gerais do Produto

5.2.1. Deve possuir possibilidade de ser fornecido em modelo appliance;

5.2.2. Deve possuir possibilidade de ser fornecido em modelo virtual-appliance, compatível com VMWARE ESX e ESXi;

5.2.3. Sistema operacional da solução “pre-hardened”, com limitação dos serviços em uso;

5.2.4. Deve ter a capacidade de integração com solução de Data Loss Prevention, para os e-mails de saída, possibilitando utilização de mais de um servidor de DLP, para um mesmo Gateway de SMTP;

5.2.5. Deve ter a capacidade de priorização dos servidores de DLP utilizados na integração com o Gateway de SMTP, possibilitando balancear o tráfego a ser analisado;

5.2.6. Deve ter a capacidade de arquivar qualquer mensagem que viole as políticas corporativas, enviando-as para a estrutura de arquivamento do órgão;

5.2.7. Deve ter capacidade de integração com servidor de criptografia, para criptografar mensagens e anexos;

5.2.8. Deve ter a capacidade de permitir ou não endereços de e-mail com caracteres especiais, para no mínimo percentagem (%), hífen (-) e caracteres 8-bit;

5.2.9. Deve ter a capacidade de rejeitar conexões que tentem serem abertas pelos comandos “HELO” e “EHLO”, sem que existam gravados seus endereços de “MX” e “A” nos servidores de DNS;

5.2.10. Deve ter a capacidade de fazer filtragem do remetente a partir de uma correlação da reputação global, informada pelo fabricante do produto, em conjunto com a reputação local, restringindo conexões indesejadas;

5.2.11. Deve ter a capacidade de implementar pesquisas de reputação, a partir da console do produto, informando seu histórico de reputação, assim como, sua reputação atual;

5.3. Console de Gerência

5.3.1. Deve permitir gerenciar mais de um servidor de gateway a partir da mesma console;

5.3.2. Deve permitir definir políticas individuais por servidor de gateway ou globais, a partir da mesma console;

5.3.3. Deve possuir capacidade de administrar de forma unificada, via interface Web (com criptografia), com diversos níveis de acesso (administração, relatórios, quarentena, apenas leitura);

5.3.4. Deve possuir possibilidade de acesso individual ao appliance via SSH, para execução de comandos via CLI (linha de comando);

5.3.5. Deve ter console de gerenciamento via tecnologia Web (HTTP ou HTTPS);

5.3.6. Deve possuir recurso para rastreamento de mensagens (Message Tracking) na própria console de gerenciamento com capacidade de pesquisa por subject, sender e recipient, verificando-se a ação tomada para especifica mensagem, sem necessidade de integração com produtos de terceiros ou "open source";

5.3.7. Deve possuir capacidade de realizar o rastreamento da mensagem, citada no item anterior (item 6.2.6), em todos os appliances /equipamentos da solução ofertada;

5.3.8. Deve permitir realizar o rastreamento da mensagem, citada no item 6.2.6), utilizando caracteres double-byte para líguas estrangeiras;

5.3.9. Deve possuir funcionalidade de criação de Alias e Mascaramento de endereço;

5.3.10. Deve ser possível realizar notificação do administrador por email caso os filtros antispam não recebam atualizações por um determinado período de tempo;

5.3.11. Deve ser capaz de integração com LDAP Microsoft Active Directory 2003, Microsoft Active Directory 2008 e Lotus Domino 6.5 ou superior para sincronização e autenticação;

5.3.12. Deve permitir a criação de políticas diferenciadas para tratamento de SPAM, Vírus, Filtragem de Conteúdo e Controle de reputação(traffic shaping), de acordo com o destinatário da mensagem e reputação de origem;

5.3.13. Deve ser capaz de sincronizar usuários e grupos do LDAP para reconhecimento do usuários válidos e ações de Vírus, Spam e Filtragem de Conteúdo diferenciadas por grupo do LDAP;

5.3.14. Deve ser capaz de utilizar a integração dos usuários do LDAP, validando existência dos mesmos possibilitando o descarte e rejeição, não enviando mensagens para o servidor de correio eletrônico, sem o devido destinatário dentro da base LDAP, evitando processamento desnecessário por parte do servidor de correio eletrônico;

5.3.15. Deve possuir mecanismos de backup/restore da configuração existente na solução;

5.4. Funcionalidades do Anti-Spam

5.4.1. Deve ser capaz de processar o tráfego de mensagens de entrada e de saída, com políticas diferenciadas para cada sentido de tráfego;

5.4.2. Deve permitir a execução de múltiplas ações para uma mesma mensagem que for categorizada como SPAM ou violação dos filtros de conteúdo, entre elas:

5.4.2.1. Apagar mensagem;

5.4.2.2. Enviar para Quarentena;

5.4.2.3. Encaminhar mensagem;

5.4.2.4. Encaminhar em BCC;

5.4.2.5. Gravar mensagem em disco;

5.4.2.6. Gravar em pasta de conformidade;
5.4.2.7. Modificar o assunto;
5.4.2.8. Adicionar informações ao cabeçalho;
5.4.2.9. Deferir a mensagem;
5.4.2.10. Rejeitar a mensagem;
5.4.3. Deve ser capaz de quando a mensagem for gravada em pasta de conformidade, permitir definir ações distintas para as mensagens aprovadas e reprovadas;
5.4.4. Deve possuir capacidade de notificar remetente, destinatário, administrador e outros e-mails, simultaneamente;
5.4.5. Deve ter precisão de identificação de spam de pelo menos 95% (spam-catching rate);
5.4.6. Deve ter precisão de filtragem de pelo menos 99,9999% (accuracy rate);
5.4.7. Deve possuir centro especializado, 24x7, com monitoramento de mais de 2 milhões de mailboxes, para processamento de SPAMs recebidos e criação automática de novos filtros/assinaturas;
5.4.8. Deve permitir atualização automática dos filtros a cada 10 minutos, sem interrupção dos serviços;
5.4.9. Deve ter suporte a listas negras e listas brancas com opção por domínio, endereço de e-mail e endereço IP;
5.4.10. Deve ter a capacidade de bloquear mensagens consideradas como SPAM baseado na utilização de listas DNSBL (DNS BlackHole) ou RBL (Real Time Black List);
5.4.11. Deve ter a capacidade de reconhecimento de ameaças Dia-Zero, com assinatura de suspeitos de vírus;
5.4.12. Deve ter capacidade de utilização de pelo menos as seguintes tecnologias de detecção de spam:
5.4.12.1. Assinaturas para corpo da mensagem e anexos;
5.4.12.2. Análise heurística, através de análise de cabeçalhos, conteúdo e estrutura da mensagem;
5.4.12.3. Filtros de reputação local (criado automaticamente através da análise das mensagens recebidas) e global (criado pela rede de monitoramento do fornecedor da solução);
5.4.12.4. Identificação de idiomas;
5.4.12.5. Filtros de URLs;
5.4.12.6. Filtros anti-phishing;
5.4.13. Deve possuir capacidade para criação de filtros baseados no cabeçalho, remetente, tipos e conteúdo de anexos, dicionários de palavras, assunto e corpo da mensagem, incluindo o uso de expressões regulares;
5.4.14. Deve permitir a criação de "compliance folders", para armazenagem de mensagens (entrada/saída) que violem alguma política de conteúdo criada pelo Administrador;
5.4.15. Deve possuir tecnologia para detecção de ataques de Spam, Vírus e Diretório (Usuários Inválidos);
5.4.16. Deve possuir recurso para a detecção de ataques, que penalize dinamicamente a origem baseado no nível de reputação, com dez níveis de sensibilidade;
5.4.17. Deve possuir a cada nível da detecção dos ataques, citados no item anterior (item 6.3.16), o controle do percentual de mensagens que serão recusadas;
5.4.18. Deve possuir a cada nível da detecção dos ataques, citados no item 6.3.16, o tempo limite para nova tentativa de conexão, número de conexões por IP e número de mensagens por conexão;

5.4.19. Deve possuir tecnologia para prevenção de ataques de “Bounce Messages”;
5.4.20. Deve possuir a capacidade de implementar Sender Policy Framework (SPF) e SenderID;
5.4.21. Deve possuir a capacidade para criação de regras baseada no tipo de arquivo anexado;
5.4.22. Deve possuir a capacidade para criação de regras baseada na detecção por “Wildcard”;
5.4.23. Deve possuir a capacidade para criação de regras baseada na detecção por expressões regulares;
5.4.24. Deve possuir a capacidade de implementar comunicação segura via TLS (Transport Layer Security);
5.4.25. Deve possuir capacidade de configurar criptografia TLS por domínio e por política;
5.4.26. Deve ter capacidade de detecção a pelo menos 10 idiomas (incluindo Português), permitindo o bloqueio de mensagens escritas nos idiomas não desejados;
5.4.27. Deve possuir capacidade de criar uma lista de IP´s confiáveis baseado no comportamento do IP originário da mensagem, visando minimizar o impacto de performance em grandes ambientes;
5.4.28. Deve possuir a capacidade de atualização automática periódica da lista de IP’s confiáveis;
5.5. Funcionalidades do Anti-malware
5.5.1. Deve ter a capacidade de deleção total de mensagens enviadas por “Mass-Mailing Worms”, com opção de ações diferenciadas por tráfego de entrada e saída;
5.5.2. Deve ter a capacidade de reconhecimento de Spywares e Adwares;
5.5.3. Deve possuir recurso para detecção dos ataques de duas escalas para Vírus e Diretório (LDAP), capaz de deferir a conexão SMTP caso a fonte emissora tenha enviado um percentual de mensagens consideradas como usuários inválidos ou infectadas com vírus, em um determinado espaço de tempo, ambos configuráveis pelo administrador;
5.5.4. Deve possuir módulo de antivírus para detecção de conteúdo malicioso nas mensagens, do mesmo fabricante da solução antispam;
5.5.5. Deve possuir engine do antivírus comprovada por pelo menos 6 anos consecutivos de êxito nos testes realizados pelo instituto "Virus Bulletin" (www.virusbtn.com) - VB100 Award;
5.5.6. Deve ter a capacidade de bloquear arquivos anexos por extensão, tipo real do arquivo (True Type File), Mime Type e nome do arquivo;
5.6. Quarentena
5.6.1. Quarentena por usuário, possibilitando que cada usuário possa administrar sua própria quarentena, removendo mensagens ou liberando as que não são SPAM, diminuindo a responsabilidade do administrador e também a possibilidade de bloqueio de e-mails legítimos;
5.6.2. O módulo de quarentena deverá ser capaz de enviar uma notificação periódica para os usuários, informando as mensagens consideradas como SPAM que foram inseridas na quarentena (digest);
5.6.3. Remoção automática das mensagens armazenadas em quarentena de acordo com as configurações definidas pelo administrador;
5.6.4. Deve permitir que o usuário cadastre endereços de email em listas negras/listas brancas pessoais;

5.7. Módulo de Simulação e Conscientização de Ataque Phishing

5.7.1. A solução deve implementar módulo educacional de uso ilimitado durante o período de garantia para reconhecimento de ataques de Phishing, contemplando todos os usuários do Órgão, caso não exista este tipo de licenciamento deverão ser entregues no mínimo 250 possibilidades de utilização do módulo educacional para cada usuário do Órgão a serem utilizados a cada 12 meses de garantia contratada, não cumulativos entre um ano e outro de garantia;

5.7.2. A solução deve implementar módulo educacional contra ataque de Phishing desenhado especificamente para este fim, onde não serão aceitas simulações executadas a partir dos softwares que compõem a proteção do tráfego de e-mail do Órgão;

5.7.3. A solução deve possuir sua própria estrutura de envio de e-mails (Servidores SMTP), não onerado os recursos do órgão para o envio dos e-mails de simulação;

5.7.4. A solução deve possuir suporte a inserção de usuários em lote através de arquivo CSV ou similar, permitindo ainda a separação dos usuários em grupos;

5.7.5. A solução deve implementar módulo educacional contra ataque de Phishing, todos no mesmo software, composto de no mínimo:

5.7.5.1. Módulo de construção de e-mail para simulação do ataque de Phishing;

5.7.5.2. Módulo de conscientização educacional de reconhecimento do ataque de Phishing;

5.7.5.3. Módulo gráfico e de relatórios que permita avaliar se o usuário reportou à área de segurança o possível ataque de Phishing sofrido;

5.7.6. A solução educacional contra ataque de Phishing deve ser capaz de criar templates educacionais exclusivos para o Órgão, em português com a logo marca do Órgão;

5.7.7. A solução educacional contra ataque de Phishing deve ser capaz de criar templates educacionais exclusivos para o Órgão, de forma departamentalisada direcionada por setor do Órgão como por exemplo, área administrativa, área jurídica, área técnica de TI, área técnica administrativa, não se limitando somente à estas áreas, em português e com a logo marca do Órgão;

5.7.8. A solução educacional contra ataque de Phishing deve possibilitar na visão do usuário atacado a inserção de dados, no entanto, sejam eles quais forem os dados não devem ser armazenados de nenhuma forma, em nenhuma área de armazenamento, sejam internas a solução quanto externas;

5.7.9. A solução educacional contra ataque de Phishing deve ser capaz de durante a criação do e-mail template customizado para o Órgão, conter no mínimo as parametrizações abaixo:

5.7.9.1. Escolha de um anexo customizado pelo Órgão a ser anexado ao e-mail de simulação de ataque Phishing;

5.7.9.2. Seleção de usuário e de grupo de usuários que farão parte da simulação;

5.7.9.3. Seleção de agendamento com data e horário para início e fim de cada campanha de conscientização, específica por grupo a ser atingido;

5.7.9.4. Definição de assunto do e-mail de simulação do ataque Phishing;

5.7.9.5. Definição do nome do remetente que enviará o e-mail de simulação do ataque Phishing;

5.7.9.6. Definição do endereço (usuário e domínio) do e-mail de simulação do ataque Phishing;

5.7.9.7. A solução deve possibilitar o uso de variáveis de ambiente, que permitam incluir individualmente no corpo do e-mail conteúdos dinâmicos, para no mínimo:

5.7.9.7.1. Nome do usuário;

5.7.9.7.2. Sobrenome;

5.7.9.7.3. Endereço de e-mail;

5.7.9.7.4. Nome da empresa;

5.7.9.7.5. Dia / Data / Hora / Ano;

5.7.10. A solução educacional contra ataque de Phishing deve ser capaz de criar relatórios executivos e mostrar de forma gráfica na console do produto no mínimo:

5.7.10.1. Verificação de quantas simulações foram enviadas para o Órgão;

5.7.10.2. Verificação de quantos usuários que acessaram o e-mail de simulação de ataque Phishing;

5.7.10.3. Verificação de quantos usuários abriram o arquivo anexo do e-mail de simulação de ataque Phishing;

5.7.10.4. Verificação de quantos usuários inseriram os dados solicitados no e-mail de simulação de ataque Phishing;

5.7.10.5. Verificação de quantos usuários reportaram para a área de TI a existência de um ataque Phishing;

5.7.10.6. Verificação de quantos usuários executaram o módulo de conscientização educacional Anti-Phishing;

5.7.10.7. Verificação da geolocalização dos usuários que sofreram a simulação do ataque de Phishing e foram capturados na simulação;

5.7.11. A solução educacional contra ataque de Phishing deve ser capaz de construir uma mensagem de conscientização direcionada para cada departamento informando que usuário foi pego em uma simulação de ataque Phishing, a qual deve ser mostrada no momento que seja caracterizado como se o usuário estivesse realmente sofrido um ataque;

5.7.12. A solução educacional contra ataque de Phishing deve ser capaz de indicar a necessidade do usuário participar de uma campanha para conscientização, a partir da mensagem de conscientização (item anterior) na qual deverá existir um link direcionando para a campanha indicada para o usuário e grupos de usuários;

5.7.13. A solução educacional contra ataque de Phishing deve apresentar de forma gráfica o resultado geográfico de qual localidade o e-mail de simulação do ataque Phishing foi efetivo com usuários sendo atacados pela simulação;

5.7.14. A solução educacional contra ataque de Phishing deve ser capaz de apresentar de forma gráfica o progresso na conscientização dos usuários, executando gráficos comparativos entre campanhas já realizadas pela ferramenta, onde poderá ser observado o declínio e a ascensão na maturidade e conscientização do Órgão;

6. Especificações da Solução de Segurança de Correio Eletrônico

6.1. A solução para "Segurança de Correio Eletrônico" deve fornecer proteção em tempo real para e-mails contra vírus, spams, spywares, phishing e outros ataques, enquanto aplica as políticas de conteúdo para o serviço de correio

eletrônico. Deve suportar ambientes de servidores Windows de 64 bits e Exchange virtualizados, com instalação fácil e administração simples.

6.2. Arquitetura da Solução

6.2.1. Deve ser compatível com os sistemas operacionais Windows Server 2003 e Windows Server 2008, ambos em 32bits e 64bits;

6.2.2. Deve suportar Cluster Ativo/passivo da solução Exchange;

6.2.3. Deve ser compatível com Exchange Server 2003, 2007 e 2010;

6.2.4. Deve ser compatível com VSAPI versões 2.0, 2.5 e 2.6;

6.2.5. Deve ser compatível com ambientes virtuais Vmware e Hyper-V;

6.2.6. Deve permitir instalação remota;

6.3. Console de Gerência

6.3.1. Deve ter console de gerenciamento via tecnologia Web (HTTP ou HTTPS);

6.3.1.1. A console "Web-base" deve contemplar além do gerenciamento do próprio produto, no mínimo, o gerenciamento dos aplicativos de segurança a seguir:

6.3.1.1.1. Software para segurança de estação de trabalho e servidores ("endpoint");

6.3.1.1.2. Software para filtro de antivírus e anti-spam de E-Mail;

6.3.1.1.3. Software para proteção de antivírus e anti-spam das caixas postais;

6.3.1.1.4. Software para proteção proativa;

6.3.1.1.5. Software para filtro de fluxo WEB;

6.3.1.1.6. Software de relatórios para segurança de estação de trabalho e servidores;

6.3.1.1.7. Software para monitoração e proteção de dados confidenciais;

6.3.2. Deve possibilitar permissionamento de acesso a console, integrando-se com o Active Directory;

6.3.3. Deve ter a capacidade de gerência centralizada de vários servidores;

6.3.4. Deve ter possibilidade de agrupamento dos servidores de correio eletrônico para configuração de políticas semelhantes;

6.3.5. Deve ter capacidade de executar mudanças de configuração em tempo-real, sem necessidade de reiniciar a aplicação;

6.3.6. Deve permitir a instalação da console fora do servidor Exchange;

6.4. Funcionalidades do Anti-Malware

6.4.1. Deve ter a capacidade de verificação em tempo real de SMTP;

6.4.2. Deve ter a capacidade de verificação em tempo real de mensagens em trânsito interno;

6.4.3. Deve ter a capacidade de verificação manual dos message stores;

6.4.4. Deve ter a capacidade de verificação agendada dos message stores;

6.4.5. Deve permitir verificar mailbox stores e public folders;

6.4.6. Deve permitir definir a "idade mínima" das mensagens a serem verificadas;

6.4.7. Deve ter a capacidade de definir limites de verificação, no mínimo, baseados em:

6.4.7.1. Tempo máximo de verificação;

6.4.7.2. Número máximo de decomposição de arquivos compactados recursivamente;

6.4.7.3. Tamanho máximo do arquivo descompactado;

6.4.7.4. Número máximo de arquivos descompactados;

6.4.8. Deve ter mecanismo de detecção de mass-mailer worms;

6.4.9. Deve permitir, no mínimo, as seguintes ações para a detecção de malware:

6.4.9.1. Reparar o anexo / corpo da mensagem;

6.4.9.2. Quarentenar o anexo / corpo da mensagem;

6.4.9.3. Substituir a mensagem por um alerta;

6.4.9.4. Apagar o anexo / corpo da mensagem;
6.4.9.5. Apagar a mensagem inteira;
6.4.9.6. Apenas alertar;
6.4.10. Deve ter capacidade de executar atualização de vacinas sem necessidade de reinício do serviço;
6.4.11. Deve ter mecanismos de detecção de epidemia baseados, no mínimo, em:
6.4.11.1. Ocorrência do mesmo malware;
6.4.11.2. Número total de malware;
6.4.11.3. Ocorrência do mesmo assunto;
6.4.11.4. Ocorrência de mesmo arquivo anexado;
6.4.12. Emissão de alertas de epidemia;
6.5. Funcionalidades do Filtro de Conteúdo
6.5.1. Deve permitir a criação de filtros distintos para entrada, saída e mensagens no message store;
6.5.2. Deve ter políticas baseadas em usuários e grupos de usuários;
6.5.3. Deve permitir, no mínimo, verificação de conteúdo em:
6.5.3.1. Corpo da mensagem;
6.5.3.2. Assunto;
6.5.3.3. Remetente;
6.5.3.4. Domínio;
6.5.3.5. Nome de anexos;
6.5.3.6. Extensão de anexos;
6.5.4. Deve permitir a utilização de valores expressos literalmente, através de expressões regulares e utilização de wildcards;
6.5.5. Deve permitir, no mínimo, as seguintes ações para o filtro de conteúdo:
6.5.5.1. Quarentenar o anexo, indicando ação no corpo da mensagem;
6.5.5.2. Substituir a mensagem por um alerta;
6.5.5.3. Apagar o anexo, indicando ação no corpo da mensagem;
6.5.5.4. Apagar a mensagem inteira;
6.5.5.5. Apenas alertar;
6.5.5.6. Adicionar texto ao assunto da mensagem;
6.5.6. Deve permitir a detecção pelo tipo real do arquivo e não apenas pela extensão do mesmo;
6.6. Funcionalidades do Anti-Spam
6.6.1. Deve ter capacidade de detecção de Spam através de mecanismos de heurística;
6.6.2. Deve ter capacidade de detecção de spam através de assinaturas;
6.6.3. Deve ter capacidade de implementar filtros de URL;
6.6.4. Deve permitir utilizar RBLs (Real-time Black lists) de terceiros;
6.6.5. Deve ter capacidade de bloquear mensagens através de serviço de reputação identificando, no mínimo:
6.6.5.1. Origens seguras;
6.6.5.2. Origens com alto tráfego de spam;
6.6.5.3. Origens de malware;
6.6.6. Deve ter capacidade de permitir configuração de uma “lista negra” centralizada;
6.6.7. Deve ter capacidade de permitir criar uma “lista branca” de remetentes e destinatários;
6.6.8. Deve ter capacidade de permitir configurar o nível de sensibilidade do mecanismo anti-spam;

6.6.9. Deve ter capacidade de permitir, no mínimo, as seguintes ações para o anti-spam:
6.6.9.1. Rejeitar / Deletar a mensagem;
6.6.9.2. Entregar a mensagem para determinado e-mail;
6.6.9.3. Adicionar texto ao assunto da mensagem (TAG);
6.6.9.4. Adicionar informações ao header da mensagem (x-header);
6.6.9.5. Enviar a mensagem à pasta de Spam do usuário;
6.6.9.6. Apenas alertar;
6.6.10. Deve ter capacidade de implementar reputação local de acordo com ambiente analisado;
6.6.11. Deve possuir uma fila rápida de entrega caso o remetente seja considerado confiável. Essa fila rápida terá menos verificações de SPAM para melhorar a performance no processamento das mensagens;
6.7. Relatórios
6.7.1. Deve ter capacidade de permitir gerar relatórios e enviar automaticamente por e-mail;
6.7.2. Deve possuir, no mínimo, os seguintes relatórios:
6.7.2.1. Resumo por Servidor;
6.7.2.2. Resumo Consolidado;
6.7.2.3. Detalhado de Malware;
6.7.2.4. Detalhado do filtro de conteúdo;
6.7.2.5. Detalhado ao anti-spam;
6.7.2.6. Detalhado de informações do sistema;

7. Suporte, Garantia e Manutenção

7.1. Detalhamento das atividades de Suporte

7.1.1. O suporte técnico deverá ser prestado para cada solução aderida e deverá ser acionado em caso de qualquer indisponibilidade da solução, devendo haver o atendimento "on-site", se requerido pelo CONTRATANTE, conforme os índices de criticidade abaixo:

<table>
<tr><th>Criticidade</th><th>Descrição</th><th>Prazo Máximo de Atendimento</th><th>Prazo Máximo de Restauração de Serviço</th></tr>
<tr><td rowspan="2">Severidade 1 (Alta)</td><td rowspan="2">Sistema parado ou produto inoperante com impacto na operações críticas de negócio. Exemplos: Servidor de produção ou outro sistema inicial está inativo. Parte substancial dos dados essenciais corre risco de perda ou corrupção. Operações relacionadas ao negócio foram afetadas, falha que compromete a integridade</td><td>Em até 2 horas deve ter um técnico do fornecedor On-site.</td><td rowspan="2">Em até 8 horas</td></tr>
<tr><td>Em até 4 horas um Engenheiro de Suporte do fabricante deve iniciar o atendimento através de transferência ao telefone. Gerente técnico do fabricante deve estar</td></tr>
<tr><td></td><td></td><td></td><td>Entrega da Solução pelo fabricante em até 6 dias.</td></tr>
</table>

	geral do sistema ou dos dados.	disponível 24x7 e ser automaticamente notificado na abertura do caso.	
Severidade 2 (Média/Baixa)	O defeito não gera impacto ao negócio. Exemplo: Ocorreu um erro que causou impacto negativo limitado na operações.	Em até 8 horas deve ter um técnico do fornecedor On-site.	Em até 24 horas
		Em até 6 horas um Engenheiro de Suporte do fabricante entra em contato.	Entrega da Solução pelo fabricante em até 15 dias ou na próxima atualização do Software
Severidade 3 (Baixa)	O problema é pequeno, ou de documentação. Exemplos: O problema não afetou as operações da contratante negativamente; Encaminhamento de solicitações e ou sugestões para novos recursos ou aprimoramento do software licenciado.	Em até 12 horas um técnico do fornecedor entra em contato.	Em até 72 horas
		No mesmo dia ou no próximo dia útil comercial	Entrega da Solução pelo fabricante em até 20 dias ou considerado para as próximas atualizações do Software

7.1.2. O atendimento pelo fabricante deve estar disponível para os produtos de segurança, disponibilidade e pela combinação de ambos;

7.1.3. O fabricante deverá disponibilizar 24x7x365 um recurso humano designado para fornecer assistência ao gerenciamento de todos os incidentes de suporte cadastrados junto ao mesmo;

7.1.4. A cada chamado de suporte categorizado como grau de severidade 1, o recurso previsto no item anterior (item 17.1.3), deverá ser notificado e iniciará o auxílio na condução do processo internamente junto ao fabricante;

7.1.5. Deverá ser fornecido um serviço a nível mundial de monitoramento proativo para ameaças de segurança que encaminhe notificações técnicas via email;

7.1.6. Deverão ser executados por parte do fabricante, relatórios trimestrais referente ao histórico dos incidentes, independente de seu estado (abertos, fechado e em andamento);

7.1.7. Para eventos caracterizados como Severidade 1 e/ou Severidade 2, conforme descritos no item 17.1.1, deverão ser disponibilizadas até 4 visitas presenciais solicitadas sob demanda no período de 12 (doze) meses em regime 24 x 7 x 120 para resolução dos chamados, atividades proativas com acesso as ferramentas de propriedade exclusivas do fabricante para análise de capacidade e reparos;

7.1.8. Deverão ser fornecidos para consumo 120 dias em meio período, durante o horário comercial de um engenheiro do fabricante, devidamente registrado no quadro de funcionários do fabricante, através do regime de CLT, e será designado para tarefas, de no mínimo, manutenção proativa, reparos e análise de capacidade, esta comprovação deverá ser entregue juntamente com a entrega dos manuais de comprovação técnica, anterior a faze da amostra;

7.1.9. Deve possibilitar a abertura de chamados de suporte, para no mínimo, os seguintes métodos via telefone, e-mail, "website" do fabricante;

7.1.10. Todos os prazos para atendimento da garantia começarão a ser contados a partir da abertura do chamado independentemente deste ter sido feito via telefone, e-mail, Website do fabricante;

7.1.11. O período de suporte deve estar diretamente atrelado ao período de garantia da solução;

7.1.12. Dentro do prazo máximo de solução está compreendido o prazo de atendimento;

7.1.13. Dentro do prazo máximo de atendimento, cabe ao fornecedor dar início, junto ao CONTRATANTE, às providências que serão adotadas para a solução do chamado;

7.1.14. Considera-se plenamente solucionado o problema quando restabelecidos os sistemas/serviços sem restrições, ou seja, quando não se tratar de uma solução paliativa;

7.1.15. Os serviços de atendimento de garantia para chamados de severidades 1 e 2 não podem ser interrompidos até o completo restabelecimento de todas as funções do sistema paralisado (indisponível), mesmo que para isso tenham que se estender por períodos noturnos e dias não úteis (sábados, domingos e feriados);

7.1.16. O fornecedor emitirá relatório sempre que solicitado pelo CONTRATANTE, em papel e em arquivo eletrônico, preferencialmente em arquivo texto, com informações analíticas e sintéticas dos chamados da garantia abertos e fechados no período, incluindo:

7.1.16.1. Quantidade de ocorrências (chamados) registradas no período;

7.1.16.2. Número do chamado registrado e nível de severidade, inclusive aqueles com reabertura;

7.1.16.3. Data e hora de abertura;

7.1.16.4. Data e hora de início e conclusão do atendimento;

7.1.16.5. Identificação do técnico do CONTRATANTE que registrou o chamado;

7.1.16.6. Identificação do técnico do CONTRATANTE que atendeu o chamado da garantia;

7.1.16.7. Descrição do problema;

7.1.16.8. Descrição da solução;

7.1.16.9. Informações sobre eventuais escalações;

7.1.16.10. Resumo com a lista de chamados concluídos fora do prazo de solução estabelecido;

7.1.16.11. Total de chamados no mês e o total acumulado até a apresentação do relatório.

7.1.17. Deverá ser emitido um relatório de histórico e revisão de casos, fornecido pelo gerente técnico do fabricante, sob os chamados abertos ou de responsabilidade do fabricante;

7.1.18. Não se encaixam nos prazos descritos nos itens referentes aos níveis de criticidade, problemas cuja solução dependa de correção de falhas (bugs) ou da liberação de novas versões e patches de correção, desde que comprovados pelo fabricante da solução;

7.1.19. Para esses problemas, o fornecedor deverá nos prazos estabelecidos nos níveis de criticidade, restabelecer o ambiente, através de uma solução paliativa e informar ao CONTRATANTE, em um prazo máximo de 24 (vinte e quatro) horas, quando a solução definitiva será disponibilizada para o CONTRATANTE;

7.1.20. Esta solução definitiva deverá ser disponibilizada no prazo máximo de 60 (sessenta) dias úteis, no caso da necessidade de criação de um patch/fix;

7.1.21. Durante o período de garantia, o licitante compromete-se a substituir, em até 15 (quinze) dias úteis, os equipamentos que apresentarem, em um período de 60 (sessenta dias), duas ocorrências de defeitos por inoperância do produto ou 3 (três) ocorrências de deficiência operacional do produto;

7.1.22. As ferramentas e equipamentos necessários à manutenção serão de responsabilidade da proponente;

7.1.23. Nos casos em que as manutenções necessitarem de paradas da solução, o CONTRATANTE deverá ser imediatamente notificado para que se proceda a aprovação da manutenção, ou para que seja agendada nova data, a ser definida pelo CONTRATANTE, para execução das atividades de manutenção;

7.1.24. O proponente deve emitir relatórios de todas as intervenções realizadas, preventivas e corretivas, programadas ou de emergência, ressaltando os fatos importantes e detalhando os pormenores das intervenções, de forma a manter registros completos das ocorrências e subsidiar as decisões da administração do Complexo Central de Tecnologia do CONTRATANTE, caso requeiram;

7.1.25. O relatório deve ser assinado por representante do CONTRATANTE, responsável pelo acompanhamento do serviço, que se obriga a acompanhar a execução das manutenções;

7.1.26. Por questão de segurança, o servidor nunca deverá ser removido da dependência do CONTRATANTE com os discos rígidos. Nesse caso, o disco rígido do equipamento deverá ser removido e entregue ao primeiro gestor da dependência do CONTRATANTE;

7.1.27. Durante o período de garantia o fornecedor executará, sem ônus adicionais, correções de falhas (bugs) de hardware e software;

7.1.28. Durante o período de vigência do contrato o CONTRATANTE terá direito, sem ônus adicional, a todas as atualizações de versões e releases dos softwares e firmwares que fazem parte da solução ofertada.

7.2. Canais de Atendimento

7.2.1. Será disponibilizado canal de atendimento e chamado técnico 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana através de site na Internet e/ou canal telefônico gratuito 0800;

7.2.2. Em caso de indisponibilidade do canal de atendimento disponibilizado, os chamados técnicos poderão ser abertos via email, "website" do fabricante, telefone, etc;

7.2.3. O fornecedor possui e informar página da Internet onde estejam disponíveis drivers atualizados, últimas versões do firmware e demais informações sobre detalhes técnicos dos equipamentos, sem restrições de acesso público ou via cadastramento de pessoas autorizadas pelo CONTRATANTE para o acesso;

7.3. Garantia

7.3.1. O fornecedor concederá ao CONTRATANTE garantia integral durante 12 (doze) meses, “on-site” com atendimento 24 horas por dia e sete dias por semana, a contar da data de homologação do produto, contra qualquer defeito ou problema em toda a solução, incluindo avarias no transporte dos equipamentos até o local de entrega, mesmo ocorrida sua aceitação/aprovação pelo contratante;

7.3.2. A garantia inclui a substituição dos equipamentos/produtos defeituosos no prazo máximo de 15 (quinze) dias corridos, a contar da comunicação do fato, sem qualquer ônus para o contratante. Neste caso, as novas unidades empregadas na substituição das defeituosas ou danificadas deverão ter prazo de garantia igual ou superior ao das substituídas;

7.3.3. O fornecedor garante por, no mínimo, 12 (doze) meses o fornecimento dos componentes de hardware e software, para manuteção, suporte técnico ou ampliações, de forma que possam ser mantidas todas as funcionalidades inicialmente contratadas. Caso haja neste período a descontinuidade de fabricação dos componentes, deve ser também garantida à total compatibilidade dos itens substitutos com os originalmente fornecidos;

7.3.4. Durante o período de garantia, deve ser efetuada manutenção preventiva, em intervalos predeterminados e de acordo com critérios prescritos pelo CONTRATANTE, destinada a reduzir a probabilidade de falha ou a degradação do funcionamento da solução, para tanto, o proponente deve fornecer, quando da assinatura do contrato, cronograma com previsão das manutenções preventivas;

7.4. Manutenção

7.4.1. Manutenção corretiva será efetuada sempre que a solução apresente falhas que impeçam o seu funcionamento normal e/ou requeiram a intervenção de técnico especializado;

7.4.2. As manutenções preventivas e corretivas serão de responsabilidade do fornecedor, sem custos adicionais ao CONTRATANTE;

7.4.3. Durante o período de garantia, qualquer componente que apresente defeito ou mau funcionamento, sem indicação de solução, deve ser substituído imediatamente;

8. DEVERES E RESPONSABILIDADES DA CONTRATANTE

8.1. Além de outras obrigações previstas neste Termo, a AGR obriga-se a:

8.1.1. Receber, conferir e testar todos os softwares a fim de determinar o aceite definitivo dos mesmos.

8.1.2. Notificar a CONTRATADA, na ocorrência de problemas com as soluções entregues para substituição das mesmas.

8.1.3. Designar um profissional para o acompanhamento técnico do contrato firmado com a CONTRATADA, designado Gestor do contrato, o qual centralizará o relacionamento com a CONTRATADA, bem como a solução das questões técnicas e/ou administrativas advindas da execução do mesmo.

8.1.4. Efetuar o pagamento à CONTRATADA de acordo com a forma e o prazo estabelecido no contrato, após a apresentação da Nota Fiscal/Fatura, que se dará somente após a emissão do Termo de Aceite Definitivo emitido pela CONTRATANTE, e o atendimento de providências necessárias ao fiel desempenho das obrigações aqui mencionadas.

8.1.5. Disponibilizar equipe de profissionais para dar suporte à CONTRATADA nas atividades de consultoria técnica.

8.1.6. Promover a fiscalização da execução e acompanhamento técnico do contrato a ser firmado com a CONTRATADA por meio do Gestor do contrato.

8.1.7. A execução do Contrato será fiscalizada pelo Gestor do Contrato da CONTRATANTE, cumprindo-lhe: Acompanhar e fiscalizar os serviços, dirimir as dúvidas que surgirem no curso da sua prestação de tudo dando ciência à CONTRATADA, para a fiel execução dos serviços durante toda a vigência do Contrato

8.1.8. Sem prejuízo da plena responsabilidade da CONTRATADA perante a CONTRATANTE e/ou a terceiros, os serviços estarão sujeitos a mais ampla e irrestrita fiscalização, a qualquer hora e em todos os locais.

8.1.9. A presença do servidor designado como Gestor do Contrato não diminuirá a responsabilidade da CONTRATADA, por quaisquer irregularidades resultantes de imperfeições técnicas, emprego de material inadequado ou de qualidade inferior, que não implicarão corresponsabilidade da CONTRATANTE ou do servidor designado para a fiscalização.

8.1.10. O Gestor do Contrato poderá sustar recusar, mandar refazer quaisquer serviços, que estejam em desacordo com as especificações técnicas, e as constantes deste documento, determinando prazo para a correção de possíveis falhas ou substituições de produtos em desconformidade com o solicitado.

8.1.11. Eventuais irregularidades de caráter urgente deverão ser comunicadas, por escrito, a contato da CONTRATADA com os esclarecimentos julgados necessários e, as informações sobre possíveis paralisações de serviços, a apresentação de relatório técnico ou razões justificadoras a serem apreciadas e decididas pelo servidor designado.

8.1.12. As decisões e providências sugeridas pela CONTRATADA ou julgadas imprescindíveis, que ultrapassarem a competência do Gestor do Contrato, deverão ser encaminhadas à autoridade superior, para a adoção das medidas cabíveis.

8.1.13. O Gestor de Contrato designado deverá conferir os relatórios dos serviços executados pela CONTRATADA e de acompanhamento do projeto, por ocasião da entrega das Notas Fiscais ou Faturas, e atestar a prestação dos serviços, quando executados satisfatoriamente, para fins de pagamento.

8.1.14. Ao Gestor do Contrato fica assegurado o direito de exigir o cumprimento de todos os itens constantes deste documento, da proposta da CONTRATADA e das cláusulas do suporte técnico, além de solicitar a substituição de qualquer profissional da CONTRATADA, que comprometa a perfeita execução dos serviços, crie obstáculos à fiscalização, não corresponda às técnicas ou às exigências disciplinares da CONTRATANTE, e cujo comportamento ou capacidade técnica sejam inadequados à execução dos serviços, que venha causar embaraço à fiscalização em razão de procedimentos incompatíveis com o exercício de sua função.

8.1.15. A CONTRATANTE obriga-se a cumprir fielmente as condições e exigências contidas neste documento, e em especial proporcionar todas as facilidades para que a CONTRATADA possa desempenhar seus serviços de suporte técnico dentro das normas e condições contratuais, inclusive permitindo que seus profissionais tenham acesso aos equipamentos nos locais onde estão instalados, observando o item referente à execução dos serviços.

8.1.16. Comunicar à CONTRATADA as eventuais irregularidades observadas na execução dos serviços de suporte técnico e/ou nos materiais entregues para adoção das providências saneadoras.

8.1.17. Aplicar as penalidades previstas para o caso do não cumprimento de cláusulas do suporte técnico ou aceitar as justificativas apresentadas pela CONTRATADA.

8.1.18. Permitir ao pessoal técnico da CONTRATADA, desde que identificado e incluído na relação de profissionais autorizados, o acesso às dependências da CONTRATANTE, respeitadas as normas de segurança vigentes.

8.1.19. Notificar a CONTRATADA quanto a defeitos ou irregularidades verificadas na execução dos serviços de suporte técnico, bem como quanto a qualquer ocorrência relativa ao comportamento de seus profissionais, quando em atendimento, que venha a ser considerado prejudicial ou inconveniente para a CONTRATANTE.

8.1.20. Comunicar à CONTRATADA a necessidade de substituição de qualquer profissional que seja considerado inadequado para o exercício da função.

8.1.21. Efetuar os pagamentos devidos à CONTRATADA, na forma convencionada, dentro do prazo previsto, desde que atendidas às formalidades necessárias, após a aceitação dos serviços faturados.

8.1.22. Verificar a regularidade da situação fiscal e dos recolhimentos sociais trabalhistas da CONTRATADA, conforme determina a Lei, antes de efetuar o pagamento devido.

8.1.23. Promover a fiscalização do contrato de concessão, sob os aspectos quantitativos e qualitativos, anotando em registro próprio as falhas detectadas e exigindo as medidas corretivas necessárias, bem como acompanhar o desenvolvimento do contrato, conferir os serviços executados e atestar os documentos fiscais pertinentes, podendo ainda sustar, recusar, mandar fazer ou desfazer qualquer procedimento que não esteja de acordo com os termos contratuais.

8.1.24. Comunicar tempestivamente à CONTRATADA as possíveis irregularidades detectadas na execução dos serviços.

8.1.25. Homologar os serviços prestados de acordo com os requisitos preestabelecidos nas Notas Fiscais/Faturas.

8.1.26. Fornecer à CONTRATADA, em tempo hábil, as informações necessárias e relevantes à consecução dos serviços a serem executados, bem como a documentação técnica e operacional de todos os sistemas envolvidos.

8.1.27. Especificar e estabelecer normas e diretrizes para a execução dos serviços ora contratados, definindo as prioridades, regras, bem como os prazos e etapas para cumprimento das obrigações.

8.1.28. Comunicar, por escrito, à CONTRATADA, as modificações realizadas no ambiente computacional da CONTRATANTE, que impliquem em mudanças no desenvolvimento e manutenção de aplicativos, e estipular prazos para adequação.

8.1.29. Realizar as atividades que necessitem de sua intervenção, previstas no cronograma.

8.1.30. Fornecer aos profissionais da CONTRATADA acesso ao ambiente de produção, supervisionado por integrantes da equipe técnica, e de acordo com o cronograma de atividades.

8.1.31. Manter a equipe, em quantidade e qualidade de recursos humanos suficientes para a execução e entrega dos produtos acordados, dentro do cronograma geral.

9. DEVERES E RESPONSABILIDADES DA CONTRATADA

9.1. Além de outras obrigações previstas neste Termo de Referência, a empresa vencedora obriga-se a:

9.2. Fornecer concessão das licenças de uso dos softwares por período de 12 meses, conforme as quantidades informadas pela CONTRATADA compatível com a infraestrutura disponível da AGR.

9.3. Todas as licenças fornecidas deverão permitir a instalação do produto em quantidade infinita de vezes e não poderão conter mecanismo de expiração, guardada a obediência ao quantitativo de licenças fornecidas.

9.4. Fornecer endereços em site do fabricante, para execução de downloads dos programas mais recentes.

9.5. Fornecer os softwares com todas as licenças, chaves de ativação e demais itens necessários à sua perfeita instalação, reinstalação e funcionamento.

9.6. Entregar os certificados de licenciamento de uso dos softwares e seus respectivos manuais de instrução, preferencialmente em língua portuguesa do Brasil.

9.7. Fornecer, sem custos adicionais para a CONTRATANTE, quaisquer atualizações de patches, releases e novas versões dos softwares, durante a vigência da garantia contratual.

9.8. Corrigir, imediatamente, às suas custas, sem qualquer ônus para a CONTRATANTE e dentro do prazo compatível, quaisquer falhas ou imperfeições originadas do fornecimento contratado durante o prazo de garantia.

9.9. Indicar os responsáveis junto ao fabricante pelas informações referentes ao suporte técnico, fornecendo a referência completa do canal de atendimento e suporte técnico do produto (no Brasil), com a nomeação e o telefone e/ou e-mail dos responsáveis técnicos que possam responder os questionamentos sobre todas as características dos softwares.

9.10. Consignar de forma clara e detalhada as especificações dos softwares entregues, inclusive no que se refere à quantidade e código de identificação.

9.11. Informar o prazo máximo para entrega, que não poderá ser superior a 15 (quinze) dias úteis, contados a partir da nota de empenho emitida e/ou assinatura do contrato.

9.12. Fornecer, juntamente com os softwares, a documentação técnica completa e atualizada dos mesmos, contendo manuais do fabricante, guia de instalação e outros pertinentes, todos originais, em língua portuguesa do Brasil, não sendo aceitas cópias, e ficando sujeita à aprovação da CONTRATANTE. A documentação poderá ser disponibilizada em site do fornecedor, com acesso liberado, por tempo indeterminado, para a CONTRATANTE.

9.13. Sempre que necessário, em razão de eventuais mudanças de nomenclatura dos produtos, a CONTRATANTE validará os nomes e os códigos alterados para as novas versões, bem como, seus técnicos deverão receber instruções, por parte da CONTRATADA, referentes às novas funcionalidades das novas versões, sem ônus para a CONTRATANTE, já que também se trata de capacitação, necessária para a continuidade das atividades pela CONTRATANTE.

9.14. Promover o isolamento, a identificação e a caracterização de eventuais falhas de laboratório dos softwares (bugs), encaminhando-as ao fabricante, e acompanhar a solução - considera-se falha de laboratório o comportamento ou características dos programas que se mostrem divergentes daqueles previstos na documentação do produto, e como tais prejudiciais à sua perfeita utilização pela CONTRATANTE.

9.15. Dar conhecimento à CONTRATANTE, por meio de e-mail, das informações referentes a novas versões e releases dos softwares lançadas no mercado.

9.16. Responsabilizar-se pela qualidade e quantidade do produto fornecido, assumindo todas as despesas necessárias ao cumprimento dos serviços contratados.

9.17. Entregar todos os itens necessários à perfeita instalação e uso das ferramentas na data informada.

9.18. Fornecer, sem ônus adicional, sempre que forem disponibilizadas pelo fabricante, todas as atualizações que visem corrigir problemas ou implementar melhorias nos produtos contratados.

9.19. Providenciar cadastros de acesso ao site de licenciamento de usuários autorizados pela CONTRATANTE, permitindo aos usuários visualizar as licenças disponíveis, podendo baixar os softwares do próprio site, mantendo a conta corporativa já existente em nome da CONTRATANTE.

9.20. Instalar, configurar, customizar e parametrizar os componentes da solução de forma que possibilite a utilização completa da solução, que deverão ser realizados de acordo com o planejamento aprovado pela CONTRATANTE.

9.21. Colocar suporte à disposição da CONTRATANTE, caso seja necessário, para resolução de problemas, esclarecimento de dúvidas e orientação com relação ao produto entregue na execução do contrato.

9.22. Para cada abertura de chamado, a CONTRATADA deverá fornecer o código do chamado, o qual servirá de referência para acompanhamento.

9.23. Fornecer documentação completa dos procedimentos de instalação e configuração dos componentes da solução no ambiente de TI – Tecnologia da Informação – da CONTRATANTE, incluindo: Instalação dos módulos, Configuração dos módulos, Configuração do banco de dados.

9.24. Suporte técnico pelo período de 12 (doze) meses, a partir do recebimento definitivo dos softwares e hardwares, preferencialmente na língua portuguesa do Brasil

9.25. Por suporte compreende-se: Fornecimento e instalação de novas versões dos softwares sob licença, otimizações e avaliações de desempenho.

9.26. Fornecer serviços de modo a manter sempre ajustada a operacionalidade do produto.

9.27. Dispor e manter atualizada toda a documentação e os procedimentos operacionais, pertinentes ao uso das ferramentas, esclarecimento de dúvidas que afetem a configuração ou operação da solução,

9.28. Por suporte telefônico compreende-se: Resolver questões relacionadas ao uso operacional dos softwares sob licença.

9.29. Obter apoio para identificar e verificar as causas de possíveis erros ou mau funcionamento dos softwares sob licença, quando exeqüível.

9.30. Obter orientação, junto ao fornecedor, sobre soluções alternativas para tais erros ou mau funcionamento dos softwares sob licença, se possíveis.

9.31. Obter informações sobre erros previamente identificados pela CONTRATANTE, devidamente comunicados por escrito à CONTRATADA, para eventual solução de contorno dos mesmos, se possível.

9.32. O suporte via base de conhecimento do site da FABRICANTE será na modalidade 24x7, durante todos os dias da semana, dentro do período de garantia.

9.33. A CONTRATADA deverá permitir contato com proprietárias dos softwares ofertados para fins de suporte.

9.34. Manter sigilo, sob pena de responsabilidade

9.35. Manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse da CONTRATANTE que tomar conhecimento em razão da execução das atividades de prestação de consultoria técnica, devendo orientar seus profissionais nesse sentido.

9.36. Responsabilizar-se por danos causados ao patrimônio da CONTRATANTE, ou de terceiros, ocasionados por seus profissionais, em virtude de dolo ou culpa, durante a execução dos serviços contratados.

9.37. Responder por todo e qualquer dano ou prejuízo eventualmente causado à CONTRATANTE, como conseqüência de atos e fatos imputáveis a seus recursos técnicos.

9.38. Cumprir, às suas próprias expensas, todas as cláusulas contratuais que definam suas obrigações.

9.39. Responsabilizar-se por quaisquer acidentes de que possam ser vítimas seus profissionais e o contato, quando nas dependências da CONTRATANTE.

10. PRAZO, LOCAL PARA PRESTAÇÃO DO SERVIÇO E FORMA DE RECEBIMENTO

10.1. A Contratada deverá fornecer o objeto deste Termo de Referência, em até 15 (quinze) dias contados a partir da data da emissão da nota de empenho e/ou da assinatura do contrato.

11. FORMA DE PAGAMENTO

11.1. O pagamento da solução contratada será efetuado em até 20 (vinte) dias após protocolização e aceitação pela Contratante das Notas Fiscais/Faturas correspondentes, devidamente atestadas pela área competente da AGR. O pagamento da Nota Fiscal/Fatura fica condicionado ao cumprimento dos critérios de recebimento.

12. QUALIFICAÇÃO TÉCNICA

12.1. Apresentação de declaração, certificado ou documento equivalente emitido por proprietária de cada componente, específico para este certame, caso a proprietária não seja a CONTRATADA, atestando que: A CONTRATADA é capacitada para serviços de fornecimento, instalação, configuração, suporte e manutenção dos componentes.

12.2. Apresentação de Atestado de Capacidade Técnica referente ao uso da tecnologia (softwares componentes da solução escolhida), do qual conste o projeto ou sistema em que foi empregada e demais informações: Nome / E-mail / Telefone do responsável pelos contatos técnicos do cliente – pessoa vinculada ao cliente responsável pelos contatos relativos ao projeto.

13. GESTOR DO CONTRATO

A gestão de contrato desta solução está sob a gestão da Coordenação de Tecnologia da Informação.

Goiânia, 17 de maio de 2017.
GESTOR/AUTOR DO TERMO DE REFERÊNCIA

ANEXO II

RELAÇÃO DE DOCUMENTOS QUE DEVERÃO SER SUBSTITUÍDOS PELA APRESENTAÇÃO DO CERTIFICADO DE REGISTRO CADASTRAL - CRC

A licitante deverá apresentar o CRC em substituição aos documentos relativos à habilitação jurídica, regularidade fiscal e qualificação econômico-financeira, conforme listados abaixo:

1. Habilitação Jurídica

a) Registro comercial, no caso de empresa individual;
b) Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, que poderá ser substituído por documento consolidado das alterações, devidamente comprovado o último registro no órgão próprio e, no caso de sociedades por ações, acompanhado dos documentos de eleição de seus administradores;
c) Inscrição do ato constitutivo, no caso de sociedades civis, acompanhada de prova da diretoria em exercício;
d) Decreto de autorização, em se tratando de empresa ou sociedade estrangeira em funcionamento no País, e ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir.

2. Regularidade Fiscal

a) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ) do Ministério da Fazenda;
b) Prova de inscrição no Cadastro de Contribuintes estadual ou municipal, relativo ao domicílio ou sede da licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;
c) Cópias das certidões negativas de débitos ou equivalentes na forma da lei, relativas:
c1) à Seguridade Social – INSS
c2) ao Fundo de Garantia por Tempo de Serviço (FGTS);
c3) à Fazenda Pública Federal:
c3.1) Receita Federal, e
c3.2) Dívida Ativa da União;
c4) à Fazenda Pública do Estado do domicílio ou sede da licitante (Certidão de Débito em Dívida Ativa);
c5) à Fazenda Pública do Município do domicílio ou sede da licitante (Tributos Mobiliários);
c6) à Fazenda Pública do Estado de Goiás (Certidão de Débito em Dívida Ativa).

2.1. Caso a participação no certame se dê através da matriz, com possibilidade de que a execução contratual se dê por filial, ou vice-versa, a prova de regularidade fiscal, mediante apresentação do CRC, deverá ser de ambas (deliberação da Procuradoria Geral do Estado através de seu Despacho "AG" nº 001930/2008).

3. Qualificação Econômico-Financeira

a) Balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados, através de índices oficiais, quando encerrado há mais de três meses da data da apresentação da proposta;

b) Comprovação da boa situação financeira da empresa através de no mínimo um dos 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 =	$\frac{AT}{PC + PNC}$	$\frac{\text{Ativo Total}}{\text{Passivo Circulante + Passivo Não Circulante}}$

c) Certidão negativa de falência e recuperação judicial, emitida pelo distribuidor da sede da pessoa jurídica.

Nota:

1) Caso o CRC traga informação a respeito da regularidade para com a justiça do trabalho (CNDT), este será aceito em substituição à apresentação da certidão exigida na alínea "d" do item 8.2 do edital.

2) O Certificado de Registro Cadastral - CRC, deverá estar dentro do prazo de validade com status homologado. Caso o CRC apresente *"status irregular"*, será assegurado à licitante o direito de apresentar a documentação atualizada e regular na própria sessão.

3) Todos os documentos de habilitação deverão estar com prazo vigente, e para as certidões que não mencionarem prazo, será considerado o de 60 (sessenta) dias, contados da data de sua expedição.

ANEXO III

MODELO DE DECLARAÇÃO DE ENQUADRAMENTO NA LEI COMPLEMENTAR Nº 123/06
(deverá ser entregue, após a fase de lances, junto com a proposta comercial)

PREGÃO ELETRÔNICO Nº 003/2017
Processo nº 201700029000979

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 n. 123/06, não possuindo nenhum dos impedimentos previstos no § 4º do artigo 3º da referida Lei.

Local e data.

_____
Representante legal

<u>Nota:</u> A falsidade desta DECLARAÇÃO, objetivando os benefícios da Lei Complementar nº 123/06, 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.