P R E G Ã O E L E T R Ô N I C O
N°. 290/2019/ÔMEGA/SUPEL/RO

S

U

P

E

L

AVISO

Recomendamos aos licitantes a leitura atenta às condições/exigências expressas neste edital e seus anexos, notadamente quanto ao credenciamento, objetivando uma perfeita participação no certame licitatório.

Dúvidas: (69) 3212-9270

MARIA DO CARMO DO PRADO
Pregoeiro (a) SUPEL-RO
Mat. 300131839

EDITAL DE LICITAÇÃO
PREGÃO ELETRÔNICO N°: 290/2019/ÔMEGA/SUPEL/RO

1 – DAS DISPOSIÇÕES GERAIS

1.1. PREÂMBULO:

A SUPERINTENDÊNCIA ESTADUAL DE LICITAÇÕES, por meio de seu(a) Pregoeiro(a) e Equipe de Apoio, nomeada por força das disposições contidas na Portaria nº 081/GAB/SUPEL, publicada no DOE do dia 23/04/2019, torna público que se encontra autorizada a realização da licitação na modalidade de **PREGÃO,** na forma **ELETRÔNICA,** sob o **nº 290/2019/ÔMEGA/SUPEL/RO,** do tipo **MENOR PREÇO POR LOTE,** tendo por finalidade a qualificação de empresas e a seleção da proposta mais vantajosa, conforme disposições descritas neste edital e seus anexos, em conformidade com as Leis Federais nº 10.520/02 e nº 8.666/93 e suas alterações a qual se aplica subsidiariamente a modalidade de Pregão, com os Decretos Estaduais nº 12.205/06, n° 16.089/2011 e n° 21.675/2017, Decreto Federal n° 5.450/05, coma Lei Complementar nº 123/06 e suas alterações, com a Lei Estadual n° 2414/2011, e demais legislações vigentes, tendo como interessada a Coordenadoria de Tecnologia da Informação e Comunicação - CTIC/SEDUC.

1.1.1. A Secretaria de Logística e Tecnologia da Informação – SLTI, do Ministério do Planejamento, Orçamento e Gestão, atua como Órgão provedor do Sistema Eletrônico;

1.1.2. Sempre será admitido que o presente Edital de Licitação, na modalidade PREGÃO, na forma ELETRÔNICA, foi cuidadosamente examinado pelas LICITANTES, sendo assim, não se isentarão do fiel cumprimento dos dispostos neste edital e seus anexos, devido à omissão ou negligência oriunda do desconhecimento ou falsa interpretação de quaisquer de seus itens;

1.1.3. O instrumento convocatório e todos os elementos integrantes encontram-se disponíveis, para conhecimento e retirada, no endereço eletrônico: https://www.comprasgovernamentais.gov.br/.

1.1.4. A sessão inaugural deste PREGÃO ELETRÔNICO dar-se-á por meio do sistema eletrônico, na data e horário, conforme abaixo:

DATA DE ABERTURA: 08 de outubro de 2019.
HORÁRIO: **às 10 h00min. (HORÁRIO DE BRASÍLIA – DF)**
ENDEREÇO ELETRÔNICO: https://www.comprasgovernamentais.gov.br/

1.1.5. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a abertura do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário e locais estabelecidos no preâmbulo deste Edital, desde que não haja comunicação do(a) Pregoeiro(a) em contrário.

1.1.6. Os horários mencionados neste Edital de Licitação referem-se ao horário oficial de Brasília - DF.

1.2. DA FORMALIZAÇÃO E AUTORIZAÇÃO:

1.2.1. Esta Licitação encontra-se formalizada e autorizada por meio do Processo Administrativo nº0029.173574/2019-04**,** e destina-se a garantir a observância do princípio constitucional da isonomia e a selecionar a proposta mais vantajosa para a Administração Pública e será processada e julgada em estrita conformidade com os princípios básicos da legalidade, da impessoalidade, da moralidade, da igualdade, da publicidade, da probidade administrativa, da vinculação ao instrumento convocatório, do julgamento objetivo de que lhe são correlatos.

1.2.2. O processo acima mencionado poderá ser consultado por meio do Sistema Eletrônico de Informações-SEI (https://www.sei.ro.gov.br/sobre).

2 – DAS DISPOSIÇÕES DO OBJETO

2.1. Do Objeto: Registro de Preço de aquisição de equipamentos e materiais permanentes e serviços – solução unificada de segurança para proteção de e-mail, proteção de endpoint e proteção contra ataques avançados, com garantia de 36 meses, contemplando pacote de instalação e configuração, treinamento (hands-on) e operação assistida.

2.1.1 Em caso de discordância existente entre as especificações deste objeto descritas no endereço eletrônico – COMPRASNET/CATMAT, e as especificações constantes no ANEXO Ideste Edital – Termo de Referência, prevalecerão as últimas;

2.2. Local/Horários/Entrega/Execução: Ficam aquelas estabelecidas no item 8.1 do Anexo I – Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

2.3. Prazo/Cronograma de Entrega: Ficam aquelas estabelecidas no item 8.2 do Anexo I – Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

2.4. Do Recebimento: Ficam aquelas estabelecidas no item 8.3 do Anexo I – Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

2.**5. DA PROVA DE CONCEITO:** Ficam aquelas estabelecidas no item 5 do Anexo I – Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

2.6. DA VISTORIA: Ficam aquelas estabelecidas no item 32 do Anexo I – Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

3 – DA IMPUGNAÇÃO AO EDITAL

3.1. Até 02 (dois) dias úteis que anteceder a abertura da sessão pública, qualquer cidadão e licitante poderá IMPUGNAR o instrumento convocatório deste PREGÃO ELETRÔNICO, conforme art. 18, § 1º e § 2º do Decreto Estadual nº 12.205/06,devendo o licitante mencionar o número do pregão, o ano e o número do processo licitatório**,**manifestando-se PREFERENCIALMENTE via e-mail**:** supel.omega@gmail.com (ao transmitir o e-mail, o mesmo deverá ser confirmado pelo(a) Pregoeiro(a) e/ou equipe de apoio responsável, para não tornar sem efeito, pelo telefone (069) 3212-9270, ou ainda,protocolar o original junto a Sede desta Superintendência de Licitações, no horário das 07h30min. às 13h30min., de segunda-feira a sexta-feira, situada na Av. Farquar, S/N -

Bairro: Pedrinhas - Complemento: Complexo Rio Madeira, Ed. Prédio Central – Rio Pacaás Novos, 2ºAndar em Porto Velho/RO - CEP: 76.903-036, Telefone: (0XX) 69.3212-9242.

3.1.1. Caberá o(a) Pregoeiro(a), auxiliada pela equipe de apoio, **decidir sobre a impugnação no prazo de até 24 (vinte e quatro) horas.**

3.1.2. A decisão do(a) Pregoeiro(a) quanto à **impugnação** será informada **preferencialmente via e-mail (aquele informado na impugnação), e ainda através do campo próprio do Sistema Eletrônico do site Comprasnet,** ficando o licitante obrigado a acessá-lo para obtenção das informações prestadas pelo(a) Pregoeiro(a).

3.1.3. Acolhida à impugnação contra o ato convocatório, desde que altere a formulação da proposta de preços, será definida e publicada nova data para realização do certame.

3.1.3.1. **Até 24 (vinte e quatro) horas da sessão inaugural**, o(a) Pregoeiro(a) deverá disponibilizar a resposta da impugnação protocolada, caso contrário, o(a) Pregoeiro(a) antes da data e horário previsto suspenderá o certame licitatório, para confecção da resposta pretendida, e assim, definir uma nova data para a realização do referido certame.

4 – DO PEDIDO DE ESCLARECIMENTOE INFORMAÇÕES ADICIONAIS QUE DEVERÃO SER INCONDICIONALMENTE OBSERVADOS

4.1. Os pedidos de esclarecimentos, decorrentes de dúvidas na interpretação deste Edital e seus anexos, e as informações adicionais que se fizerem necessárias à elaboração das propostas**,** referentes ao processo licitatório deverão ser enviados o(a) Pregoeiro(a), até 03 (três) dias úteis anteriores à data fixada para abertura da sessão pública do PREGÃO ELETRÔNICO, conforme art. 19 do Decreto Estadual n.º 12.205/06,manifestando-se PREFERENCIALMENTE via e-mail: supel.omega@gmail.com (ao transmitir o e-mail, o mesmo deverá ser confirmado pelo(a) Pregoeiro(a) e/ou equipe de apoio responsável, para não tornar sem efeito, pelo telefone (069) 3212-9270 ou ainda, protocolar o original junto a Sede desta Superintendência, no horário das 07h: 30min. às 13h:30min. (Horário de Rondônia), de segunda-feira a sexta-feira, situada na Av. Farquar, S/N - Bairro: Pedrinhas - Complemento: Complexo Rio Madeira, Ed. Pacaás Novos - 2º Andar, em Porto Velho/RO - CEP: 76.903-036, Telefone: (0XX) 69.3212-9242, devendo o licitante mencionar o número do Pregão, o ano e o número do processo licitatório.

4.1.1.Até a data definida para a sessão inaugural, o(a) Pregoeiro(a) deverá disponibilizar a resposta dos esclarecimentos protocolados, caso contrário, o(a) Pregoeiro(a) antes da data e horário previsto suspenderá o certame licitatório, para confecção da resposta pretendida, e assim, definir uma nova data para a realização do referido certame.

4.2. As respostas às dúvidas formuladas, bem como as informações que se tornarem necessárias durante o período de elaboração das propostas, ou qualquer modificação introduzida no edital no mesmo período, serão encaminhadas em forma de aviso de erratas, adendos modificadores ou notas de esclarecimentos,às licitantes que tenham adquirido o Edital.

5 – DAS CONDIÇÕES PARA PARTICIPAÇÃO

5.1. A participação nesta licitação importa à proponente na irrestrita aceitação das condições estabelecidas no presente Edital, bem como, a observância dos regulamentos, normas

MARIA DO CARMO DO PRADO
Pregoeiro (a) SUPEL-RO
Mat. 300131839

administrativas e técnicas aplicáveis, inclusive quanto a recursos. A não observância destas condições ensejará no sumário IMPEDIMENTO da proponente, no referido certame.

5.1.1. Não cabe aos licitantes, após sua abertura, alegação de desconhecimento de seus itens ou reclamação quanto ao seu conteúdo. Antes de elaborar suas propostas, as licitantes deverão ler atentamente o Edital e seus anexos, devendo estar em conformidade com as especificações do **ANEXO I (TERMO DE REFERÊNCIA).**

5.2. Como requisito para participação no PREGÃO ELETRÔNICO o Licitante deverá manifestar, em campo próprio do Sistema Eletrônico, que cumpre plenamente os requisitos de habilitação e que sua proposta de preços está em conformidade com as exigências do instrumento convocatório, bem como a descritiva técnica constante do ANEXO I (TERMO DE REFERÊNCIA).

5.2.1. A declaração falsa relativa ao cumprimento dos requisitos de habilitação e proposta sujeitará o licitante às sanções previstas neste Edital e nas demais cominações legais (Art. 7º, Lei n. 10.520/02)

5.3. Poderão participar deste PREGÃO ELETRÔNICO as empresas que:

5.3.1. Atendam às condições deste EDITAL e seus Anexos, inclusive quanto à documentação exigida para habilitação, e estiverem devidamente credenciados na Secretaria de Logística e Tecnologia da Informação – SLTI, do Ministério do Planejamento, Orçamento e Gestão, por meio do site www.comprasgovernamentais.gov.br/;

5.3.2. Poderão participar desta Licitação, somente empresas que estiverem regularmente estabelecidas no País, cuja finalidade e ramo de atividade seja compatível com o objeto desta Licitação;

5.3.3. Poderão participar cooperativas e outras formas de associativismo, desde que, dependendo da natureza do serviço, não haja, quando da execução contratual, a caracterização do vínculo empregatício entre os executores diretos dos serviços (cooperados) e a pessoa jurídica da cooperativa ou a própria Administração Pública.

5.3.4. As Licitantes interessadas deverão proceder ao credenciamento antes da data marcada para início da sessão pública via internet.

5.3.5.O credenciamento dar-se-á pela atribuição de chave de identificação e de senha, pessoal e intransferível, para acesso ao Sistema Eletrônico, no sitewww.comprasgovernamentais.gov.br.

5.3.6. O credenciamento junto ao provedor do Sistema implica na responsabilidade legal única e exclusiva do Licitante, ou de seu representante legal e na presunção de sua capacidade técnica para realização das transações inerentes ao Pregão Eletrônico.

5.3.7. O uso da senha de acesso pelo Licitante é de sua responsabilidade exclusiva, incluindo qualquer transação efetuada diretamente ou por seu representante, não cabendo ao provedor do Sistema, ou da Superintendência Estadual de Licitações - SUPEL, promotora da licitação, responsabilidade por eventuais danos decorrentes do uso indevido da senha, ainda que, por terceiros.

5.3.8. A perda da senha ou a quebra de sigilo deverão ser comunicadas ao provedor do Sistema para imediato bloqueio de acesso.

5.3.9. Como requisito para participação deste Pregão Eletrônico, a licitante deverá manifestar, em campo próprio do Sistema Eletrônico, que cumpre plenamente os requisitos de habilitação e que sua proposta encontra-se em conformidade com as exigências previstas neste Edital, ressalvados os casos de participação de microempresa e de empresa de pequeno porte, no que concerne a regularidade fiscal.

5.4. Não poderão participar deste PREGÃO ELETRÔNICO, empresas que estejam enquadradas nos seguintes casos:

5.4.1. Que se encontrem sob falência, concurso de credores, dissolução ou liquidação;

5.4.2. Sob a forma de consórcio;

5.4.3. Empresa declarada inidônea para licitar ou contratar com a Administração Pública (Federal, Estadual e Municipal), durante o prazo de sanção; conforme art. 87, inciso IV, da Lei n° 8.666/93;

5.4.3.1. Tratando-se de sanção do art. 7° da Lei do Pregão, os seus efeitos recaem apenas na esfera administrativa do órgão que a aplicou".

5.4.4. Empresa impedida de licitar e contratar com o Estado de Rondônia, durante o prazo da sanção; conforme art. 7º, da Lei n° 10.520/2002;

5.4.5. Empresa punida com suspensão temporária (art. 87, inciso III, da Lei n° 8.666/93) do direito de licitar e contratar com a Administração Pública (Federal, Estadual e Municipal), durante o prazo de sanção;

5.4.6. Empresário proibido de contratar com o Poder público, nos termos do art. 12 da Lei n° 8.429/92 (Lei de Improbidade Administrativa), durante o prazo de sanção;

5.4.7. Empresário proibido de contratar com a Administração Pública, em razão do disposto no art. 72, parágrafo 8°, inciso V, da Lei n° 9.605/98 (Lei de Crimes ambientais), durante o prazo de sanção;

5.4.8. Estrangeiras que não funcionem no País;

5.5. Não poderão concorrer direta ou indiretamente nesta licitação:

5.5.1. Servidor ou dirigente de órgão ou Entidade contratante ou responsável pela licitação, conforme art. 9º, inciso III, da Lei Federal nº 8.666/93.

5.5.2. É vedada a participação de servidor público na qualidade de diretor ou integrante de conselho da empresa licitante, participante de gerência ou Administração da empresa, ou exercer o comércio, exceto na qualidade de acionista, cotista ou comanditário. Conforme preceitua artigo 12 da Constituição Estadual c/c artigo 155 da Lei Complementar 68/92.

5.5.3. A Licitante arcará integralmente com todos os custos de preparação e apresentação de sua proposta de preços, independente do resultado do procedimento licitatório.

5.5.4. Uma Licitante, ou grupo, suas filiais ou empresas que fazem parte de um mesmo grupo econômico ou financeiro, somente poderá apresentar uma única proposta de preços. Caso uma Licitante participe em mais de uma proposta de preços, estas propostas de preços não serão levadas em consideração e serão rejeitadas pela Entidade de Licitação.

5.5.4.1. Para tais efeitos entende-se que, fazem parte de um mesmo grupo econômico ou financeiro, as empresas que tenham diretores, acionistas (com participação em mais de 5%), ou representantes legais comuns, e aquelas que dependam ou subsidiem econômica ou financeiramente a outra empresa.

6 – DA QUALIFICAÇÃO DAS ME, EPP, AGRICULTORES FAMILIARES, PRODUTORES RURAIS PESSOA FÍSICA, MICROEMPREENDEDORES INDIVIDUAIS E SOCIEDADES COOPERATIVAS DE CONSUMO.

6.1 As microempresas e das empresas de pequeno porte e empresas equiparadas a ME/EPP, agricultores familiares, produtores rurais, pessoa física, microempreendedores individuais e sociedades cooperativas de consumo devem atender as disposições estabelecidas na Lei Complementar nº 123, de 14 de dezembro de 2006 e demais normas de estilo para fins de fruição dos benefícios ali dispostos.

7 – DO CRITÉRIO DE JULGAMENTO DA PROPOSTA DE PREÇOS

7.1.O julgamento da Proposta de Preços dar-se-á pelo critério de **MENOR PREÇO POR LOTE,** observadas as especificações técnicas e os parâmetros mínimos de desempenho definidos no Edital.

8– DO REGISTRO (INSERÇÃO) DA PROPOSTA DE PREÇOS NO SISTEMA ELETRÔNICO

8.1.A participação no Pregão Eletrônico dar-se-á por meio da digitação da senha privativa da Licitante e subsequente encaminhamento da proposta de preços **COM VALOR TOTAL DO LOTE (CONFORME EXIGÊNCIA DO SISTEMA ELETRÔNICO),**a partir da data da liberação do Edital no site **www.comprasgovernamentais.gov.br**,até o horário limite de início da Sessão Pública**,** horário de Brasília, exclusivamente por meio do Sistema Eletrônico, quando, então, encerrar-se-á, automaticamente, a fase de recebimento da proposta de preços. Durante este período a Licitante poderá incluir ou excluir proposta de preços.

8.1.1. O Licitante será inteiramente responsável por todas as transações assumidas em seu nome no sistema eletrônico, assumindo como verdadeiras e firmes suas propostas e subsequentes lances, se for o caso (inciso III, Art. 13, Decreto nº 12.205/2006), bem como acompanhar as operações no sistema durante a sessão, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão (inciso IV, art. 13, Decreto nº 12.205/2006).

8.1.2. As propostas de preços registradas no Sistema Comprasnet, implicarão em plena aceitação, por parte da Licitante, das condições estabelecidas neste Edital e seus Anexos;

8.2. Após a divulgação do Edital no endereço eletrônico **www.comprasgovernamentais.gov.br,** as Licitantes deverão **REGISTRAR** suas propostas de preços, no campo **"DESCRIÇÃO**

DETALHADA DO OBJETO", contendo a **DESCRIÇÃO DO OBJETO OFERTADO,**incluindo **QUANTIDADE, PREÇO** e a **MARCA (CONFORME SOLICITA O SISTEMA COMPRASNET),** até a data e hora marcada para a abertura da sessão, exclusivamente por meio do sistema eletrônico, quando, então, encerrar-se-á, automaticamente, a fase de recebimento de proposta, **SOB PENA DE DESCLASSIFICAÇÃO DE SUA PROPOSTA.**

8.2.1. As propostas registradas no Sistema **COMPRASNETNÃO DEVEM CONTER NENHUMA IDENTIFICAÇÃO DA EMPRESA PROPONENTE**, visando atender o princípio da impessoalidade e preservar o sigilo das propostas. Em caso de identificação da licitante na proposta registrada, esta será **DESCLASSIFICADA** pelo(a) Pregoeiro(a).

8.3. A Licitante será responsável por todas as transações que forem efetuadas em seu nome no Sistema Eletrônico, assumindo como firmes e verdadeiras sua proposta de preços e lances inseridos em sessão pública.

8.4. O licitante deverá obedecer rigorosamente aos termos deste Edital e seus anexos. Em caso de discordância existente entre as especificações **do objeto** descritas **no COMPRASNET e as especificações constantes no ANEXO I (TERMO DE REFERÊNCIA)**, prevalecerão as últimas.

8.5. Na Proposta de Preços registrada/inserida no sistema deverão estar incluídos todos os insumos que o compõem, tais como: despesas com mão-de-obra, materiais, equipamentos, impostos, taxas, fretes, descontos e quaisquer outros que incidam direta ou indiretamente na execução do objeto desta licitação, os quais deverão compor sua proposta.

09 – DA FORMULAÇÃO DE LANCES, CONVOCAÇÃO DAS ME/EPPE CRITÉRIOS DE DESEMPATE

9.1. A partir da data e horário estabelecido no subitem 1.1.4de conformidade com o estabelecido neste Edital, o(a) Pregoeiro(a) abrirá a sessão pública, verificando as propostas de preços lançadas no sistema, as quais deverão estar em perfeita consonância com as especificações e condições detalhadas no **Item8.2**do Edital.

9.1.1. O(a) Pregoeiro(a) poderá suspender a sessão para visualizar e analisar, preliminarmente, a proposta ofertada que se encontra inserida no campo **"DESCRIÇÃO DETALHADA DO OBJETO"** do sistema, confrontando suas características com as exigências do Edital e seus anexos**(podendo, ainda, ser analisado pelo órgão requerente),DESCLASSIFICANDO,** motivadamente, aquelas que não estejam em conformidade, que forem omissas ou apresentarem irregularidades insanáveis**.**

9.2. Constatada a existência de proposta incompatível com o objeto licitado ou manifestadamente inexequível, o(a) Pregoeiro(a) obrigatoriamente justificará, por meio do sistema, e então **DESCLASSIFICARÁ**.

9.3.AS LICITANTES DEVERÃO MANTER A IMPESSOALIDADE, NÃO SE IDENTIFICANDO, SOB PENA DE SEREM **DESCLASSIFICADAS** DO CERTAME PELO(A) PREGOEIRO(A).

9.4. Em seguida ocorrerá o início da etapa de lances, via Internet, única e exclusivamente, no site https://www.comprasgovernamentais.gov.br/conforme Edital.

9.5. Todas as licitantes poderão apresentar lances para os **ITENS** cotados, exclusivamente por meio do Sistema Eletrônico, sendo o licitante imediatamente informado do seu recebimento e respectivo horário de registro e valor.

9.5.1.Assim como será lançado na proposta de preços, que deverá conter o menor preço ofertado, os lances serão ofertados observando que somente **serão aceitos somente lances em moeda corrente nacional (R$), com VALORES UNITÁRIOS E TOTAIS com no máximo 02 (duas) casas decimais, considerando as quantidades constantes no ANEXO I – TERMO DE REFERÊNCIA.**

9.6. A abertura e o fechamento da fase de lances "via Internet" será feita pelo(a) Pregoeiro(a), a qual é responsável somente pelo prazo iminente, sendo o Sistema Comprasnet, responsável pelo fechamento do prazo aleatório.

9.7. As licitantes poderão oferecer lances menores e sucessivos, observado o horário fixado e as regras de sua aceitação;

9.8. A licitante somente poderá oferecer lances inferiores ao último por ele ofertado e registrado no sistema;

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

9.10. Durante o transcurso da sessão pública, as licitantes serão informadas, em tempo real, do valor do menor lance registrado que tenha sido apresentado pelas demais licitantes, vedada a identificação do detentor do lance;

9.11. Sendo efetuado lance manifestamente inexequível, o(a) Pregoeiro(a) poderá alertar o proponente sobre o valor cotado para o respectivo item, através do sistema, o excluirá, podendo o mesmo ser confirmado ou reformulado pelo proponente;

9.11.1. A exclusão de lance é possível somente durante a fase de lances, conforme possibilita o sistema eletrônico, ou seja, antes do encerramento do item;

9.11.2. O proponente que encaminhar o lance com valor aparentemente inexequível durante o período de encerramento aleatório, e, não havendo tempo hábil, para exclusão e/ ou reformulação do lance, caso o mesmo não honre a oferta encaminhada, terá sua proposta **DESCLASSIFICADA** na fase de aceitabilidade;

9.12. No caso de desconexão com o(a) Pregoeiro(a), no decorrer da etapa competitiva do Pregão Eletrônico, o Sistema Eletrônico poderá permanecer acessível às licitantes para a recepção dos lances;

9.12.1. O(a) Pregoeiro(a), quando possível, dará continuidade a sua atuação no certame, sem prejuízo dos atos realizados;

9.12.2. Quando a desconexão persistir por tempo superior a **10 (dez) minutos**, a sessão do Pregão Eletrônico será suspensa e terá reinício somente após comunicação expressa aos participantes, através do CHAT MENSAGEM, no endereço eletrônico utilizado para divulgação no site https://www.comprasgovernamentais.gov.br/

MARIA DO CARMO DO PRADO
Pregoeiro (a) SUPEL-RO
Mat. 300131839

9.13. A etapa de lances da sessão pública será encerrada mediante aviso de fechamento iminente dos lances de **01 (um) a 60 (sessenta) minutos**, determinado pelo(a) Pregoeiro(a), de acordo com a comunicação às licitantes, emitido pelo próprio Sistema Eletrônico. Decorrido o tempo de iminência, os ITENS entrarão no horário de encerramento aleatório do sistema, **no prazo máximo de** até **30 (trinta) minutos**, determinado pelo Sistema Eletrônico, findo o qual o ITEM estará automaticamente encerrado, não sendo mais possível reabri-lo;

9.14. Incumbirá à licitante acompanhar as operações no Sistema Eletrônico durante a sessão pública do Pregão Eletrônico, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de quaisquer mensagens emitidas pelo Sistema ou de sua desconexão;

9.15. A desistência em apresentar lance implicará exclusão da licitante da etapa de lances e na manutenção do último preço por ela apresentado, para efeito de ordenação das propostas de preços;

9.16. Após o encerramento da etapa de lances, será verificado se há empate entre as licitantes que neste caso,por força da aplicação da exclusividade obrigatoriamente se enquadram como Microempresa – ME ou Empresa de Pequeno Porte – EPP, conforme determina a Lei Complementar n. 123/06, CONTROLADO SOMENTE PELO SISTEMA COMPRASNET;

9.17.Será assegurada preferência, sucessivamente, aos bens e serviços, na forma preconizada no art.art. 3º, § 2º, incisos II, III, IV e V e art. 45, §2°, ambos da Lei Federal n° 8.666/93, após obedecido o disposto nos subitens antecedentes, o sistema Comprasnet**classificará automaticamente o licitante que primeiro ofertou o último lance.**

10 – DA NEGOCIAÇÃO E ATUALIZAÇÃO DOS PREÇOS

10.1. Após finalização dos lances haverá negociações e atualizações dos preços por meio do CHAT MENSAGEM do sistema Comprasnet, devendo o(a) Pregoeiro(a)examinar a compatibilidade dos preços em relação ao estimado para contratação, **apurado pelo Setor de Pesquisa e Cotação de Preços da SUPEL/RO, bem como, se o valor unitário e total encontram-se com no máximo 02 (duas) casas decimais;**

10.1.1. O(a) Pregoeiro(a) não aceitará e não adjudicará o item cujo preço seja superior ao estimado (valor de mercado) para a contratação, apurado pelo Setor de Pesquisa e Cotação de Preços da SUPEL/RO.

10.1.2. Serão aceitos somente preços em moeda corrente nacional (R$), com VALORES UNITÁRIOS E TOTAIS com no máximo 02 (duas) casas decimais, considerando as quantidades constantes no ANEXO I – TERMO DE REFERÊNCIA.Caso seja encerrada a fase de lances, e a licitante divergir com o exigido, o(a) Pregoeiro(a), poderá convocar no CHAT MENSAGEM para atualização do referido lance, e/ou realizar a atualização dos valores arredondando-os PARA MENOS automaticamente caso a licitante permaneça inerte.

11 – DA ACEITAÇÃO DA PROPOSTA DE PREÇOS

11.1. Cumpridas as etapas anteriores, o(a) Pregoeiro(a) verificará a aceitação da licitante conforme disposições contidas no presente Edital.

11.1.1. Toda e qualquer informação, referente ao certame licitatório, será transmitida pelo(a) Pregoeiro(a), por meio do CHAT MENSAGEM;

11.2. Se a proposta de preços não for aceitável, o(a) Pregoeiro(a) examinará a proposta de preços subsequente e, assim sucessivamente, na ordem de classificação, até a apuração de uma proposta de preços que atenda ao Edital;

11.2.1 Constatada a existência de proposta incompatível com o objeto licitado ou manifestadamente inexequível, o(a) Pregoeiro(a) obrigatoriamente justificará, por meio do sistema, e então **DESCLASSIFICARÁ**.

11.2.1.1 O proponente que encaminhar o valor inicial de sua proposta manifestadamente inexequível, caso o mesmo não honre a oferta encaminhada, terá sua proposta rejeitada na fase de aceitabilidade.

11.2.1.2Quando houver indícios de inexequibilidade da proposta de preço, será oportunizado ao licitante o Princípio do Contraditório e da Ampla Defesa, para que querendo esclareça a composição do preço da sua proposta, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, na forma do § 3° do artigo 43 da Lei Federal n° 8.666/93.

11.3. Não poderá haver desistência dos lances ofertados, sujeitando-se o proponente desistente às penalidades estabelecidas neste Edital;

11.4. O julgamento da Proposta de Preços dar-se-á pelo critério estabelecido no **ITEM 7.1** deste edital de licitação;

11.5. Para ACEITAÇÃO do valor de menor lance, o(a) Pregoeiro(a) e equipe de apoio analisará a conformidade do objeto proposto com o solicitado no Edital. Para tanto, após a fase de lances, o(a) Pregoeiro(a), antes da aceitação do item, **convocará todas as licitantes, que estejam dentro do valor estimado para contratação, no prazo máximo de 120 (cento e vinte) minutos, se outro prazo não for fixado,** para enviar:

11.5.1. A **PROPOSTA DE PREÇOS**, com o valor devidamente atualizado do lance ofertado com a especificação completa do objeto, contendo marca/modelo/fabricante, SOB PENA DE DESCLASSIFICAÇÃO, EM CASO DE DESCUMPRIMENTO DAS EXIGÊNCIAS E DO PRAZO ESTIPULADO;

11.5.2. O **PROSPECTO/FOLDER/CATÁLOGO/ ENCARTES/FOLHETOS TÉCNICOS EM PORTUGUÊS OU LINKS OFICIAIS QUE O DISPONIBILIZEM**, onde constem as especificações técnicas e a caracterização dos mesmos, permitindo a consistente avaliação dos itens.

11.5.2.1. DOCUMENTOS ESPECIAIS PARA APRESENTAR JUNTAMENTE COM A PROPOSTA DE PREÇOS.

a) A empresa deverá apresentar, **juntamente com a proposta comercial**, se possível, catálogos ou folders ou prospectos e/ou folhetos em português, ofertados com descrição detalhada do modelo, marca, características, especificações técnicas e outras informações que possibilitem a avaliação ou ficha técnica do produto, contendo no mínimo as

especificações constantes no item 3.3. **Das Especificações Técnicas e Quantidades Estimadas**.

b) A Licitante deverá apresentar ficha técnica descritiva do item e deverá conter, inclusive, a afirmação do compromisso de entrega dos produtos nas características e especificações descritas. Ficando ressalvado que a descrição a ser ofertada deverá ser o da realidade do objeto, não podendo ser cópia fiel do contido no presente aviso Especifico, salvo se este corresponder em sua integralidade às especificações requisitadas.

c) Na Proposta Técnica, a licitante deverá apresentar uma Matriz ponto a ponto comprovando cada especificação dos itens, com a indicação da página do datasheet e/ou manuais dos equipamentos que serão ofertados;

d) Não serão aceitas outras expressões para o preenchimento, tais como, "Ciente", "De acordo", "Em anexo" e "Consultar Documentação da Proposta ou Manual", sendo considerado como item não atendido; e,

e) As documentações que comprovem as características técnicas devem ser feitas através de catálogos públicos dos próprios fabricantes dos softwares e seus componentes oferta.

f) Apresentar atestado comprovando a existência de equipe técnica com pessoas capacitadas pelo fabricante em todas as soluções adquiridas. O Certificado/Atestado/Carta, deverá ser fornecido pelo fabricante.

11.5.3. O ENVIO DA PROPOSTA DE PREÇOS, SOLICITADA NO SUBITEM 11.5, DEVERÁ SER ANEXADA CORRETAMENTE NO SISTEMA COMPRASNET, SENDO A MESMA COMPACTADA EM 01 (UM) ÚNICO ARQUIVO (excel, word, Zip, doc, docx, .JPG ou PDF), TENDO EM VISTA QUE O CAMPO DE INSERÇÃO É ÚNICO; A SUPEL CUMPRIRÁ RIGOROSAMENTE O ART. 7º DA LEI Nº. 10.520/02.

11.5.3.1.Caso a licitante de menor lance seja desclassificada, serão convocadas as licitantes na ordem de classificação de lance.

11.6. Toda e qualquer informação, referente à convocação do anexo será transmitida pelo(a) Pregoeiro(a), via sistema ou por meio do CHAT MENSAGEM, ficando os licitantes obrigados a acessá-lo;

11.7. O(A) PREGOEIRO(A), EM HIPÓTESE ALGUMA, CONVOCARÁ O LICITANTE PARA REENVIO DA PROPOSTA DE PREÇOS FORA DO PRAZO PREVISTO NO SUBITEM 11.5.

11.7.1. Caso a empresa identifique a necessidade de reenvio de documento (proposta ou prospecto) a solicitação deverá ser realizada dentro do prazo estabelecido no subitem 11.5 do Edital.

11.8. Havendo apenas uma oferta, esta poderá ser aceita, desde que atenda a todos os termos do Edital e seu preço seja compatível com o valor estimado da contratação, e atualizado;

11.9. Se a proposta ou lance de menor valor não for aceitável, o(a) Pregoeiro(a) examinará a proposta ou o lance subsequente, verificando a sua aceitabilidade, e assim sucessivamente, até a apuração de uma proposta ou lance que atenda este Edital.

11.10. Na situação em que houver oferta ou lance considerado qualificado para a classificação, o(a) Pregoeiro(a) poderá negociar com a licitante para que seja obtido um preço melhor.

11.11. A aceitação da proposta poderá ocorrer em momento ou data posterior a sessão de lances, a critério do(a) Pregoeiro(a) que comunicará às licitantes por meio do sistema eletrônico, via CHAT MENSAGEM;

11.12. O(a) Pregoeiro(a) poderá encaminhar, pelo Sistema Eletrônico, contraproposta diretamente a licitante que tenha apresentado o lance de menor valor, para que seja obtido um preço justo, bem assim decidir sobre a sua aceitação, divulgando ACEITO, e passando para a fase de habilitação;

12 – DAS CORREÇÕES ADMISSÍVEIS

12.1. Nos casos em que o(a) Pregoeiro(a) constatar a existência de erros numéricos nas propostas de preços, sendo estes não significativos, proceder-se-á as correções necessárias para a apuração do preço final da proposta, obedecendo às seguintes disposições:

12.1.1. Havendo divergências entre o preço final registrado sob a forma numérica e o valor apresentado por extenso, prevalecerá este último;

12.1.2. Havendo divergências nos subtotais, provenientes dos produtos de quantitativos por preços unitários, o(a) Pregoeiro(a) procederá à correção dos subtotais, mantendo os preços unitários e alterando em consequência o valor da proposta.

13 – DA HABILITAÇÃO DA(S) LICITANTE(S)

13.1. Concluída a fase de ACEITAÇÃO, ocorrerá a fase de habilitação da(s) licitantes(s);

13.1.2.A documentação de habilitação das Licitantes poderá ser substituída pelo **Sistema de Cadastramento de Fornecedores - SICAF, e pelo Certificado de Registro Cadastral - CRC**, expedido pela Superintendência Estadual de Licitações – SUPEL/RO, **NOS DOCUMENTOS POR ELES ABRANGIDOS;**

13.2.1. Os cadastros supramencionados serão consultados pelo(a) Pregoeiro(a), onde seus respectivos certificados, relatórios e declarações, serão inclusos aos autos.

13.1.2.1. O licitante que não possuir o cadastro nesta Superintendência poderá providenciá-lo antes da data de abertura da sessão, no Setor de Protocolo da SUPEL, podendo obter informações por meio do telefone (69) 3212-9242.

13.1.2.2. Caso as licitantes tenham algum tipo de dificuldade em anexar no sistema os documentos exigidos para a habilitação, as mesmas deverão entrar em contato com a Central de Serviços SERPRO, via telefone 0800 9789001, ou e-mail:css.serpro@serpro.gov.brou através do formulário eletrônico:
https://cssinter.serpro.gov.br/SCCDPortalWEB/pages/dynamicPortal.jsf?ITEMNUM=2348

13.2. O licitante deverá declarar, em campo próprio do Sistema, sob pena de inabilitação, que não emprega menores de dezoito anos em trabalho noturno, perigoso ou insalubre, nem menores de dezesseis anos em qualquer trabalho, salvo na condição de aprendiz, a partir dos quatorze anos, na

forma do art. 27, inciso V, da Lei n° 8.666/93, com a redação dada pela Lei nº 9.854, de 27 de outubro de 1999.

13.3.O licitante deverá declarar, em campo próprio do sistema, que se compromete a informar a SUPERVENIÊNCIA DE FATO IMPEDITIVO de sua habilitação, nos termos do § 2º do art. 32 da Lei n° 8.666/93, observadas as penalidades cabíveis.

13.4. RELATIVOS À REGULARIDADE FISCAL:

a) Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02/10/2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional;

b) Certidão de Regularidade de Débitos com a Fazenda Estadual, admitida comprovação também, por meio de "certidão positiva com efeito de negativo", diante da existência de débito confesso, parcelado e em fase de adimplemento;

c) Certidão de Regularidade de Débitos com a Fazenda Municipal, admitida comprovação também, por meio de "certidão positiva com efeito de negativo", diante da existência de débito confesso, parcelado e em fase de adimplemento;

d) Certidão de Regularidade do FGTS, admitida comprovação também, por meio de "certidão positiva com efeito de negativo", diante da existência de débito confesso, parcelado e em fase de adimplemento

e) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

13.5. RELATIVOS À REGULARIDADE TRABALHISTA:

a) **Certidão de Regularidade de Débito –CNDT**, para comprovar a inexistência de débitos inadimplidos perante a Justiça do Trabalho, admitida comprovação também, por meio de "certidão positiva com efeito de negativo", diante da existência de débito confesso, parcelado e em fase de adimplemento.

b) Caso a certidão acima mencionada não indicar prazo de validade só será aceita, pela Pregoeira, se emitida nos últimos 60 (sessenta) dias corridos.

13.6. RELATIVOS À HABILITAÇÃO JURÍDICA:

a) No caso de empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

b) Em se tratando de microempreendedor individual – MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio http://www.portaldoempreendedor.gov.br/;

c) No caso de sociedade empresária ou empresa individual de responsabilidade limitada - EIRELI: ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial da respectiva sede, acompanhado de documento comprobatório de seus administradores;

d) No caso de sociedade simples: inscrição do ato constitutivo no Registro Civil das Pessoas Jurídicas do local de sua sede, acompanhada de prova da indicação dos seus administradores;

e) No caso de microempresa ou empresa de pequeno porte: certidão expedida pela Junta Comercial ou pelo Registro Civil das Pessoas Jurídicas, conforme o caso, que comprove a condição de microempresa ou empresa de pequeno porte, segundo determinado pelo Departamento de Registro Empresarial e Integração - DREI;

f) No caso de cooperativa: ata de fundação e estatuto social em vigor, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, bem como o registro de que trata o art. 107 da Lei nº 5.764, de 1971;

i) No caso de empresa ou sociedade estrangeira em funcionamento no País: decreto de autorização, e se for o caso, ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir.

13.6.1. Os documentos acima deverão estar acompanhados da última alteração ou da consolidação respectiva.

13.7. RELATIVOS À QUALIFICAÇÃO ECONÔMICO-FINANCEIRA:

a) Certidão Negativa de Recuperação Judicial – Lei n°. 11.101/05**(recuperação judicial, extrajudicial e falência)** emitida pelo órgão competente, **expedida nos últimos 90 (noventa)** dias caso não conste o prazo de validade.

a.1). Na hipótese de apresentação de Certidão Positiva de recuperação judicial, o (a) Pregoeiro verificará se a licitante teve seu plano de recuperação judicial homologado pelo juízo, conforme determina o art.58 da Lei 11.101/2005.

a.2) Caso a empresa licitante não obteve acolhimento judicial do seu plano de recuperação judicial, a licitante será inabilitada, uma vez que não há demonstração de viabilidade econômica.

b) Balanço Patrimonial, referente ao último exercício social, ou o Balanço de Abertura, caso a licitante tenha sido constituída em menos de um ano, devidamente autenticado ou registrado na Junta Comercial do Estado, para que o(a) Pregoeiro(a) possa aferir se esta possui Patrimônio Líquido (licitantes constituídas a mais de um ano) ou Capital Social (licitantes constituídas a menos de um ano), a não inferior a 5% (cinco por cento) do valor estimado do item que o licitante estiver participando.

b.1) no caso do licitante classificado em mais de um item/lote, o aferimento do cumprimento da disposição acima levará em consideração a soma de todos os valores referencias;

b.2) caso seja constatada a insuficiência de patrimônio líquido ou capital social para a integralidade dos itens/lotes em que o licitante estiver classificado, o Pregoeiro o convocará para que decida sobre a desistência do(s) item(ns)/lote(s) até o devido enquadramento a regra acima disposta;

b.3) as regras descritas nos itens b.1 e b.2 deverão ser observadas em caso de ulterior classificação de licitante que já se consagrou classificado em outro item(ns)/lote(s).

13.8. RELATIVOS À QUALIFICAÇÃO TÉCNICA

13.8.1.Para fins de aferimento da qualificação técnica, as empresas interessadas em participar do certame, deverão apresentar **atestado de capacidade técnica**, (declaração ou certidão) fornecido(s) por pessoa jurídica de direito público ou privado, comprovando o fornecimento em contrato pertinente e compatível **com o objeto da licitação,** observando-se para tanto o disposto na Orientação Técnica 01/2017/GAB/SUPEL de 14/02/2017.

a) O (s) Atestado (s) de Capacidade Técnica (declaração ou certidão), fornecido por pessoa jurídica de direito público e privado, comprovando o desempenho da licitante em contrato pertinente e compatível em características e quantidades com o objeto da licitação, deverá estar de acordo com Orientação Técnica nº. 001/2017/SUPEL alterada pela OT nº. 002/2017/SUPEL, conforme delimitado abaixo:

a.1) Entende-se por pertinente e compatível **em características** e **quantidade** o (s) atestado (s) que em sua individualidade ou soma de atestados, contemplem que a licitante forneceu materiais de permanentes e prestou serviços, objetos do presente termo de referência, no mínimo 2% (dois por cento) para o (s) item (ns) que o licitante apresentar proposta;

13.8.2. Os atestados deverão indicar dados da entidade emissora (razão social, CNPJ, endereço, telefone e data de emissão) e dos signatários do documento (nome, função, telefone, etc.). Além da descrição do objeto, quantidade e prazos de fornecimento dos objetos.

13.8.3. Os atestados de capacidade técnica apresentados estarão sujeitos à confirmação de autenticidade, exatidão e veracidade conforme previsto no art. 43, parágrafo 3º da Lei Federal nº 8.666/93, sujeitando o emissor às penalidades previstas em lei caso ateste informações inverídicas.

13.9. **Do Cumprimento do Disposto no Inciso XXXIII do Art. 7º da Constituição Federal: Declaração** de cumprimento do inciso XXXIII do art. 7º da Constituição Federal**.**

13.10.Caso a licitante esteja com algum documento de Habilitação desatualizado, ou que não seja contemplado pelo CADASTRO DA SUPEL ou pelo SICAF, o mesmo **DEVERÁ SER ANEXADO EM CAMPO PRÓPRIO DO SISTEMA COMPRASNET,** quando o Pregoeiro realizar a convocação da licitante para enviar o ANEXO**, no prazo máximo de 120 (cento e vinte) minutos,se outro prazo não for fixado, SOB PENA DE INABILITAÇÃO.**

13.10.1. Toda e qualquer informação, referente à convocação do anexo será transmitida pelo Pregoeiro, através do sistema eletrônico.

13.10.2. A DOCUMENTAÇÃO DE HABILITAÇÃO ANEXADA NO SISTEMA COMPRASNET TERÁ EFEITO PARATODOS OS ITENS, OS QUAIS A EMPRESA ENCONTRA-SE CLASSIFICADA.

13.10.3. O ENVIO DE TODA DOCUMENTAÇÃO SOLICITADA, DEVERÁ SER ANEXADA CORRETAMENTE NO SISTEMA COMPRASNET, SENDO A MESMA COMPACTADA EM 01 (UM) ÚNICO ARQUIVO (excel, word, .Zip, .doc, .docx, .JPG ou PDF), TENDO EM VISTA

QUE O CAMPO DE INSERÇÃO É ÚNICO; A SUPEL CUMPRIRÁ RIGOROSAMENTE O ART. 7º DA LEI Nº. 10.520/02.

13.10.4. O(A) PREGOEIRO(A), EM HIPÓTESE ALGUMA, CONVOCARÁ O LICITANTE PARA REENVIO DA DOCUMENTAÇÃO DE HABILITAÇÃO FORA DO PRAZO PREVISTO NO SUBITEM 13.10.

13.10.4.1.Caso a empresa identifique a necessidade de reenvio de documento(habilitação) a solicitação deverá ser realizada dentro do prazo estabelecido no subitem 13.10 do Edital.

13.11. A documentação de habilitação enviada implicará em plena aceitação, por parte da licitante, das condições estabelecidas neste Edital e seus Anexos, vinculando o seu autor ao cumprimento de todas as condições e obrigações inerentes ao certame;

13.12. O(a) Pregoeiro(a) poderá suspender a sessão para análise da documentação de habilitação.

13.13. O não envio dos anexos ensejará à licitante, as sanções previstas neste Edital e nas normas que regem este Pregão.

13.14. Para fins de habilitação, a verificação pelo(a) Pregoeiro(a) nos sítios oficiais de órgão e entidades emissores de certidões constitui meio legal de prova;

13.14.1.A Administração não se responsabiliza pela perda de negócios quanto aos documentos exigidos para habilitação que puderem ser emitidos pelo(a) Pregoeiro(a) via *online*, gratuitamente, quando da ocorrência de eventuais problemas técnicos de sistemas ou quaisquer outros, pois é de inteira responsabilidade das licitantes a apresentação dos documentos exigíveis legalmente quando da convocação, pelo(a) Pregoeiro(a), para o envio dos mesmos.

13.15. As LICITANTES que deixarem de apresentar quaisquer dos documentos exigidos para a Habilitação na presente licitação ou os apresentar em desacordo com o estabelecido neste Edital, serão inabilitadas.

13.16. As microempresas e empresas de pequeno porte deverão apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal e trabalhista, mesmo que esta apresente alguma restrição.

13.16.1. Havendo alguma restrição na comprovação da Regularidade Fiscal e Trabalhista, será assegurado o prazo de 5 (cinco) dias úteis, cujo termo inicial corresponderá ao momento em que o proponente for declarado o vencedor do certame, prorrogável por igual período, a critério da administração pública, para a regularização da documentação, pagamento ou parcelamento do débito e emissão de eventuais certidões negativas ou positivas com efeito de certidão negativa, nos termos do Decreto Estadual n° 21.675/2017.

13.16.2. A não-regularização da documentação, no prazo previsto no subitem **13.16.1**, implicará decadência do direito à contratação, sem prejuízo das sanções previstas no art. 81 da Lei nº 8.666, de 21 de junho de 1993, sendo facultado à SUPEL convocar os licitantes remanescentes, na ordem de classificação, para a assinatura/retirada do Instrumento Contratual, ou revogar a licitação;

13.17. Serão realizadas consultas, ao **Cadastro de Fornecedores Impedidos de Licitar e Contratar com a Administração Pública Estadual - CAGEFIMP,** instituído pela Lei Estadual

MARIA DO CARMO DO PRADO
Pregoeiro (a) SUPEL-RO
Mat. 300131839

nº 2.414, de 18 de fevereiro de 2011, ao **Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS/CGU (**Lei Federal nº 12.846/2013),**Sistema de Cadastramento Unificado de Fornecedores – SICAF, Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa, mantido pelo Conselho Nacional de Justiça** (www.cnj.jus.br/improbidade_adm/consultar_requerido.php) e Lista de Inidôneos, mantida pelo Tribunal de Contas da União – TCU, a fim de evitar contratação e empresas que tenham sido impedidas de licitar e contratar com a Administração Pública.

13.18. Sob pena de inabilitação, os documentos apresentados deverão estar:

13.18.1. Em nome da licitante com o n° do CNPJ e o endereço respectivo, conforme segue:

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

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

13.18.2. No caso das alíneas anteriores, serão dispensados da filial aqueles documentos que, comprovadamente, forem emitidos somente em nome da matriz e vice-versa.

13.19. Na fase de Habilitação, após ACEITA e comprovada a Documentação de Habilitação, o(a) Pregoeiro(a) HABILITARÁ a licitante, em campo próprio do sistema eletrônico**.**

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

14 – DOS RECURSOS

14.1. Após a fase de HABILITAÇÃO, declarada a empresa VENCEDORA do certame, qualquer Licitante poderá manifestar em campo próprio do Sistema Eletrônico, de forma imediata e motivada, explicitando sucintamente suas razões sua intenção de recorrer no prazo mínimo de 20 (vinte) minutos.

14.2. Será concedido à licitante que manifestar a intenção de interpor recurso o prazo de **03 (três) dias para apresentar as razões recursais**, ficando as demais licitantes, desde logo, intimados para, querendo, apresentarem contrarrazões em igual prazo, que começará a contar do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos autos (redação conforme o inc. XVIII, art. 4°, Lei Federal n.º 10.520/2002).

14.2.1. A manifestação de interposição do recurso e contrarrazão, somente será possível por meio eletrônico (campo próprio do sistema Comprasnet), devendo o licitante observar as datas registradas.

14.3. A falta de manifestação imediata e motivada da Licitante importará a decadência do direito de recurso e adjudicação do objeto pelo(a) Pregoeiro(a) ao vencedor.

14.4. O acolhimento do recurso importará na invalidação apenas dos atos insuscetíveis de aproveitamento.

14.5. A decisão do(a) Pregoeiro(a) a respeito da apreciação do recurso deverá ser motivada e submetida à apreciação da Autoridade Competente pela licitação, caso seja mantida a decisão anterior.

14.6 A decisão do(a) Pregoeiro(a) e da Autoridade Competente será informada em campo próprio do Sistema Eletrônico, ficando todos os licitantes obrigados a acessá-lo para obtenção das informações prestadas pelo(a) Pregoeiro(a).

14.7. Decididos os recursos e constatada a regularidade dos atos praticados, a **Autoridade Competente adjudicará o objeto e homologará** o resultado da licitação para determinar a contratação.

14.8. Durante o prazo recursal, os autos do processo permanecerão com vista franqueada aos interessados, na SUPERINTENDÊNCIA ESTADUAL DE LICITAÇÕES – SUPEL, caso não esteja disponível no Sistema de Eletrônico de Informação (SEI).

14.9. Cabe ainda, recurso contra a decisão de:

a) Anular ou revogar o Pregão Eletrônico;

b) Determinar a aplicação das penalidades de advertência, multa, suspensão temporária do direito de licitar e contratar com o Governo do Estado de Rondônia.

14.9.1. Os recursos acima deverão ser interpostos no prazo de 05 (cinco) dias úteis a contar da intimação do ato, e terão efeito suspensivo;

14.9.2. A intimação dos atos referidos no subitem 14.9, alíneas “a” e “b”, será feita mediante publicação na imprensa oficial e comunicação direta às licitantes participantes do Pregão Eletrônico, que poderão impugná-los no prazo de 05 (cinco) dias úteis;

14.9.3. Os recursos interpostos fora do prazo não serão acolhidos;

14.9.4. O recurso será dirigido à autoridade superior, por intermédio da que praticou o ato recorrido, a qual poderá reconsiderar a sua decisão, no prazo de 05 (cinco) dias úteis, ou nesse mesmo prazo fazê-lo subir, devidamente informados, devendo, nesse caso, a decisão ser proferida no prazo de 05 (cinco) dias úteis, contado do recebimento do recurso.

15 – DA ADJUDICAÇÃO E DA HOMOLOGAÇÃO

15.1. Atendidas as especificações do Edital, estando habilitada a Licitante e tendo sido aceito o menor preço apurado, o(a) Pregoeiro(a) declarará a(s) empresa(s) vencedora(s) do(s) respectivo(s) ITENS ADJUDICANDO-O.

15.2. A indicação do lance vencedor, a classificação dos lances apresentados e demais informações relativas à sessão pública do Pregão Eletrônico constarão de ata divulgada no Sistema Eletrônico https://www.comprasgovernamentais.gov.br/sem prejuízo das demais formas de publicidade prevista na legislação pertinente.

15.3. A adjudicação do objeto do presente certame será viabilizada pelo(a) Pregoeiro(a) sempre que não houver recurso. Havendo recurso, a adjudicação será efetuada pela Autoridade Competente que decidiu o recurso.

15.4. A homologação da licitação é de responsabilidade da Autoridade Competente e só poderá ser realizada depois da adjudicação.

15.5. Quando houver recurso e o(a) Pregoeiro(a) mantiver sua decisão, essa deverá ser submetida à Autoridade Competente para decidir acerca dos atos do(a) Pregoeiro(a).

16 – DO TERMO DE CONTRATO OU INSTRUMENTO EQUIVALENTE

16.1. Após a homologação da licitação, o adjudicatário terá o prazo de 05 dias úteis, contados a partir de sua convocação, para assinar o Termo de Contrato, cuja vigência será de 12 meses, podendo ser prorrogado por interesse da contratante, na forma do art.57 da Lei 8.666/93.

16.2. O prazo previsto para assinatura ou aceite poderá ser prorrogado, por igual período, por solicitação justificada do adjudicatário e aceita pela Administração.

17 – DO PAGAMENTO

Conforme estabelecido no item 10 do Termo de Referência – Anexo I deste Edital.

18 – DAS SANÇÕES ADMINISTRATIVAS

Conforme estabelecido no item 21 do Termo de Referência – Anexo I deste Edital.

19– DAS OBRIGAÇÕES DA CONTRATADA

Conforme estabelecido no item 20.2 do Termo de Referência – Anexo I deste Edital.

20 – DASOBRIGAÇÕES DA CONTRATANTE

Conforme estabelecido no item 20.1 do Termo de Referência – Anexo I deste Edital.

21 – DA DOTAÇÃO ORÇAMENTÁRIA

Os recursos financeiros necessários para acobertar as despesas decorrentes da contratação, objeto deste Termo de Referência, Unidade Gestora**SEDUC,Fonte** 112**, Programa/Projeto Atividade**12.126.1076/12.122.1015, **Elemento de Despesa**33.90.39/44.90.40**.**

22 – DAS CONDIÇÕES GERAIS

22.1. A Administração Pública se reserva no direito de:

22.1.1. Anular a licitação se houver vício ou ilegalidade, a modo próprio ou por provocação de terceiros;

22.1.2. Revogar por interesse da Administração Pública em decorrência de fato superveniente devidamente comprovado, pertinente e suficiente para justificar o ato, ou anulada por vício ou ilegalidade, a modo próprio ou por provocação de terceiros, sem que à Licitante tenha direito a qualquer indenização.

22.2. Qualquer modificação no presente Edital será divulgada pela mesma forma que se divulgou o texto original, reabrindo-se o prazo inicialmente estabelecido, exceto quando, inquestionavelmente, a alteração não afetar a formulação da proposta de preços.

22.3. O(a) Pregoeiro(a) ou a Autoridade Competente, é facultado, em qualquer fase da licitação a promoção de diligência, destinada a esclarecer ou complementar a instrução do processo, vedada a inclusão posterior de documentos ou informações que deveriam constar do mesmo desde a realização da sessão pública.

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

22.5. Após apresentação da proposta de preços, não caberá desistência desta, sob pena da licitante sofrer as sanções previstas no art. 7º, da Lei Federal nº. 10.520/2002 c/c as demais normas que regem esta licitação, salvo se houver motivo justo, decorrente de fato superveniente e aceita pelo(a) Pregoeiro(a).

22.6. A homologação do resultado desta licitação não implicará direito à contratação do objeto.

22.7. O Licitante que, convocado dentro do prazo de validade da sua proposta de preços, não celebrar o instrumento contratual, deixar de entregar documentação exigida no Edital, apresentar documentação falsa, ensejar o retardamento da execução de seu objeto, não mantiver a proposta de preços, falhar ou fraudar na execução do contrato, comportar-se de modo inidôneo, fizer declaração falsa, ou cometer fraude fiscal, garantido o direito à ampla defesa, ficará impedido de contratar com a União, Estados, Distrito Federal ou Municípios e, será descredenciado no SICAF, ou nos sistemas de cadastramento de fornecedores a que se refere o inciso XIV do art. 4° da Lei ° 10.520/2002, **pelo prazo de até 05 (cinco) anos,** sem prejuízo das multas previstas em Edital e no contrato e das demais cominações legais.

22.8. Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Vencendo-se os prazos somente em dias de expediente normais no órgão responsável pela licitação.

22.9. O desatendimento de exigências formais não essenciais, não importará no afastamento da Licitante, desde que seja possível a aferição da sua qualificação, e a exata compreensão da sua proposta de preços de preços, durante a realização da sessão pública do Pregão Eletrônico.

22.10. Para fins de aplicação das Sanções Administrativas constantes no presente Edital, o lance é considerado o da proposta de preços.

22.11. As normas que disciplinam este Pregão Eletrônico serão sempre interpretadas, em favor da ampliação da disputa entre os interessados, sem comprometimento do interesse da Administração Pública, a finalidade e a segurança da contratação.

22.12. O objeto da presente licitação poderá sofrer acréscimos ou supressões, conforme previsto no § 1°, do Art. 65, da Lei Federal nº. 8.666/93.

MARIA DO CARMO DO PRADO
Pregoeiro (a) SUPEL-RO
Mat. 300131839

22.13. As Licitantes não terão direito à indenização em decorrência da anulação do procedimento licitatório, ressalvado o direito do CONTRATADO de boa-fé de ser ressarcido pelos encargos que tiver suportado no cumprimento do instrumento contratual.

22.14. O presente Edital e seus Anexos, bem como a proposta da proponente vencedora, farão parte integrante do Instrumento Contratual como se nele estivesse transcrito, ressalvado o valor proposto, porquanto prevalecerá o melhor lance ofertado ou valor negociado;

22.15. Dos atos praticados, o sistema gerará Ata circunstanciada, na qual estarão registrados todos os atos do procedimento e as ocorrências relevantes, que estará disponível para consulta no endereço eletrônico **www.comprasgovernamentais.gov.br**, sem prejuízo das demais formas de publicidade prevista na legislação pertinente.

22.16. Havendo divergência entre as exigências contidas no Edital e em seus Anexos, prevalecerá pela ordem, o Edital, o Termo de Referência, e por último os demais anexos.

22.17. Aos Casos Omissos, serão solucionados diretamente pelo(a) Pregoeiro(a) ou autoridade Competente, observados os preceitos de direito público e as disposições que se aplicam as demais condições constantes na Lei Federal nº.10.520, de 17 de julho de 2002, no Decreto Estadual nº. 12.205, de 02.06.2006, e subsidiariamente, na Lei Federal nº. 8.666, de 21 de junho de 1993, com suas alterações, e ainda, Lei complementar nº. 123/06 e alterações.

22.18. A Administração convocará regularmente o interessado para assinar o termo de contrato, aceitar ou retirar o instrumento equivalente, dentro do prazo e condições estabelecidos, sob pena de decair o direito à contratação, sem prejuízos das sanções previstas na Lei 8.666/93.

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

22.18.2**.** É facultado à Administração, quando o convocado não assinar o termo de contrato ou não aceitar ou retirar o instrumento equivalente no prazo e condições estabelecidos, convocar os licitantes remanescentes, na ordem de classificação, para fazê-lo em igual prazo e nas mesmas condições propostas pelo primeiro classificado, inclusive quanto aos preços atualizados de conformidade com o ato convocatório, ou revogar a licitação independentemente da cominação prevista naLei n° 8.666/93.

22.20. O Edital e seus Anexos poderão ser lidos e retirados somente por meio da Internet no sitehttps://www.comprasgovernamentais.gov.br/e alternativamente no site**www.supel.ro.gov.br.**

22.21. Este Edital deverá ser lido e interpretado na íntegra e, após a apresentação da documentação e da proposta, não serão aceitas alegações de desconhecimento e discordâncias de seus termos.

22.22. Quaisquer informações complementares sobre o presente Edital e seus Anexos poderão ser obtidas pelo telefone/fax **(069) 3212-9270** ou na sede SUPERINTENDÊNCIA ESTADUAL DE LICITAÇÕES – SUPEL/RO.

22.23. O Foro para dirimir os possíveis litígios que decorrerem do presente procedimento licitatório será o da Comarca de Porto Velho/RO.

MARIA DO CARMO DO PRADO
Pregoeiro (a) SUPEL-RO
Mat. 300131839

23 – ANEXOS

23.1. Fazem parte deste instrumento convocatório, como se nele estivessem transcritos, os seguintes documentos:

ANEXO I -Termo de Referência;
ANEXO II -Quadro Estimativo de Preços;
ANEXO III– Minuta da Ata de Registro de Preços;

Porto Velho-RO,**31 de Julho de 2019.**

MARIA DO CARMO DO PRADO
Pregoeiro(a)SUPEL-RO
Mat. 300131839

ANEXO I DO EDITAL – TERMO DE REFERÊNCIA

TR 023/2019 - SEI 0029.173574/2019-04
REGISTRO DE PREÇOS - SEDUC-RO

1. IDENTIFICAÇÃO

Unidade Orçamentária: 16.0001 **– Secretaria de Estado da Educação - SEDUC**

Unidade Administrativa: Coordenadoria de Tecnologia da Informação e Comunicação - CTIC/SEDUC

2. INTRODUÇÃO E BASE LEGAL

O presente Termo de Referência foi elaborado em atendimento ao disposto no inciso I do art. 8º, do Decreto Estadual **nº 12.234**, **de 13 de junho de 2006**, cujas regras se pautam nos princípios estabelecidos na Constituição Federal, ***art. 37, caput,*** nas Leis Federais **nº 8.666/93 (Lei Geral de Licitações) e 10.520/02 (Pregão)**, nos Decretos Estaduais **nº 12.205/06, 12.234/06 (Pregão Eletrônico e Presencial)** e suas alterações e outras normas que lhes sejam correlatas, e tem a finalidade de instruir procedimento licitatório a ser deflagrado para **Aquisição de Material de Permanente e Serviços Terceiros – Pessoa Jurídica**.

3. OBJETO E OBJETIVO

3.1. Do Objeto

Constitui o objeto do presente Termo de Referência, Aquisição de Equipamentos e Materiais Permanentes e Serviços – Solução unificada de segurança para proteção de *e-mail*, proteção de *endpoint* e proteção contra ataques avançados, com garantia de **36** meses, contemplando pacote de instalação e configuração, **treinamento (hands-on)** e **operação assistida**, por meio da formação de registro de preços, para futuras e eventuais aquisições, conforme condições, quantidades e exigências estabelecidas neste instrumento.

3.2. Do Objetivo

Manter e melhorar a segurança da rede da SEDUC, de ataques de vírus externos e internos, que são disseminados de maneira involuntária pelos usuários quando utilizam mídias removíveis infectadas e vírus propagados por e-mail, como um arquivo anexado, cujo conteúdo tenta induzir o usuário a clicar sobre o arquivo ou acessar um endereço eletrônico, fazendo com que seja executado, quando entram em ação, infectam arquivos e programas e auto se enviam para os e-mails encontrados nas listas de contatos gravadas no computador, ou até mesmo vírus de scripts, que são recebidos ao acessar uma página web que poder automaticamente executado sem conhecimento de nossos usuários.

3.3. Das Especificações Técnicas e Quantidades Estimadas

ITEM	DESCRIÇÃO DO OBJETO	UNIDADE DE MEDIDA	QUANTIDADE SOLICITADA
1	**SOLUÇÃO DE SEGURANÇA PARA DESKTOPS (ENDPOINT),** com garantia de 36 meses.	**UNIDADE**	**4.300**
2	**SOLUÇÃO DE SEGURANÇA COMPLETA PARA DESKTOPS (COMPLETA), com garantia de 36 Meses.**	**UNIDADE**	**4.300**
3	**SOLUÇÃO DE SEGURANÇA PARA AMBIENTE VIRTUALIZADO, DATACENTER E NUVEM, com garantia de 36 Meses.**	**UNIDADE**	**150**
4	**SOLUÇÃO DE PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS, com garantia de 36 meses.**	**UNIDADE**	**02**
5	**SOLUÇÃO DE SANDBOX (ANÁLISE DE DIA ZERO), com garantia de 36 meses.**	**UNIDADE**	**02**
6	**SOLUÇÃO DE ANTI-SPAM (GATEWAY DE E-MAIL) , com garantia de 36 meses.**	**UNIDADE**	**4.300**
7	**SOLUÇÃO DE PROTEÇÃO WEB(FILTROWEB) , com garantia de 36 meses.**	**UNIDADE**	**4.300**
8	**SOLUÇÃO DE PREVENÇÃO DE INTRUSÃO DE PROXIMA GERAÇÃO (NGIPS) - 1 GB, com garantia de 36 meses.**	**UNIDADE**	**02**
9	**NGIPS EXPANÇÃO DE LICENÇA 2 Gbps(Upgrade 1,5Gbps IPS + 500Mbps SSL) - REFERENTE AO ITEM NGIPS, com garantia de 36**	**UNIDADE**	**02**

	meses.		
10	**PACOTES DE INSTALAÇÃO E CONFIGURAÇÃO (serviços)**	**UNIDADE**	**20**
11	**TREINAMENTO (HANDS-ON) - 30 HORAS CADA**	**UNIDADE**	**03**
12	**OPERAÇÃO ASSISTIDA/HORAS (suporte técnico)**	**HORAS**	**2.000**

3.4. CARACTERÍSTICA DO OBJETO - DESCRIÇÃO DOS PRODUTOS

3.4.1.1. SOLUÇÃO DE SEGURANÇA PARA DESKTOPS (ENDPOINT)

Módulo de proteção anti-malware

Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

Windows 7 (x86/x64);

Windows 8.1 (x86/x64);

Windows 10 (x86/x64);

Deve disponibilizar evidências de varredura em todas as estações de trabalho, identificando as atualizações de sucesso e as ações de insucesso. Para garantir que os casos de insucesso sejam monitorados para tomada de ações pontuais;

Deve ser integrada ao Windows Security center, quando utilizado plataforma Microsoft;

Deve detectar, analisar e eliminar programas maliciosos, tais como vírus, spyware, worms, cavalos de tróia, key loggers, programas de propaganda, rootkits, phishing, dentre outros;

Deve detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos em:

Processos em execução em memória principal (RAM);

Arquivos executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou Shell);

Arquivos compactados automaticamente, em pelo menos nos seguintes formatos: zip, exe, arj, mime/uu, Microsoft cab;

Arquivos recebidos por meio de programas de comunicação instantânea (msn messenger, yahoo messenger, google talk, icq, dentre outros);

Deve detectar e proteger em tempo real a estação de trabalho contra vulnerabilidades e ações maliciosas executadas em navegadores web por meio de scripts em linguagens tais como javascript, vbscript/Activex;

Deve possuir detecção heurística de vírus desconhecidos;

Deve permitir configurar o consumo de cpu que será utilizada para uma varredura manual ou agendada;

Deve permitir diferentes configurações de detecção (varredura ou rastreamento):

Em tempo real de arquivos acessados pelo usuário;

Em tempo real dos processos em memória, para a captura de programas maliciosos executados em memória, sem a necessidade de escrita de arquivo;

Manual, imediato ou programável, com interface gráfica em janelas, personalizável, com opção de limpeza;

Por linha-de-comando, parametrizável, com opção de limpeza;

Automáticos do sistema com as seguintes opções:

Escopo: todos os discos locais, discos específicos, pastas específicas ou arquivos específicos;

Ação: somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena);

Frequência: horária, diária, semanal e mensal;

Exclusões: pastas ou arquivos (por nome e/ou extensão) que não devem ser rastreados;

Deve possuir mecanismo de cache de informações dos arquivos já escaneados;

Deve possuir cache persistente dos arquivos já escaneados para que nos eventos de desligamento e reinicialização das estações de trabalho e notebooks, a cache não seja descartada;

Deve possuir ferramenta de alterações de parâmetros de comunicação entre o cliente antivírus e o servidor de gerenciamento da solução de antivírus;

Deve permitir a utilização de servidores locais de reputação para análise de arquivos e URL's maliciosas, de modo a prover, rápida detecção de novas ameaças;

Deve ser capaz de aferir a reputação das URL's acessadas pelas estações de trabalho e notebooks, sem a necessidade de utilização de qualquer tipo de programa adicional ou plug-in ao navegador web, de forma a proteger o usuário independentemente da maneira de como a URL está sendo acessada;

Deve ser capaz de detectar variantes de malwares que possam ser geradas em tempo real na memória da estação de trabalho ou notebook, permitindo que seja tomada ação de quarentena a ameaça;

Deve ser capaz de bloquear o acesso a qualquer site não previamente analisado pelo fabricante;

Deve permitir a restauração de maneira granular de arquivos quarentenados sob suspeita de representarem risco de segurança;

Deve permitir em conjunto com a restauração dos arquivos quarentenados a adição automática as listas de exclusão de modo a evitar novas detecções dos arquivos;

Deverá ter funcionalidade de Machine Learning para detectar e tomar ações sobre ameaças desconhecidas e suspeitas;

Deverá ter funcionalidade de Machine Learning em runtime para evitar possíveis métodos de ofuscação que o módulo de Machine Learning em pré execução não consiga detectar.

Deve fornecer um informativo compreensivo de cada simulação que descreva as ações e respectivos meta-dados, bem como, o porquê do veredito emitido pela Machine Learning.

Deve bloquear processos comuns associados a ransomware.

Funcionalidade de atualização

Deve permitir a programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, ou de site seguro da internet, com frequência (no mínimo diária) e horários definidos pelo administrador da solução;

Deve permitir atualização incremental da lista de definições de vírus;

Deve permitir a atualização automática do engine do programa de proteção a partir de localização na rede local ou na internet, a partir de fonte autenticável;

Deve permitir o rollback das atualizações das listas de definições de vírus e engines;

Deve permitir a indicação de agentes para efetuar a função de replicador de atualizações e configurações, de forma que outros agentes possam utiliza-los como fonte de atualizações e configurações, não sendo necessária a comunicação direta com o servidor de anti-malware para essas tarefas;

Deve permitir que os agentes de atualização possam replicar os componentes de vacinas, motores de escaneamento, versão de programas, hotfix e configurações específicas de domínios da árvore de gerenciamento;

O servidor da solução de anti-malware, deve ser capaz de gerar localmente versões incrementais das vacinas a serem replicadas com os agentes replicadores de atualizações e configurações, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização;

O agente replicador de atualizações e configurações, deve ser capaz de gerar localmente versões incrementais das vacinas a serem replicadas com os demais agentes locais, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização;

Funcionalidade de administração

Deve permitir proteção das configurações da solução instalada na estação de trabalho através de senha ou controle de acesso, em ambos os casos, controlada por política gerenciada pela console de administração da solução completa;

Deve possibilitar instalação "silenciosa";

Deve permitir o bloqueio por nome de arquivo;

Deve permitir o travamento de pastas e diretórios;

Deve permitir o travamento de compartilhamentos;

Deve permitir o rastreamento e bloqueio de infecções;

Deve possuir mecanismo de detecção de ameaças baseado em comportamento de processos que estão sendo executados nas estações de trabalho e notebooks;

Deve efetuar a instalação remota nas estações de trabalho, sem requerer outro software ou agente adicional, previamente instalado e sem necessidade de reiniciar a estação de trabalho;

Deve desinstalar automática e remotamente a solução de antivírus atual, sem requerer outro software ou agente;

Deve permitir a desinstalação através da console de gerenciamento da solução;

Deve ter a possibilidade de exportar/importar configurações da solução através da console de gerenciamento;

Deve ter a possibilidade de backup da base de dados da solução através da console de gerenciamento;

Deve ter a possibilidade de designação do local onde o backup automático será realizado;

Deve permitir realização do backup da base de dados através de mapeamento de rede controlado por senha;

Deve ter a possibilidade de determinar a capacidade de armazenamento da área de quarentena;

Deve permitir a deleção dos arquivos quarentenados;

Deve permitir remoção automática de clientes inativos por determinado período de tempo;

Deve permitir integração com Active Directory para acesso a console de administração;

Identificar através da integração com o Active Directory, quais máquinas estão sem a solução de anti-malware instalada;

Deve permitir criação de diversos perfis e usuários para acesso a console de administração;

Deve permitir que a solução utilize consulta externa a base de reputação de sites integrada e gerenciada através da solução de anti-malware, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;

Deve possuir solução de consulta do hash dos arquivos integrada e gerenciada através da solução de antivírus, cancelando o download ou execução do arquivo, de forma automática, baseado na resposta à consulta da base do fabricante;

Deve permitir agrupamento automático de estações de trabalho e notebooks da console de gerenciamento baseando-se no escopo do Active Directory ou IP;

Deve permitir criação de subdomínios consecutivos dentro da árvore de gerenciamento;

Deve possuir solução de reputação de sites local para sites já conhecidos como maliciosos integrada e gerenciada através da solução de antivírus, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;

Deve registrar no sistema de monitoração de eventos da console de anti-malware informações relativas ao usuário logado no sistema operacional;

Deve prover ao administrador relatório de conformidade do status dos componentes, serviços, configurações das estações de trabalho e notebooks que fazem parte do escopo de gerenciamento da console de antivírus;

Deve prover ao administrador informações sobre quais estações de trabalho e notebooks fazem parte do escopo de gerenciamento da console de anti-malware não realizaram o escaneamento agendado ou o escaneamento demandado pelo administrador no período determinado de dias;

Deve prover segurança através de SSL para as comunicações entre o servidor e a console de gerenciamento web;

Deve prover segurança através de SSL para as comunicações entre o servidor e os agentes de proteção;

Deve suportar múltiplas florestas e domínios confiáveis do Active Directory;

Deve utilizar de chave de criptografia que seja/esteja em conformidade com o Active Directory para realizar uma conexão segura entre servidor de antivírus e o controlador de domínio;

Deve permitir a criação de usuários locais de administração da console de anti-malware;

Deve possuir a integração com o Active Directory para utilização de seus usuários para administração da console de anti-malware;

Deve permitir criação de diversos perfis de usuários que permitam acessos diferenciados e customizados a diferentes partes da console de gerenciamento;

Deve bloquear acessos indevidos a área de administração do agente que não estejam na tabela de políticas definidas pelo administrador;

Deve se utilizar de mecanismo de autenticação da comunicação entre o servidor de administração e os agentes de proteção distribuídos nas estações de trabalho e notebooks;

Deve permitir a gerência de domínios separados para usuários previamente definidos;

Deve ser capaz de enviar notificações específicas aos respectivos administradores de cada domínio definido na console de administração;

Deve permitir configuração do serviço de reputação de sites da web em níveis: baixo, médio e alto;

Funcionalidade de controle de dispositivos

Deve possuir controle de acesso a discos removíveis reconhecidos como dispositivos de armazenamento em massa através de interfaces USB e outras, com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura, e bloqueio total;

Deve possuir o controle de acesso a drives de mídias de armazenamento como cdrom, dvd, com as opções de acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;

Deve ser capaz de identificar smartphones e tablets como destinos de cópias de arquivos e tomar ações de controle da transmissão;

Deve possuir o controle a drives mapeados com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;

Deve permitir escaneamento dos dispositivos removíveis e periféricos (USB, disquete, cdrom) mesmo com a política de bloqueio total ativa;

Módulo de proteção anti-malware para estações Linux

Distribuições homologadas pelo fabricante;

SUSE Linux Enterprise 10 e 11;

Red Hat enterprise Linux 4.0, 5.0 e 6.0;

Centos 4.0, 5.0 e 6.0

O agente deve possuir código aberto possibilitando assim adequação a qualquer kernel e distribuição Linux, incluindo desenvolvidas ou alteradas internamente e para versões não homologadas pelo fabricante;

Deve permitir a varredura manual com interface gráfica, personalizável, com opção de limpeza dos malwares encontrados;

Deve permitir a varredura manual por linha de comando, parametrizável e com opção de limpeza automática em todos os sistemas operacionais;

Deve possuir a capacidade de detecção e remoção de todos os tipos de malware, incluindo spyware, adware, grayware, cavalos de tróia, rootkits e outros;

Deve Detectar e remover códigos maliciosos de macro do pacote Microsoft office, em tempo real;

O cliente da solução deve armazenar localmente, e enviar para o servidor (para fins de armazenamento) logs de ocorrência de ameaças, contendo no mínimo os seguintes dados: nome da ameaça, caminho do arquivo

comprometido (quando disponível), data e hora da detecção, endereço ip do cliente e ação realizada;

Deve gerar cópia de segurança dos arquivos comprometidos antes de realizar o processo de remoção de ameaças. Esta cópia deve ser gravada na máquina local, e o acesso ao arquivo deve ser permitido somente pela solução de segurança ou o administrador;

A desinstalação do cliente nas estações de trabalho deverá ser completa, removendo arquivos, entradas de registro e configurações, logs diversos, serviços do sistema operacional e quaisquer outros mecanismos instalados;

Deve possibilitar o rastreo de ameaças em arquivos compactados em, no mínimo, 15 níveis recursivos de compactação;

Deve exibir mensagens aos usuários em português do brasil;

Módulo de proteção anti-malware para estações macOS

O cliente para instalação deverá possuir compatibilidade com os sistemas operacionais:

MacOS 10.14 (Mojave) em processadores 32 e 64 bits;

MacOS 10.13 (High Sierra) em processadores 32 e 64 bits;

MacOS 10.12 (Sierra) em processadores 32 e 64 bits;

OS X 10.11 (El Capitan) em processadores 32 e 64 bits;

OS X 10.10 (Yosemite) em processadores 32 e 64 bits;

Deve suportar o apple remote desktop para instalação remota da solução;

Gerenciamento integrado à console de gerência central da solução

Deve permitir a proteção em tempo real contra vírus, trojans, worms, cavalos-de-tróia, spyware, adwares e outros tipos de códigos maliciosos;

Deve permitir a verificação das ameaças da maneira manual e agendada;

Deve permitir a criação de listas de exclusões para pastas e arquivos que não serão verificados pelo antivírus;

Deve permitir a ações de reparar arquivo ou colocar em quarentena em caso de infeções a arquivos;

Deve possuir mecanismo de proteção contra uso não autorizado no qual o agente do antivírus deve ser protegido contra mudança do seu estado (não possibilitar que um administrador da estação de trabalho e notebook possa parar o serviço do antivírus) bem como mecanismo para restaurar seu estado normal;

Deve possuir no mecanismo de autoproteção as seguintes proteções:

Autenticação de comandos ipc;

Proteção e verificação dos arquivos de assinatura;

Proteção dos processos do agente de segurança;

Proteção das chaves de registro do agente de segurança;

Proteção do diretório de instalação do agente de segurança.

Funcionalidade de HIPS – Host IPS e Host Firewall

Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

Windows 7 (x86/x64);

Windows 8.1 (x86/x64);

Windows 10 (x86/x64);

Deve possuir módulo para proteção de vulnerabilidades com as funcionalidades de host ips e host firewall;

Todas as regras das funcionalidades de firewall e ips de host devem permitir apenas detecção (log) ou prevenção (bloqueio);

Deve permitir ativar e desativar o produto sem a necessidade de remoção;

Deve permitir a varredura de portas logicas do sistema operacional para identificar quais estejam abertas e possibilitando tráfego de entrada ou saída

A funcionalidade de host ips deve possuir regras para controle do tráfego de pacotes de determinadas aplicações;

Deve prover proteção contra as vulnerabilidades do sistema operacional Windows XP ou superior, por meio de regras de host ips;

Deve efetuar varredura de segurança automática ou sob demanda que aponte vulnerabilidades de sistemas operacionais e aplicações e atribua automaticamente as regras de host ips para proteger a estação de trabalho ou notebook contra a possível exploração da vulnerabilidade;

A varredura de segurança deve ser capaz de identificar as regras de host ips que não são mais necessárias e desativá-las automaticamente;

Deve prover proteção contra as vulnerabilidades de aplicações terceiras, por meio de regras de host ips, tais como oracle java, abobe pdf reader, adobe flash player, realnetworks real player, Microsoft office, apple itunes, apple quick time, apple safari, google chrome, mozilla firefox, opera browser, ms internet explorer, entre outras;

Deve permitir a criação de políticas diferenciadas em múltiplas placas de rede no mesmo sistema operacional;

Deve permitir a criação de políticas de segurança personalizadas;

Deve permitir limitar o número de conexões simultâneas no sistema operacional

Deve permitir a emissão de alertas via smtp e snmp;

Deve permitir configuração e manipulação de políticas de firewall através de prioridades;

Deve permitir criação de regras de firewall utilizando os seguintes protocolos:

Icmp, icmpv6, igmp, ggp, tcp, pup, udp, idp, nd, raw, tcp+udp.

Deve permitir criação de regras de firewall por origem de ip ou mac ou porta e destino de ip ou mac ou porta;

Deve permitir a criação de regras de firewall pelos seguintes frames types:

Ip, ipv4, ipv6, arp, revarp.

Deve permitir também escolher outros tipos de frame type de 4 dígitos em hex code;

Deve permitir a criação de grupos lógicos através de lista de ip, mac ou portas;

Deve permitir a criação de contextos para a aplicação para criação de regras de firewall;

Deve permitir o isolamento de interfaces de rede, possibilitando o funcionamento de uma interface por vez;

Deve permitir a criação de múltiplos painéis (dashboards) personalizáveis, compostos por blocos de informações (widgets), visualizados através de gráficos ou tabelas;

Os blocos de informações pertencentes aos painéis personalizáveis devem permitir filtros personalizados para facilitar a visualização e gerenciamentos;

A seleção de uma informação específica dentro de um bloco de informações, através de um clique, deve redirecionar ao log detalhado que gerou aquela informação;

Módulo para controle de aplicações

Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

Windows 7 (x86/x64);

Windows 8.1 (x86/x64);

Windows 10 (x64);

Deve permitir a criação de políticas de segurança personalizadas;

As políticas de segurança devem permitir a seleção dos alvos baseados nos seguintes critérios:

Nome parcial ou completo das estações de trabalho, permitindo a utilização de caractere coringa para identificação do nome parcial da máquina;

Range de endereços IPS;

Sistema operacional;

Grupos de máquinas espelhados do Active Directory;

Usuários ou grupos do Active Directory;

As políticas de segurança devem permitir a combinação lógica dos critérios para identificação do(s) alvo(s) de cada política;

As políticas de segurança devem permitir a definição dos logs que serão recebidos de acordo com os seguintes critérios:

Nenhum;

Somente bloqueios;

Somente regras específicas;

Todas as aplicações executadas;

As políticas de segurança devem permitir o controle do intervalo de envio dos logs;

As políticas de segurança devem permitir o controle do intervalo para envio de atualização de cada política;

As políticas de segurança devem permitir a definição de qual servidor de gerenciamento o agente de segurança deverá comunicar-se;

As políticas de segurança devem permitir a ocultação do ícone do agente, que reside da barra de tarefas, e de notificações ao usuário;

As políticas de segurança devem permitir o controle do intervalo de quando os inventários de aplicações são executados;

As políticas de segurança devem permitir o controle através de regras de aplicação;

As regras de controle de aplicação devem permitir as seguintes ações:

Permissão de execução;

Bloqueio de execução;

Bloqueio de novas instalações;

As regras de controle de aplicação devem permitir o modo de apenas coleta de eventos (logs), sem a efetivação da ação regra;

As regras de controle de aplicação devem permitir os seguintes métodos para identificação das aplicações:

Assinatura sha-1 do executável;

Atributos do certificado utilizado para assinatura digital do executável;

Caminho lógico do executável;

Base de assinaturas de certificados digitais válidos e seguros;

As regras de controle de aplicação devem possuir categorias de aplicações;

As políticas de segurança devem permitir a utilização de múltiplas regras de controle de aplicações.

Deve permitir a criação de múltiplos painéis (dashboards) personalizáveis, compostos por blocos de informações (widgets), visualizados através de gráficos ou tabelas;

Os blocos de informações pertencentes aos painéis personalizáveis devem permitir filtros personalizados para facilitar na visualização e gerenciamentos;

A seleção de uma informação específica dentro de um bloco de informações, através de um clique, deve redirecionar ao log detalhado que gerou aquela informação;

Módulo de proteção contra vazamento de informações - DLP

Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais: Windows 7 (x86/x64);Windows 8.1 (x86/x64);Windows 10 (x64)

Deve possuir nativamente templates para atender as seguintes regulamentações:

PCI/DSS;

HIPA;

Glba;

SB-1386;

US PII.

Deve ser capaz de detectar informações, em documentos nos formatos:

Documentos: Microsoft office (doc, docx, xls, xlsx, ppt, pptx) openoffice, rtf, wordpad, text; xml, html;

Gráficos: visio, postscript, pdf, tiff,

Comprimidos: win zip, rar, tar, jar, arj, 7z, rpm, cpio, gzip, bzip2, unix/linux zip, lzh;

Códigos: c/c++, java, verilog, autocad;

Deve ser capaz de detectar informações, com base em:

Dados estruturados, como dados de cartão de crédito, dados pessoais, endereços de e-mail, CPF, entre outros;

Palavras ou frases configuráveis;

Expressões regulares;

Extensão dos arquivos;

Deve ser capaz de detectar em arquivos compactados;

Deve permitir a configuração de quantas camadas de compressão serão verificadas;

Deve permitir a criação de modelos personalizados para identificação de informações;

Deve permitir a criação de modelos com base em regras e operadores lógicos;

Deve possuir modelos padrões;

Deve permitir a importação e exportação de modelos;

Deve permitir a criação de políticas personalizadas

Deve permitir a criação de políticas baseadas em múltiplos modelos;

Deve permitir mais de uma ação para cada política, como:

Apenas registrar o evento da violação;

Bloquear a transmissão;

Gerar alertar para o usuário;

Gerar alertar na central de gerenciamento;

Capturar informação para uma possível investigação da violação;

Deve permitir criar regras distintas com base se a estação está fora ou dentro da rede;

Deve ser capaz de identificar e bloquear informações nos meios de transmissão:

Cliente de e-mail;

Protocolos http, https, ftp;

Mídias removíveis;

Discos óticos cd/dvd;

Gravação cd/dvd;

Aplicações de mensagens instantâneas;

Tecla de print screen;

Aplicações p2p;

Área de transferência do Windows;

Webmail;

Armazenamento na nuvem (cloud);

Impressoras;

Scanners;

Compartilhamentos de arquivos;

Activesync;

Criptografia PGP;

Disquete;

Portas com, lpt, firewire (ieee 1394);

Modems;

Infravermelho;

Bluetooth;

Deve permitir a criação de exceções nas restrições dos meios de transmissão;

Módulo de criptografia

Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

Windows 7 (x86/x64);

Windows 8.1 (x86/x64);

Windows 10 (x64);

Deve possuir módulo de criptografia para as estações de trabalho (desktops e notebooks), com as seguintes funcionalidades de criptografia para:

Disco completo (fde – full disk encryption);

Pastas e arquivos;

Mídias removíveis;

Anexos de e-mails;

Automática de disco;

Deve possuir autenticação durante a inicialização (boot) da estação de trabalho, antes do carregamento do sistema operacional, para a funcionalidade de criptografia do disco completo;

A autenticação durante a inicialização (boot) deve ser a partir das credenciais sincronizadas com o Active Directory;

Deve possuir suporte ao algoritmo de criptografia aes-256;

Deve possuir a capacidade de exceções para criptografia automática;

Deve possuir criptografia no canal de comunicação entre as estações de trabalho e o servidor de políticas;

Deve possuir certificação FIPS 140-2;

Deve possuir funcionalidade de criptografia por software ou hardware;

Deve ser compatível com os padrões SED ('self-encrypting drive), opal e opal2

Deve possuir compatibilidade de autenticação por múltiplos fatores;

Deve permitir atualizações do sistema operacional mesmo quando o disco está criptografado;

Deve possuir a possibilidade de configurar senha de administração local na estação de trabalho para desinstalação do módulo;

Deve possuir políticas por usuários, grupos e dispositivos;

Deve possuir os métodos de autenticação seguintes para desbloquear um disco:

Sequência de cores;

Autenticação com ad;

Single sign-on com ad;

Senha pré-definida;

Número pin;

Smart card;

Deve possuir auto ajuda para usuários que esquecerem a senha com a combinação de perguntas e respostas;

Deve possuir mecanismos de criptografia transparentes para o usuário;

Deve possuir mecanismos para wipe (limpeza) remoto;

Deve possuir mecanismo para desativar temporariamente a autenticação de pré-inicialização (boot);

Deve possuir mecanismo que permita desfazer a criptografia do disco no evento em que se torne corrompido, impedindo a inicialização da estação/notebook;

O ambiente de autenticação pré-inicialização deve permitir a conexão a redes sem fio (wireless);

Deve ser possível especificar o tipo de autenticação das redes wireless disponíveis;

O ambiente de autenticação pré-inicialização deve conter indicação visual do estado de conectividade de rede da estação/notebook;

O ambiente de autenticação deve disponibilizar um teclado virtual na tela do dispositivo, independente do teclado físico;

O ambiente de autenticação pré-inicialização deve permitir a mudança do leiaute do teclado;

O ambiente de autenticação pré-inicialização deve prover um mecanismo de assistência remota que permita a autenticação da estação de trabalho no evento que o usuário não se lembre de sua senha de autenticação;

O ambiente de autenticação pré-inicialização deve prover um mecanismo que permita a substituição da senha e outros códigos de autenticação através da resposta correta a perguntas definidas previamente pelo administrador;

Ambiente de autenticação pré-inicialização deve prover uma ferramenta que permita a execução de procedimentos de identificação de problema, assim como a realização das seguintes tarefas administrativas: desfazer a criptografia do disco, restaurar o registro mestre de inicialização (mbr – master boot record) ao estado anterior ao estado alterado pelo ambiente de autenticação pré-inicialização, montar partições criptografadas, modificar a política de criptografia aplicada à estação de trabalho, adicionar, remover e editar atributos dos usuários existentes na lista de usuários permitidos a se autenticar na estação de trabalho, visualizar os registros (logs) das atividades da solução de criptografia e visualizar, testar e modificar as configurações de rede;

O acesso a este ambiente de execução de procedimentos de identificação de problema e realização de tarefas administrativos deve ser controlado através de política gerenciada remotamente pelo componente de gerenciamento da solução;

Deve prover ferramenta presente na estação de trabalho que possibilite migrá-la para um servidor de gerenciamento diferente;

Deve permitir a gerência das seguintes soluções terceiras de criptografia:

Microsoft bitlocker;

Apple filevault;

As capacidades de gerência das soluções terceiras de criptografia devem incluir:

Habilitar a criptografia

Exibir o estado da criptografia (ativado, desativado)

Habilitar o aviso legal

Editar o intervalo de sincronia

Deve permitir a visualização das estações de trabalho que tenham aplicação de política pendente a partir da console de administração centralizada;

Deve permitir a visualização do autor de determinada política a partir da console de administração centralizada;

Deve permitir a visualização de estações de trabalho que não possuam nenhuma política aplicada a partir da console de administração centralizada;

Deve permitir a adição de informações de contato a serem exibidas ao usuário final com texto customizável;

Deve permitir a exibição de aviso legal quando o agente de criptografia é instalado na estação de trabalho;

Deve permitir a exibição de aviso legal quando a estação é inicializada;

Deve permitir, em nível de política, a indicação de pastas a serem criptografadas;

Deve possibilitar que cada política tenha uma chave de criptografia única;

Deve permitir, em nível de política, a escolha da chave de criptografia a ser utilizada, entre as seguintes opções:

Chave do usuário: somente o usuário tem acesso aos arquivos;

Chave da empresa: qualquer usuário da empresa tem acesso aos arquivos;

Chave da política: qualquer estação de trabalho que tenha aplicada a mesma política tem acesso aos arquivos;

Deve permitir a escolha dos diretórios a serem criptografados em dispositivos de armazenamento USB;

Deve possibilitar a desativação de dispositivos de gravação de mídias óticas;

Deve possibilitar a desativação de dispositivos de armazenamento USB;

Deve possibilitar o bloqueio da desinstalação do agente de criptografia por usuários que não sejam administradores da estação de trabalho;

Deve possibilitar o bloqueio da autenticação de usuários baseado no intervalo em que o dispositivo não tenha as políticas sincronizadas com o componente de administração centralizada;

Deve possibilitar o atraso, em intervalo personalizado de tempo, para uma nova tentativa de autenticação de usuários na ocorrência de um número personalizável de tentativas inválidas de autenticação;

Deve possibilitar apagar todos os dados do dispositivo na ocorrência de um número personalizável de tentativas inválidas de autenticação;

Deve possibilitar a instauração de política de gerenciamento de complexidade e intervalo de troca de senha com os seguintes critérios:

Definição do intervalo de dias em que o usuário será forçado a mudar sua senha;

Definição de número de senhas imediatamente anteriores que não poderão ser reutilizadas como nova senha;

Definição do número de caracteres iguais consecutivos que não poderão ser utilizados na nova senha;

Definição do comprimento de caracteres mínimo a ser utilizado na nova senha;

Definição do número de caracteres especiais, caracteres numéricos, caracteres em caixa alta e caracteres em caixa baixa que deverão ser utilizados para a nova senha;

Deve permitir a criação de múltiplos painéis (dashboards) personalizáveis, compostos por blocos de informações (widgets), visualizados através de gráficos ou tabelas;

Os blocos de informações pertencentes aos painéis personalizáveis devem permitir filtros personalizados para facilitar na visualização e gerenciamentos;

A seleção de uma informação específica dentro de um bloco de informações, através de um clique, deve redirecionar ao log detalhado que gerou aquela informação;

Módulolo de proteção para Smartphones e tables

O módulo de proteção de dispositivos móveis deve possuir agente para os seguintes sistemas operacionais:

IOS, Android, Blackberry, Windows mobile, Windows phone e Symbian

Deve permitir o provisionamento de configurações de:

Wi-fi, Exchange Activesync, vpn, proxy http global e certificados;

Deve possuir proteção de anti-malware;

Deve ser capaz de realizar escaneamento de malwares em tempo real, do cartão sd e após atualização de vacinas;

Deve possuir capacidade de detecção de spam proveniente de SMS;

Deve possuir funcionalidade de filtro de chamadas que possibilita a criação de lista de número bloqueados para recebimento de chamadas;

Deve possuir funcionalidade de filtro de chamadas que possibilita a criação de lista de número permitidos para efetuação de chamadas;

Deve possuir funcionalidade de firewall para bloqueio de tráfego de entrada e saída, com possibilidades de enumeração de regras de exceção;

Deve permitir a proteção contra ameaças provenientes da web por meio de um sistema de reputação de segurança das URL’s acessadas;

Deve permitir o controle de acesso a websites por meio de listas de bloqueio e aprovação;

Deve permitir o bloqueio de aplicativos de acordo com sua faixa etária indicativa;

Controle da política de segurança de senhas, com critérios mínimos de:

Padrão de senha;

Uso obrigatório de senha;

Tamanho mínimo;

Tempo de expiração;

Bloqueio automático da tela;

Bloqueio por tentativas inválidas;

Controle de acesso à seguinte lista funções e status de ativação de funções dos dispositivos móveis:

Bluetooth

Descoberta de dispositivos bluetooth

Câmera

Cartões de memória

Wlan/wifi

Aceitar TLS não confiável

Instalação de aplicativos

Sincronia automática enquanto em modo roaming

Dados de diagnostico

Forçar backups criptografados

Itunes

Imessage

Compra dentro de aplicativos

Remoção de aplicativos

Safari

Autopreenchimento

Javascript

Popups

Forçar aviso de fraude

Aceitar cookies

Captura de tela

Siri

Siri com tela bloqueada

Filtro de profanidade

Jogos multijogador

Discagem por voz

Youtube

Abertura de documentos de aplicativos gerenciados em aplicativos terceiros

Abertura de documentos de aplicativos terceiros em aplicativos gerenciados

GPS

Microsoft Activesync

MMS/SMS

Porta infravermelha

Porta serial

Alto-falante

Armazenamento USB

3g

Modo de desenvolvedor

Ancoragem (tethering)

Gerenciamento centralizado para todos os itens

A solução de gerenciamento centralizado deve permitir a integração com a solução de segurança para proteção de estações de trabalho (desktops e notebooks), com todos os seus módulos.

Instalação do servidor na plataforma Windows 2008 Server ou superior, seja o servidor físico ou virtual;

Suportar base de dados Microsoft SQL;

Deve gerenciar logs das atividades e eventos gerados pela solução;

Deve possuir integração com Microsoft Active Directory;

Deve permitir níveis de administração por usuários ou grupos de usuários;

Deve permitir a constituição de políticas genéricas aplicáveis a grupos de máquinas, ou aplicáveis a grupos de usuários;

Deve disponibilizar sua interface através dos protocolos http e https;

Deve permitir a alteração das configurações das ferramentas ofertadas, de maneira remota;

Deve permitir diferentes níveis de administração, de maneira independente do login da rede;

Geração de relatórios e gráficos e parametrizáveis nos formatos html, pdf, xml e csv;

Deve gerar relatórios e gráficos pré-definidos nos formatos rtf, pdf, Activex e crystal report (*.rpt);

Deve permitir criação de modelos de relatórios customizados;

Deve permitir logon via single sign-on com os demais produtos da solução;

Deve permitir a atualização de todos os componentes de todos os módulos gerenciados;

Deve permitir a criação de planos de entrega das atualizações, com hora de início ou postergação da entrega após o download dos componentes;

Deve permitir o controle individual de cada componente a ser atualizado;

Deve permitir a definição de exceções por dias e horas para não realização de atualizações;

Deve permitir ter como fonte de atualização um compartilhamento de rede no formato UNC;

Deve gerar relatórios e gráficos com o detalhamento das versões dos produtos instalados;

Deve possuir o acompanhamento dos comandos administrativos em execução, tal como seu status de conclusão, alvo e usuário;

Deve permitir a configuração dos eventos administrativos ou de segurança que geram notificações, tal como o método de envio e o destinatário;

Os métodos de envio suportados devem incluir: e-mail, gravação de registros de eventos do Windows, SNMP e SYSlog;

Deve permitir a configuração do intervalo de comunicação com os módulos gerenciados;

Deve permitir a escolha do intervalo de tempo necessário para que um módulo seja considerado fora do ar (off-line);

Deve permitir o controle do intervalo de expiração de comandos administrativos;

Deve possuir a configuração do tempo de expiração da sessão dos usuários;

Deve permitir a configuração do número de tentativa inválidas de login para o bloqueio de usuários;

Deve permitir a configuração da duração do bloqueio;

Deve permitir pesquisas personalizadas para a consulta de eventos (logs) através de categorias

Deve permitir pesquisas personalizadas para a consulta de eventos (logs), através de critérios lógicos, com base em todos os campos pertencentes aos eventos consultados;

Deve permitir a configuração das informações que não são enviadas dos módulos à solução de gerenciamento centralizado;

Deve permitir a configuração da manutenção dos registros de eventos (logs), com base no intervalo de tempo que devem ser mantidos e no número máximo de registros, por tipo de evento;

Deve de permitir a criação de políticas de segurança personalizadas;

As políticas de segurança devem permitir a seleção dos alvos baseados nos seguintes critérios:

Nome parcial ou completo das estações de trabalho, permitindo a utilização de caractere coringa para identificação do nome parcial da máquina;

Range de endereços IPS;

Sistema operacional;

Agrupamento lógicos dos módulos;

As políticas de segurança devem permitir a combinação lógica dos critérios para identificação do(s) alvo(s) de cada política;

Deve permitir visualização de eventos de violação de segurança de todos os módulos gerenciados, agrupado por usuário numa linha de tempo, configurável;

Deve permitir a gerência dos módulos baseados no modelo de nuvem (cloud), quando existentes;

Deve permitir a criação de múltiplos painéis (dashboards) personalizáveis, compostos por blocos de informações (widgets), visualizados através de gráficos ou tabelas;

Os blocos de informações pertencentes aos painéis personalizáveis devem permitir filtros personalizados para facilitar na visualização e gerenciamentos;

A seleção de uma informação específica dentro de um bloco de informações, através de um clique, deve redirecionar ao log detalhado que gerou aquela informação;

Deve possuir repositório central de identificadores de dados, que podem ser utilizados para a criação de políticas contra possíveis vazamentos de informações;

Deve permitir a investigação de incidentes de vazamento de informação através de um número identificador de incidentes;

3.4.1.2. SOLUÇÃO DE SEGURANÇA COMPLETA PARA DESKTOPS (COMPLETA)

Módulo de proteção anti-malware

Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

Windows 7 (x86/x64);

Windows 8.1 (x86/x64);

Windows 10 (x86/x64);

Deve disponibilizar evidências de varredura em todas as estações de trabalho, identificando as atualizações de sucesso e as ações de insucesso. Para garantir que os casos de insucesso sejam monitorados para tomada de ações pontuais;

Deve ser integrada ao Windows Security center, quando utilizado plataforma Microsoft;

Deve possuir capacidade nativa de integração com modulo da análise virtual para ameaças desconhecidas com suporte a sandbox do mesmo fabricante da solução ofertada

Deve detectar, analisar e eliminar programas maliciosos, tais como vírus, spyware, worms, cavalos de tróia, key loggers, programas de propaganda, rootkits, phishing, dentre outros;

Deve detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos em:

Processos em execução em memória principal (RAM);

Arquivos executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou Shell);

Arquivos compactados automaticamente, em pelo menos nos seguintes formatos: zip, exe, arj, mime/uu, Microsoft cab;

Arquivos recebidos por meio de programas de comunicação instantânea (msn messenger, yahoo messenger, google talk, icq, dentre outros).

Deve detectar e proteger em tempo real a estação de trabalho contra vulnerabilidades e ações maliciosas executadas em navegadores web por meio de scripts em linguagens tais como javascript, vbscript/Activex;

Deve possuir detecção heurística de vírus desconhecidos;

Deve permitir configurar o consumo de cpu que será utilizada para uma varredura manual ou agendada;

Deve permitir diferentes configurações de detecção (varredura ou rastreamento):

Em tempo real de arquivos acessados pelo usuário;

Em tempo real dos processos em memória, para a captura de programas maliciosos executados em memória, sem a necessidade de escrita de arquivo;

Manual, imediato ou programável, com interface gráfica em janelas, personalizável, com opção de limpeza;

Por linha-de-comando, parametrizável, com opção de limpeza;

Automáticos do sistema com as seguintes opções:

Escopo: todos os discos locais, discos específicos, pastas específicas ou arquivos específicos;

Ação: somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena);

Frequência: horária, diária, semanal e mensal;

Exclusões: pastas ou arquivos (por nome e/ou extensão) que não devem ser rastreados;

Deve possuir mecanismo de cache de informações dos arquivos já escaneados;

Deve possuir cache persistente dos arquivos já escaneados para que nos eventos de desligamento e reinicialização das estações de trabalho e notebooks, a cache não seja descartada;

Deve possuir ferramenta de alterações de parâmetros de comunicação entre o cliente antivírus e o servidor de gerenciamento da solução de antivírus;

Deve permitir a utilização de servidores locais de reputação para análise de arquivos e URL's maliciosas, de modo a prover, rápida detecção de novas ameaças;

Deve ser capaz de aferir a reputação das URL's acessadas pelas estações de trabalho e notebooks, sem a necessidade de utilização de qualquer tipo de programa adicional ou plug-in ao navegador web, de forma a proteger o usuário independentemente da maneira de como a URL está sendo acessada;

Deve ser capaz de detectar variantes de malwares que possam ser geradas em tempo real na memória da estação de trabalho ou notebook, permitindo que seja tomada ação de quarentena a ameaça;

Deve ser capaz de bloquear o acesso a qualquer site não previamente analisado pelo fabricante;

Deve permitir a restauração de maneira granular de arquivos quarentenados sob suspeita de representarem risco de segurança;

Deve permitir em conjunto com a restauração dos arquivos quarentenados a adição automática as listas de exclusão de modo a evitar novas detecções dos arquivos;

A solução de antivírus deverá submeter arquivos suspeitos a solução de análise de ameaças avançadas locais, não sendo realizada de maneira externa ao ambiente, apresentado como resultado na análise informações:

Processos de AutoStart;

Modificações de Arquivos de Sistema;

Serviços criados e modificados;

Atividade de Rede Suspeita;

Modificações de Registros;

A solução de análise de ameaças avançadas deverá realizar automaticamente o bloqueio em ações suspeitas nos Desktops infectados com aquela ameaça analisada em sandbox.

Funcionalidade de atualização

Deve permitir a programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, ou de site seguro da internet, com frequência (no mínimo diária) e horários definidos pelo administrador da solução;

Deve permitir atualização incremental da lista de definições de vírus;

Deve permitir a atualização automática do engine do programa de proteção a partir de localização na rede local ou na internet, a partir de fonte autenticável;

Deve permitir o rollback das atualizações das listas de definições de vírus e engines;

Deve permitir a indicação de agentes para efetuar a função de replicador de atualizações e configurações, de forma que outros agentes possam utiliza-los como fonte de atualizações e configurações, não sendo necessária a comunicação direta com o servidor de anti-malware para essas tarefas;

Deve permitir que os agentes de atualização possam replicar os componentes de vacinas, motores de escaneamento, versão de programas, hotfix e configurações específicas de domínios da árvore de gerenciamento;

O servidor da solução de anti-malware, deve ser capaz de gerar localmente versões incrementais das vacinas a serem replicadas com os agentes replicadores de atualizações e configurações, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização;

O agente replicador de atualizações e configurações, deve ser capaz de gerar localmente versões incrementais das vacinas a serem replicadas com os demais agentes locais, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização;

Funcionalidade de administração

Deve permitir proteção das configurações da solução instalada na estação de trabalho através de senha ou controle de acesso, em ambos os casos, controlada por política gerenciada pela console de administração da solução completa;

Deve possibilitar instalação "silenciosa";

Deve permitir o bloqueio por nome de arquivo;

Deve permitir o travamento de pastas e diretórios;

Deve permitir o travamento de compartilhamentos;

Deve permitir o rastreamento e bloqueio de infecções;

Deve possuir mecanismo de detecção de ameaças baseado em comportamento de processos que estão sendo executados nas estações de trabalho e notebooks;

Deve efetuar a instalação remota nas estações de trabalho, sem requerer outro software ou agente adicional, previamente instalado e sem necessidade de reiniciar a estação de trabalho;

Deve desinstalar automática e remotamente a solução de antivírus atual, sem requerer outro software ou agente;

Deve permitir a desinstalação através da console de gerenciamento da solução;

Deve ter a possibilidade de exportar/importar configurações da solução através da console de gerenciamento;

Deve ter a possibilidade de backup da base de dados da solução através da console de gerenciamento;

Deve ter a possibilidade de designação do local onde o backup automático será realizado;

Deve permitir realização do backup da base de dados através de mapeamento de rede controlado por senha;

Deve ter a possibilidade de determinar a capacidade de armazenamento da área de quarentena;

Deve permitir a deleção dos arquivos quarentenados;

Deve permitir remoção automática de clientes inativos por determinado período de tempo;

Deve permitir integração com Active Directory para acesso a console de administração;

Identificar através da integração com o Active Directory, quais máquinas estão sem a solução de anti-malware instalada;

Deve permitir criação de diversos perfis e usuários para acesso a console de administração;

Deve permitir que a solução utilize consulta externa a base de reputação de sites integrada e gerenciada através da solução de anti-malware, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;

Deve possuir solução de consulta do hash dos arquivos integrada e gerenciada através da solução de antivírus, cancelando o download ou execução do arquivo, de forma automática, baseado na resposta à consulta da base do fabricante;

Deve permitir agrupamento automático de estações de trabalho e notebooks da console de gerenciamento baseando-se no escopo do Active Directory ou IP;

Deve permitir criação de subdomínios consecutivos dentro da árvore de gerenciamento;

Deve possuir solução de reputação de sites local para sites já conhecidos como maliciosos integrada e gerenciada através da solução de antivírus, com opção de configuração para estações dentro e fora da rede, cancelando a

conexão de forma automática baseado na resposta à consulta da base do fabricante;

Deve registrar no sistema de monitoração de eventos da console de anti-malware informações relativas ao usuário logado no sistema operacional;

Deve prover ao administrador relatório de conformidade do status dos componentes, serviços, configurações das estações de trabalho e notebooks que fazem parte do escopo de gerenciamento da console de antivírus;

Deve prover ao administrador informações sobre quais estações de trabalho e notebooks fazem parte do escopo de gerenciamento da console de anti-malware não realizaram o escaneamento agendado ou o escaneamento demandado pelo administrador no período determinado de dias;

Deve prover segurança através de SSL para as comunicações entre o servidor e a console de gerenciamento web;

Deve prover segurança através de SSL para as comunicações entre o servidor e os agentes de proteção;

Deve suportar múltiplas florestas e domínios confiáveis do Active Directory;

Deve utilizar de chave de criptografia que seja/esteja em conformidade com o Active Directory para realizar uma conexão segura entre servidor de antivírus e o controlador de domínio;

Deve permitir a criação de usuários locais de administração da console de anti-malware;

Deve possuir a integração com o Active Directory para utilização de seus usuários para administração da console de anti-malware;

Deve permitir criação de diversos perfis de usuários que permitam acessos diferenciados e customizados a diferentes partes da console de gerenciamento;

Deve bloquear acessos indevidos a área de administração do agente que não estejam na tabela de políticas definidas pelo administrador;

Deve se utilizar de mecanismo de autenticação da comunicação entre o servidor de administração e os agentes de proteção distribuídos nas estações de trabalho e notebooks;

Deve permitir a gerência de domínios separados para usuários previamente definidos;

Deve ser capaz de enviar notificações específicas aos respectivos administradores de cada domínio definido na console de administração;

Deve permitir configuração do serviço de reputação de sites da web em níveis: baixo, médio e alto;

Funcionalidade de controle de dispositivos

Deve possuir controle de acesso a discos removíveis reconhecidos como dispositivos de armazenamento em massa através de interfaces USB e outras,

com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura, e bloqueio total;

Deve possuir o controle de acesso a drives de mídias de armazenamento como cdrom, dvd, com as opções de acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;

Deve ser capaz de identificar smartphones e tablets como destinos de cópias de arquivos e tomar ações de controle da transmissão;

Deve possuir o controle a drives mapeados com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;

Deve permitir escaneamento dos dispositivos removíveis e periféricos (USB, disquete, cdrom) mesmo com a política de bloqueio total ativa;

Módulo de proteção anti-malware para estação Linux

Distribuições homologadas pelo fabricante

SUSE Linux Enterprise 10 e 11;

Red Hat enterprise Linux 4.0, 5.0 e 6.0;

Centos 4.0, 5.0 e 6.0

O agente deve possuir código aberto possibilitando assim adequação a qualquer kernel e distribuição Linux, incluindo desenvolvidas ou alteradas internamente e para versões não homologadas pelo fabricante;

Deve permitir a varredura manual com interface gráfica, personalizável, com opção de limpeza dos malwares encontrados;

Deve permitir a varredura manual por linha de comando, parametrizável e com opção de limpeza automática em todos os sistemas operacionais;

Deve possuir a capacidade de detecção e remoção de todos os tipos de malware, incluindo spyware, adware, grayware, cavalos de tróia, rootkits e outros;

Deve detectar e remover códigos maliciosos de macro do pacote Microsoft office, em tempo real;

O cliente da solução deve armazenar localmente, e enviar para o servidor (para fins de armazenamento) logs de ocorrência de ameaças, contendo no mínimo os seguintes dados: nome da ameaça, caminho do arquivo comprometido (quando disponível), data e hora da detecção, endereço ip do cliente e ação realizada;

Deve gerar cópia de segurança dos arquivos comprometidos antes de realizar o processo de remoção de ameaças. Esta cópia deve ser gravada na máquina local, e o acesso ao arquivo deve ser permitido somente pela solução de segurança ou o administrador;

A desinstalação do cliente nas estações de trabalho deverá ser completa, removendo arquivos, entradas de registro e configurações, logs diversos, serviços do sistema operacional e quaisquer outros mecanismos instalados;

Deve rastrear ameaças em arquivos compactados em, no mínimo, 15 níveis recursivos de compactação;

As mensagens exibidas aos usuários devem ser traduzidas para o português do brasil;

Módulo de proteção anti-malware para estações de macOS

O cliente para instalação deverá possuir compatibilidade com os sistemas operacionais:

MacOS 10.14 (Mojave) em processadores 32 e 64 bits;

MacOS 10.13 (High Sierra) em processadores 32 e 64 bits;

MacOS 10.12 (Sierra) em processadores 32 e 64 bits;

OS X 10.11 (El Capitan) em processadores 32 e 64 bits;

OS X 10.10 (Yosemite) em processadores 32 e 64 bits;

Suporte ao apple remote desktop para instalação remota da solução;

Gerenciamento integrado à console de gerência central da solução

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

Permitir a verificação das ameaças da maneira manual e agendada;

Permitir a criação de listas de exclusões para pastas e arquivos que não serão verificados pelo antivírus;

Permitir a ações de reparar arquivo ou colocar em quarentena em caso de infeções a arquivos;

Deve possuir mecanismo de proteção contra uso não autorizado no qual o agente do antivírus deve ser protegido contra mudança do seu estado (não possibilitar que um administrador da estação de trabalho e notebook possa parar o serviço do antivírus) bem como mecanismo para restaurar seu estado normal;

Deve possuir no mecanismo de autoproteção as seguintes proteções:

Autenticação de comandos ipc;

Proteção e verificação dos arquivos de assinatura;

Proteção dos processos do agente de segurança;

Proteção das chaves de registro do agente de segurança;

Proteção do diretório de instalação do agente de segurança.

Funcionalidade de HIPS – Host IPS e Host Firewall

Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

Windows XP SP3 (x86/x64);

Windows 7 (x86/x64);

Windows 8.1 (x86/x64);

Windows 10 (x86/x64)

Deve possuir módulo para proteção de vulnerabilidades com as funcionalidades de host ips e host firewall;

Todas as regras das funcionalidades de firewall e ips de host devem permitir apenas detecção (log) ou prevenção (bloqueio);

Deve permitir ativar e desativar o produto sem a necessidade de remoção;

Deve permitir a varredura de portas logicas do sistema operacional para identificar quais estejam abertas e possibilitando tráfego de entrada ou saída;

A funcionalidade de host ips deve possuir regras para controle do tráfego de pacotes de determinadas aplicações;

Deve prover proteção contra as vulnerabilidades do sistema operacional Windows XP ou superior, por meio de regras de host ips;

Deve efetuar varredura de segurança automática ou sob demanda que aponte vulnerabilidades de sistemas operacionais e aplicações e atribua automaticamente as regras de host ips para proteger a estação de trabalho ou notebook contra a possível exploração da vulnerabilidade;

A varredura de segurança deve ser capaz de identificar as regras de host ips que não são mais necessárias e desativá-las automaticamente;

Deve prover proteção contra as vulnerabilidades de aplicações terceiras, por meio de regras de host ips, tais como oracle java, abobe pdf reader, adobe flash player, realnetworks real player, Microsoft office, apple itunes, apple quick time, apple safari, google chrome, mozilla firefox, opera browser, ms internet explorer, entre outras;

Deve permitir a criação de políticas diferenciadas em múltiplas placas de rede no mesmo sistema operacional;

Deve permitir a criação de políticas de segurança personalizadas;

Deve permitir limitar o número de conexões simultâneas no sistema operacional

Deve permitir a emissão de alertas via smtp e snmp;

Deve permitir configuração e manipulação de políticas de firewall através de prioridades;

Deve permitir criação de regras de firewall utilizando os seguintes protocolos:

Icmp, icmpv6, igmp, ggp, tcp, pup, udp, idp, nd, raw, tcp+udp.

Deve permitir criação de regras de firewall por origem de ip ou mac ou porta e destino de ip ou mac ou porta;

Deve permitir a criação de regras de firewall pelos seguintes frames types:

Ip, ipv4, ipv6, arp, revarp.

Deve permitir também escolher outros tipos de frame type de 4 dígitos em hex code;

Deve permitir a criação de grupos lógicos através de lista de ip, mac ou portas;

Deve permitir a criação de contextos para a aplicação para criação de regras de firewall;

Deve permitir o isolamento de interfaces de rede, possibilitando o funcionamento de uma interface por vez;

Deve permitir a criação de múltiplos painéis (dashboards) personalizáveis, compostos por blocos de informações (widgets), visualizados através de gráficos ou tabelas;

Os blocos de informações pertencentes aos painéis personalizáveis devem permitir filtros personalizados para facilitar a visualização e gerenciamentos;

A seleção de uma informação específica dentro de um bloco de informações, através de um clique, deve redirecionar ao log detalhado que gerou aquela informação;

Módulo para controle de aplicações

Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

Windows XP SP3 (x86/x64);

Windows 7 (x86/x64);

Windows 8.1 (x86/x64);

Windows 10 (x86/x64)

Deve permitir a criação de políticas de segurança personalizadas;

As políticas de segurança devem permitir a seleção dos alvos baseados nos seguintes critérios:

Nome parcial ou completo das estações de trabalho, permitindo a utilização de caractere coringa para identificação do nome parcial da máquina;

Range de endereços IPS;

Sistema operacional;

Grupos de máquinas espelhados do Active Directory;

Usuários ou grupos do Active Directory;

As políticas de segurança devem permitir a combinação lógica dos critérios para identificação do(s) alvo(s) de cada política;

As políticas de segurança devem permitir a definição dos logs que serão recebidos de acordo com os seguintes critérios:

Nenhum;

Somente bloqueios;

Somente regras específicas;

Todas as aplicações executadas;

As políticas de segurança devem permitir o controle do intervalo de envio dos logs;

As políticas de segurança devem permitir o controle do intervalo para envio de atualização de cada política;

As políticas de segurança devem permitir a definição de qual servidor de gerenciamento o agente de segurança deverá comunicar-se;

As políticas de segurança devem permitir a ocultação do ícone do agente, que reside da barra de tarefas, e de notificações ao usuário;

As políticas de segurança devem permitir o controle do intervalo de quando os inventários de aplicações são executados;

As políticas de segurança devem permitir o controle através de regras de aplicação;

As regras de controle de aplicação devem permitir as seguintes ações:

Permissão de execução;

Bloqueio de execução;

Bloqueio de novas instalações;

As regras de controle de aplicação devem permitir o modo de apenas coleta de eventos (logs), sem a efetivação da ação regra;

As regras de controle de aplicação devem permitir os seguintes métodos para identificação das aplicações:

Assinatura sha-1 do executável;

Atributos do certificado utilizado para assinatura digital do executável;

Caminho lógico do executável;

Base de assinaturas de certificados digitais válidos e seguros;

As regras de controle de aplicação devem possuir categorias de aplicações;

As políticas de segurança devem permitir a utilização de múltiplas regras de controle de aplicações.

Deve permitir a criação de múltiplos painéis (dashboards) personalizáveis, compostos por blocos de informações (widgets), visualizados através de gráficos ou tabelas;

Os blocos de informações pertencentes aos painéis personalizáveis devem permitir filtros personalizados para facilitar na visualização e gerenciamentos;

A seleção de uma informação específica dentro de um bloco de informações, através de um clique, deve redirecionar ao log detalhado que gerou aquela informação;

Módulo de proteção contra vazamento de informações - DLP

Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

Windows 7 (x86/x64);

Windows 8.1 (x86/x64);

Windows 10 (x86/x64)

Deve possuir nativamente templates para atender as seguintes regulamentações:

PCI/DSS;

HIPA;

Glba;

SB-1386;

US PII.

Deve ser capaz de detectar informações, em documentos nos formatos:

Documentos: Microsoft office (doc, docx, xls, xlsx, ppt, pptx) openoffice, rtf, wordpad, text; xml, html;

Gráficos: visio, postscript, pdf, tiff,

Comprimidos: win zip, rar, tar, jar, arj, 7z, rpm, cpio, gzip, bzip2, unix/linux zip, lzh;

Códigos: c/c++, java, verilog, autocad;

Deve ser capaz de detectar informações, com base em:

Dados estruturados, como dados de cartão de crédito, dados pessoais, endereços de e-mail, CPF, entre outros;

Palavras ou frases configuráveis;

Expressões regulares;

Extensão dos arquivos;

Deve ser capaz de detectar em arquivos compactados;

Deve permitir a configuração de quantas camadas de compressão serão verificadas;

Deve permitir a criação de modelos personalizados para identificação de informações;

Deve permitir a criação de modelos com base em regras e operadores lógicos;

Deve possuir modelos padrões;

Deve permitir a importação e exportação de modelos;

Deve permitir a criação de políticas personalizadas

Deve permitir a criação de políticas baseadas em múltiplos modelos;

Deve permitir mais de uma ação para cada política, como:

Apenas registrar o evento da violação;

Bloquear a transmissão;

Gerar alertar para o usuário;

Gerar alertar na central de gerenciamento;

Capturar informação para uma possível investigação da violação;

Deve permitir criar regras distintas com base se a estação está fora ou dentro da rede;

Deve ser capaz de identificar e bloquear informações nos meios de transmissão:

Cliente de e-mail;

Protocolos http, https, ftp;

Mídias removíveis;

Discos óticos cd/dvd;

Gravação cd/dvd;

Aplicações de mensagens instantâneas;

Tecla de print screen;

Aplicações p2p;

Área de transferência do Windows;

Webmail;

Armazenamento na nuvem (cloud);

Impressoras;

Scanners;

Compartilhamentos de arquivos;

Activesync;

Criptografia PGP;

Disquete;

Portas com, lpt, firewire (ieee 1394);

Modems;

Infravermelho;

Bluetooth;

Deve permitir a criação de exceções nas restrições dos meios de transmissão;

Módulo de criptografia

Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

Windows 7 (x86/x64);

Windows 8.1 (x86/x64);

Windows 10 (x86/x64)

Deve possuir módulo de criptografia para as estações de trabalho (desktops e notebooks), com as seguintes funcionalidades de criptografia para:

Disco completo (fde – full disk encryption);

Pastas e arquivos;

Mídias removíveis;

Anexos de e-mails;

Automática de disco;

Deve possuir autenticação durante a inicialização (boot) da estação de trabalho, antes do carregamento do sistema operacional, para a funcionalidade de criptografia do disco completo;

A autenticação durante a inicialização (boot) deve ser a partir das credenciais sincronizadas com o Active Directory;

Deve possuir suporte ao algoritmo de criptografia aes-256;

Deve possuir a capacidade de exceções para criptografia automática;

Deve possuir criptografia no canal de comunicação entre as estações de trabalho e o servidor de políticas;

Deve possuir certificação FIPS 140-2;

Deve possuir funcionalidade de criptografia por software ou hardware;

Deve ser compatível com os padrões SED ('self-encrypting drive), opal e opal2

Deve possuir compatibilidade de autenticação por múltiplos fatores;

Deve permitir atualizações do sistema operacional mesmo quando o disco está criptografado;

Deve possuir a possibilidade de configurar senha de administração local na estação de trabalho para desinstalação do módulo;

Deve possuir políticas por usuários, grupos e dispositivos;

Deve possuir os métodos de autenticação seguintes para desbloquear um disco:

Sequência de cores;

Autenticação com ad;

Single sign-on com ad;

Senha pré-definida;

Número pin;

Smart card;

Deve possuir auto ajuda para usuários que esquecerem a senha com a combinação de perguntas e respostas;

Deve possuir mecanismos de criptografia transparentes para o usuário;

Deve possuir mecanismos para wipe (limpeza) remoto;

Deve possuir mecanismo para desativar temporariamente a autenticação de pré-inicialização (boot);

Deve possuir mecanismo que permita desfazer a criptografia do disco no evento em que se torne corrompido, impedindo a inicialização da estação/notebook;

O ambiente de autenticação pré-inicialização deve permitir a conexão a redes sem fio (wireless);

Deve ser possível especificar o tipo de autenticação das redes wireless disponíveis;

O ambiente de autenticação pré-inicialização deve conter indicação visual do estado de conectividade de rede da estação/notebook;

O ambiente de autenticação deve disponibilizar um teclado virtual na tela do dispositivo, independente do teclado físico;

O ambiente de autenticação pré-inicialização deve permitir a mudança do leiaute do teclado;

O ambiente de autenticação pré-inicialização deve prover um mecanismo de assistência remota que permita a autenticação da estação de trabalho no evento que o usuário não se lembre de sua senha de autenticação;

O ambiente de autenticação pré-inicialização deve prover um mecanismo que permita a substituição da senha e outros códigos de autenticação através da resposta correta a perguntas definidas previamente pelo administrador;

Ambiente de autenticação pré-inicialização deve prover uma ferramenta que permita a execução de procedimentos de identificação de problema, assim como a realização das seguintes tarefas administrativas: desfazer a criptografia do disco, restaurar o registro mestre de inicialização (mbr – master boot record) ao estado anterior ao estado alterado pelo ambiente de autenticação pré-inicialização, montar partições criptografadas, modificar a política de criptografia aplicada à estação de trabalho, adicionar, remover e editar atributos dos usuários existentes na lista de usuários permitidos a se autenticar na estação de trabalho, visualizar os registros (logs) das atividades da solução de criptografia e visualizar, testar e modificar as configurações de rede;

O acesso a este ambiente de execução de procedimentos de identificação de problema e realização de tarefas administrativos deve ser controlado através de política gerenciada remotamente pelo componente de gerenciamento da solução;

Deve prover ferramenta presente na estação de trabalho que possibilite migrá-la para um servidor de gerenciamento diferente;

Deve permitir a gerência das seguintes soluções terceiras de criptografia:

Microsoft bitlocker;

Apple filevault;

As capacidades de gerência das soluções terceiras de criptografia devem incluir:

Habilitar a criptografia

Exibir o estado da criptografia (ativado, desativado)

Habilitar o aviso legal

Editar o intervalo de sincronia

Deve permitir a visualização das estações de trabalho que tenham aplicação de política pendente a partir da console de administração centralizada;

Deve permitir a visualização do autor de determinada política a partir da console de administração centralizada;

Deve permitir a visualização de estações de trabalho que não possuam nenhuma política aplicada a partir da console de administração centralizada;

Deve permitir a adição de informações de contato a serem exibidas ao usuário final com texto customizável;

Deve permitir a exibição de aviso legal quando o agente de criptografia é instalado na estação de trabalho;

Deve permitir a exibição de aviso legal quando a estação é inicializada;

Deve permitir, em nível de política, a indicação de pastas a serem criptografadas;

Deve possibilitar que cada política tenha uma chave de criptografia única;

Deve permitir, em nível de política, a escolha da chave de criptografia a ser utilizada, entre as seguintes opções:

Chave do usuário: somente o usuário tem acesso aos arquivos;

Chave da empresa: qualquer usuário da empresa tem acesso aos arquivos;

Chave da política: qualquer estação de trabalho que tenha aplicada a mesma política tem acesso aos arquivos;

Deve permitir a escolha dos diretórios a serem criptografados em dispositivos de armazenamento USB;

Deve possibilitar a desativação de dispositivos de gravação de mídias óticas;

Deve possibilitar a desativação de dispositivos de armazenamento USB;

Deve possibilitar o bloqueio da desinstalação do agente de criptografia por usuários que não sejam administradores da estação de trabalho;

Deve possibilitar o bloqueio da autenticação de usuários baseado no intervalo em que o dispositivo não tenha as políticas sincronizadas com o componente de administração centralizada;

Deve possibilitar o atraso, em intervalo personalizado de tempo, para uma nova tentativa de autenticação de usuários na ocorrência de um número personalizável de tentativas inválidas de autenticação;

Deve possibilitar apagar todos os dados do dispositivo na ocorrência de um número personalizável de tentativas inválidas de autenticação;

Deve possibilitar a instauração de política de gerenciamento de complexidade e intervalo de troca de senha com os seguintes critérios:

Definição do intervalo de dias em que o usuário será forçado a mudar sua senha;

Definição de número de senhas imediatamente anteriores que não poderão ser reutilizadas como nova senha;

Definição do número de caracteres iguais consecutivos que não poderão ser utilizados na nova senha;

Definição do comprimento de caracteres mínimo a ser utilizado na nova senha;

Definição do número de caracteres especiais, caracteres numéricos, caracteres em caixa alta e caracteres em caixa baixa que deverão ser utilizados para a nova senha;

Deve permitir a criação de múltiplos painéis (dashboards) personalizáveis, compostos por blocos de informações (widgets), visualizados através de gráficos ou tabelas;

Os blocos de informações pertencentes aos painéis personalizáveis devem permitir filtros personalizados para facilitar na visualização e gerenciamentos;

A seleção de uma informação específica dentro de um bloco de informações, através de um clique, deve redirecionar ao log detalhado que gerou aquela informação;

Módulo de proteção para smastphones e tablets

O módulo de proteção de dispositivos móveis deve possuir agente para os seguintes sistemas operacionais:

iOS e Android

Deve permitir o provisionamento de configurações de:

Wi-fi, Exchange Activesync, vpn, proxy http global e certificados;

Deve possuir proteção de anti-malware;

Deve ser capaz de realizar escaneamento de malwares em tempo real, do cartão sd e após atualização de vacinas;

Deve possuir capacidade de detecção de spam proveniente de SMS;

Deve possuir funcionalidade de filtro de chamadas que possibilita a criação de lista de número bloqueados para recebimento de chamadas;

Deve possuir funcionalidade de filtro de chamadas que possibilita a criação de lista de número permitidos para efetuação de chamadas;

Deve possuir funcionalidade de firewall para bloqueio de tráfego de entrada e saída, com possibilidades de enumeração de regras de exceção;

Deve permitir a proteção contra ameaças provenientes da web por meio de um sistema de reputação de segurança das URL's acessadas;

Deve permitir o controle de acesso a websites por meio de listas de bloqueio e aprovação;

Deve permitir o bloqueio de aplicativos de acordo com sua faixa etária indicativa;

Controle da política de segurança de senhas, com critérios mínimos de:

Padrão de senha;

Uso obrigatório de senha;

Tamanho mínimo;

Tempo de expiração;

Bloqueio automático da tela;

Bloqueio por tentativas inválidas;

Controle de acesso à seguinte lista funções e status de ativação de funções dos dispositivos móveis:

Bluetooth

Descoberta de dispositivos bluetooth

Câmera

Cartões de memória

Wlan/wifi

Aceitar TLS não confiável

Instalação de aplicativos

Sincronia automática enquanto em modo roaming

Dados de diagnostico

Forçar backups criptografados

Itunes

Imessage

Compra dentro de aplicativos

Remoção de aplicativos

Safari

Autopreenchimento

Javascript

Popups

Forçar aviso de fraude

Aceitar cookies

Captura de tela

Siri

Siri com tela bloqueada

Filtro de profanidade

Jogos multijogador

Discagem por voz

Youtube

Abertura de documentos de aplicativos gerenciados em aplicativos terceiros

Abertura de documentos de aplicativos terceiros em aplicativos gerenciados

GPS

Microsoft Activesync

MMS/SMS

MARIA DO CARMO DO PRADO
Pregoeiro (a) SUPEL-RO
Mat. 300131839

Porta infravermelha

Porta serial

Alto-falante

Armazenamento USB

3g

Modo de desenvolvedor

Ancoragem (tethering)

Modulo de anti-spam (gateway de e-mail)

Pré-Filtro

Permitir configurar filtro de vírus (em nuvem) antes da chegada ao ambiente interno;

Permitir configurar filtro de SPAMs por reputação antes da chegada ao ambiente (na nuvem);

Permitir configurar filtro de SPAMs por característica (heurística) antes da chegada ao ambiente (na nuvem);

Permitir balanceamento de carga (Load Balance) para o mesmo domínio;

Possui gerenciamento de configurações em nuvem de forma integrada em uma única console de gerenciamento, interna e externa ao ambiente;

SPAM / Phishing

Bloqueio de servidores spammers através da metodologia conhecida por Domain Keys Identified Mail (DKIM);

Deverá fazer listas de exceções para domínios utilizando-se de DKIM;

Possuir a detecção de SPAMs utilizando tecnologia heurística,

Possuir configurações de sensibilidade na detecção de SPAMs, no mínimo em 4 níveis;

Permitir a criação de White e Black Lists para detecção de SPAMs;

Possuir proteção contra Phishings;

Possuir proteção inteligente contra-ataques de Engenharia Social.

Deverá verificar o cabeçalho das mensagens em tempo real para proteção contra SPAMs;

Possuir inteligência contra ataques dos tipos, exploração de Códigos Avançados (Exploits) e Ataque de dia-zero (Zero-Day)

Possui reputação de links que estejam dentro do corpo das mensagens;

Possui reputação de links que estejam dentro do corpo das mensagens;

Possui níveis de sensibilidade no bloqueio de mensagens com links de má reputação;

Possui White List para a checagem de reputação em URL's dentro de mensagens;

Vírus:

Permitir a verificação heurística contra vírus recém-lançados, mesmo sem uma vacina disponível;

Permitir a verificação do tipo real do arquivo, mesmo que o mesmo for renomeado;

Permitir que arquivos suspeitos sejam enviados ao fabricante sem intervenção do administrador;

Permitir o escaneamento de arquivos executáveis comprimidos em tempo real;

Proteção contra Spywares, sem a necessidade de um software ou agente adicional;

Proteção contra Dialers, sem a necessidade de um software ou agente adicional;

Proteção contra Ferramentas Hackers, sem a necessidade de um software ou agente adicional;

Proteção contra Ferramentas para descobrir senhas de aplicativos, sem a necessidade de um software ou agente adicional;

Proteção contra Adwares, sem a necessidade de um software ou agente adicional;

Proteção contra Ferramentas, sem a necessidade de um software ou agente adicional;

Bloqueio de malware empacotado (packed malware) de forma heurística;

A solução de anti-spam deverá submeter e-mails suspeitos a solução de análise de ameaças avançadas locais, não sendo realizada de maneira externa ao ambiente, apresentado como resultado na alise informações;

Processos de AutoStart;

Modificações de Arquivos de Sistema;

Serviços criados e modificados;

Atividade de Rede Suspeita;

Modificações de Registros;

O Fabricante ofertado deve possuir conhecimento em mais de 190 milhões de ameaças conhecidas;

Filtros:

Possuir um filtro de conteúdo com pesquisa por palavras-chave no cabeçalho e corpo da mensagem, e em arquivos Microsoft Office anexados, utilizando

operadores lógicos tais como AND, OR, OCCUR, NEAR, (,), [,] e assim por diante;

Permitir bloquear anexos pela extensão, pelo tipo real do arquivo, nome, tamanho, e número de anexos;

Permitir criar filtros definidos pelo tamanho de mensagem;

Possuir proteção contra Graymail;

Permitir criar exceções para os filtros, definidos por rotas, grupos de usuários ou usuários específicos;

Possuir recurso que retire anexos indesejados e entregue a mensagem original para o destinatário;

Possibilitar a criação de áreas de quarentenas separadas para cada tipo de filtro;

Permitir o bloqueio de arquivos anexos baseado em sua extensão, tamanho, tipo real do arquivo (independente da extensão) e dentro de arquivos compactados;

Permitir a verificação em arquivos compactados nos formatos mais utilizados em até 20 níveis de compactação;

Permitir criar regras distintas para mensagens que entram e saem do ambiente;

Permitir a verificação contra conteúdos não autorizados dentro dos arquivos anexados nas mensagens;

Permitir a criação de grupos de usuários para configuração de regras por grupo ou usuário;

Permitir limitar o número de destinatários por mensagem;

Possui regra específica para anexos protegidos por senha

Possuir módulo de Data Loss Prevention (DLP), prevenido ações de vazamento de informações, com regras baseadas em:

Palavras chaves;

Expressões regulares;

Extensões de arquivos.

Possuir verificação de mensagens criptográficas de cliente que suporte os seguintes cipher suítes:

AES128-SHA

DHE-RSA-AES128-SHA

AES256-SHA

ADH-RC4-MD5

RC4-SHA

RC4-MD5

DHE-DSS-AES128-SHA

IDEA-CBC-SHA

Filtros por IP

Permitir a checagem na rede Global (colaborativa) da reputação dos IPs que tentam se conectar ao ambiente para enviar mensagens;

Permitir a configuração individual entre Reputação Global (da empresa prestadora do serviço) e Reputação Local (personalizada);

Possibilidade de exceções ao bloqueio por reputação com base em pais range de ip ou ip

Configurar nível de sensibilidade da reputação de Ips em até quatro níveis;

Permitir configurar o código de erro para mensagens rejeitadas;

Permitir a verificação de endereços IPs para checar a sua legitimidade, sendo:

Realizar a busca em no mínimo cinco bases de dados localizados no site do fabricante;

Não necessitar instalação adicional;

As bases devem ser do mesmo fabricante do software para gateway SMTP;

Possuir configuração personalizada para cada tipo de ataque (SPAM, Vírus, Dicionário (DHA) e Mensagens de Retorno (Bounced Mails));

Permitir personalizar os filtros baseado em:

Tempo;

Total de mensagens;

Porcentagem de mensagens;

Ação a ser tomada;

Prevenir contra-ataques de SPAM, permitindo rejeitar a conexão quando exceder configuração personalizada para esse ataque;

Prevenir contra-ataques de Vírus, permitindo rejeitar a conexão quando exceder configuração personalizada para esse ataque;

Prevenir contra ataques DHA (Directory Harvest Attack);

Permitir verificar conexões suspeitas, apresentando o domínio responsável pela conexão, apresentado total de conexões e dessas, o percentual de conexões maliciosas;

Ações:

Possuir recurso que permita adiar a entrega de determinadas mensagens para um horário específico;

Permitir enviar notificações de ocorrências customizadas ao administrador, remetente, destinatário;

Permitir customizar as ações que a ferramenta deve tomar de acordo com as necessidades do ambiente;

Permitir inserção de carimbo no assunto da mensagem;

Permitir a inserção de um header customizado (X-header);

Permitir o direcionamento da mensagem para servidor diferente do padrão (próximo hop) de acordo com a necessidade do ambiente;

Permitir apagar anexos indesejados, mas entregar a mensagem ao destinatário informando da ação;

Permitir a inserção de texto no corpo da mensagem;

Permitir customizar a mensagem que será inserida no corpo das mensagens;

Permitir a escolha do local onde se irá colocar a notificação customizada para o começo ou fim da mensagem original;

Permitir inserir variáveis nas notificações, onde informem:

Remetente;

Destinatário;

Assunto;

Data;

Nome do arquivo detectado;

Nome do vírus detectado;

Protocolo de escaneamento;

Tamanho total da mensagem e seus anexos;

Tamanho total do anexo;

Número de anexos detectados pela regra;

Ação tomada pela ferramenta;

Nome da quarentena para onde a mensagem foi enviada;

Permitir configurar ações para mensagens fora do padrão (mensagens mal formadas);

Permitir ação personalizada para mensagens com anexos protegidos por senha;

Permitir quarentenar mensagens de SPAM;

Permitir encaminhar as mensagens em cópia oculta para destinatário não inserido originalmente na mensagem;

Permitir arquivar as mensagens sem que o remetente ou destinatário saibam para fins de auditoria;

Quarentena:

Capacidade de apresentar uma console web para que os usuários possam verificar as mensagens que estejam em quarentena por motivo de spam;

Capacidade de usuários criarem lista de exceções a remetentes nessa console web de quarentena de mensagens;

Permitir que os usuários verifiquem mensagens suspeitas postas em quarentena e aprovar os remetentes sem intervenção do administrador;

Permitir exclusão automática das mensagens em quarentena;

Deverá utilizar LDAP para autenticação ao portal de quarentena, suportando no mínimo:

Microsoft Active Directory

OpenLDAP

Sun iPlanet Directory

Administração:

Gerenciamento via console web HTTPS (Internet Explorer / Firefox);

A solução deve possuir um modo de instalação passo a passo, na própria console de gerenciamento.

Gerenciamento das áreas de quarentena, com pesquisa, reprocessamento, entrega ou exclusão de mensagem;

Realizar atualização de vacinas de forma incremental

Realizar atualização de e da versão do software. A atualização deve permitir conexão através de serviço Proxy;

Possibilidade de configurar o “greeting” SMTP;

Permitir o controle de relay baseado no domínio e/ou endereço IP;

Possuir recurso que faça uma monitoração do sistema, alertando o administrador caso haja falta de espaço em disco, se o serviço estiver indisponível e se a fila de mensagens chegarem a um número estabelecido como máximo pelo administrador;

Permitir a verificação de mensagens no protocolo POP3, permitindo configurar que porta TCP será utilizada;

Capacidade de checagem por DNS reverso com até quatro diferentes níveis de bloqueio

Definição de timeout de conexão SMTP

Suporte a ilimitadas conexões SMTP

Capacidade de ter vários servidores de rastreamento de tráfego SMTP gerenciado por console único.

Ter a capacidade de proteger o tráfego POP3;

Ter gerencia de área exclusiva para quarentena ou cópia de mensagens;

A solução deve ofertar possibilidade de ter domínio mascarado;

Possuir autenticação via TLS (Transport Layer Security);

Possuir mecanismo de alerta especifico para ataques do tipo Command & Control (C&C).

Relatórios:

A solução deve apresentar relatórios criados através de console web;

A solução deve disponibilizar relatórios gerenciais que podem ser "on demand" ou agendados;

A solução deve disponibilizar relatórios gerenciais de utilização de mensagens por destinatário, remetente, assunto;

A solução deve ter templates predefinidos para relatórios de forma a facilitar a geração de relatórios;

Possuir integração com LDAP (Microsoft Active Directory, Lotus Domino, Sun iPlanet Directory).

A solução deve ser capaz de receber trafego em TLS e realizar conexões em TLS para outros servidores;

A solução deve possibilitar trafego via Secure SMTP;

A solução deve permitir reindexação da base de dados de forma agendada;

É preciso que a solução permita importação e exportação de suas políticas através da console de gerenciamento;

A solução deve permitir a criação de usuários com acessos diferentes de administrador à console de gerenciamento;

A solução deve integrar o login da console de gerenciamento com o serviço de LDAP pré-configurado;

Características Gerais da Solução de anti-spam

A solução deve ser oferecida em formato de software appliance;

Não serão aceitas soluções Open Source;

A solução deve ser gerenciada totalmente por sua console Web, além de possui interface CLI intuitiva com gerenciamento dedica a solução;

A solução precisa ser compatível com as seguintes plataformas de virtualização:

VmWare™ ESX server;

VmWare ESXi 5.0

VmWare ESXi 5.5;

Hyper-V

Microsoft Hyper-V Server 2008 R2 SP1

Microsoft Hyper-V Server 2012 R2

Anti-spam para Exchange

Suporte a Cluster Microsoft bem como as versões do MS-Exchange 2003, 2007 e 2010. No caso do MS-Exchange 2007, suportar a instalação na plataforma Windows 2008;

Deve ter o serviço clusterizado e trabalho em cluster ativo-ativo e ativo-passivo

Permitir a instalação remota a múltiplos servidores Exchange, monitorando o status de cada instalação;

Permitir possibilidade de instalação silenciosa sem intervenção do administrador;

Possuir capacidade de gerar um certificado para o servidor web, para um acesso seguro;

Permitir configurar as portas de comunicação para o gerenciamento;

Realizar a verificação em background, para não impactar na performance;

Possuir verificação em memória e multi-threaded;

Possuir ação de limpeza para os arquivos anexados;

Permitir a verificação em tempo real, manual ou agendada de grupos e bases de dados no Exchange;

A verificação no Information Store deve ser realizada nas Public e Private Stores;

Permitir o bloqueio de arquivos anexos baseado em sua extensão, tamanho, tipo real do arquivo (independente da extensão) e também dentro de arquivos compactados;

Bloqueio dos arquivos em anexos deve ser com base em política por usuário e integrado com o active directory para a criação dessas políticas;

Permitir a verificação no Internet Mail Connector (IMC);

Prover proteção para mensagens enviadas via Outlook Web Access (OWA);

Permitir a filtragem baseado no tamanho da mensagem;

Realizar a verificação contra códigos maliciosos no corpo da mensagem;

Realizar a verificação em arquivos baseado em seu tipo real, independente da extensão apresentada;

Realizar a verificação somente em arquivos passíveis de códigos maliciosos, permitindo assim um melhor desempenho da solução;

Possuir a detecção de SPAMs utilizando tecnologia heurística, podendo ser configurada a sensibilidade da ferramenta;

Deve ter approved list para recebimento de mensagens de determinados senders;

Deve ter integração com a pasta JUNK MAIL ou SPAM do Outlook de modo que os spams sejam direcionados diretamente para essa pasta;

Os usuários devem ter a capacidade de se permitido criarem suas exceções de recebimento através de white list gerenciada no próprio Outlook;

Avaliar reputação de links HTTP que estejam dentro do email quanto a sua reputação e caso reputação negativa deve ser tomada uma ação na mensagem;

Permitir criar regras de controle de conteúdo definidos por rotas, usuários e grupos;

Regra de controle de conteúdo deve procurar por conteúdo no subject, corpo e cabeçalho da mensagem;

Deve ter a possibilidade de em caso de um conteúdo malicioso, executar as seguintes ações: substituir por um texto, quarentenar a mensagem inteira, quarentenar parte da mensagem, deletar a mensagem inteira, fazer o backup/cópia da mensagem, passar parte da mensagem;

Possuir uma área de quarentena para o usuário final, integrada à ferramenta, para serem armazenados os e-mails detectados como SPAM, para que o usuário possa refinar a ferramenta;

Deve possuir área de quarentena no servidor com gerência pelo administrador através da liberação de mensagens ou deleção;

Deve possuir exceções nas políticas de bloqueio de anexo e de bloqueio de conteúdo;

No caso de violação de anexo não desejado deve possuir capacidade de executar as seguintes ações:

Substituir por um texto, quarentenar a mensagem inteira, quarentenar parte da mensagem, deletar a mensagem inteira, fazer o backup/cópia da mensagem;

Permitir a verificação contra conteúdos não autorizados dentro dos arquivos anexados nas mensagens;

Marcar as mensagens detectadas como SPAM no campo "assunto", preservando também o conteúdo original;

Permitir o gerenciamento de vários servidores Exchange simultaneamente;

Gerenciamento via console web (Internet Explorer);

Possuir controle de time-out para a console de gerenciamento;

Permitir configurar as notificações a serem enviadas para o administrador, via email e SNMP;

Realizar ações específicas para cada tipo de código malicioso;

Capacidade para, em caso de epidemia, bloquear a entrada de determinados emails, baseado nas características de códigos maliciosos, restaurando as configurações originais ao término da epidemia, ambos de forma automática através de políticas recebidas do fabricante;

Permitir um gerenciamento da quarentena, podendo enviar, encaminhar e apagar mensagens que estiverem nela;

Proteção contra spywares, sem a necessidade de um software ou agente adicional;

Deve detectar e bloquear malwares empacotados (packed malwares);

Para mensagens infectadas, deve poder tomar as seguintes ações: limpar, substituir por um texto, quarentenar a mensagem inteira, deletar a mensagem inteira, passar, quarentenar parte da mensagem;

Produto deve ter capacidade de fazer reputação dos IPs que estejam conectando no Exchange server e caso IP seja de má reputação que a mensagem seja bloqueada;

Produto deve executar rastreamento agendado ou manual nas mailboxes dos usuários;

Deve possuir acessos por papéis em sua console com diferentes perfis de acessos e diferentes acessos a menus;

Deve possuir capacidade de single sing on para acesso da console web de gerenciamento;

Deve reconhecer e ser compatível com IPV6;

Deve integrar-se com MOM/SCOM da Microsoft para envio de notificações;

Deve limitar uso de CPU em agendamento de rastreamento ou rastreamento manual;

Deve fazer filtro de conteúdo realizando o rastreamento dentro do anexo da mensagem;

Deve gerar relatórios de:

Vírus, spyware, grayware e outros malwares, com gráficos em escala horária, diária, semanal e mensal;

Principais vírus/malwares, spywares e graywares;

Principais senders de vírus/malwares, spywares e graywares;

Resumo das ações tomadas contra vírus/malwares, spywares e graywares;

Resumo do bloqueio de anexos;

Gráfico do bloqueio de anexos, com escala horária, diária, semanal e mensal;

Principais tipos de anexos bloqueados;

Principais nomes de anexos bloqueados;

Principais extenções de anexos bloqueados;

Gráfico do filtro de mensagens, com escala horária, diária, semanal e mensal;

Principais remetentes e destinatários filtrados;

Resumo de spam;

Gráfico do filtro de spams, com escala horária, diária, semanal e mensal;

Principais fontes e destinatários de spam;

Tráfego por hora, dia e mês;

Módulo de inspeção de emails entre caixas de correio e serviços online Microsoft

Aplicar proteções anti-malware, verificação de URL's maliciosas para a proteção dos serviços.

A verificação Anti-malware deverá permitir a customização das ações a serem tomadas por exemplo: quarentena, deletar e passar.

Exchange Online, SharePoint Online e OneDrive for Business da Microsoft;

Deve aplicar proteções contra Comprometimento de E-mail utilizando análise de escrita;

Realizar integração nuvem-a-nuvem, através de API da Microsoft, realizando a análise de malware em sandbox;

Monitorar em tempo real para bloquear, colocar em quarentena, ou fazer relatórios de políticas de conformidade;

Empregar detecção de malware por meio de sandbox sem assinaturas, para diminuir seu risco de violação;

Monitorar o comportamento real de arquivos suspeitos em ambientes sandbox virtuais usando múltiplas versões de sistemas operacionais e aplicações;

As políticas deverão possuir a capacidade de serem realizadas por usuário ou grupo;

Possuir um dashboard com as principais ameaças detectadas do tipo Ransomware, Phishing, Comprometimento de E-mail;

Deve ser capaz de implementar políticas com base no filtro de conteúdo das mensagens;

Deve compartilhar objetos suspeitos previamente analisados em Sandbox com gerência centralizad;.

A Sandbox deverá ter a opção para funcionar em modo monitor não tomando nenhuma ação nos arquivos detectados;

Os alertas enviados deverão permitir a customização tanto para o usuário quanto para o administrator;

Deverá possui a funcionalidade de verificação de SPAM com níveis de detecções diferentes;

As ações realizadas pelo antispam deverão possuir as seguintes opções: quarentena, adicionar uma tag no assunto, deletar ou mover para a pasta de lixo;

Deverá permitir o administrador adicionar ou bloquear um endereço na lista de remetentes;

Modulo de inspeção de entrada e saída de e-mails;

A proteção de e-mails para Office 365 deverá possuir os seguintes níveis de serviço:

Disponibilidade do serviço 100% de uptime;

Efetividade no bloqueio de SPAM 99% ou maior;

Ocorrência de Falsos-positivos não mais que 0,0003%;

Latência máxima na entrega de mensagens não mais que um minuto;

Proteção AntiSpam;

Deve ser capaz de:

Permitir a Filtragem baseada em reputação IP para no mínimo:

Remetentes permitidos com base no endereço IP;

Remetentes bloqueados com base no endereço IP;

Bloqueio de e-mails baseados em países / regiões;

Permitir a Filtragem de Remetente e Destinatários para no mínimo: Remetentes aprovados por endereço de e-mail ou domínio, Remetentes bloqueados por endereço de e-mail ou domínio;

Validar destinatário de entrada de e-mail;

Detectar spam baseado em assinatura e padrões;

Proteção anti-phishing;

Proteção anti- ransomware;

Proteção contra-ataques de Engenharia Social;

Identificar mensagens de marketing;

Análise de spam com base no contexto da mensagem;

Realizar ajustes do nível de Sensibilidade de Spam para no mínimo: O mais baixo (mais conservador), Baixo, moderadamente baixo, moderadamente alto, alto e Máximo (mais agressivo);

As opções de configuração devem ser no mínimo as seguintes:

Filtrar por nome do anexo;

Filtrar por extensão de anexo;

Filtrar por tipo de arquivo anexado (true file type);

Filtrar por tamanho de anexo;

Filtrar por número de anexos;

Filtrar por tamanho total da mensagem;

Filtrar por palavras-chave no assunto;

Filtrar por palavras-chave no corpo;

Filtrar por palavras-chave no cabeçalho;

Filtrar por tipo de arquivo dentro de arquivos zip;

Filtro de arquivos protegidos por senha;

A solução deverá ser capaz de realizar a quarentena de mensagens através de políticas implementadas para este fim, com as seguintes opções:

Quantidade de e-mails a serem exibidos no Portal de Administração de Quarentena;

Período de Retenção de Quarentena (antes de ser descartada);

Campo de Pesquisa de Quarentena;

Consulta de mensagens de quarentena usando curinga ou domínio, remetente e destinatário;

Pesquisar mensagens de quarentena por assunto;

Identificar o motivo pelo qual a mensagem foi quarentenada;

Excluir e-mail quarentemado;

Reprocessar mensagem na quarentena;

Quarentena Digest;

Modelos pré-definidos personalizáveis com de texto simples e versões HTML;

Redefinir para padrão modelos de texto sem formatação e HTML;

Suporta a adição de tokens / variáveis para acesso à quarentena;

Frequência diária com opção de enviar mais de uma vez durante o dia;

Frequência semanal;

Rastreamento de e-mail;

Deve possuir:

Campo de pesquisa de mensagem;

Controle de conteúdo de mensagens End-to-end;

Pesquisa de Mensagens usando curinga ou domínio;

Mostrar eventos de rastreamento completos das mensagens;

Mostrar desencadeamento de política;

Mostrar endereço IP do MTA do remetente e do destinatário;

Rastrear a mensagem por assunto, remetente e destinatário;

Plataforma SMTP.

Deve ser capaz de tratar:

Tamanho máximo de mensagem permitida;

Número máximo de destinatários em um e-mail;

O número máximo de camadas em um arquivo compactado;

Tamanho máximo de arquivos permitido após a descompressão;

Número máximo de arquivos permitidos em ZIP, Office;

Taxa de compressão máxima (%) de um arquivo compactado;

Restrição de conexões simultâneas;

ESMTP, 8bitmime, DSN;

Suprimir informações de MTA no cabeçalho recebido;

Autenticação Básica (SASL);

SSL / TLS para SMTP;

Proteção Antivírus e SMTP;

Deve ser capaz de:

Realizar a Detecção Anti-Malware;

Realizar a Detecção de vírus através de Assinatura;

Realizar a Detecção de vírus via heurística;

Realizar a Inspeção de malware no corpo da mensagem;

Realizar a Inspeção de malware em anexos;

Realizar a Proteção anti-spyware;

Detectar URLs maliciosas no corpo da mensagem;

Detectar malwares em arquivos compactados;

Utilizar tecnologia de detecção própria para a 'Scan Engine' (o motor de escaneamento e a solução Anti-spam devem ser do mesmo fabricante);

Ter a opção para desativar a filtragem de malware;

Permitir realizar a detecção anti-malware em e-mails de saída;

Verificar a reputação de Endereço IP do remetente;

Analisa de URLs no momento do clique e bloquear caso a URL seja maliciosa;

Possuir Analise Preditiva para ameaças desconhecidas com alto risco;

Deve suportar o padrão SPF – Sender Policy Framework - para a verificação das mensagens;

Deve suportar o padrão DKIM - Domain Keys Indentified Mail - para a verificação das mensagens;

Deve suportar o padrão DMARC - Domain Message Authentication Reporting & Conformance - para a verificação das mensagens;

Módulo de Filtro WEB

O software deve ser atualizado gratuitamente, incluindo melhorias e novas versões durante o período de vigência do contrato;

Gerenciamento via console web;

Deve possuir a certificação da VmWare para Software Appliance ou a possibilidade de instalação no formato de Bare Metal, formato no qual depende da homologação do hardware por parte do fabricante;

Virtual Appliance: Suportar VmWare ESX e ESXi 5.5 ou superior e Microsoft Hyper-v 2.0 Windows Server 2012 R2 ou superior.

A solução Virtual appliance deve fornecer junto da sua ISO de instalação um banco PostgreeSQL

Possuir verificação contra códigos maliciosos como vírus, worms, trojans, phishing, spyware e applets e activex maliciosos, sem a necessidade de um agente ou software adicional;

Toda deve ser do mesmo fabricante;

Permitir criar políticas de verificação baseado no perfil do usuário ou grupo, range ou endereço IP, permitindo uma navegação mais segura;

Permitir um controle de quota em Megabytes ou por tempo para o acesso à internet, por usuário ou grupo de usuário, por dia, semana e mês;

Permitir a utilização da ferramenta em modo Transparent Bridge, Forward Proxy, Proxy Reverso;

Possuir suporte ao protocolo ICAP e WCCP,

Utilizar os seguintes serviços de diretório: Microsoft Active Directory, Linux OpenLDAP Directory e Sun Java System Directory Server 5.2;

Permitir configurar os usuários que terão acesso à internet, baseado em seus logins, endereço IP e range IP;

Realizar a verificação somente em arquivos passíveis de códigos maliciosos, permitindo assim um melhor desempenho da solução;

Permitir a geração de relatórios, de forma manual ou agendada, com todos os eventos da ferramenta: códigos maliciosos, páginas acessadas, URL's bloqueadas, atividade por período e spywares detectados;

Atualização automática das vacinas de forma incremental e da versão do software;

Gerenciamento centralizado com a mesma console que administra o resto da solução;

Possibilidade de funcionamento e administração independente da ferramenta de gerenciamento centralizado;

Possuir um tratamento especial para Java Applets, onde esse é verificado quanto à sua assinatura e certificado, podendo tomar ações distintas para cada combinação entre elas, podendo ainda configurar que operações um Applet pode executar na máquina do usuário e como seus certificados serão validados;

A análise anti-malware da tecnologia deve ser realizada em Real Time, possibilitando uma ação imediata quando identificada uma ameaça;

O tratamento da análise de tráfego da tecnologia quando detectado um vírus deve ser de limpar, deletar ou quarentenar;

Possuir um tratamento especial para Activex, onde esse é verificado quanto à sua assinatura, e podendo tomar ações distintas para elas e como seus certificados serão validados;

Permitir configurar os certificados digitais que são seguros, colocando também os não seguros em uma lista negra;

A tecnologia deve ser capaz de identificar e bloquear conexões com redes zumbis (Botnets);

Possuir banco de dados de URL categorizados em, no mínimo, 80 categorias e tomar as seguintes ações para o acesso a estas categorias: PERMITIR, BLOQUEAR, MONITORAR, ALERTAR, TEMPO de ACESSO e ACESSO com SENHA, este banco de dados deve estar hospedado na Internet para que se tenha uma atualização mais rápida das categorias;

A tecnologia deve possuir integrado a mesma solução um Cache de páginas HTTP que visa a melhorar o desempenho da navegação;

A configuração do tamanho dos objetos que serão armazenados no cache devem passíveis de modificação pelo Administrador da tecnologia;

Possibilidade de permissão de acesso websites definidos nas categorias em períodos pré-determinados;

Possuir integração com Safe Search do Google e do Yahoo

Possuir análise de malware sobre o tráfego HTTPS;

Possibilidade de permitir customizar notificações para o usuário de acordo com a política de acesso definida:

HTTPS Access Denied;

HTTPS Certificate Failure;

HTTP/HTTPS Scanning;

HTTP/HTTPS Blocked File Type;

URL Blocking;

FTP Scanning;

FTP Blocked File Type;

IntelliTunnel (bloqueio de Instant Messaging);

Applets and ActiveX Instrumentation;

Pattern File Updates;

URL Filtering and Scan Engines Update;

Possuir recurso para permitir / bloquear no mínimo 420 aplicações diferentes e este recurso deve funcionar no mínimo em dois modos de instalação (Forward Proxy e Bridge);

Possuir recurso para permitir / bloquear conexões Peer-to-Peer (BitTorrent, Gnutella, eDonkey, ...);

Possuir recurso de Web Reputation (reputação de HTTP), integrada com a solução de antivírus, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;

Deve possuir a funcionalidade de replicar as configurações entre outros servidores de proteção do gateway HTTP através de uma tecnologia auxiliar de centralização de logs, reports e configurações;

Deve possuir capacidade de criar os seguintes perfis de acesso a console de gerência: Administrador, Auditor e Reports;

Possuir ferramenta integrada para Back-up e restore das configurações da solução;

Possuir ferramenta standalone de relatórios com as seguintes características:

A tecnologia deve contemplar a funcionalidade de Data Loss Prevention, afim, de evitar o vazamento de informações;

A solução deve contemplar templates contra vazamento de informações que atendam regulamentações de compliance;

A tecnologia deve possibilitar a criação de novos templates que visam a customização da tecnologia, afim, de proteger dados específicos;

A tecnologia deve permitir o acesso a redes sociais restringindo jogos e a possibilidade de submeter posts;

A geração dos relatórios pode ser realizada através de uma tecnologia Standalone, afim, de garantir base de dados diferentes entre reports e políticas de configurações de acesso à internet através do proxy;

Os relatórios devem permitir que a partir da sua console seja possível submeter configurações das políticas de acesso à internet entre diversas instâncias da tecnologia de WEB Gateway;

Os relatórios devem possuir no mínimo 50 tipos de relatórios pré-definidos, que tragam visibilidade de acesso: URLS mais acessadas, usuários que mais acessam a internet, acesso por categoria da web site, consumo de banda e violações de regra;

Os relatórios devem disponibilizar uma Dashboard de visualização dos acessos dos usuários ao WEB Gateway em tempo real;

A tecnologia standalone de relatórios deve permitir que geração seja agendada e submetida por e-mail;

A solução de filtro web deverá submeter arquivos suspeitos a solução de análise de ameaças avançadas locais, não sendo realizada de maneira externa ao ambiente, apresentado como resultado na alise informações;

Processos de AutoStart;

Modificações de Arquivos de Sistema;

Serviços criados e modificados;

Atividade de Rede Suspeita;

Modificações de Registros;

A análise de ameaças avançadas deverá realizar automaticamente o bloqueio em ações suspeitas nos filtros web contra a ameaça analisada em sandbox.

3.4.1.3. SOLUÇÃO DE SEGURANÇA PARA AMBIENTE VIRTUALIZADO, DATACENTER E NUVEM

Características Gerais da Solução

Deve ser compatível com pelo menos os seguintes sistemas operacionais:

Windows XP SP3 (x86/x64)

Windows Server 2003 R2 SP2 (x86/x64)

Windows Server 2008 (x86/x64)

Windows Server 2008 R2 (x64)

Windows Server 2012 (x64)

Windows Server 2012 R2 (x64)

Windows Server 2016 (x64)

Red Hat Enterprise 5 (x86/x64)

Red Hat Enterprise 6 (x86/x64)

Red Hat Enterprise 7 (x64)

CentOS 5 (x86/x64)

CentOS 6 (x86/x64)

CentOS 7 (x64)

Oracle Linux 5 (x86/x64)

Oracle Linux 6 (x86/x64)

Oracle Linux 7 (x64)

SUSE Linux Enterprise Server 11 (x86/x64)

SUSE Linux Enterprise Server 12 (x64)

Ubuntu 14.04 (x64)

Ubuntu 16.04 (x64)

Ubuntu 18.04 (x64)

Debian 7 (x64)

Debian 8 (x64)

Debian 9 (x64)

Cloud Linux 6 (x64)

Cloud Linux 7 (x64)

Cloud Linux 7.1 (x64)

Solaris 10 1/13 Sparc

Solaris 10 1/13 (x86/x64)

Solaris 11.2/ 11.3 Sparc

Solaris 11.2/ 11.3 (x86/x64)

Amazon Linux 2 (x64)

Deve ser totalmente compatível e homologada com o ambiente Vmware: VMware® vSphere: 5.5/6.0, View 4.5/5.0/5.1, ESX 5.5, 6.2.X, 6.5, NSX 6.2.X, 6.3;

Deve permitir a integração com VMware vSphere 6 e com NSX estendendo os benefícios da micro-segmentação em um datacenter definido por softwares e fazendo com que as políticas de segurança estejam atreladas às Vms onde quer que elas estejam;

Deve permitir a integração com Vmware Vrealize para o monitoramento do ambiente;

Deve permitir a integração com pelo menos as seguintes plataformas de nuvem: Vmware Vcloud, Ms Azure e AWS;

Deve ter a capacidade de controlar e gerenciar as regras de segurança de múltiplas plataformas e sistemas operacionais, incluindo máquinas em nuvens externas a partir de uma console centralizada;

Deve permitir a entrega de agentes por pelo menos duas dentre as principais ferramentas de distribuição de software do mercado: Microsoft System Center Configuration Manager, Novel Zen Works e Puppet;

Deve ser gerenciada por console Web, compatível com pelo menos os browsers Internet Explorer e Firefox. Deve ainda suportar certificado digital para gerenciamento;

A console de administração deverá permitir o envio de notificações via SMTP;

Todos os eventos e ações realizadas na console de gerenciamento precisam ser gravados para fins de auditoria;

Deve possuir a funcionalidade tags para identificar falsos positivos ou facilitar a visualização de determinados alertas;

Deve permitir a criação de widgets para facilitar a administração e visualização dos eventos;

Deve permitir que a distribuição de patterns e novos componentes possa ser efetuada por agentes de atualização espalhados pelo ambiente;

Deve detectar comportamentos anormais de, pelo menos, 10 (dez) administradores da solução: Acesso a partir de máquinas incomuns, IPs irregulares e desconhecidos, durante horários e dias irregulares, excessivos a contas privilegiadas, Usuários incomuns logando de uma máquina de origem conhecida, Suspeita de roubo de credenciais, Acesso privilegiado realizado fora da solução;

Deve possuir as sessões administrativas acessadas e monitoradas ao vivo, com compartilhamento de tela e controle de periféricos, como teclado e mouse (assistência remota), e por meio de gravação de vídeos das mesmas, em formato padrão de execução não proprietário da solução, possibilitando que os vídeos gerados possam ser indexados para pesquisa futura;

Deve permitir o filtro de comandos executados ao longo da sessão gravada, possibilitando pesquisar ações específicas no vídeo gravado;

Deve proteger contra a perda, roubo e gestão inadequada de credenciais através de regras de complexidade da senha que incluem comprimento da senha (quantidade de caracteres), frequência de troca da senha, especificação de caracteres permitidos ou proibidos na composição da senha e outras medidas;

Deve mitigar problemas de segurança relacionados ao compartilhamento indevido de credenciais privilegiadas que são armazenadas localmente em dispositivos e também para as contas que não são gerenciadas de forma centralizada por serviços de diretórios;

Deve descobrir credenciais privilegiadas referenciadas por serviços e processos automatizados. Além disso, a solução deve propagar as senhas geradas de forma aleatória onde quer que estas estejam referenciadas;

Deve gerenciar de forma segura senhas utilizadas por contas de serviço com as do item acima, evitando a utilização de senhas em texto claro por scripts ou rotinas dos equipamentos, garantindo a aplicação apenas dos privilégios adequados, provendo acesso às senhas das contas privilegiadas ao pessoal autorizado;

Deve permitir a criação de múltiplos perfis de segurança, que serão vinculados aos diferentes tipos de servidores do ambiente;

A solução precisa permitir a criação de relatórios. A criação e envio destes relatórios deverá ocorrer sob-demanda, ou agendado com o envio automático do relatório via e-mail;

Deve fornecer pelo menos dois tipos de relatórios nos seguintes formatos PDF e RTF;

A solução precisa permitir que relatórios no formato PDF, possam ser enviados com uma senha única para cada destinatário;

Deve prover relatórios contendo no mínimo as seguintes informações; malware, regras de IPS e Firewall;

A console de gerenciamento deve armazenar políticas e logs em base de dados. A escolha da base de dados pode ser facultativa entre Oracle e SQL;

A console de gerenciamento deve apresentar alta disponibilidade de modo que na ausência da principal os clientes automaticamente se comuniquem com a secundária e todas as configurações devem permanecer;

Quando operando em modo alta disponibilidade, ambos os consoles devem compartilhar a mesma database;

A console deve se integrar com o Active Directory para que os usuários do Active Directory possam administrar a solução de acordo com as permissões;

A console deve se integrar com o Active Directory para que possa ser efetuado o controle das máquinas no Active Directory;

Para efeito de administração, deve ser possível de se replicar a estrutura do Active Directory na console de administração;

A solução de segurança para data center deverá suportar Docker para proteger os containers;

Os usuários devem ter a capacidade de receber determinados papéis para administração como "acesso total" e "acesso parcial", podendo ser customizado o que compõe o "acesso parcial";

Quando configurado o acesso parcial, este deve permitir que um usuário tenha permissões de poder gerenciar a segurança de um único computador, podendo ainda definir em quais módulos de proteção será possível ou não editar ou criar novas políticas de segurança;

A comunicação entre a console de gerenciamento e os agentes deverá ser criptografada;

Cada agente deverá ter sua própria chave para criptografia de modo que a comunicação criptografada seja feita de forma diferente para cada agente;

A console de gerenciamento deverá ter dashboards para facilidade de monitoração, as quais deverão ser customizadas pelo administrador em quantidade e período de monitoração;

Os agentes de atualização deverão buscar os updates das assinaturas e distribuí-las para os agentes. Quando ocorrer a atualização, esta deverá ocorrer de modo absolutamente seguro utilizando-se SSL com o servidor de onde ela buscará as informações;

Os agentes para plataforma Microsoft deverão ser instalados por pacote MSI e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente;

Os agentes para plataforma Linux deverão ser instalados por pacote RPM ou DEB e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente;

Para efeito de administração, deve avisar quando um agente se encontrar não conectado a sua console de gerenciamento;

A solução deve possuir a capacidade de criar políticas de forma global para todas as máquinas, por perfis e individualmente para cada host;

Cada perfil poderá ser atribuído para um host ou um conjunto de hosts;

Deve vir com perfis default pré-definidos e aptos a funcionarem de acordo com sua denominação;

Deverá possuir uma hierarquia de prevalecimento de configurações, seguindo no mínimo a ordem: Global -> Perfis -> hosts;

Deve mostrar quais máquinas estão usando determinada política;

Os agentes deverão ser capazes de executar rastreamento nas máquinas onde estão instalados e após isso deverão fornecer uma lista de todas as recomendações de segurança para os softwares que estejam instalados nas máquinas bem como do sistema operacional;

Esses rastreamentos devem ocorrer de forma periódica a ser definida pelo administrador;

Brechas de segurança descobertas deverão ser protegidas de forma automática e transparente, interrompendo somente o tráfego de rede malicioso;

O administrador do sistema de segurança deverá ter a possibilidade de não aplicar automaticamente a proteção para as vulnerabilidades escolhendo o perfil ou o host;

Também deverá ser possível realizar o rastreamento por portas abertas, identificando possíveis serviços ativos e escutando;

A solução deve possuir a capacidade de isolamento de placa de rede de forma que apenas uma fique funcionando de acordo com preferência do administrador;

Deve ser capaz de aplicar políticas diferentes para placas de redes diferentes em um mesmo servidor;

Deve ser capaz de executar bypass completo de rastreamento de tráfego de forma que os módulos não atuem em determinado tipo de conexão ou pacote;

Deve ter a capacidade de se integrar com os principais softwares de SIEMs, no mínimo com: IBMQradar, HPArcSight, RSA Envision e NetIQ de modo a permitir enviar os seus logs para essas soluções;

Deve ter a possibilidade de enviar logs para SYSLOG servers;

Deve ter a possibilidade de enviar eventos da console via SNMP;

Solução deverá permitir criar relatórios customizados de todas as suas funcionalidades;

Deve permitir exportar relatórios para no mínimo os formatos PDF e RTF;

Deve permitir enviar os relatórios para uma lista de contatos independente de login na console de administração;

A lista de contatos de recebimento de relatório poderá ser obtida através do Active Directory;

As atualizações de assinaturas deverão ocorrer de forma agendada e automática possibilitando ser até mesmo de hora em hora;

Após a atualização deve ser informado o que foi modificado ou adicionado;

Deve ser possível baixar as assinaturas na console de gerenciamento, mas não as distribuir aos clientes;

A console de gerenciamento deve apresentar a capacidade de gerar roll back de suas atualizações de regras;

Deve ter capacidade de gerar pacote de auto diagnóstico de modo a coletar arquivos relevantes para envio ao suporte do produto;

Deverá ter a capacidade de colocar etiquetas para a ocorrência de determinados eventos de modo a facilitar o gerenciamento, relatórios e visualização;

No gerenciamento de licenças, deve ser informada quantidade contratada e quantidade em utilização de clientes;

Solução deverá ter mecanismo de procura em sua console de gerenciamento de modo que seja facilitada a busca de regras;

Deverá possuir a capacidade de classificar eventos para que facilite a identificação e a visualização de eventos críticos em servidores críticos;

Possibilidade de customizar a escolha do serviço de Whois para a identificação dos IPs que estejam realizando ataques;

Deverá possibilitar colocar etiquetas em eventos para que se possam visualizar apenas os eventos desejados;

A solução deve possuir ao menos um participante no programa "Microsoft Application Protection Program" para obtenção de informações de modo a permitir a criação de regras de proteção antes mesmo dos patches serem publicados pelo fabricante;

A console de gerenciamento deve se integrar com o Vmware vCenter 4.0 ou Superior, de modo a importar e sincronizar os objetos (hosts vmware e guests vm) para a console de gerenciamento da solução;

A partir desta integração, deverá ser possível gerir a segurança dos guests vm, podendo ser atribuídos perfis de segurança, regras únicas para cada host, além de possibilitar a coleta dos logs gerados para cada módulo habilitado;

Esta integração deve possibilitar que, a partir da instalação e integração de um virtual appliance do fabricante da solução de segurança com o ambiente Vmware e suas APIs, seja possível proteger as guests VMs sem a necessidade de instalação de agentes de segurança do fabricante da solução nas guests VMs.

Este virtual appliance deverá permitir integração com as seguintes APIs VMware: Vmsafe API e vShield Endpoint API, possibilitando que funcionalidades de Firewall, Proteção de Aplicações Web, Antimalware, Controle de Acesso a Sites Maliciosos, Monitoramento de Integridade de Arquivos, Controle de Aplicações e IDS/IPS, possam ser efetuados diretamente via hypervisor e virtual appliance em conjunto, não necessitando a instalação de agentes adicionais de segurança do fabricante nos guests VMs protegidos;

Deve ser capaz de implementar as funcionalidades de Antimalware, Controle de Acesso a Sites Maliciosos, Firewall, IDS/IPS, Controle de Aplicações, Proteção de aplicações Web, Inspeção de Logs e Monitoramento de Integridade nos sistemas operacionais Windows através de um único agente;

Deve ser capaz de implementar as funcionalidades de Antimalware, Firewall, IDS/IPS, Controle de Aplicações, Proteção de aplicações Web, Inspeção de Logs e Monitoramento de Integridade nos sistemas operacionais Linux através de um único agente;

Deve ser capaz de implementar as funcionalidades de Firewall, IDS/IPS, Controle de Aplicações, Proteção de aplicações Web, Inspeção de Logs e Monitoramento de Integridade nos sistemas operacionais Solaris através de um único agente;

Deve ser capaz de implementar as funcionalidades de Inspeção de Logs e Monitoramento de Integridade nos sistemas operacionais HP-UX e AIX através de um único agente;

Precisa ter a capacidade de detectar e aplicar as regras necessárias dos módulos de IDS/IPS, Monitoramento de Integridade e Inspeção de Logs, para cada servidor, de forma automática e sem a intervenção do administrador;

Precisa ter a capacidade de desabilitar as regras não mais necessárias dos módulos de IDS/IPS, Monitoramento de Integridade e Inspeção de Logs, para cada servidor, de forma automática e sem a intervenção do administrador;

Deve ser possuir no mínimo as seguintes certificações de validação e/ou compatibilidade com padrões de mercado:

Certified Red Hat Ready

Cisco UCS validated

Common Criteria EAL 4+

EMC VSPE X validated

NetApp FlexPod validated

VCE Vblock validated

Antimalware

A solução deve permitir a proteção contra códigos maliciosos através da instalação de agentes, permitindo rastrear ameaças em tempo real, varredura sob demanda e conforme agendamento, possibilitando a tomada de ações distintas para cada tipo de ameaça;

A solução deve possibilitar a criação de listas de exclusão, para que o processo do antivírus não execute a varredura de determinados diretórios ou arquivos do SO;

A solução deve possibilitar a verificação de ameaças dentro de arquivos compactados, efetuando a limpeza apenas de arquivos maliciosos em casos de detecção;

A mesma solução deve ter a capacidade de realizar o rastreamento de códigos maliciosos em tempo real, por demanda e agendado em ambiente VMware sem a necessidade de agentes nas máquinas virtuais.

Deve ter a capacidade de impedir a gravação de malwares realtime em ambiente VMware 4.1 ou superior com Vshield Endpoint sem ter agente instalado nos guests Vms.

A solução deve permitir proteção de antimalware em ambientes Linux (Ubuntu,CentOS, Red Hat e SuSe) utilizando agentes.

Deve permitir a proteção de antimalware em ambientes Windows com e sem agentes.

Deve possuir a funcionalidade de Monitoramento de Comportamento para detectar mudanças e atividades suspeitas não autorizadas.

Deve oferecer scanear processos em memória em busca de Malware.

O scan de arquivos comprimidos deverá ser de no mínimo 6 camadas de compressão;

O scan de arquivos comprimidos do tipo OLE deverá ser de no minimo 20 camadas de compressão;

Deve possuir ações pré-configuradas para cada tipo de ameaça detectada ou tomar uma ação baseada na configuração padrão da ferramenta.

Deve mostrar informação de data sobre o último scan agendado ou manual executado.

Possuir a capacidade de efetuar backup e restore de arquivos comprometidos por Ransomware.

Web Reputation

Deve permitir a proteção contra acesso a websites ou url consideradas maliciosas ou de baixa reputação;

A lista de URLs deve ser fornecida e atualizada automaticamente pelo fabricante, permitindo a consulta em uma base local ou na nuvem da reputação das URLs acessadas;

Deve permitir a criação de listas de exclusão, permitindo que usuários acessem determinadas URLs especificadas pelo administrador do sistema;

A proteção deve suportar implementação sem a necessidade de instalação de agentes de segurança do fabricante da solução de segurança, através de integração com tecnologia VMware;

A proteção deve possibilitar proteção através da instalação de agente de segurança do fabricante da solução de segurança;

Em ambientes Linux deverá realizar a proteção de Web Reputation sem agentes.

Em ambiente Windows à solução de Web Reputation deverá prover proteção com e sem agentes.

Firewall

Operar como firewall de host, através da instalação de agente nos servidores protegidos;

Precisa ter a capacidade de controlar o tráfego baseado no Endereço MAC, Frame types, Tipos de Protocolos, Endereços IP e intervalo de portas;

Precisa ter a capacidade de controlar conexões TCP baseado nas Flags TCP;

Precisa ter a capacidade de definir regras distintas para interfaces de rede distintas;

Deve ser capaz de reconhecer e possibilitar o bloqueio endereços IP que estejam realizando Network Scan, Port Scan, TCP Null Scan, TCP FYNSYN Scan, TCP Xmas Scan e Computer OS FIngerprint por até 30 minutos.

Precisa ter a capacidade de implementação de regras em determinados horários que podem ser customizados pelo administrador;

Precisa ter a capacidade de definição de regras para contextos específicos;

Precisa ter a capacidade de realização de varredura de portas nos servidores;

Para facilitar a criação e administração de regras de firewall, as mesmas poderão se apoiar em objetos que podem ser lista de ips, lista de MACs, lista de portas;

Regras de firewall poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo, se está no domínio ou não);

Regras de firewall poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana;

O firewall deverá ser stateful bidirecional;

O firewall deverá permitir liberar ou apenas logar eventos;

O firewall deverá ser passível de criação de regras através do protocolo, origem do tráfego, frame type, TCP header flags, destino e direção;

As regras de Firewall deverão ter as seguintes ações, ou equivalentes: Allow, log only, bypass, force allow, deny;

A solução, para facilidade de administração, deverá utilizar o conceito de regras implícitas para a regra ALLOW, negando o tráfego para todo o restante que não estiver liberado;

As ações também deverão ser possíveis de terem prioridades diferentes, sendo que a prioridade maior prevalece sobre a prioridade menor;

Deverá realizar pseudo stateful em tráfego UDP;

Deverá logar a atividade stateful;

Deverá permitir limitar o número de conexões entrantes e o número de conexões de saída de um determinado computador;

Deverá permitir limitar o número de meias conexões vindas de um computador;

Deverá prevenir ack storm;

Deverão existir regras default que possam ser utilizadas como modelo para a criação e adição de novas regras;

Poderá atuar no modo em linha para proteção contra-ataques ou modo escuta para monitoração e alertas;

Inspeção de Pacotes

Precisa ter a capacidade de detectar e bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do SO e demais aplicações;

Precisa ter a capacidade de varrer o servidor protegido detectando o tipo e versão do SO, detectando também as demais aplicações, recomendando e aplicando automaticamente regras IDS/IPS que blindem vulnerabilidades existentes no SO e aplicações. Esta varredura deverá poder ser executada sob demanda ou agendada;

Deve conter regras pré-definidas para detecções de ransonware para as principais famílias deste tipo de malware;

Precisa ter a capacidade de detectar uma conexão maliciosa, com a possibilidade de bloquear esta conexão. A opção de detecção e bloqueio deverá possibilitar ser implementada de forma global (todas as regras) e apenas para uma regra ou grupos de regras;

Precisa conter regras de defesa para blindagem de vulnerabilidades e ataques que explorem os seguintes sistemas operacionais: Windows 2003, 2008, 2012, 2016, Linux Red Hat, Suse, CentOS, Ubuntu, Debian, Solaris além de regras para aplicações padrão de mercado, incluindo Microsoft IIS, SQL Server, Microsoft Exchange, Oracle Database, Adobe Acrobat, Mozilla Firefox, Microsoft Internet Explorer, Google Chrome e Web Server Apache.

Precisa ter a capacidade de armazenamento do pacote capturado quando detectado um ataque;

Deverá possibilitar a criação de regras de IPS customizadas, para proteger aplicações desenvolvidas pelo cliente;

Precisa possuir a capacidade de detectar e controlar conexões de aplicações específicas incluindo Team Viewer, programas P2P e instant Messaging;

Precisa ter a capacidade de detectar e bloquear ataques em aplicações Web tais como SQL Injection e Cross Site Scripting. Deverá ainda existir a possibilidade de captura do pacote relacionado ao ataque para fins de investigação do incidente;

Deverá permitir customização avançada e criação de novas regras de proteção de aplicações web, protegendo contra vulnerabilidades específicas de sistemas web legados e/ou proprietários;

Ser capaz de permitir ou negar que métodos utilizados por Webservers por regras de IPS;

Regras de IDS/IPS poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo se está no domínio ou não);

Regras de IDS/IPS poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana;

Deverá ser capaz de inspecionar tráfego incoming SSL;

Deverá inspecionar tráfego de aplicações Web em servidores buscando identificar: Sql injection, Crossite script, tamanho de URI fora de padrão, caracteres fora de padrão para requisição de URI, Double Decoding Exploit;

As regras de blindagem contra vulnerabilidades deverão conter links com referências externas, isto quando aplicável, explicando a vulnerabilidade do fabricante ou CVE relacionado;

Deverá possibilitar a criação de regras manuais para o bloqueio de tráfego customizado. Como por exemplo, bloquear acesso a um determinado website ou bloquear acesso de uma aplicação X;

Deverá possibilitar a criação de regras manuais baseadas em padrão XML, forma de assinatura ou padrões que possuam começo e fim coincidentes;

Deverá bloquear tráfego por aplicação independente da porta que a aplicação utilize, de modo que a aplicação não consiga comunicar na rede, como por exemplo, bloqueio de tráfego de uma determinada web browser ou aplicação de backup;

Solução deve ser capaz de habilitar modo debug na coleta dos pacotes de forma a capturar o tráfego anterior e posterior ao que foi bloqueado para facilidade de análise;

As regras de IPS deverão obrigatoriamente ter descrições de seu propósito;

As regras de IPS poderão atuar detectando ou bloqueando os eventos que as violem de modo que o administrador possa optar por qual ação tomar;

As regras de IPS de vulnerabilidade deverão apresentar severidade baseada em CVES;

As regras de IPS poderão ter sua capacidade de LOG desabilitado;

As regras de IPS quando disparadas poderão ter a possibilidade de emitir um alerta;

As regras devem ser atualizadas automaticamente pelo fabricante;

Poderá atuar no modo em linha para proteção contra-ataques ou modo escuta para monitoração e alertas;

Monitoramento de Integridade

Deve permitir a implantação nas plataformas Linux, Microsoft, Solaris, HP-UX, AIX, através da instalação de agentes;

Em plataformas Microsoft, deve permitir o monitoramento de integridade de arquivos sem a necessidade de instalação de agentes adicionais do fabricante na máquina virtual a ser monitorada;

Precisa ter a capacidade de detectar mudanças de integridade em arquivos e diretórios do SO e aplicações terceiras;

Deve fazer uso da tecnologia Intel TPM/TXT para monitorar a integridade contra mudanças não autorizadas a nível do Hypervisor;

Precisa ser capaz de detectar mudanças no estado de portas em sistemas operacionais Linux;

Precisa ter a capacidade de monitorar o status de serviços e processos do sistema operacional;

Precisa ter a capacidade de monitorar mudanças efetuadas no registro do Windows;

Precisa ter a capacidade de criação de regras de monitoramento em chaves de registro, diretórios e subdiretórios e customização de XML para criação de regras avançadas;

Precisa ter a capacidade de varrer o sistema operacional e aplicações, recomendando e aplicando automaticamente regras de monitoramento de

acordo com o resultado desta varredura. Esta varredura deverá poder ser executada sob demanda ou agendada;

O monitoramento poderá ser realizado em Real-time ou utilizando de scans periódicos para detectar mudanças de integridade;

Deverá alertar toda vez que uma modificação ocorrer em real time para ambiente Windows e pseudo real time para ambiente Linux, quando utilizamos agente.

Deverá logar e colocar em relatório todas as modificações que ocorram;

As regras de monitoramento de integridade deverão ser atualizadas pelo fabricante ou melhoradas de forma automática;

Deverá poder classificar as regras de acordo com severidade para melhor verificação nos logs e recebimento de alertas;

Deverá possibilitar escolher o diretório onde o arquivo será monitorado e incluir ou não incluir determinados tipos de arquivos dentro desse mesmo diretório;

Algumas regras podem ser modificadas pelo administrador para adequação ao seu ambiente;

Inspeção de Logs

Deve permitir sua implantação nas plataformas Linux, Microsoft, Solaris, HP-UX, AIX;

Precisa ter a capacidade de monitorar e inspecionar arquivos de log do sistema operacional e demais aplicações, gravando uma cópia deste log em um banco de dados externo e notificando o administrador sobre eventos suspeitos;

Precisa ter a capacidade de varrer o sistema operacional e aplicações, recomendando e aplicando automaticamente regras de inspeção de logs de acordo com o resultado desta varredura. Esta varredura deverá poder ser executada sob demanda ou agendada;

Precisa permitir a criação de regras de inspeção de logs adicionais para auditoria de logs de aplicações terceiras;

Precisa permitir a customização de regras existentes, adicionando, removendo ou modificando regras de inspeção de logs;

Deverá rastrear e indicar/sugerir ao administrador do sistema quais softwares estão instalados e que possuem logs passíveis de inspeção;

Deverá possibilitar a criação de regras de inspeção de logs para aplicações customizadas;

Deverá ter inteligência para que a cada violação relevante no log inspecionado que possa comprometer a segurança do ambiente ou do servidor seja alertada;

Deverá ter inteligência para que a cada violação relevante no log inspecionado que seja suspeita no servidor seja alertada;

Deverá logar cada violação e colocar em relatório todas as violações relevantes que ocorram;

As regras poderão ser modificadas por severidade de ocorrência de eventos;

As regras devem se atualizar automaticamente pelo fabricante;

Permitir modificação pelo administrador em regras para adequação ao ambiente;

Controle de Aplicações

Deve permitir sua implantação nas plataformas Linux e Microsoft Windows;

O controle de aplicações deverá ser realizado através de Hash, suportando no mínimo MD5, SHA1 e SHA256

O agrupamento dos eventos deverá ser realizado pelo menos por Hash ou por máquina;

A console deverá exibir eventos de no mínimo 30 dias;

Deve possuir um mecanismo ao qual permita a execução de aplicações e scripts automaticamente, sem intervenção manual, por um determinado período de tempo que deve ser no máximo 10 horas;

Deve possuir no mínimo as funcionalidades de bloquear o que não for permitido explicitamente e permitir o que não for bloqueado explicitamente;

3.4.1.4. SOLUÇÃO DE PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS

Deverá fornecer solução integrada de proteção contra ameaças avançadas de acordo com funcionalidades e características técnicas especificadas neste documento, contendo, no mínimo os seguintes módulos:

Monitoramento, Identificação, análise e Resposta de Incidentes de Segurança

Detecção de ataques direcionados;

Analisador virtual de ameaças;

Correlação de regras para detecção de conteúdo malicioso;

Análise de todos os estágios de uma sequência de ataques;

Características Gerais da Solução

Esta solução deve ser atendida através do fornecimento de solução de um único Fabricante, contendo:

Serviço de Monitoração e Análise de Ameaças Digitais em rede;

Serviço de Monitoração e gestão de riscos que permita a identificação de ameaças digitais conhecidas e não conhecidas por soluções de antivírus tradicionais, permitindo a composição de serviços de mitigação complementares para a segurança do ambiente;

Serviço que entenda ameaça digital como a representação de um software malicioso ou ação maliciosa tal como: spyware, phishing, worms, bot, trojan, adware, network Exploit, web Exploit, Cross-site scripting, spear phishing, information stealing malware e outras ações que podem compor ataques ao patrimônio computacional do ambiente;

Visibilidade e relatório de incidentes de conexões da rede interna com sites maliciosos ou servidores de central de comando (C&C) externos;

Análise e correlação de atividades maliciosas tais como:

Detecção específica de malwares conhecidos e arquivos contaminados através de assinaturas de antivírus tradicional no tráfego da rede;

Detecção de vermes de rede e de e-mail no tráfego de rede;

Detecção de programas de exploração de vulnerabilidades (Exploits) na rede;

Detecção de empacotamentos maliciosos no tráfego da rede;

Validação de tráfego web malicioso através de consultas a sistemas de reputação na Internet;

Visibilidade e relatório de estatísticas de ameaças, fontes de infecção na rede monitorada e máquinas comprometidas;

Permitir a rápida identificação da criticidade dos eventos de segurança;

Permitir realizar pesquisas avançadas e customizadas dos incidentes de segurança através da console de gerenciamento;

Possibilidade de criação de filtros para visualização de eventos específicos conforme contexto, localização e outras variáveis que permitam investigação profunda sobre causa raiz de incidentes de segurança;

Permitir a customização de alertas em base ao tipo de incidente de segurança através da console de gerenciamento;

Permitir a integração com sistemas de serviço de diretório;

Capacidade de verificar em tempo real a reputação de endereços web (URL's) e servidores de correio SMTP;

A análise de SMTP será realizada em uma solução separada do sensor de HTTP e demais protocolos;

A análise em SMTP será realizando de modo MTA (Inline);

A análise de e-mail em sandbox deverá ocorrer em arquivos Microsoft Office, PDF, arquivos compactados e executáveis do tipo PE;

A análise em sandbox será realizada na própria solução, não sendo necessário integrações com demais soluções ofertadas;

Deve possuir mecanismo de deriva senhas de arquivos protegidos, para análise em sandbox;

Deve possuir mecanismo de conhecimento de senhas de pelo menos 90 palavras chaves em seu vocabulário de conhecimento, para derivação de arquivos protegidos;

Capacidade de criar e salvar investigações customizadas dos incidentes de segurança;

Deve possuir pelo menos 1 sensor para "escutar" o tráfego de rede de throughput de 1GB/s de análise;

Deve possuir a capacidade de detectar ameaças direcionadas, ataques do dia zero e documentos que viabilizem ataques;

Deve detectar atividades maliciosas que trafegam na rede através de motor de análise de comportamento de tráfego até o nível 7 (camada de aplicação) em protocolo TCP/IP;

Capacidade de detectar ameaças web tais como vulnerabilidades e download de conteúdo malicioso;

Os módulos de captura de rede deverão suportar a coleta de arquivos pelo menos nos protocolos HTTP e HTTPS;

Deve possuir a habilidade de detectar e analisar os seguintes protocolos e aplicativos: P2P, SMTP, POP3, IRC, DNS, HTTP, FTP, TFTP, SMB, MSN, AIM, YMSG, Yahoo Mail, Hotmail, RDP, DHCP, TELNET, File Transfer, VNC, Cisco-TELNET, Kerberos, DCE-RPC, SQL, HTTPS, SMB2, MMS, IMAP4, RTSP/RTP-UDP, RTSP/RTP-TCP, RTSP/RDT-UDP, RTSP/RDT-TCP, WMSP, SHOUTCast, RTMP, Bittorent, Kazaa, Blubster, eDonkeyeMule, Gnucleus LAN, Gnutella/Limewire/Bearshare/Shareaza, Winny, WinMX, MLDonkey, DirectConnect, SoulSeek, OpenNap, Kuro, iMesh, Skype, Google Talk, Zultrax, Foxy, eDonkey, Ares, Miranda, Kceasy, MoodAmp, Deepnet Explorer, FreeWire, Gimme, GnucDNA GWebCache, Jubster, MyNapster, Nova GWebCache, Swapper GWebCache, Xnap, Xolox, Ppstream, AIM Express, Chikka SMS Messenger, eBuddy, ICQ2Go, ILoveIM Web Messenger, IMUnitive, mabber, meebo, Yahoo Web Messenger, GPass, IP, ARP, TCP, UDP e IGMP.

Deve possuir capacidade de disponibilizar facilmente as amostras dos arquivos suspeitos detectados e do arquivo PCAP do contexto de captura;

Capacidade de oferecer informações para análise forense de artefatos suspeitos de serem maliciosos;

Gerenciamento centralizado de todas as etapas dos eventos de segurança identificados como possíveis ameaças;

Capacidade de identificar artefatos maliciosos direcionados para dispositivos moveis rodando o sistema operacional Android, tais como telefones inteligentes e tablets;

Deve analisar em tempo real o comportamento através de simulação de execução de arquivos provenientes do tráfego de rede incluindo arquivos PDF´s, executáveis, PPT, DOC, XLS, ZIP e RAR;

A solução deve detectar ameaças do dia zero, vulnerabilidade, URL's maliciosas e spams dirigidos no protocolo SMTP;

Deve possuir tecnologia de análise de arquivos binários através de simulação e avaliação de execução dos artefatos suspeitos para identificação de comportamento malicioso, com capacidade de operar vários ambientes simultâneos e integrados a solução para processamento de alto desempenho;

Deve permitir o uso de base de conhecimento na Internet do próprio fabricante para correlacionamento de informações sobre ameaças conhecidas e prover recomendações de ações;

Deve permitir o uso de portas espelhadas de switch (mirror port) para monitorar o tráfego e detectar potenciais riscos à Segurança;

Deverá permitir o rastreio por malwares utilizando métodos de detecção baseados no tipo de arquivo (True File Type), múltiplas camadas de empacotamento (Multi-packed/Multi-layered files) e arquivos comprimidos (compactados);

Deverá analisar arquivos maliciosos na rede utilizando vacinas e técnicas de heurística;

Deve possuir foco em proteção contra APTs (Advanced Persistent Threats);

Deve possuir tecnologia de proteção contra ameaças desconhecidas (ataques dirigidos e ameaças de dia zero), sendo que este módulo deve pertencer ao mesmo fabricante;

Deverá possuir suporte para monitorar múltiplas interfaces de rede conectadas a diferentes VLANs ou Switches;

Deverá possuir suporte para balanceamento de carga no sensor de inspeção de tráfego, possibilitando assim obter uma melhor performance;

Deverá permitir a análise específica de eventos de segurança de computadores suspeitos de atividade maliciosa;

Os módulos que compõem a solução devem atuar de forma integrada, centralizando logs de incidentes em ponto único;

Deve possuir atualização automática de regras e assinaturas, sendo que estas devem ser disponibilizadas via web pelo fabricante da solução;

Deve possuir mecanismo de consultas automáticas em bases de reputação externas de propriedade do fabricante da solução;

Deve ser capaz de identificar movimentos laterais em uma rede corporativa;

Deve atuar de forma passiva na captura de tráfego sem oferecer impacto no desempenho da rede;

Deve possuir interface web para busca e investigação local de incidentes;

Deve possuir capacidade de envio de artefatos para analisador virtual dedicado, externo, sendo que este deverá suportar no mínimo os sistemas operacionais Windows XP e Windows 7;

Deve possuir possibilidade de habilitação e desabilitação de regras de inspeção, individualmente, através de interface de gerenciamento web;

Deve possuir capacidade de análise virtual de artefatos internamente;

Deve possuir regras que identifiquem comunicações dos seguintes tipos: C&C, Exploits, Executáveis Maliciosos, Comunicação com Sites Maliciosos, backdoors e Botnets;

Deve possuir regras que identifiquem comunicações de estações de trabalho e servidores com serviços não autorizados, tais como: consultas DNS em servidor não autorizado, utilização de SMTP server não autorizado, Proxy Server não autorizado;

Deve possuir regras que identifiquem comunicações p2p, instant messengers e streaming;

Deve possuir capacidade de geração de relatórios dos seguintes tipos e contendo as seguintes características:

Resumidos;

Visão Geral dos Incidentes de Segurança

Discriminação dos Tipos de Incidentes

Top Ameaças Analisadas

Top Hosts Infectados

Recomendações de Segurança

Executivos;

Deve possuir detalhes técnicos dos incidentes detectados;

Deve possuir estatística do tráfego analisado;

Deve possuir indicadores de risco do ambiente;

Recomendações de Segurança;

Deve ser capaz de identificar, filtrar e exibir em interface gráfica, e dinamicamente atualizada, hosts com alto nível de risco, classificando os tipos de riscos/eventos detectados;

Deve possuir interface que apresente em Real Time estatísticas de top ameaças detectadas, top arquivos analisados, top hosts afetados, top URL's maliciosas acessadas, etc.;

Quando detectada uma ameaça, a solução deve prover, podendo esta realizar consultas em site do fabricante, informações sobre ameaça, família da ameaça, estatísticas de segmentos de mercado afetados e recomendações de segurança para eliminar ameaça, correlacionando estas informações com sites ou outros vetores por onde esta ameaça é disseminada;

As atualizações do produto (patterns e outros componentes) não devem causar downtime ou impacto na operação;

Deve possibilitar customização de Sandbox, permitindo ao cliente simular seu padrão de imagens e sistemas operacionais no módulo de análise virtual;

Deve ser capaz de identificar ameaças que afetam dispositivos móveis (Ex. Detecção de comunicação de aplicativo malicioso na plataforma Android);

Deve ser capaz de detectar tentativas de mascaramento ou evasão de detecção através do uso de portas comuns ou protocol tunneling;

Deve ser capaz de detectar tentativas de scan de rede;

Deve ser capaz de detectar propagação de malwares na rede;

Deve ser capaz de detectar tentativas de brute-force;

Deve ser capaz de detectar tentativas de fuga e roubo de informação;

Deve ser capaz de detectar ameaças que se replicam na rede;

Deve ser capaz de detectar Exploits na rede;

O Monitoramento de protocolos de comunicação deve ser feito através de appliance único (ou virtual appliance);

A console de gerenciamento deve possuir mapa mundial, onde são marcadas origens de ataques e eventos de segurança monitorados pela solução;

Deve permitir busca por informações do destino e origem, incluindo estas: endereço IP, endereço MAC, porta e protocolo.

Deve permitir consultas personalizáveis, usando comandos SQL ou atributos pré-definidos;

Capacidade de salvar uma investigação antes de ser finalizada.

Capacidade de restaurar uma investigação para continuá-la ou consultá-la.

Capacidade de emitir relatórios baseados nas investigações;

Deve permitir apresentação dos dados consultados em vários formatos, incluindo tabela e gráficos;

Deve trabalhar com geo-localização para identificar a origem geográfica de um ataque;

Deve ter a capacidade de sugerir termos de busca, de acordo com o conteúdo já buscado numa investigação, para agilizar a obtenção do resultado;

Deve permitir exportar sob demanda os logs em texto puro (CSV ou similar);

Deve sugerir consultas a bases de reputação e whois quando encontrados hosts e nomes de domínio;

Deve permitir investigação por tags (palavras-chave) pré-configuradas para facilitar a busca de eventos;

Deve permitir recebimento de logs via syslog;

Deve permitir encaminhamento de logs via syslog;

Deve permitir receber logs de diferentes dispositivos;

Deve possuir engine de correlação de eventos;

Deve inserir tags personalizadas nos logs, de acordo com regras especificadas pelo usuário;

Deve enviar alertas via e-mail para pelo menos 100 e-mails diferentes;

Deve permitir a configuração de alarmes personalizados, com base em investigações;

Deve informar em sua console alarmes que dispararam, até que o usuário tome alguma ação;

Características do Módulo de Análise Virtual;

Deve suportar análise de documentos do Microsoft Office (DOC, DOCX, XLS, XLSX, PPT, PPTX);

Deve suportar análise de documentos em PDF;

Deve submeter um documento PDF a pelo menos duas versões do Adobe Reader;

Deve analisar dinamicamente arquivos compactados (ZIP, BZIP2, RAR);

Deve analisar dinamicamente binários PE de 32-bits;

Deve analisar dinamicamente binários PE de 64-bits;

Deve permitir criação de sandbox personalizada pelo usuário;

Deve permitir criação de sandbox local utilizando Windows XP 32-bits em inglês e português;

Deve permitir criação de sandbox local utilizando Windows 7 em inglês e português;

Deve permitir criação de sandbox local utilizando Windows 8 em inglês e português;

Deve permitir criação de sandbox local utilizando Windows 8.1 em inglês e português;

Deve permitir criação de sandbox local utilizando Windows 10 em inglês e português;

Deve permitir criação de sandbox local utilizando Windows 2003/2003 R2 em inglês e português;

Deve permitir criação de sandbox local utilizando Windows 2008/2008 R2 em inglês e português;

Deve permitir criação de sandbox local utilizando Windows 2012/2012 R2 em inglês e português;

Deve permitir criação de sandbox local utilizando Windows 2016 em inglês e português;

Deve analisar dinamicamente bibliotecas dinâmicas (DLL);

Deve analisar dinamicamente binários BHO;

Deve poder funcionar em ambiente totalmente virtualizado;

Deve possuir tecnologia própria de análise de artefatos em sandboxing;

Deve prover possibilidade de isolamento total da rede de sandbox da rede de gerência;

Deve prover possibilidade de uso da rede dedicada para a internet na análise de sandbox;

Deve analisar dinamicamente arquivos do Adobe Flash (SWF);

Deve realizar a análise localmente podendo ter consultas externas para reputação de IP e URL, mas sem envio da amostra;

Deve ter a capacidade de gerar relatórios com eventos realizados pela amostra no sistema alvo, ao nível de API, exibindo as funções com argumentos e retornos de execução;

Deve analisar dinamicamente rootkits;

Caso uma ameaça baixe outra enquanto na sandbox, essa também deverá ser analisada num evento correlacionado;

Deve submeter uma amostra a sistemas operacionais diferentes, a fim de detectar ações específicas para um sistema;

Capacidade de integração via API com soluções terceiras;

O Fabricante deverá disponibilizar acesso a base de dados externa que possibilite a correlação entre informações geradas no ambiente com informações de outros clientes que foram afetados pelo mesmo padrão ou tipo de ameaça. Este acesso deverá ser web, e deverá possuir referências e atalhos nos próprios relatórios e logs locais da solução;

Características da Console de Gerenciamento da Solução de Proteção Contra Ameaças Avançadas;

A console de gerenciamento deverá ser web, apresentando alta disponibilidade de modo que na ausência da principal, o restante da solução permaneça ativa e funcionando;

A solução deve ser escalável horizontalmente, permitindo que novas instâncias sejam habilitadas, aumentando suas capacidades de detecção e análise;

A console de gerenciamento deverá ter dashboards para facilidade de monitoração. As janelas deverão ser customizadas pelo administrador em quantidade e período de monitoração;

O administrador deve poder optar por janelas de monitoramento no dashboard a sua disposição e poderá livremente adicionar ou remover de acordo com sua necessidade de visualização;

Deverá possuir mapa geográfico que permita a identificação visual sobre a origem de ameaças de modo a facilitar a visualização de eventos críticos para que ações imediatas sejam providenciadas;

Deverá possuir a capacidade de atualizar as vacinas, engines, assinaturas e recursos de inspeção de conteúdo de forma agendada e automática;

A console de gerenciamento deverá ser gerenciada por Internet Explorer e Firefox;

Solução deverá ter mecanismo de busca em sua console de gerenciamento de modo que seja facilitada a busca por detecções;

Deverá ser capaz de identificar ameaças evasivas em tempo real com o provimento de análise profunda e inteligência para identificar e prevenir ataques;

Deverá possuir capacidade de identificar a origem de ataques direcionados, incluindo a análise de artefatos por meio de analisador virtual com a capacidade de gerar no mínimo 24 máquinas virtuais de análise;

Deverá ser capaz de correlacionar regras de detecção de conteúdo malicioso durante todas as fases de um ataque;

Deve permitir a adição e remoção dos diversos recursos de visualização de informações na tela principal de monitoramento da ferramenta, permitindo no mínimo a visualização das seguintes informações:

Uso de CPU;

Uso de Disco;

Uso de Memória;

Tráfego malicioso analisado;

Todo o tráfego analisado;

Logs e Relatórios da Solução de Proteção Contra Ameaças Avançadas;

Deve permitir o envio de logs dos recursos para servidor de logs por meio do protocolo syslog e deverá conter no mínimo:

Tipo de evento de detecções: Conteúdo malicioso, reputação de URL's, comportamentos maliciosos, comportamentos suspeitos, Exploits, correlações de eventos, Grayware;

Tipo de eventos de sistemas: Eventos de sistema e eventos de atualizações;

Deve ter integração com ferramentas de SIEM;

Deve possuir capacidade de entregar relatório contendo informações da sequência de execução do artefato malicioso, assim como, detalhes de alterações locais da máquina, conexões externas e envio da informação para fora da rede corporativa;

A solução deve prover serviço de agregação e correlação de logs de eventos de segurança possibilitando coleta de fontes de monitoração para proporcionar informação e identificação de ameaças digitais conhecidas e desconhecidas em trânsito através de logs de sensor;

Solução deverá apresentar relatórios customizados de todas as suas funcionalidades e deverá conter no mínimo:

Computadores infectados;

Origem de infecções;

Estatísticas de ameaças;

Riscos potenciais de segurança;

Riscos de perda de informações;

Risco de sistema comprometido;

Risco de disseminação de ameaças;

Eventos suspeitos;

Infecções de malware

Deve apresentar função de pesquisa por logs contendo no mínimo:

Critérios de pesquisa por dia, mês e ano;

Possibilidade de pesquisa pelo nome do computador, domínio ou conta, endereço IP, endereço MAC e grupos;

Possibilidade de pesquisa por ameaças, URL's maliciosas, análises virtuais, correlação de incidentes, nome de malware, protocolo e direção da detecção;

Os relatórios e logs deverão ser exportados nos formatos PDF ou CSV;

Características Gerais de Pré-Requisitos para Proteção de Camada de Estação de Trabalho

A contratante deverá disponibilizar 3 (três) máquinas virtuais com os seguintes requisitos mínimos para atendimento desta solução (Implantação do Módulo para Investigação de Ameaças Avançadas que será utilizado pela Solução de Segurança para Proteção para camada de Estações de Trabalho):

Tipo de Servidor/CPU: 08 Cores de 64-bit, Intel-VT – 2.6 GHz;

Memória RAM: mínimo de 16 GB;

Disco: mínimo de 200 GB;

Plataforma de virtualização: VMware vCenter 5.1 ou superior e ESXi 5.1 ou superior;

Sistema Operacional: Windows Server 2008 R2 (x64);

Software: Microsoft Internet Information Services (IIS);

A contratante irá disponibilizar os seguintes requisitos mínimos em cada Estação de Trabalho e/ou Notebook para atendimento desta solução (Implantação dos agentes do Módulo de Proteção contra Ameaças Avançadas que será utilizado pela Solução de Segurança para Proteção para camada de Estações de Trabalho):

CPU: mínimo de 01 Core de 1 GHz;

Memória RAM: mínimo de 512 MB;

Disco: mínimo de 500 MB;

Gerenciamento centralizado para todos os itens

A solução de gerenciamento centralizado deve permitir a integração com a solução de segurança para proteção de estações de trabalho (desktops e notebooks), com todos os seus módulos, solução de anti-spam e solução contra ameaças avançadas;

Instalação do servidor na plataforma Windows 2008 Server ou superior, seja o servidor físico ou virtual;

Suportar base de dados Microsoft SQL;

Deve gerenciar logs das atividades e eventos gerados pela solução;

Deve possuir integração com Microsoft Active Directory;

Deve permitir níveis de administração por usuários ou grupos de usuários;

Deve permitir a constituição de políticas genéricas aplicáveis a grupos de máquinas, ou aplicáveis a grupos de usuários;

Deve disponibilizar sua interface através dos protocolos http e https;

Deve permitir a alteração das configurações das ferramentas ofertadas, de maneira remota;

Deve permitir diferentes níveis de administração, de maneira independente do login da rede;

Geração de relatórios e gráficos e parametrizáveis nos formatos html, pdf, xml e csv;

Deve gerar relatórios e gráficos pré-definidos nos formatos rtf, pdf, Activex e crystal report (*.rpt);

Deve permitir criação de modelos de relatórios customizados;

Deve permitir logon via single sign-on com os demais produtos da solução;

Deve permitir a atualização de todos os componentes de todos os módulos gerenciados;

Deve permitir a criação de planos de entrega das atualizações, com hora de início ou postergação da entrega após o download dos componentes;

Deve permitir o controle individual de cada componente a ser atualizado;

Deve permitir a definição de exceções por dias e horas para não realização de atualizações;

Deve permitir ter como fonte de atualização um compartilhamento de rede no formato UNC;

Deve gerar relatórios e gráficos com o detalhamento das versões dos produtos instalados;

Deve possuir o acompanhamento dos comandos administrativos em execução, tal como seu status de conclusão, alvo e usuário;

Deve permitir a configuração dos eventos administrativos ou de segurança que geram notificações, tal como o método de envio e o destinatário;

Os métodos de envio suportados devem incluir: e-mail, gravação de registros de eventos do Windows, SNMP e SYSlog;

Deve permitir a configuração do intervalo de comunicação com os módulos gerenciados;

Deve permitir a escolha do intervalo de tempo necessário para que um módulo seja considerado fora do ar (off-line);

Deve permitir o controle do intervalo de expiração de comandos administrativos;

Deve possuir a configuração do tempo de expiração da sessão dos usuários;

Deve permitir a configuração do número de tentativa inválidas de login para o bloqueio de usuários;

Deve permitir a configuração da duração do bloqueio;

Deve permitir pesquisas personalizadas para a consulta de eventos (logs) através de categorias

Deve permitir pesquisas personalizadas para a consulta de eventos (logs), através de critérios lógicos, com base em todos os campos pertencentes aos eventos consultados;

Deve permitir a configuração das informações que não são enviadas dos módulos à solução de gerenciamento centralizado;

Deve permitir a configuração da manutenção dos registros de eventos (logs), com base no intervalo de tempo que devem ser mantidos e no número máximo de registros, por tipo de evento;

Deve de permitir a criação de políticas de segurança personalizadas;

As políticas de segurança devem permitir a seleção dos alvos baseados nos seguintes critérios:

Nome parcial ou completo das estações de trabalho, permitindo a utilização de caractere coringa para identificação do nome parcial da máquina;

Range de endereços IPS;

Sistema operacional;

Agrupamento lógicos dos módulos;

As políticas de segurança devem permitir a combinação lógica dos critérios para identificação do(s) alvo(s) de cada política;

Deve permitir visualização de eventos de violação de segurança de todos os módulos gerenciados, agrupado por usuário numa linha de tempo, configurável;

Deve permitir a gerência dos módulos baseados no modelo de nuvem (cloud), quando existentes;

Deve permitir a criação de múltiplos painéis (dashboards) personalizáveis, compostos por blocos de informações (widgets), visualizados através de gráficos ou tabelas;

Os blocos de informações pertencentes aos painéis personalizáveis devem permitir filtros personalizados para facilitar na visualização e gerenciamentos;

A seleção de uma informação específica dentro de um bloco de informações, através de um clique, deve redirecionar ao log detalhado que gerou aquela informação;

Deve possuir repositório central de identificadores de dados, que podem ser utilizados para a criação de políticas contra possíveis vazamentos de informações;

Deve permitir a investigação de incidentes de vazamento de informação através de um número identificador de incidentes;

3.4.1.5. SOLUÇÃO DE SANDBOX (ANÁLISE DE DIA ZERO)

Deve ser executada em Hardware e Software específicos (appliance ou solução de software + hardware homologado) contanto que o conjunto da solução seja suportado pela contratada. Todas as funcionalidades deverão ser executadas no mesmo equipamento;

A solução deve se integrar as outras soluções contidas nesse documento;

Deve suportar ao menos 3 imagens diferentes e até 30 instancias simultâneas.

Deve ser gerenciada por console Web suportando no mínimo os browsers Internet Explorer e Firefox.

A console de gerenciamento deverá ter dashboards para facilidade de monitoração. As janelas deverão ser customizadas pelo administrador em quantidade e período de monitoração;

Deverá permitir a customização das janelas de monitoramento no dashboard através de widgets, podendo o administrador livremente adicionar ou remover widgets de acordo com sua necessidade de visualização;

Deverá possuir a capacidade de atualizar as vacinas, engines, assinaturas e recursos de inspeção de conteúdo de forma agendada e automática;

Deverá ser capaz de identificar ameaças evasivas em tempo real com o provimento de análise profunda e inteligência para identificar e prevenir ataques;

Deve permitir a geração de logs e integração com SYSLOG Servers e deverá conter no mínimo:

Tipo de evento de detecções: Conteúdo malicioso, reputação de URL’s, comportamentos maliciosos, comportamentos suspeitos, Exploits, correlações de eventos, Grayware;

Tipo de eventos de sistemas: Eventos de sistema e eventos de atualizações.

Deve ter integração com ferramentas de SIEM tais como (IBM Qradar, HP ArcSight e Splunk)

Deverá possuir capacidade de geração de relatórios executivos e detalhados com no mínimo as seguintes informações: relatórios diários, semanais e mensais.

Deve ser capaz de suportar a retenção de logs por no mínimo 120 dias;

Deve permitir exportar Logs nos formatos PDF;

Deve suportar a geração de logs, no mínimo, nos padrões CEF Common Event Format (CEF) e LEEF Log Event Extended Format (LEEF);

Deverá analisar em tempo real o comportamento através de simulação de execução de arquivos provenientes do tráfego de rede incluindo arquivos PDF´s, executáveis, PPT, DOC, XLS, ZIP e RAR;

Deverá possuir tecnologia de análise de arquivos binários através de simulação e avaliação de execução dos artefatos suspeitos para identificação de comportamento malicioso, com capacidade de operar vários ambientes simultâneos e integrados a solução para processamento de alto desempenho;

Deverá permitir o uso de base de conhecimento na Internet do próprio fabricante, com atualização automática de regras e assinaturas, para consultas automáticas em bases de reputação e correlacionamento de informações sobre ameaças conhecidas, identificando assim as respectivas recomendações de ações;

Deverá permitir o rastreio por malwares utilizando métodos de detecção baseados no tipo de arquivo (True File Type), múltiplas camadas de empacotamento (Multi-packed/Multi-layered files) e arquivos comprimidos (compactados);

Deverá identificar por comportamento ameaças do tipo ransomware

Deverá identificar e executar arquivos de scripts no formato Visual Basic e Javascript inclusive quando estiverem obfuscadas

Quando detectada uma ameaça, a solução deve prover informações sobre a ameaça, família da ameaça, estatísticas de segmentos de mercado afetados e recomendações de segurança para eliminar a ameaça, correlacionando estas informações com sites ou outros vetores por onde esta ameaça é disseminada;

Deverá possibilitar customização de Sandbox, permitindo ao cliente simular seu padrão de imagens e sistemas operacionais no módulo de análise virtual;

Deve suportar análise de documentos do Microsoft Office (DOC, DOCX, XLS, XLSX, PPT, PPTX)

Deve suportar análise de documentos em PDF

Deve submeter um documento PDF a pelo menos duas versões do Adobe Reader

Deve analisar dinamicamente arquivos compactados (ZIP, BZIP2, RAR)

Deve analisar dinamicamente binários PE de 32-bits

Deve analisar dinamicamente binários PE de 64-bits

Deve permitir criação de 1 (uma) sandbox personalizada pelo usuário, em um dos seguintes tipos de Sistemas Operacionais:

Utilizando Windows XP 32-bits em português.

Utilizando Windows 7 32-bits em português.

Utilizando Windows Server 2008 64-bits em inglês e português.

Utilizando Windows 7 64-bits em português.

Utilizando Windows 10 64-bits versão 1709;

Utilizando Windows Server 2012;

Utilizando Windows Server 2016;

Deve analisar dinamicamente bibliotecas dinâmicas (DLL)

Deve analisar dinamicamente binários BHO

Deve poder funcionar em ambiente totalmente virtualizado

Deve possuir tecnologia própria de análise de artefatos em sandboxing

Deve prover possibilidade de isolamento total da rede de sandbox da rede de gerência

Deve prover possibilidade de uso da rede dedicada para a internet na análise de sandbox

Deve analisar dinamicamente arquivos do Adobe Flash (SWF)

Deve realizar a análise localmente podendo ter consultas externas para reputação de IP e URL, mas sem envio da amostra

Deve ter a capacidade de gerar relatórios com eventos realizados pela amostra no sistema alvo, ao nível de API, exibindo as funções com argumentos e retornos de execução.

Deve analisar dinamicamente rootkits

Caso uma ameaça baixe outra enquanto na sandbox, essa também deverá ser analisada num evento correlacionado

Deve submeter uma amostra a sistemas operacionais diferentes, a fim de detectar ações específicas para um sistema;

Capacidade de integração via API com soluções terceiras;

3.4.1.6. SOLUÇÃO DE ANTI-SPAM (GATEWAY DE E-MAIL)

Pré-Filtro

Permitir configurar filtro de vírus (em nuvem) antes da chegada ao ambiente interno;

Permitir configurar filtro de SPAMs por reputação antes da chegada ao ambiente (na nuvem);

Permitir configurar filtro de SPAMs por característica (heurística) antes da chegada ao ambiente (na nuvem);

Permitir balanceamento de carga (Load Balance) para o mesmo domínio;

Possui gerenciamento de configurações em nuvem de forma integrada em uma única console de gerenciamento, interna e externa ao ambiente;

Spam / Phishing

Bloqueio de servidores spammers através da metodologia conhecida por Domain Keys Identified Mail (DKIM);

Deverá fazer listas de exceções para domínios utilizando-se de DKIM;

Possuir a detecção de SPAMs utilizando tecnologia heurística,

Possuir configurações de sensibilidade na detecção de SPAMs, no mínimo em 4 níveis;

Permitir a criação de White e Black Lists para detecção de SPAMs;

Possuir proteção contra Phishings;

Possuir proteção inteligente contra-ataques de Engenharia Social.

Deverá verificar o cabeçalho das mensagens em tempo real para proteção contra SPAMs;

Possuir inteligência contra ataques dos tipos, exploração de Códigos Avançados (Exploits) e Ataque de dia-zero (Zero-Day)

Possui reputação de links que estejam dentro do corpo das mensagens;

Possui reputação de links que estejam dentro do corpo das mensagens;

Possui níveis de sensibilidade no bloqueio de mensagens com links de má reputação;

Possui White List para a checagem de reputação em URL’s dentro de mensagens;

Vírus

Permitir a verificação heurística contra vírus recém-lançados, mesmo sem uma vacina disponível;

Permitir a verificação do tipo real do arquivo, mesmo que o mesmo for renomeado;

Permitir que arquivos suspeitos sejam enviados ao fabricante sem intervenção do administrador;

Permitir o escaneamento de arquivos executáveis comprimidos em tempo real;

Proteção contra Spywares, sem a necessidade de um software ou agente adicional;

Proteção contra Dialers, sem a necessidade de um software ou agente adicional;

Proteção contra Ferramentas Hackers, sem a necessidade de um software ou agente adicional;

Proteção contra Ferramentas para descobrir senhas de aplicativos, sem a necessidade de um software ou agente adicional;

Proteção contra Adwares, sem a necessidade de um software ou agente adicional;

Proteção contra Ferramentas, sem a necessidade de um software ou agente adicional;

Bloqueio de malware empacotado (packed malware) de forma heurística;

A solução de anti-spam deverá submeter e-mails suspeitos a solução de analise de ameaças avançadas locais, não sendo realizada de maneira externa ao ambiente, apresentado como resultado na alise informações;

Processos de AutoStart;

Modificações de Arquivos de Sistema;

Serviços criados e modificados;

Atividade de Rede Suspeita;

Modificações de Registros;

O Fabricante ofertado deve possuir conhecimento em mais de 190 milhões de ameaças conhecidas;

Filtros

Possuir um filtro de conteúdo com pesquisa por palavras-chave no cabeçalho e corpo da mensagem, e em arquivos Microsoft Office anexados, utilizando operadores lógicos tais como AND, OR, OCCUR, NEAR, (,), [,] e assim por diante;

Permitir bloquear anexos pela extensão, pelo tipo real do arquivo, nome, tamanho, e número de anexos;

Permitir criar filtros definidos pelo tamanho de mensagem;

Possuir proteção contra Graymail;

Permitir criar exceções para os filtros, definidos por rotas, grupos de usuários ou usuários específicos;

Possuir recurso que retire anexos indesejados e entregue a mensagem original para o destinatário;

Possibilitar a criação de áreas de quarentenas separadas para cada tipo de filtro;

Permitir o bloqueio de arquivos anexos baseado em sua extensão, tamanho, tipo real do arquivo (independente da extensão) e dentro de arquivos compactados;

Permitir a verificação em arquivos compactados nos formatos mais utilizados em até 20 níveis de compactação;

Permitir criar regras distintas para mensagens que entram e saem do ambiente;

Permitir a verificação contra conteúdos não autorizados dentro dos arquivos anexados nas mensagens;

Permitir a criação de grupos de usuários para configuração de regras por grupo ou usuário;

Permitir limitar o número de destinatários por mensagem;

Possui regra específica para anexos protegidos por senha

Possuir módulo de Data Loss Prevention (DLP), prevenindo ações de vazamento de informações, com regras baseadas em:

Palavras chaves

Expressões regulares

Extensões de arquivos

Possuir verificação de mensagens criptográficas de cliente que suporte os seguintes cipher suítes:

AES128-SHA

DHE-RSA-AES128-SHA

AES256-SHA

ADH-RC4-MD5

RC4-SHA

RC4-MD5

DHE-DSS-AES128-SHA

IDEA-CBC-SHA

Filtros por IP

Permitir a checagem na rede Global (colaborativa) da reputação dos IPs que tentam se conectar ao ambiente para enviar mensagens;

Permitir a configuração individual entre Reputação Global (da empresa prestadora do serviço) e Reputação Local (personalizada);

Possibilidade de exceções ao bloqueio por reputação com base em pais range de ip ou ip

Configurar nível de sensibilidade da reputação de Ips em até quatro níveis

Permitir configurar o código de erro para mensagens rejeitadas;

Permitir a verificação de endereços IPs para checar a sua legitimidade, sendo:

Realizar a busca em no mínimo cinco bases de dados localizados no site do fabricante;

Não necessitar instalação adicional;

As bases devem ser do mesmo fabricante do software para gateway SMTP;

Possuir configuração personalizada para cada tipo de ataque (SPAM, Vírus, Dicionário (DHA) e Mensagens de Retorno (Bounced Mails));

Permitir personalizar os filtros baseado em:

Tempo;

Total de mensagens;

Porcentagem de mensagens;

Ação a ser tomada;

Prevenir contra-ataques de SPAM, permitindo rejeitar a conexão quando exceder configuração personalizada para esse ataque;

Prevenir contra-ataques de Vírus, permitindo rejeitar a conexão quando exceder configuração personalizada para esse ataque;

Prevenir contra ataques DHA (Directory Harvest Attack);

Permitir verificar conexões suspeitas, apresentando o domínio responsável pela conexão, apresentado total de conexões e dessas, o percentual de conexões maliciosas;

Ações

Possuir recurso que permita adiar a entrega de determinadas mensagens para um horário específico;

Permitir enviar notificações de ocorrências customizadas ao administrador, remetente, destinatário;

Permitir customizar as ações que a ferramenta deve tomar de acordo com as necessidades do ambiente;

Permitir inserção de carimbo no assunto da mensagem;

Permitir a inserção de um header customizado (X-header);

Permitir o direcionamento da mensagem para servidor diferente do padrão (próximo hop) de acordo com a necessidade do ambiente;

Permitir apagar anexos indesejados, mas entregar a mensagem ao destinatário informando da ação;

Permitir a inserção de texto no corpo da mensagem;

Permitir customizar a mensagem que será inserida no corpo das mensagens;

Permitir a escolha do local onde se irá colocar a notificação customizada para o começo ou fim da mensagem original;

Permitir inserir variáveis nas notificações, onde informem:

Remetente;

Destinatário;

Assunto;

Data;

Nome do arquivo detectado;

Nome do vírus detectado;

Protocolo de escaneamento;

Tamanho total da mensagem e seus anexos;

Tamanho total do anexo;

Número de anexos detectados pela regra;

Ação tomada pela ferramenta;

Nome da quarentena para onde a mensagem foi enviada;

Permitir configurar ações para mensagens fora do padrão (mensagens malformadas);

Permitir ação personalizada para mensagens com anexos protegidos por senha;

Permitir quarentenar mensagens de SPAM;

Permitir encaminhar as mensagens em cópia oculta para destinatário não inserido originalmente na mensagem;

Permitir arquivar as mensagens sem que o remetente ou destinatário saibam para fins de auditoria;

Quarentena

Capacidade de apresentar uma console web para que os usuários possam verificar as mensagens que estejam em quarentena por motivo de spam;

Capacidade de usuários criarem lista de exceções a remetentes nessa console web de quarentena de mensagens;

Permitir que os usuários verifiquem mensagens suspeitas postas em quarentena e aprovar os remetentes sem intervenção do administrador;

Permitir exclusão automática das mensagens em quarentena;

Deverá utilizar LDAP para autenticação ao portal de quarentena, suportando no mínimo:

Microsoft Active Directory

OpenLDAP

Sun iPlanet Directory

Administração

Gerenciamento via console web HTTPS (Internet Explorer / Firefox);

A solução deve possuir um modo de instalação passo a passo, na própria console de gerenciamento.

Gerenciamento das áreas de quarentena, com pesquisa, reprocessamento, entrega ou exclusão de mensagem;

Realizar atualização de vacinas de forma incremental

Realizar atualização de e da versão do software. A atualização deve permitir conexão através de serviço Proxy;

Possibilidade de configurar o “greeting” SMTP;

Permitir o controle de relay baseado no domínio e/ou endereço IP;

Possuir recurso que faça uma monitoração do sistema, alertando o administrador caso haja falta de espaço em disco, se o serviço estiver indisponível e se a fila de mensagens chegarem a um número estabelecido como máximo pelo administrador;

Permitir a verificação de mensagens no protocolo POP3, permitindo configurar que porta TCP será utilizada;

Capacidade de checagem por DNS reverso com até quatro diferentes níveis de bloqueio

Definição de timeout de conexão SMTP

Suporte a ilimitadas conexões SMTP

Capacidade de ter vários servidores de rastreamento de tráfego SMTP gerenciado por console único.

Ter a capacidade de proteger o tráfego POP3;

Ter gerencia de área exclusiva para quarentena ou cópia de mensagens;

A solução deve ofertar possibilidade de ter domínio mascarado;

Possuir autenticação via TLS (Transport Layer Security);

Possuir mecanismo de alerta específico para ataques do tipo Command & Control (C&C).

Relatórios

A solução deve apresentar relatórios criados através de console web;

A solução deve disponibilizar relatórios gerenciais que podem ser "on demand" ou agendados;

A solução deve disponibilizar relatórios gerenciais de utilização de mensagens por destinatário, remetente, assunto;

A solução deve ter templates predefinidos para relatórios de forma a facilitar a geração de relatórios;

Possuir integração com LDAP (Microsoft Active Directory, Lotus Domino, Sun iPlanet Directory).

A solução deve ser capaz de receber trafego em TLS e realizar conexões em TLS para outros servidores;

A solução deve possibilitar trafego via Secure SMTP;

A solução deve permitir reindexação da base de dados de forma agendada;

É preciso que a solução permita importação e exportação de suas políticas através da console de gerenciamento;

A solução deve permitir a criação de usuários com acessos diferentes de administrador à console de gerenciamento;

A solução deve integrar o login da console de gerenciamento com o serviço de LDAP pré-configurado;

Características Gerais da Solução de Anti-Spam

A solução deve ser oferecida em formato de software appliance;

Não serão aceitas soluções Open Source.

A solução deve ser gerenciada totalmente por sua console Web, além de possui interface CLI intuitiva com gerenciamento dedica a solução;

A solução precisa ser compatível com as seguintes plataformas de virtualização:

VmWare™ ESX server;

VmWare ESXi 5.0

VmWare ESXi 5.5;

Hyper-V

Microsoft Hyper-V Server 2008 R2 SP1

Microsoft Hyper-V Server 2012 R2

Anti-Spam para Exchange

Suporte a Cluster Microsoft bem como as versões do MS-Exchange 2003, 2007 e 2010. No caso do MS-Exchange 2007, suportar a instalação na plataforma Windows 2008;

Deve ter o serviço clusterizado e trabalho em cluster ativo-ativo e ativo-passivo

Permitir a instalação remota a múltiplos servidores Exchange, monitorando o status de cada instalação;

Permitir possibilidade de instalação silenciosa sem intervenção do administrador

Possuir capacidade de gerar um certificado para o servidor web, para um acesso seguro;

Permitir configurar as portas de comunicação para o gerenciamento;

Realizar a verificação em background, para não impactar na performance;

Possuir verificação em memória e multi-threaded;

Possuir ação de limpeza para os arquivos anexados;

Permitir a verificação em tempo real, manual ou agendada de grupos e bases de dados no Exchange;

A verificação no Information Store deve ser realizada nas Public e Private Stores;

Permitir o bloqueio de arquivos anexos baseado em sua extensão, tamanho, tipo real do arquivo (independente da extensão) e também dentro de arquivos compactados;

Bloqueio dos arquivos em anexos deve ser com base em política por usuário e integrado com o active directory para a criação dessas políticas

Permitir a verificação no Internet Mail Connector (IMC);

Prover proteção para mensagens enviadas via Outlook Web Access (OWA);

Permitir a filtragem baseado no tamanho da mensagem.

Realizar a verificação contra códigos maliciosos no corpo da mensagem;

Realizar a verificação em arquivos baseado em seu tipo real, independente da extensão apresentada;

Realizar a verificação somente em arquivos passíveis de códigos maliciosos, permitindo assim um melhor desempenho da solução;

Possuir a detecção de SPAMs utilizando tecnologia heurística, podendo ser configurada a sensibilidade da ferramenta;

Deve ter approved list para recebimento de mensagens de determinados senders;

Deve ter integração com a pasta JUNK MAIL ou SPAM do Outlook de modo que os spams sejam direcionados diretamente para essa pasta;

Os usuários devem ter a capacidade de se permitido criarem suas exceções de recebimento através de white list gerenciada no próprio Outlook;

Avaliar reputação de links HTTP que estejam dentro do email quanto a sua reputação e caso reputação negativa deve ser tomada uma ação na mensagem;

Permitir criar regras de controle de conteúdo definidos por rotas, usuários e grupos;

Regra de controle de conteúdo deve procurar por conteúdo no subject, corpo e cabeçalho da mensagem;

Deve ter a possibilidade de em caso de um conteúdo malicioso, executar as seguintes ações: substituir por um texto, quarentenar a mensagem inteira, quarentenar parte da mensagem, deletar a mensagem inteira, fazer o backup/cópia da mensagem, passar parte da mensagem;

Possuir uma área de quarentena para o usuário final, integrada à ferramenta, para serem armazenados os emails detectados como SPAM, para que o usuário possa refinar a ferramenta;

Deve possuir área de quarentena no servidor com gerência pelo administrador através da liberação de mensagens ou deleção;

Deve possuir exceções nas políticas de bloqueio de anexo e de bloqueio de conteúdo;

No caso de violação de anexo não desejado deve possuir capacidade de executar as seguintes ações: substituir por um texto, quarentenar a mensagem inteira, quarentenar parte da mensagem, deletar a mensagem inteira, fazer o backup/cópia da mensagem;

Permitir a verificação contra conteúdos não autorizados dentro dos arquivos anexados nas mensagens;

Marcar as mensagens detectadas como SPAM no campo "assunto", preservando também o conteúdo original;

Permitir o gerenciamento de vários servidores Exchange simultaneamente;

Gerenciamento via console web (Internet Explorer);

Possuir controle de time-out para a console de gerenciamento;

Permitir configurar as notificações a serem enviadas para o administrador, via email e SNMP;

Realizar ações específicas para cada tipo de código malicioso;

Capacidade para, em caso de epidemia, bloquear a entrada de determinados emails, baseado nas características de códigos maliciosos, restaurando as configurações originais ao término da epidemia, ambos de forma automática através de políticas recebidas do fabricante;

Permitir um gerenciamento da quarentena, podendo enviar, encaminhar e apagar mensagens que estiverem nela;

Proteção contra spywares, sem a necessidade de um software ou agente adicional;

Deve detectar e bloquear malwares empacotados (packed malwares);

Para mensagens infectadas, deve poder tomar as seguintes ações: limpar, substituir por um texto, quarentenar a mensagem inteira, deletar a mensagem inteira, passar, quarentenar parte da mensagem;

Produto deve ter capacidade de fazer reputação dos IPs que estejam conectando no Exchange server e caso IP seja de má reputação que a mensagem seja bloqueada;

Produto deve executar rastreamento agendado ou manual nas mailboxes dos usuários;

Deve possuir acessos por papéis em sua console com diferentes perfis de acessos e diferentes acessos a menus;

Deve possuir capacidade de single sing on para acesso da console web de gerenciamento;

Deve reconhecer e ser compatível com IPV6;

Deve integrar-se com MOM/SCOM da Microsoft para envio de notificações;

Deve limitar uso de CPU em agendamento de rastreamento ou rastreamento manual;

Deve fazer filtro de conteúdo realizando o rastreamento dentro do anexo da mensagem;

Deve gerar relatórios de:

Vírus, spyware, grayware e outros malwares, com gráficos em escala horária, diária, semanal e mensal;

Principais vírus/malwares, spywares e graywares;

Principais senders de vírus/malwares, spywares e graywares;

Resumo das ações tomadas contra vírus/malwares, spywares e graywares;

Resumo do bloqueio de anexos;

Gráfico do bloqueio de anexos, com escala horária, diária, semanal e mensal;

Principais tipos de anexos bloqueados;

Principais nomes de anexos bloqueados;

Principais extenções de anexos bloqueados;

Gráfico do filtro de mensagens, com escala horária, diária, semanal e mensal;

Principais remetentes e destinatários filtrados.

Resumo de spam;

Gráfico do filtro de spams, com escala horária, diária, semanal e mensal;

Principais fontes e destinatários de spam;

Tráfego por hora, dia e mês;

3.4.1.7. SOLUÇÃO DE PROTEÇÃO WEB(FILTROWEB)

Gerenciamento via console web

Deve possuir a certificação da VmWare para Software Appliance ou a possibilidade de instalação no formato de Bare Metal, formato no qual depende da homologação do hardware por parte do fabricante;

Virtual Appliance: Suportar VmWare ESX e ESXi 5.5 ou superior e Microsoft Hyper-v 2.0 Windows Server 2012 R2 ou superior;

Possuir verificação contra códigos maliciosos como vírus, worms, trojans, phishing, spyware e applets e activex maliciosos, sem a necessidade de um agente ou software adicional;

Toda a solução deve ser do mesmo fabricante;

Permitir criar políticas de verificação baseado no perfil do usuário ou grupo, range ou endereço IP, permitindo uma navegação mais segura;

Permitir um controle de quota em Megabytes ou por tempo para o acesso à internet, por usuário ou grupo de usuário, por dia, semana e mês;

Permitir a utilização da ferramenta em modo Transparent Bridge, Forward Proxy, Proxy Reverso;

Possuir suporte ao protocolo ICAP e WCCP;

Utilizar os seguintes serviços de diretório: Microsoft Active Directory, Linux OpenLDAP Directory e Sun Java System Directory Server 5.2;

Permitir configurar os usuários que terão acesso à internet, baseado em seus logins, endereço IP e range IP;

Possuir um tratamento especial para Java Applets, onde esse é verificado quanto à sua assinatura e certificado, podendo tomar ações distintas para cada combinação entre elas, podendo ainda configurar que operações um Applet pode executar na máquina do usuário e como seus certificados serão validados;

A análise anti-malware da tecnologia deve ser realizada em Real Time, possibilitando uma ação imediata quando identificada uma ameaça;

Permitir configurar os certificados digitais que são seguros, colocando também os não seguros em uma lista negra;

A tecnologia deve ser capaz de identificar e bloquear conexões com redes zumbis (Botnets);

Possuir banco de dados de URL categorizados em, no mínimo, 80 categorias e tomar as seguintes ações para o acesso a estas categorias: PERMITIR, BLOQUEAR, MONITORAR, ALERTAR, TEMPO de ACESSO e ACESSO com SENHA, este banco de dados deve estar hospedado na Internet para que se tenha uma atualização mais rápida das categorias;

A tecnologia deve possuir integrado a mesma solução um Cache de páginas HTTP que visa a melhorar o desempenho da navegação;

A configuração do tamanho dos objetos que serão armazenados no cache devem passíveis de modificação pelo Administrador da tecnologia;

Possibilidade de permissão de acesso websites definidos nas categorias em períodos pré-determinados;

Possuir integração com Safe Search do Google e do Yahoo;

Possuir analise de malware sobre o tráfego HTTPS;

Possibilidade de permitir customizar notificações para o usuário de acordo com a política de acesso definida:

HTTPS Access Denied;

HTTPS Certificate Failure;

HTTP/HTTPS Scanning;

HTTP/HTTPS Blocked File Type;

URL Blocking;

FTP Scanning;

FTP Blocked File Type;

IntelliTunnel (bloqueio de Instant Messaging);

Applets and ActiveX Instrumentation;

Pattern File Updates;

URL Filtering and Scan Engines Update;

Possuir recurso para permitir / bloquear no mínimo 420 aplicações diferentes e este recurso deve funcionar no mínimo em dois modos de instalação (Forward Proxy e Bridge);

Possuir recurso para permitir / bloquear conexões Peer-to-Peer (BitTorrent, Gnutella, eDonkey, ...);

Possuir recurso de Web Reputation (reputação de HTTP), integrada com a solução de antivírus, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;

Deve possuir a funcionalidade de replicar as configurações entre outros servidores de proteção do gateway HTTP através de uma tecnologia auxiliar de centralização de logs, reports e configurações;

Deve possuir capacidade de criar os seguintes perfis de acesso a console de gerência: Administrador, Auditor e Reports

Os relatórios devem possuir no mínimo 50 tipos de relatórios pré-definidos, que tragam visibilidade de acesso: URLS mais acessadas, usuários que mais acessam a internet, acesso por categoria do web site, consumo de banda e violações de regra;

Os relatórios devem disponibilizar uma Dashboard de visualização dos acessos dos usuários ao WEB Gateway em tempo real;

A tecnologia standalone de relatórios deve permitir que geração seja agendada e submetida por e-mail;

3.4.1.8. SOLUÇÃO DE PREVENÇÃO DE INTRUSÃO DE PROXIMA GERAÇÃO (NGIPS) - 1 GB

Plataforma e Performance

A solução NGIPS (NEXT GENERATION INTRUSION PREVENTION SYSTEM) ofertada deverá ser disponibilizada em hardware do próprio fabricante, não sendo aceitos hardwares de fabricantes terceiros, não sendo aceitos também hardwares homologados (quando o fabricante da solução-software e do hardware são empresas diferentes).

Não serão aceitas soluções NGFW ou UTM.

O NGIPS deverá suportar a importação de regras no padrão SNORT, podendo esta ocorrer de forma direta e nativa via interface de gerenciamento, ou então através de ferramenta de conversão, onde o arquivo padrão SNORT deverá ser importado e convertido para o padrão utilizado pela solução ofertada;

A solução NGIPS deverá possuir as interfaces de rede de cobre, com pelo menos 8 interfaces 10/100/1000Gbps com by-pass embutido, assim como deverá possui interfaces de rede fibra optica, com pelo menos 8 interfaces 1Gbps SFP e também 4 interfaces 10G SFP+ (Os transceivers deverão ser entregues em conjunto da solução);

Para atendimento do by-pass das interfaces cobre, não serão aceitos dispositivos externos. Nas interfaces de fibra óptica deverá ser ofertado módulo de by-pass, que poderá ser embutido ou externo;

A solução NGIPS deverá usar discos de estado sólido (SSD), não sendo aceitos equipamentos com discos mecânicos;

Deverão ser entregues 2 (dois) equipamentos NGIPS que atendam as seguintes especificações:

A solução NGIPS proposta deverá atender no mínimo os seguintes requisitos:

IPS com throughput de inspeção de 1 Gbps, podendo ser expandido até 2GB sem necessitar trocar o equipamento;

Deverá gerar latência igual ou inferior a 100 Microsegundos;

Deverá suportar pelo menos 115.000 novas conexões por segundo;

Deverá suportar pelo menos 10 milhões de sessões concorrentes;

Deverá suportar pelo menos 40 mil sessões SSL concorrentes;

Deverá suportar pelo menos 1200 novas conexões SSL por segundo;

Deverá suportar inspeção de tráfego SSL Inbound (tráfego de entrada) de até 500Mbps;

O hardware ofertado deverá possuir fontes redundantes do tipo hot-swap;

O hardware ofertado deverá operar entre 0°C até 40°C;

O hardware ofertado deverá operar em ambientes com umidade entre 5% e 95%;

O hardware ofertado deverá operar em altitudes de até 2000 metros;

Requisitos técnicos e de segurança

A solução NGIPS ofertada deverá prover funcionalidades de prevenção de intrusão, em seu modo default (configuração básica) com pelo menos 2000 regras ativas (habilitadas automaticamente quando uma nova política de segurança é criada, em modo bloqueio e com criação de notificação).

Os filtros providos pelo NGIPS deverão permitir a seleção de ações de resposta. Deverão existir pelo menos as seguintes ações: Block (drop packet), Block (TCP Reset), Permit, Trust, Notify, Trace (Captura de Pacotes), além de ações condicionais, que permitam a definição de ações que alternam entre permitir e bloquear determinados tráfegos / ataques de acordo com condições encontradas no ambiente como por exemplo, Permitir as 1000 primeiras conexões de um único IP para determinado tráfego de rede em um período de 15 minutos. Após a conexão 1001 na mesma janela de tempo, a ação deverá ser alternada para bloqueio.

A solução NGIPS deverá suportar assinaturas de IPS para proteger vulnerabilidades, detectar exploits, detectar roubo de informações, detecção de virus, detecção de spywares, detectar tentativas de reconhecimento de rede, possuir regras que ajudem a controlar comportamentos de rede (exemplo: permitir ou bloquear resposta de comandos ping, detectar falhas de autenticação no MS SQL Server), possuir regras que blindem equipamentos de rede contra ataques que explorem vulnerabilidades, regras que efetuem a normalização de tráfego, ou seja, detectem tunelamento de protocolos, e cabeçalhos IP incompletos, além de filtros que permitam e detecção e controle de aplicações, tais como youtube, skype, TOR e facebook.

Os filtros do NGIPS precisam estar segmentados por categorias, com o objetivo de facilitar o gerenciamento da solução. Deverão existir pelo menos as seguintes categorias: Políticas de Segurança, Exploits, Normalização de Tráfego, Vírus, Reconhecimento de Rede, P2P e Vulnerabilidades.

O total de filtros disponíveis na solução (não necessariamente para uso simultâneo) não deve ser inferior a 16.000.

A solução NGIPS deverá ser capaz de permitir a criação e uso de políticas de segurança granulares baseados nos seguintes métodos:

Por NGIPS (todos os segmentos de rede de um IPS);

Por segmento físico, podendo selecionar o modo bi-direcional e direcional (deverá permitir ativar a política de segurança de nos sentidos de comunicação de A para B e B para A (na mesma politica de segurança), de A para B (politica de segurança dedicada para esta direção de comunicação) e também de B > A).

Por TAG de VLAN (802.1Q), de forma direcional e bi-direcional.

Por CIDR (Range de endereços IP)

Baseado no horário do dia

A solução NGIPS deverá ser capaz de detectar e bloquear ataques de reconhecimento de rede.

A solução NGIPS deverá prover filtros de detecção de aplicações tais como P2P, Online Games, permitindo a ativação de controles de banda.

Deverá possuir ferramenta para criação de filtros customizados, sendo que estes deverão permitir a customização de parâmetros tais como:

Nome do filtro;

Descrição do filtro;

Protocolo, permitindo a criação de filtros de proteção baseados nos protocolos IPv4, ICMPv4, UDP, TCP, HTTP, IPv6 e ICMPv6.

Severidade do filtro, devendo possuir pelo menos 4 níveis;

Customização da categoria do filtro;

Classe do filtro (devendo possuir pelo menos as classes DoS, Exploit, Virus e Acesso)

Gatilhos de acionamento (triggers), onde parâmetros ou informações/dados contidos no streaming de rede serão utilizados como gatilho para validação de parâmetros adicionais da regra.

Detecção de payload, permitindo o uso de strings e expressão regular para detecção avançada de instruções no streaming de rede;

Detecção de payload dentro do protocolo HTTP, permitindo o uso de strings e expressão regular para buscar e validar a existência de informações no cabeçalho HTTP, distinguindo métodos GET, POST, OPTIONS, PUT, DELETE, TRACE, CONNECT, HEAD, LOCK, UNLOCK, PROPFIND. Também deverá permitir a validação de dados específicos em URI, URI PATH, URI Target, Header e Payload.

Criação de customizações a nível TCP, sendo possível definir portas de origem e destino, além de validação de flags TCP.

A solução NGIPS ofertada deverá suportar processamento de tráfego assimétrico;

Deverá ser possível colocar a solução em modo by-pass total forçado;

A solução NGIPS deverá possuir inteligência Machine Learning, ou seja, deverá possuir filtros que implementem Machine Learning na detecção de por exemplo conteúdo obfuscado em HTML associado/relacionado a exploit kits;

Deverá possuir filtros de gerenciamento de tráfego, ou seja, deverá ser possível criar regras para controlar o tráfego no sentido de A para B, de B para A, liberando o tráfego (com inspeção de riscos de segurança), liberando o tráfego (sem inspecioná-lo, confiando na conexão), bloqueando o tráfego, e também permitindo a criação de políticas de controle de banda, permitindo limitar por exemplo determinado fluxo de dados de rede a 100kbps;

A solução de NGIPS deverá possuir controles de proteção contra ataques de DDOS, atuando como um SYN PROXY.

A solução de NGIPS deverá possuir filtros que detectem a tentativa de uso de TOR, TeamViewer.

A solução de NGIPS deverá detectar e bloquear tráfego Skype.

A solução de NGIPS deverá detectar e permitir o bloqueio de tunelamento de conexões DNS

A solução de NGIPS deverá possuir assinatura que permita a validação de requisições HTTP 2.0.

A solução de NGIPS deve bloquear nativamente a transferência de arquivos maliciosos via FTP.

A solução deve detectar ataques baseados em SSL, como por exemplo detectar o uso de certificados SSL/TLS maliciosos.

Atualizações de Segurança

A solução de NGIPS ofertada precisa entregar detalhes sobre a cobertura para vulnerabilidades Microsoft reportadas nos últimos 12 meses.

O fabricante da solução NGIPS deve prover estatísticas do número de vulnerabilidades de dia zero descobertas nos últimos 5 anos.

O fabricante da solução NGIPS deverá possuir times de pesquisa de vulnerabilidades de dia zero e de riscos de segurança, com pelo menos 1500 pesquisadores, sejam contratados ou parceiros, sendo que deverão ser apresentadas estatísticas dos últimos 3 anos de vulnerabilidades pesquisadas e descobertas. O fabricante deverá estar entre os Top 5 maiores pesquisadores do mundo nos relatórios publicados pela entidade Frost & Sullivan (Analysis of the Global Public Vulnerability Research).

A solução NGIPS deverá suportar atualizações automáticas dos filtros/assinaturas, possuindo frequência de atualizações mínima semanal (fabricante deverá entregar 1 atualização por semana).

Sempre que a solução NGIPS atualizar-se, o novo pacote de atualizações deverá conter descritivo visualizável na própria solução (console local do NGIPS ou gerenciamento centralizado), indicando quais filtros foram incluídos, quais foram modificados e quais foram removidos. O mesmo deve ocorrer para os filtros de ameaças (malwares), sendo exigidos os mesmos parâmetros para permitir o acompanhamento e monitoramento dos novos filtros adicionados pela solução.

Correlação de Informações e Consultas em Nuvem

O fabricante da solução NGIPS deverá prover um portal disponível via internet, com estatísticas em real-time de eventos e incidentes de segurança ocorridos globalmente, desta forma permitindo o uso desta ferramenta em investigações de incidentes ocorridos no ambiente além de tunning da

solução com base em estatísticas de ameaças e ataques monitorados globalmente.

Este portal deverá permitir a visualização de atividades baseada em países.

Este portal deverá permitir drill-down para monitorar ameaças novas e emergentes.

O portal deverá permitir uma vista detalhada de origens e destinos de cada tipo de ataque.

Deverá ser possível consultar neste portal os filtros mais acionados em escala global, top origem de ataques, identificar potencial impacto de performance que cada filtro pode gerar, e ações normalmente utilizados em cada filtro.

Reputação de Endereços IP, DNS e URLs

A solução NGIPS ofertada precisa permitir o bloqueio de tráfego baseado na reputação do endereço de IP de origem da conexão, de destino da conexão, através da reputação de DNS e URLs.

O serviço de reputação deverá contar com categorias tais como: Malware, Botnet, Spyware, SPAM, TOR, Web Application Attackers, P2P e Network Worm.

Deverá ser possível criar exceções baseadas em domínio e endereços IP, assim como deverá ser possível estabelecer as políticas de reputação individuais para cada perfil de segurança em uso no ambiente.

A base de reputação IP deverá suportar IPv4 e IPV6.

A base de reputação IP deverá ser baseada em informações do próprio fabricante, e também permitir o uso de bases terceiras.

Os filtros de reputação de IP deverão atuar tanto no sentido inbound quanto outbound.

As políticas de reputação deverão permitir a customização de ações tanto para bloquear ou permitir determinados acessos.

Deverá ser possível criar filtros de controle de acesso inbound e outbound baseados em geolocalização.

Proteção Avançada Contra Ameaças

A solução NGIPS deverá possuir funcionalidade que permita a identificação e proteção contra atividades maliciosas relacionadas a virus e spywares, no sentido inbound e outbound.

A solução NGIPS deverá possuir assinaturas de proteção contra malwares.

As assinaturas de malware deverão detectar a infiltração, exfiltração e comunicação com servidores de comando e controle através da inspeção do tráfego de rede.

Deve ser capaz de interromper atividades maliciosas tais como ransomware, fuga de dados, click fraud, etc.

Deverá bloquear ameaças do tipo drive-by-downloads.

Deverá detectar atividades de comunicação com servidores de comando e controle de botnets.

Os filtros de malware deverão ser atualizados de forma regular pelo fabricante da solução.

Alta Disponibilidade

Deve operar de forma redundante, suportando os cenários de operação Ativo-Passivo e Ativo-Ativo, para isto tanto o NGIPS quanto a solução de gerenciamento centralizado deverão ser entregues em duplicidade para implantação em alta disponibilidade.

A solução NGIPS ofertada deverá suportar fontes do tipo hot-swappable.

A solução NGIPS deverá suportar software bypass.

A solução NGIPS nas situações que o NGIPS for atualizado e em situações onde o NGIPS for reiniciado, não deverá gerar nenhuma interrupção de rede.

Gerenciamento Centralizado

A solução NGIPS precisa suportar ser gerenciado de maneira centralizada por solução de gerenciamento centralizado fornecido pelo mesmo fabricante.

A solução de gerenciamento centralizado entregue deverá permitir o gerenciamento de pelo menos 2 equipamentos NGIPS, sendo possível efetuar os mesmos níveis de configuração existentes na solução NGIPS.

A solução de gerenciamento centralizado necessita operar em modo alta disponibilidade, sendo que se o primeiro servidor falhar, o segundo deverá continuar operando normalmente sem prejuízos ao gerenciamento do ambiente.

A solução NGIPS deverá permitir integração com ferramentas de monitoramento de rede e SIEM tais como, HP ArcSight, além de permitir o envio de alertas por e-mail notificando incidentes de segurança.

A solução de gerenciamento centralizado deverá possui um painel de monitoramento de eventos, contendo pelo menos as estatísticas dos principais filtros acionados, principais atacantes, principais alvos dos ataques, etc.

A solução de gerenciamento centralizado deverá permitir a integração com dispositivos de rede, tais como switchs e roteadores, com recursos que permitam alterar a configuração de VLAN de portas de rede, e também desligar determinada porta de um switch de rede. Este recurso poderá ser utilizado para contenção de incidentes internos de segurança.

A solução de gerenciamento centralizado deverá possuir API que permita soluções externas, como o próprio SIEM, a interagir com a solução NGIPS,

devendo permitir pelo menos a adição e remoção de endereços IP suspeitos em listas de reputação, e também permitindo adicionar e remover endereços IP suspeitos da quarentena dos NGIPS.

A solução de gerenciamento centralizado deverá possuir recurso para relacionar relatórios de testes de penetração realizados no ambiente da empresa, permitindo comparar tais relatórios com políticas de segurança em uso, indicando quais regras ou filtros são necessários ativar para alinhar a política de segurança com as vulnerabilidades identificadas no ambiente. Deve possuir suporte nativo a pelo menos as seguintes ferramentas: Qualys, Nessus e Nexpose.

A solução de gerenciamento centralizado deverá possui módulo de relatórios próprio, possuindo templates que indiquem os principais riscos de segurança detectados no ambiente, contando com pelo menos 20 modelos pré-estabelecidos. Deverá ser possível agendar o envio destes relatórios, sendo exigidos no mínimo os seguintes formatos de arquivo: PDF, DOCX, XLS, CVS e XML.

A solução de gerenciamento centralizado deverá suportar o gerenciamento paralelo de pelo menos 2 IPS. A solução ofertada deverá estar dimensionada para atender o exigido neste edital, com folga para crescimento de até 20 NGIPS.

A solução de gerenciamento centralizado deverá ser entregue em formato virtualizado com sizing adequado, operando em alta disponibilidade, de modo que se a console de gerenciamento principal sair fora o ar, a secundária possa ser utilizada sem gerar prejuízos ao ambiente;

A solução de gerenciamento centralizado deverá permitir a integração com soluções de Sandboxes (detecção de ameaças desconhecidas) de modo a permitir que URLs contendo executáveis sejam analisados e testados por soluções de sandboxes que devem ser do próprio fabricante, a fim de identificar novas ameaças direcionadas ao ambiente. Indicadores como endereços IP e DNS relacionados a novas ameaças devem ser passíveis de bloqueio através da própria solução NGIPS (solução de sandbox deverá fazer o feedback dos indicadores relacionados a novas ameaças).

A solução de gerenciamento centralizado deverá possuir dashboard que permita a adição ou remoção de painéis que serão utilizados no monitoramento do ambiente, indicando os hosts comprometidos, hosts vulneráveis que sofreram ataques, lista de objetos suspeitos com quantidades de hits identificados,

A solução de gerenciamento centralizado deverá permitir a integração com serviços de diretório, tendo suporte aos métodos de autenticação CAC, RADIUS, TACACS+ e Active Directory, além de autenticação local (para uso enquanto solução não é integrada com restante da infraestrutura).

Quando implementado em modo alta disponibilidade, a solução de gerenciamento centralizado deverá permitir a operação usando IP Virtual;

A solução de gerenciamento deverá possuir API que permita que soluções terceiras interajam podendo por exemplo quarantenar determinado endereço

IP, desquarentenar determinado endereço IP, inserir e remover endereços IP de uma lista de reputação.

A solução de gerenciamento centralizado deverá atuar como ponto central para o gerenciamento de políticas de IPS, devendo possuir versionamento de políticas, capacidade de roll-back, além de capacidade de importação e exportação de configurações.

3.4.1.9. NGIPS EXPANÇÃO DE LICENÇA 2 Gbps(Upgrade 1,5Gbps IPS + 500Mbps SSL) - REFERENTE AO ITEM NGIPS

Esse item é somente uma licença referente ao item NGIPS deste Termo de Referência, não necessitando troca de software ou hardware contratado previamente

A troca de licença não deve afetar a garantia atual do hardware

Com a troca de licença a data de validade do software será alterada para nova contratação, não será somado ao tempo restante da licença anterior

O upgrade de licença deve ser feito sem a necessidade de upgrade físicos no equipamento

O upgrade de licença deve ser feito sem afetar as regras e filtros criados anteriormente.

3.4.1.10. PACOTES DE INSTALAÇÃO

Os softwares de solução de segurança a serem instalados deverão ser configurados em equipamentos (estações de trabalho e servidores) fornecidos pela CONTRATANTE.

Caberá à CONTRATADA a implantação da solução sob o acompanhamento da CONTRATANTE.

No que tange ao processo de implantação da solução, a CONTRATADA deve apresentar um cronograma para a implantação e seguir as atividades tomando como base o seguinte escopo do serviço:

Planejamento da instalação incluindo identificação de pré-requisitos;

Instalação e configuração do módulo de gerenciamento central;

Criar a senha de acesso com privilégio administrativo para a SEDUC/RO.

Instalação e configuração do software de endpoint protection em pelo menos 10 (dez) equipamentos;

Realizar customizações caso sejam solicitadas ou necessárias;

Realizar testes e apresentar os resultados que comprovem a correta e completa implantação da solução;

Realizar backup das configurações;

Documentar todas as configurações realizadas no ambiente;

Após a conclusão da instalação e implantação, deve ser formalmente homologada pelo SEDUC/RO, o qual possuirá o prazo de 5(cinco) dias consecutivos contados a partir da data de conclusão do serviço de instalação e configuração contratado, para emitir o relatório de homologação (aceite)

3.4.1.11. TREINAMENTO (HANDS-ON)

A CONTRATADA deverá ministrar treinamento on-site do tipo prático cobrindo todos os softwares inclusos na suíte de solução de segurança;

O conteúdo do treinamento deve abordar os assuntos de natureza teórica e prática, abrangendo todos os módulos envolvidos na solução de segurança em seus aspectos mais relevantes;

O treinamento pode ser separado conforme o produto a ser instalado no ambiente da SEDUC/RO, contendo ao menos os seguintes módulos:

Instalação do módulo de gerenciamento central;

Instalação do software de endpoint protection em estações de trabalho e servidores;

Descrição e configuração de todas as funcionalidades contratadas da solução;

Resolução de problemas – troubleshooting;

Melhores práticas utilizadas no mercado para aproveitamento dos softwares e suas funcionalidades.

A carga horária mínima será de 30 horas divididas em expedientes de 6h/dia, das 8h às 14h.

O treinamento terá um total de cinco (5) participantes definidos pelo SEDUC/RO

O material didático fornecido deve abordar todos os tópicos do curso (não oficial do fabricante)

A CONTRATADA deverá fornecer apostilas em formato digital que incluam o conteúdo referente ao produto;

É de responsabilidade da contratante a disponibilização de instalações físicas para a realização do treinamento;

Após a conclusão, o serviço de treinamento deverá ser formalmente homologado pela SEDUC/RO o qual possuirá o prazo de 5 (quinze) dias consecutivos contados a partir da data de conclusão do treinamento contratado, para emitir o relatório de homologação (aceite).

3.4.1.12. OPERAÇÃO ASSISTIDA/HORAS

Por operação assistida entende-se a transferência de conhecimento, o esclarecimento de dúvidas para a equipe técnica da CONTRATANTE, o acompanhamento presencial do funcionamento dos equipamentos instalados e a pronta intervenção em caso de qualquer problema detectado no ambiente. A CONTRATADA deverá prover o serviço de operação assistida pela

quantidade de pacotes de horas contratadas após a conclusão da implantação dos serviços. Durante este período a CONTRATADA deverá manter O AMBIENTE da CONTRATANTE monitorada e acompanhada remotamente e eventualmente através de presença in loco de profissional competente.

As horas de Operação Assistida serão utilizadas sob demanda por meio de Ordem de Serviço/OS, a critério do CONTRATANTE e serão consumidas para realização de atividades críticas. O serviço de operação assistida poderá ser prestado de forma presencial no endereço local do CONTRATANTE ou outro indicado por ele; bem como com todos os recursos ferramentais necessários para tanto, sem custos adicionais para o CONTRATANTE, durante todo o período de suporte técnico e garantia, sendo indispensável a apresentação de documentação original do fabricante que comprove a validade da certificação enquanto durar o vínculo contratual. A Ordem de Serviço deverá conter no mínimo: descrição do serviço, prazo para a execução do serviço, período para a execução do serviço, local da execução do serviço, horas de apoio técnico especializado a serem utilizadas, especificações técnicas do serviço e produtos esperados; Os serviços prestados deverão estar de acordo com as especificações constantes na Ordem de Serviço; O controle da execução dos serviços se dará em 03 (três) momentos, a saber: no início da execução. – quando a "Ordem de Serviço – OS" é emitida pelo CONTRATANTE, durante a execução – com o acompanhamento e supervisão de responsáveis do CONTRATANTE, e ao término da execução – com o fornecimento de "Relatórios de Atividade da Operação Assistida" pela CONTRATADA e atesto dos mesmos por responsáveis do CONTRATANTE; A partir da emissão da "Ordem de Serviço – OS", a CONTRATADA terá até 05 (cinco) dias corridos para iniciar a sua execução, ressalvados os casos em que comprovadamente seja necessário um agendamento para início dos trabalhos; O CONTRATANTE comunicará à CONTRATADA quando uma "Ordem de Serviço – OS" estiver sendo elaborada para que a CONTRATADA possa se manifestar no interesse de agendamento de reunião para definição de procedimentos necessários para execução dos serviços; As horas e procedimentos previstos inicialmente quando da abertura da "Ordem de Serviço – OS" serão validados no final das atividades e poderão sofrer adequações para estarem de acordo com o que foi efetivamente executado; As horas efetivamente utilizadas nos procedimentos executados serão computadas de acordo com os dias e horários de entrada e saída do responsável da CONTRATADA às dependências do CONTRATANTE; Para efeito de pagamento, somente após o término do computo dessas horas, a contratada emitirá fatura correspondente aos serviços concluídos na referida ordem de serviço; Somente as ordens de serviço efetivamente concluídas, com o devido levantamento das horas computadas poderão ser faturadas; Este serviço, de operação assistida, deverá estar disponível para acionamento no sistema 24 horas por dia vezes 7 dias por semana.

3.5. DA PROPOSTA TÉCNICA/DE PREÇO

3.5.1. Todas as documentações deverão ser assinadas e ter suas folhas rubricadas pelo(s) representante(s) legal(is) do Licitante Vencedor.

3.5.2. Na Proposta Técnica, a licitante deverá apresentar uma Matriz ponto a ponto comprovando cada especificação do itens, com a indicação da página do datasheet e/ou manuais dos equipamentos que serão ofertados;

3.5.3. Não serão aceitas outras expressões para o preenchimento, tais como, "Ciente", "De acordo", "Em anexo" e "Consultar Documentação da Proposta ou Manual", sendo considerado como item não atendido; e,

3.5.4. As documentações que comprovem as características técnicas devem ser feitas através de catálogos públicos dos próprios fabricantes dos softwares e seus componentes oferta.

3.6. DOS REQUISITOS COMUNS PARA TODOS OS ITENS

3.6.1. A LICITANTE deve informar na proposta comercial e na planilha de formação de preços marca e modelo do(s) produto(s) ofertado(s);

3.6.2. A LICITANTE deverá realizar a instalação dos produtos de segurança contratados pelo presente certame;

3.6.3. A LICITANTE deverá fornecer atestado comprovando a existência de equipe técnica com pessoas capacitadas pelo fabricante em todas as soluções adquiridas. O Certificado/Atestado/Carta, deverá ser fornecido pelo fabricante.

3.6.4. A LICITANTE deverá apresentar declaração emitida pelo fabricante específica para este certame comprovando que a empresa faz parte do programa de parcerias e que possui autorização para comercializar os seus produtos e serviços;

3.6.5. A LICITANTE deverá emitir declaração que cumpre todos os requisitos técnicos do edital se responsabilizando por isso, sendo que os requisitos técnicos serão validados pela equipe técnica de homologação; e,

3.6.5. A LICITANTE deverá fornecer atestado comprovando a existência de equipe técnica com pessoas capacitadas pelo fabricante em todas as soluções adquiridas. O Certificado/Atestado/Carta, deverá ser fornecido pelo fabricante.

4. DA EXECUÇÃO DO OBJETO

4.1. A solução de unificada de segurança para proteção de e-mail e endpoint contra ataques avançados deverá operar de forma unificada, ou seja, todos os equipamentos, softwares fornecidos e configurações aplicadas pela CONTRATADA deverão operar como um conjunto plenamente ajustado, de forma a garantir a perfeita integração entre todos os pontos da solução, seja em gateway ou endpoint, para a proteção do ambiente tecnológico da SEDUC;

4.2. Todos componentes da solução de unificada de segurança para proteção de e-mail e endpoint contra ataques avançados deverão ser do mesmo fabricante, visando a plena compatibilidade, o gerenciamento centralizado e completa integração de todos os itens da solução;

4.3. Todas as soluções, independentemente do fabricante, deverão atender as condições, características e especificações técnicas previstas neste Termo de Referência e demais itens não previstos que possam influir direta ou indiretamente no ambiente computacional do CONTRATANTE, bem como nos aspectos de disponibilidade e segurança requeridos;

4.4. Toda a solução deverá ser compatível com o ambiente tecnológico da SEDUC;

4.5. Os modelos e versões dos equipamentos (hardware) que compõe a solução deverão ser ofertados novos, sem uso anterior, e deverão permanecer em linha de produção pelos próximos 12 (doze) meses e com previsão de suporte pelos próximos 5 (cinco) anos, contados da data de assinatura do Contrato;

4.6. Caso algum softwareque compõe a solução conste em lista de end-of-support, end-of-engineering-support ou end-of-life do fabricante, durante o período de vigência das licenças de uso, a CONTRATADA deverá fornecer, configurar e promover a substituição por novo software equivalente, que atenda as especificações técnicas descritas neste Termo e que não impacte na perda de funcionalidade da solução;

4.7. As licenças de uso de software necessárias para o funcionamento dos diversos elementos da solução serão adquiridas em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante ou seu representante;

4.8. Os softwares deverão ser fornecidos em sua versão mais atualizada; e,

4.9. Caso a solução a ser fornecida, utilize software de proteção de endpoint diferente do atualmente instalado na SEDUC, a CONTRATADA deverá providenciar a desinstalação automática de todas as cópias instaladas do software em estações e servidores e a instalação do novo software em um único processo.

5. DA PROVA DE CONCEITO

5.1. Poderá ser solicitada, a critério exclusivo da CONTRATANTE, prova de conceito da solução à empresa classificada, antes da adjudicação, com o objetivo de realizar testes de comprovação de atendimento às especializações e requisitos exigidos nas Especificações Técnicas deste Termo de Referência caso a documentação entregue pela LICITANTE seja considerada insuficiente para comprovar o atendimento a todos os itens exigidos.

5.2. Para a realização da prova de conceito da solução, a LICITANTE deverá disponibilizar conjunto de elementos que atendas as funcionalidades: solução de segurança para proteção de e-mail, solução de segurança para proteção de endpoint e solução de segurança contra Ataques Avançados Persistentes – APT, devendo ser da mesma marca, modelo e especificações detalhadas na proposta.

5.3. A realização da prova de conceito deverá ser presencial e realizada, preferencialmente, na Coordenadoria de Tecnologia da Informação e Comunicação – SEDUC/CTIC, localizada na sede do CONTRATANTE, em dias úteis, ou, a critério exclusivo do SEDUC, devendo iniciar no prazo de até 05 (cinco) dias úteis, contados a partir da data de convocação do CONTRATANTE para a realização da prova de conceito.

5.4. A CONTRATANTE, a seu critério, poderá prorrogar a duração da prova de conceito por mais 02 (dois) dias úteis.

5.5. A prova de conceito utilizará como base as especificações técnicas constantes neste Termo de Referência.

5.6. Será rejeitada a prova de conceito que:

5.6.1. Não comprovar o atendimento de, pelo menos, 01 (um) requisito técnico descrito no ANEXO I - Especificações Técnicas deste Termo de Referência, executada nos equipamentos e softwares entregues para a prova de conceito.

5.6.2. Apresentar divergências entre as especificações dos equipamentos e softwares entregues para a prova de conceito em relação às especificações técnicas da proposta entregue pela LICITANTE.

5.7. Não será aceita a proposta da LICITANTE que tiver a prova de conceito rejeitada ou não entregue no prazo estabelecido.

5.8. Nesse caso, a proposta subsequente será examinada.

5.9. Desde que oficialmente solicitado à Coordenadoria de Tecnologia da Informação e Comunicação – SEDUC/CTIC, e, com a devida aquiescência, a prova de conceito, poderá ser acompanhada pelos demais licitantes interessados, participantes do certame licitatório.

6. CLASSIFICAÇÃO DOS BENS E SERVIÇOS COMUNS (Lei nº. 10.520/02, art. 1º)

6.1. Os bens e serviços descritos neste Termo de Referência, nos termos da Lei nº. 10.520/2002, enquadram-se na classificação de bens comuns, uma vez que possuem padrões de desempenho e qualidade segundo especificações usuais no mercado.

6.2. A prestação dos serviços não gera vínculo empregatício entre os empregados da Contratada e a Administração, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta.

7. JUSTIFICATIVA PARA CONTRATAÇÃO (Lei nº. 8.666/93, art. 3º, § 1º e Lei nº. 10.520/02, art. 3º, I)

7.1. Do Interesse Público na Despesa

A Secretaria de Estado da Educação - SEDUC, aqui representada pela Coordenadoria de Tecnologia da Informação e Comunicação - CTIC, deseja efetuar registro de preço, visando atender a demanda desta Secretaria, pois a mesma encontra-se com suas licenças de Antivírus já vencidas, onde estamos ja completamente desassistidos em toda a rede, computadores e arquivos governamentais desta Secretaria.

A aquisição objetiva manter e melhorar a segurança da rede da SEDUC/RO de ataques de vírus externos e internos, que são disseminados de maneira involuntária pelos usuários quando utilizam mídias removíveis infectadas e/ou vírus propagados por e-mail, como um arquivo anexado, cujo conteúdo tenta induzir o usuário a clicar sobre o arquivo ou acessar um endereço eletrônico, fazendo com que seja executado, quando entram em ação, infectam arquivos e programas e de forma automática se enviam para os e-mails encontrados nas listas de contatos gravadas no computador, ou até mesmo vírus de scripts, que são recebidos ao acessar uma página web que pode automaticamente ser executado sem conhecimento de nossos usuários. Vivemos uma época em que as tecnologias estão ativamente presentes em nosso cotidiano, enquanto nos tornamos beneficiários dessa evolução tecnológica, também nos tornamos vítimas das constantes ameaças que os acompanham, como o recente ataque cibernético global de 2017, onde na ocasião, 74 países, incluindo o Brasil, foram afetados com o ransonware WannaCry. Após a ampla contaminação, que chegou a paralisar inúmeros órgãos do governo e empresas, como o Serviço Nacional de Saúde do Reino Unido, a Telefônica, o Tribunal de Justiça e o Ministério Público de São Paulo, milhões de pessoas se sentiram ameaçadas. Infelizmente ainda não há como descriptografar os arquivos sequestrados pelo vírus WannaCry, mas, em geral, para as vítimas de ataques de sequestro de dados há uma iniciativa internacional que consegue recuperar os arquivos atacados, evitando que o usuário pague o resgate, porém o prejuízo de ter

a operação do Governo Estadual, especificamente neste Secretaria de Estado da Educação, exige que sejam tomadas várias medidas no sentido de minimizar a possibilidade, uma delas e mais importante é a solução de antivírus proposta por esta ARP.

Cada tipo de código malicioso possui características próprias que o diferencia dos demais tipos, como forma de obtenção, forma de instalação, meios usados para disseminação e ações maliciosas mais comuns executadas nos computadores infectados, podendo inclusive bloquear conteúdos de arquivos muito importantes para esta Secretaria (documentos de textos, planilhas, bancos de dados, etc), bem como sequestrar servidores inteiros, onde esse material é armazenado.

É importante ressaltar que definir e identificar essas características tem se tornado tarefa cada vez mais dificil, devido às diferentes classificações existentes e ao surgimento de variantes e novas ameaças que mesclam características dos demais códigos maliciosos. Desta forma a necessidade de contratação de licenciamento de software especifico para esta finalidade para minimizar o impacto dessas pragas virtuais em nossa Secretaria, além de resguardar as informações constantes nos servidores de arquivos, servidores de aplicações e estações de trabalho, a fim de evitar indisponibilidade e sequestro de informações causadas por códigos maliciosos.

A tendência é de que os cibercriminosos continuem atacando grandes alvos por meio da personalização do ransomware. Com base nas semelhanças entre os principais ataques de ransomware dos anos passados, verificou-se que o próprio malware foi codificado para procurar arquivos no banco de dados do servidor. Os hackers continuarão a utilizar a abordagem “spray-and-pray” em seus ataques de ransomware, ou seja, vão enviar o ransomware em massa, na esperança de conseguirem infectar um sistema de usuários vinculado a uma rede corporativa/governamental.

No entanto, o ransomware não será o único método utilizado para extorsão digital, grupos de invasores vão usar também campanhas digitais de difamação e propagandas falsas contra celebridades e empresas que estejam tentando promover um produto especifico. Até mesmo sites de avaliação podem ser explorados pelos cibercriminosos. As redes sociais também podem ser usadas para comprometer serviços. Por fim, a extorsão digital continuará usando técnicas de phishing e de engenharia social para infectar computadores e sistemas de executivos privados ou governamentais, ou para abrir uma porta para roubar dados.

As estatísticas podem ser facilmente verificadas, além da própria imprensa nacional e internacio, também no Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil (https://www.cert.br/csirts/), através dos relatórios de acompanhamento dos incidentes reportados (5723134) e dos spams reportados (5723139), além de outras ameaças conhecidas.

O parque computacional desta Secretaria, que foi levantado até a presente data, são de aproximadamente 4.300 estações de trabalho, considerando as unidades administrativas e escolares reportadas através do processo **0029.108960/2019-17**, iniciado por esta Coordenadoria em 18/03/2019, que encontra-se ainda em tramitação. Como não podemos aguardar indefinidamente a manifestação dos interessados, iremos estimar um quantitativo de 50% para futuras contratações ou aumento deste referido parque, durante a vigência desta ARP, considerando que temos processo de aquisição em andamento.

7.2. Justificativa das Quantidades Estimadas

As demandas apresentadas neste Termo de Referência constantes no **ITEM 3. ESPECIFICAÇÕES TÉCNICAS/QUANTIDADES ESTIMADAS e** foram estabelecidas,

com base na necessidade retratada no processo 0029.108960/2019-17, de responsabilidade técnica da Gerência de Infraestrutura e Suporte da Coordenadoria de Tecnologia da Informação e Comunicação – SEDUC-CTIC, bem como nas informações contidas na Solicitação de Compras – Contratação de Serviços (5671866), e sua proposição está amparada no Memo. 053/2019/SEDUC-CTIC (56712226) contendo a competente **AUTORIZAÇÃO** (6105762)do ordenador de despesas e identificação dos demais responsáveis.

7.3. Do Agrupamento dos Itens por Lote

O objeto do presente Termo de Referência a formação de Registro de Preços, para futura e eventual aquisição pela Secretaria de Estado da Educação, de Equipamentos e Materiais Permanentes e Serviços – Solução unificada de segurança para proteção de *e-mail*, proteção de *endpoint* e proteção contra ataques avançados, com garantia de **36** meses, contemplando pacote de instalação e configuração, **treinamento (hands-on)** e **operação assistida**, onde os mesmos foram agrupados em **LOTE ÚNICO**, à luz do art. 23, §1º da Lei Geral de Licitações e da Súmula nº. 8/TCE-RO, de maneira que a fragmentação em itens **acarretaria a perda do conjunto; perda da econômica de escala; redundaria em prejuízo à celeridade da licitação; ocasionaria a excessiva pulverização de contratos ou resultaria em contratos de pequena expressão econômica.**
Segundo o Doutor Marçal Justen Filho, o fracionamento [1]*"respeita limites de ordem técnica e econômica. Não se admite o fracionamento quando tecnicamente isso não for viável ou, mesmo, recomendável"*.

1. ***Do agrupamento por lote de itens que guardem homogeneidade entre si***

Nas licitações de objetos divisíveis o Tribunal de Contas da União entende que o julgamento seja feito por item, e não por preço global. Contudo, há situações em que se faz necessário aglutinar os itens com o intento de casar aquisições, visto que poderá haver um vínculo entre eles, ou se comprados separadamente prejudicarão o resultado esperado pela Administração.
Nesse caso, apesar dos objetos serem divisíveis, eles guardam estrita identidade de natureza e características semelhantes, além de guardar correspondência com sua composição, podendo ser fornecidos por um mesmo fornecedor, por se tratarem de objetos comuns ao ramo de empresa de comercialização de equipamentos eletros eletrônicos, tecnologia de informação, concretizando, assim, os princípios da competitividade.

2. ***Da fragmentação em itens acarretar a perda do conjunto***

O parcelamento do objeto somente se justifica e fundamenta quando houver viabilidade técnica e, principalmente, ganho econômico para a Administração Pública. No presente caso não há viabilidade técnica, **uma vez que a falta de um componente prejudicaria todo o conjunto**, e, de nada adiantaria ter por tratar-se de um conjunto de soluções que precisam trabalhar de forma integrada para garantir sua eficiência e compatibilidade. Ter uma gerência integrada diminui a curva do aprendizado e possibilita sua gestão com poucos colaboradores especializados o que não aconteceria caso fosse adjudicação por item. Em se tratando de segurança nas unidades administrativas e escolares, e considerando ainda que envolve alunos menores de idade, não podemos considerar o fator econômico como preponderante, mas mesmo assim entendemos que a adjudicação global, dentro da economia de escala, também possibilitará um desembolso menor dos cofres públicos do que se todos os itens fossem adquiridos de forma distinta. Podemos acrescentar também, caso a adjudicação fosse por item, quanto a dificuldade de gestão dos contratos de suporte e de sua eficiência, além da possibilidade de conflito na utilização dos recursos e sua complexidade, como por exemplo. Há necessidade que todos os itens estejam disponíveis para a instalação e utilização dos Estúdios para as gravações e transmissões das aulas do Projeto de Ensino Médio com Mediação Tecnologia nas comunidades de difícil acesso.

3. ***Da perda da economia de escala***

O § 1° do art. 23, da Lei n. 8.666/1993 determina que as compras efetuadas pela Administração sejam divididas em tantas parcelas quantas se comprovarem técnica e economicamente viáveis, procedendo-se à licitação com vistas ao melhor aproveitamento dos recursos disponíveis no mercado e à ampliação da competitividade sem perda da economia de escala.

Quanto maior a quantidade a ser comprada, maior poderá ser o desconto na compra de bens e serviços. Esse ganho está relacionado com o aumento da quantidade adquirida sem um aumento proporcional no custo e está intrinsicamente relacionado ao princípio da economicidade esculpido no art. 70 de nossa Carta Magna.

A economia de escala é definida como aquela que ocorre a partir de determinado patamar de quantidade de itens comercializados e pode acarretar relevante desconto na aquisição dos bens e serviços.

De tal modo, que no caso em tela a adoção critério de julgamento menor preço permite o melhor aproveitamento dos recursos disponíveis no mercado e a ampliação da competitividade, sem perda da economia de escala, como por exemplo, a empresa que ganhar o lote fornecerá todos os itens, acarretando, consequentemente, uma diminuição nos custos e economia de escala.

4. ***Do prejuízo à celeridade da licitação***

Um dos fatores que pode ser levado em conta na elaboração de um edital por lote é o interesse na celeridade do processo.

Neste caso, trata-se de Lote Único, com quantidades distintas, totalizando 13 (treze) itens. Assim, a aquisição de Equipamentos e Materiais Permanentes e Serviços – Solução unificada de segurança para proteção de *e-mail*, proteção de *endpoint* e proteção contra ataques avançados, com garantia de **36** meses, contemplando pacote de instalação e configuração, **treinamento (hands-on)** e **operação assistida**, *conjuntamente, por uma única empresa por lote, fica mais célere o julgamento das propostas. Caso contrário, seriam estabelecidos vários prazos entre várias empresas para conclusão do objeto contratado, e com isso, poderia haver um grande embaraço.*

5. ***Da pulverização de contratos***

A licitação por itens corresponde, na verdade, a uma multiplicidade de licitações, cada qual com existência própria e dotada de autonomia jurídica, mas todas desenvolvidas conjugadamente em um único procedimento, documentado nos mesmos autos. Esta exagerada divisão de objeto pode ocasionar uma excessiva pulverização dos contratos, tornando mais dispendiosa a contratação.

No caso em questão, a adoção do critério de julgamento menor preço global para a aquisição de Equipamentos e Materiais Permanentes e Serviços – Solução unificada de segurança para proteção de *e-mail*, proteção de *endpoint* e proteção contra ataques avançados, com garantia de **36** meses, contemplando pacote de instalação e configuração, **treinamento (hands-on)** e **operação assistida**, resultaria na contratação de 1 (uma) única empresas fornecedora/licitantes por lote, não ocorrendo a pulverização de contratos. Ainda há, com base no interesse público, maior segurança ao cumprimento do contrato.

Por fim, há que se observar o caso concreto, avaliando a conveniência e oportunidade, de modo a satisfazer da melhor forma o interesse público, pois cada contratação tem suas especificidades, in casu a aquisição por lote é mais vantajosa para a Administração, em decorrência dos riscos inerentes à própria execução, pois, não restam dúvidas, o objeto pretendido, quando executado por vários contratados, poderá não ser integralmente entregue, tendo em vista problemas na relações jurídicas mantidas com diversos contratados.

6. ***Dos contratos de pequena expressão econômica***

Em razão da adoção do critério de **menor preço global**, não será celebrado contrato de pequena expressão econômica, uma vez que apenas uma empresa fornecerá todos os itens do lote. Em caso contrário a licitação por itens sim geraria a situação de celebrar vários contratos de pequena expressão econômica.

MARIA DO CARMO DO PRADO
Pregoeiro (a) SUPEL-RO
Mat. 300131839

Como se extrai, o fracionamento dos objetos de modo global é necessário no presente caso, pois o desmembramento dos objetos poderia acarretar prejuízo ao erário, uma vez que não podemos garantir a entrega na sua totalidade, descaracterizando a funcionalidade e a finalidade da aquisição.
[1] JUSTEN FILHO, Marçal. *Comentários à Lei de Licitações e Contratos Administrativos.* 13ª Edição. Dialética. São Paulo: 2009, p.265.

8. LOCAL E PRAZO DE ENTREGA / CONDIÇÕES DE FORNECIMENTO E DE RECEBIMENTO

8.1. Local

8.1.1. A **ENTREGA** dos equipamentos, *softwares* e acessórios da solução, previstos neste termo deverão ser entregues na Diretoria de Almoxarifado e Patrimônio da Secretaria de Estado da Educação – DAP/SEDUC, na Rua dos Imigrantes, nº 1699, Bairro São Sebastião II, ao lado do IDARON, em Porto Velho-RO, de segunda à sexta-feira, no horário das 07h30m às 13h30min, **mediante prévio agendamento** junto ao DAP/SEDUC, pelos telefones: (69) 3216-5901 e (69) 3216-5923.

8.1.2. A **EXECUÇÃO** dos Serviços de Instalação, Configuração e demais necessários, descritos ou não, neste termo deverão ser realizados na sede do CONTRATANTE, na Secretaria de Estado da Educação, situada na Rua Padre Chiquinho s/n, Bairro Pedrinhas, palácio Rio Madeira, Edifício Reto 1, CEP: 76.801-468 – Porto Velho/RO, aos cuidados da Coordenadoria de Tecnologia da Informação e Comunicação – CTIC/SEDUC, nos dias e horários definidos em programação específica.

8.1.3. As entregas sem agendamento somente serão aceitas, excepcionalmente, desde que não prejudique os demais recebimentos agendados, a critério do GAP/SEDUC.

8.2. Prazo

8.2.1. Os materiais, objeto do presente termo, deverão ser entregues, no prazo de até **60** (sessenta), **dias corridos,** contados a partir do primeiro dia útil após o recebimento da Nota de Empenho – NE.

8.2.2. O prazo de entrega **somente poderá ser prorrogado** mediante o cumprimento, pela Contratada, dos seguintes requisitos cumulativos:

a) A solicitação de prorrogação protocolada dentro do prazo de entrega dos bens;

b) Comprovação documental da ocorrência de motivo imprevisível (caso fortuito, força maior ou fato do príncipe), ocorrido depois da apresentação de sua proposta, que tenha correlação direta de causa e efeito sobre a necessidade do atraso.

8.2.2.1. Não se admitirá prorrogação se:

a) o atraso ocorrer por culpa da contratada;

b)se não cumprir os requisitos do item **8.2.2**; ou

c)houver interesse público devidamente justificado nos autos que demonstre ser a escolha mais vantajosa para a administração.

8.2.2.2. Ocorrendo recusa ou atraso na entrega total ou parcial do bem, o responsável pela fiscalização do contrato se obriga por força do Art. 4º da Lei Estadual nº. 2.414/11, a produzir parecer técnico e o encaminhará ao ordenador de despesas para instauração de procedimento

administrativo, instrução dos autos para fins de penalização da contratada e inserção no "*Cadastro de Fornecedores Impedidos de Licitar e Contratar com a Administração Pública Estadual*".

8.2.3. O objeto contratado deverá ser entregue de forma integral/ ou parcial, conforme quantidade e especificações pactuadas, observando as disposições da Nota de Empenho, da Ordem de Fornecimento ou outro documento equivalente, devendo também ser acondicionado adequadamente a fim de permitir completa segurança no transporte.

8.2.4. Qualquer solicitação por parte da Contratada deverá ser dirigida ou entregue na Secretaria de Estado da Educação, situada na Rua Padre Chiquinho s/n, Bairro Pedrinhas, palácio Rio Madeira, Edifício Reto 1, CEP: 76.801-468 – Porto Velho/RO, aos cuidados da Diretoria Administrativa e Financeira – DAF/SEDUC, de segunda à sexta-feira, no horário das 7h30min às 13h30min.

8.3. Condições de Recebimento

8.3.1. O recebimento do (s) material (is) se dará da seguinte forma:

a) Provisoriamente no prazo de até 10 (dez) dias úteis, pelo responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com a especificações constantes neste Termo de Referência e na proposta, mediante termo de recebimento provisório.

b) Definitivamente no prazo de até 10 (dez) dias úteis, contados da entrega dos materiais, softwares, serviços de instalação e configuração e garantia por 36 (trinta e seis) meses **recebimento provisório,** pela comissão ou pelo servidor responsável pelo acompanhamento e fiscalização do contrato, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo circunstanciado.

8.3.2. O recebimento provisório **NÃO** liquida a despesa e **NÃO** se presta para autorizar o pagamento dos materiais/bens.

8.3.4. O recebimento provisório ou definitivo não exclui a responsabilidade civil do CONTRATADO em face da eventual existência de vícios redibitórios.

8.3.5. O objeto será rejeitado, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser reparado, corrigido ou substituído no prazo de até 15 (quinze) dias úteis, a contar da notificação da Contratada, às suas custas, sem prejuízo da aplicação das penalidades. Nesse caso, será suspenso o prazo de recebimento definitivo, até que seja sanada a situação.

8.3.6. Se a Contratada realizar a substituição, adequação e/ou reparos necessários dentro do prazo estipulado, adequando o objeto aos termos pactuados, será recebido provisoriamente e, após constatar a conformidade em face dos termos pactuados, em definitivo, no prazo de até 10 (dez) dias, pelos agentes acima mencionados.

8.3.7. Caso se verifique que não se mostra possível a adequação do objeto deste Termo de Referência ou que, mesmo depois de concedido prazo para reparações, não foi alcançado o resultado esperado, será cabível a rescisão unilateral do Contrato, com base no que dispõe o art. 77 c/c art. 78, inc. II, da Lei nº. 8.666/93, bem como a aplicação de penalidades, conforme o disposto no art. 87 da referida Lei, com abertura de processo administrativo em que se garantirá o contraditório e a ampla defesa.

9. DA DOTAÇÃO ORÇAMENTÁRIA

9.1. As despesas do presente processo correrão por conta das Atividades abaixo detalhada**,** conforme o Plano Plurianual, PPA 2016-2019 e a LOA 2019 nº 4.454, de 07 de janeiro de 2019:

PROGRAMA	AÇÃO	ESPECIFICAÇÃO	FONTE	NATUREZA DA DESPEZA
12.126.1076.	**2204**	Modernizar a Infraestrutura Tecnológica de TI na Educação	**112 Tesouro Estadual**	**33.90.39**. – Outros Serviços de Terceiros – Pessoa Jurídica. **44.90.40**. – Aquisição de Software
12.122.1015.	**2087**	Assegurar a Manutenção Administrativa da Unidade		

10. CONDIÇÕES DE PAGAMENTO (Lei 8.666/93, art. 40, XIV)

10.1. O pagamento será efetuado no prazo de até 30 (trinta) dias, contados a partir da apresentação formal da respectiva documentação, respeitada a ordem cronológica das exigibilidades, depois da liquidação da despesa:

a) Nota fiscal;

b) Termo de Recebimento Definitivo do objeto;

c) Certidão Regularidade perante a Fazenda Federal (conforme PGFN/RFB Nº 1751, de 02/10/2014);

d) Certidão Regularidade perante a Fazenda Estadual;

e) Certidão de Regularidade perante a Fazenda Municipal;

f) Certificado de Regularidade do FGTS;

g) Certidão de Regularidade perante a Justiça do Trabalho – CNDT (Lei Federal nº 12.440/2011, de 07/07/2011).

10.2. A CONTRATADA deverá emitir Notas Fiscais/Faturas relativas aos valores dos equipamentos, softwares, serviços de instalação e configuração e garantia por 36 (trinta e seis) meses, após receber cópia do Termo de Recebimento Definitivo;

10.3. **36** (trinta e seis) meses, contados da data de emissão do Termo de Recebimento Definitivo, referente à garantia e suporte técnico da solução unificada de segurança para proteção de e-mail e endpoint contra ataques avançados.

10.4. As Notas Fiscais/Faturas, emitidas em 2 (duas) vias, devendo conter no corpo da Nota Fiscal/Fatura, a descrição do objeto, o número do empenho e o número da Conta Bancária da CONTRATADA, para depósito do pagamento.

10.5. O pagamento será efetuado através de Ordem Bancária - OB e depósito em conta corrente, indicada pela Contratada.

10.6. A Nota Fiscal deverá ser emitida em nome da SECRETARIA DE ESTADO DA EDUCAÇÃO, CNPJ: 04.564.530/0001-13 – Endereço: Rua Padre Chiquinho, Bairro Pedrinhas – CEP 76.801-468 – Porto Velho/ RO - Palácio Rio Madeira, Edifício Rio Guaporé, Reto 01.

10.7. Na hipótese das Notas Fiscais/Faturas apresentarem erros ou dúvidas quanto à exatidão ou documentação, a CONTRATANTE poderá pagar apenas a parcela não controvertida no prazo fixado para pagamento, ressalvado o direito da CONTRATADA de reapresentar, para cobrança as partes controvertidas com as devidas justificativas, nestes casos a CONTRATANTE terá o prazo de 05 (cinco) dias úteis, a partir do recebimento, para efetuar uma análise e o respectivo pagamento no mesmo prazo estipulado no item **10.1**.

10.8. Demais regras, se pertinentes, relativas ao pagamento, seguirão a legislação relacionada.

11. DA HABILITAÇÃO

11.1. Habilitação Jurídica

11.1.1. Registro na Junta Comercial, no caso de empresa individual, com demonstração atualizada dos objetos sociais, indicando ramo de atividade compatível com o objeto licitado.

11.1.2. Ato Constitutivo, Estatuto ou Contrato Social ou outro instrumento equivalente, com todas as suas alterações em vigor, com a demonstração do ramo de atividades compatível com o objeto licitado, devidamente registrado ou inscrito, em se tratando de sociedades comerciais, e, no caso de sociedade por ações, acompanhado de documentos de eleição de seus administradores.

11.1.3. Inscrição do ato constituído, no caso de sociedade civis, acompanhada de prova de diretoria em exercício.

11.1.4. Decreto de autorização, em se tratando de empresa ou sociedade estrangeira em funcionamento no País e ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir.

11.1.5. Cédula de identificação dos sócios, ou do diretor, ou do proprietário, ou do representante legal da empresa, se for o caso.

11.2. Qualificação Técnica

11.2.1. O (s) Atestado (s) de Capacidade Técnica (declaração ou certidão), fornecido por pessoa jurídica de direito público e privado, comprovando o desempenho da licitante em contrato pertinente e compatível em características e quantidades com o objeto da licitação, será conforme indicado abaixo.

11.2.2. O (s) Atestado (s) emitido (s) por pessoa de direito privado deverá (rão) ter firma do emitente reconhecida em cartório competente; o (s) atestado (s) emitido (s) por pessoa de direito público deverá (rão) constar órgão, cargo e matricula do emitente (art. 6º da OT nº. 001/2017/SUPEL alterada pela OT nº. 002/2017/SUPEL);

a) Entende-se por pertinente e compatível **em características** o(s) atestado(s) que em sua individualidade ou soma, contemplem que a licitante forneceu equipamentos/materiais, objetos do presente termo de referência, conforme o (s) item (ns) que o licitante apresentar proposta;.

b) Entende-se por pertinente e compatível em **quantidade** o (s) atestado (s) que em sua individualidade ou soma de atestados, contemplem que a licitante forneceu materiais de permanentes e prestou serviços, objetos do presente termo de referência, no mínimo 2% (dois por cento) para o (s) item (ns) que o licitante apresentar proposta;

c)) Quanto à compatibilidade pertinente e compatível em prazo com o objeto desta licitação não será exigida, por não haver complexidade nesta contratação.

11.2.3. As exigências quanto aos atestados de capacidade técnica estão estabelecidas conforme art. 4º da Orientação Técnica n°. 001/2017/GAB/SUPEL, de 14/02/2017, DOE nº. 38, de 21/02/2017, retificada pela Orientação Técnica nº 002/2017/GAB/SUPEL, DE 08/03/2017, DOE n° 46, de 10/03/2017.

11.2.4. Documentos Especiais: Para esta contratação NÃO serão exigidos documentos especiais.

11.2.5. Fica a Superintendência Estadual de Licitações, por meio de sua Comissão de Licitação estabelecer no Edital a apresentação ou dispensa de Atestado de Capacidade Técnica, seguindo os critérios previstos na Orientação Técnica nº 001/2017/GAB/SUPEL, de 14/02/2017, D.O.E. nº 38, de 24/02/2017, retificada pela Orientação Técnica nº 002/2017/GAB/SUPEL, de 08/03/2017, D.O.E. nº 46, de 10/03/2017.

11.3. Qualificação Econômico-Financeira

11.3.1. Certidão (ões) Negativa (s) de Recuperação Judicial – Lei n° 11.101/05 (recuperação judicial e falência) expedida pelo órgão competente, expedida nos últimos 90 (noventa) dias, dias caso não conste o prazo de validade. NÃO DISPONIBILIZADO PELO SICAF, mas contemplado no CAGEFOR, podendo ser consultado pela Pregoeira desde que a licitante tenha cadastrado e esteja atualizado.

11.3.1.1. Na hipótese de apresentação de Certidão Positiva de recuperação judicial, o (a) Pregoeiro verificará se a licitante teve seu plano de recuperação judicial homologado pelo juízo, conforme determina o art.58 da Lei 11.101/2005.

11.3.1.2. Caso a empresa licitante não obteve acolhimento judicial do seu plano de recuperação judicial, a licitante será inabilitada, uma vez que não há demonstração de viabilidade econômica.

11.3.1. Balanço Patrimonial, referente ao exercício social, ou o Balanço de Abertura, caso a licitante tenha sido constituída em menos de um ano, devidamente autenticado ou registrado no órgão competente, para que a Pregoeira, possa aferir se esta possui Patrimônio Líquido (licitantes constituídas a mais de um ano) ou Capital Social (licitantes constituídas a menos de um ano), a não inferior a 5% (cinco por cento) do valor estimado da contratação.

11.4. Regularidade Fiscal

11.4.1. Certidão de Regularidade perante a Fazenda Federal - unificada da Secretaria da Receita Federal, da Procuradoria da Fazenda Nacional e do INSS (relativa às Contribuições Sociais - unificada pela Portaria PGFN/RFB Nº 1751, de 02 de outubro de 2014), podendo ser Certidão Negativa ou Certidão Positiva com efeitos de negativa.

11.4.2. Certidão de Regularidade perante a Fazenda Estadual, expedida na sede ou domicílio da Empresa; podendo ser Certidão Negativa ou Certidão Positiva com efeitos de negativa.

11.4.3. Certidão de Regularidade perante a Fazenda Municipal, expedida na sede ou domicílio da Empresa; podendo ser Certidão Negativa ou Certidão Positiva com efeitos de negativa.

11.4.4. Certificado de Regularidade do FGTS, admitida comprovação também por meio de "certidão positiva, com efeito, de negativa" diante da existência de débito confesso, parcelado e em fase de adimplemento.

11.5. <u>Regularização Trabalhista</u>

11.5.1. Certidão de Regularidade perante a Justiça do Trabalho – CNDT, relativa a comprovar a inexistência de débitos inadimplidos perante a Justiça do Trabalho (Art. 642-A da C.L.T.), podendo ser certidão negativa ou positiva com efeitos de negativa. Certidão expedida gratuita e eletronicamente. NÃO CONTEMPLADA PELO SICAF podendo a Pregoeira emitir via on-line caso as participantes deixem de apresentar.

11.5.2. Caso a certidão acima mencionada não indicar prazo de validade só será aceita, pela Pregoeira, se emitida nos últimos 60 (sessenta) dias corridos.

11.6. <u>Do Cumprimento do Disposto no Inciso XXXIII do Art. 7º da Constituição Federal</u>

11.6.1. Declaração de cumprimento do inciso XXXIII do art. 7º da Constituição Federal**.**

12. CONDIÇÕES CONTRATUAIS

12.1. A formalização da contratação se dará através de Contrato Administrativo, conforme disposto no Art. 62 da Lei nº. 8.666/93;

12.2. Administração convocará regularmente o interessado para aceitar ou retirar o instrumento equivalente, no prazo de 05 (cinco) dias úteis, contado da data da ciência ao chamamento, para no local indicado, firmar o instrumento de Contrato, nas condições estabelecidas no respectivo Termo de Referência e Edital de licitação sob pena de decair o direito à contratação, sem prejuízo das sanções previstas no art. 81 da Lei n.º 8.666/93;

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

12.4. É facultado à Administração, quando o convocado não assinar o termo de contrato ou não aceitar ou retirar o instrumento equivalente no prazo e condições estabelecidos, convocar os licitantes remanescentes, na ordem de classificação, para fazê-lo obedecida a ordem de classificação e examinada a aceitabilidade da proposta classificada quanto ao objeto, valor ofertado e habilitação, podendo inclusive negociar diretamente com o proponente para que seja obtido melhor preço, independentemente da cominação prevista no art. 81 da Lei n.º 8.666/93;

12.5. A recusa injustificada do licitante vencedor em receber o documento de contração, ou aceitar/retirar o instrumento equivalente dentro do prazo estabelecido pela Administração, caracteriza o descumprimento total da obrigação assumida, sujeitando-o às penalidades legalmente estabelecidas na Lei. 8.666/93 e art. 7º da Lei Federal 10.520/2002);

12.6. Toda e qualquer modificação, redução ou acréscimo nas disposições do Contrato será formalizada através de Termo Aditivo, exceto as previstas no § 8, do art. 65 da Lei 8.666/93;

12.7. Acatar, nas mesmas condições ofertadas, nos termos do art. 65, § 1º, da Lei nº 8.666/93, as solicitações da CONTRATANTE para acréscimos ou supressões que se fizerem necessárias à execução do objeto licitado; e,

12.8. É obrigação do contratado de manter, durante toda execução do contrato, em compatibilidade com as obrigações por ele assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

13. PRAZO DA VIGÊNCIA CONTRATUAL

13.1. A vigência do (s) contrato (s) será de 36 (trinta e seis) meses a contar de sua assinatura, podendo ser prorrogado, caso ocorra interesse da administração conforme Art. 57, Inciso I, da Lei 8.666/93.

14. GARANTIA CONTRATUAL

14.1. Para o integral cumprimento de todas as obrigações contratuais assumidas, inclusive indenização a terceiros e multas eventualmente aplicadas, será exigida garantia correspondente a 5% (cinco porcento) do valor total contratado, nos 20 (vinte) dias subsequentes à emissão da ordem de Serviço, em uma das modalidades do art. 56, §1º da Lei n. 8.666/93, nos termos constantes da Minuta de Contrato.

14.1.1. A CONTRATADA ficará obrigada a apresentar nova garantia sempre que necessário, seja por expirar o vencimento, alteração por aumento no valor do contrato ou outra necessidade indispensável.

14.2. Não serão aceitos instrumentos de garantia que contenham cláusulas conflitantes com dispositivos contratuais ao até mesmo restrinjam-lhe a cobertura ou a sua eficácia.

14.3. O termo de garantia será restituído à empresa licitante, após o cumprimento integral de todas as obrigações contratuais.

15. REAJUSTE CONTRATUAL

15.1. Os valores contratados serão fixos e irreajustáveis pelo período de 12 (doze) meses, de acordo com o art. 2º, da Lei Federal nº 10.192/01.

16. RESCISÃO CONTRATUAL

16.1. O Termo de Contrato poderá ser rescindido nas hipóteses previstas no art. 78 da Lei nº 8.666, de 1993, com as consequências indicadas no art. 80 da mesma Lei, sem prejuízo das sanções aplicáveis.

16.2. Os casos de rescisão contratual serão formalmente motivados, assegurando-se à CONTRATADA o direito à prévia e ampla defesa.

16.3. A CONTRATADA reconhece os direitos da CONTRATANTE em caso de rescisão administrativa prevista no art. 77 da Lei nº 8.666, de 1993.

17. ACOMPANHAMENTO E FISCALIZAÇÃO

17.1. A Secretaria de Estado da Educação, conforme os termos do art. 67, § 1º e 2º, da Lei nº. 8.666/93, designará uma equipe gestão e fiscalização representante para acompanhar e fiscalizar a execução do contrato, anotando em registro próprio todas as ocorrências relacionadas a execução do contrato, determinando o que for necessário à regularização das faltas ou defeitos observados. As decisões e providências que ultrapassarem a sua competência deverão ser solicitadas a seus superiores em tempo hábil para a adoção das medidas conveniente.

17.2. O exercício da fiscalização pela CONTRATANTE, não excluirá ou reduzirá a responsabilidade da CONTRATADA.

18. SUBCONTRATAÇÃO CESSÃO E/OU TRANSFERÊNCIA

18.1. É vedada a subcontratação, cessão e/ou transferência total ou parcial do objeto deste termo.

19. PARTICIPAÇÃO DE EMPRESAS REUNIDAS SOB A FORMA DE CONSÓRCIO

19.1. Tendo em vista que, é prerrogativa do Poder Público, na condição de contratante, a escolha da participação, ou não, de empresas constituídas sob a forma de consórcio, com as devidas justificativas, conforme se depreende da literalidade do texto da Lei Federal nº 8.666/93, art. 33 e ainda o entendimento do Acórdão TCU nº 1316/2010, que atribui à Administração a prerrogativa de admissão de consórcios em licitações por ela promovidas.

19.2. Fica vedada a participação de empresas reunidas sob a forma de consórcio, sendo que neste caso o objeto a ser licitado não envolve questões de alta complexidade técnica, ao ponto de haver necessidade de parcelamento do objeto, através da união de esforços.

20. DAS OBRIGAÇÕES CONTRATANTE

20.1. <u>São obrigações da Contratante:</u>

20.1.1. Promover o acompanhamento e a fiscalização do fornecimento dos produtos, sob o aspecto quantitativo e qualitativo, anotando em registro próprio as falhas detectadas.

20.1.2. Comunicar prontamente à Contratada, qualquer anormalidade no objeto do instrumento contratual, podendo recusar o recebimento, caso não esteja de acordo com as especificações e condições estabelecidas no Termo de Referência.

20.1.3. Notificar previamente à Contratada, quando da aplicação de sanções administrativas.

20.1.4. Realizar os atos relativos à cobrança do cumprimento pela Contratada das obrigações contratualmente assumidas e aplicar sanções, garantida a ampla defesa e o contraditório, decorrentes do descumprimento das obrigações contratuais.

20.1.5. Efetuar o pagamento à Contratada, de acordo com o estabelecido no item 8, do presente Termo de Referência.

<u>20.2. Da Contratada/Fornecedor</u>

20.2.1. Fornecer os produtos, objeto da licitação, de acordo com as especificações contidas no item **3.3** do presente Termo de Referência;

20.2.2. Fornecer os produtos nas quantidades indicadas pelo órgão requisitante em cada nota de empenho, da qual constarão: data de expedição, especificações, quantitativo, prazo, local de entrega e preços unitário e total;

20.2.3. Nos preços propostos deverão estar inclusos todos os tributos, encargos sociais, trabalhistas e financeiros, taxas, seguros, frete até o destino e quaisquer outros ônus que porventura possam recair sobre a execução do objeto da presente licitação, os quais ficarão a cargo única e exclusivamente da Contratada;

20.2.4. Entregar os produtos, objetos da licitação no local, prazo e condições determinados no **item 6 e seus subitens;**

20.2.5. Fornecer os equipamentos e softwares da solução com todos os itens acessórios necessários à sua perfeita instalação, funcionamento e integração ao ambiente computacional da **CONTRANTE**, incluindo cabos, conectores, interfaces, suportes, drivers de controle e programas de configuração;

20.2.6. Submeter à prévia aprovação da **CONTRATANTE** toda e qualquer alteração pretendida na prestação dos serviços;

20.2.7. Sujeitar-se à fiscalização da **CONTRATANTE**, no tocante ao fornecimento e a prestação dos serviços, prestando todos os esclarecimentos solicitados e atendendo de imediato às reclamações fundamentadas, caso venham a ocorrer;

20.2.8. Prestar as atividades objeto da licitação, por meio de mão de obra especializada e devidamente certificada pelos fabricantes dos equipamentos e softwares que compõem a solução;

20.2.9. Responsabilizar-se por todos os ônus referentes aos serviços objeto deste Termo de Referência, inclusive salários de pessoal, alimentação, diárias, hospedagem, transporte e seguros, bem como tudo que as leis trabalhistas e previdenciárias preveem e demais exigências legais para o exercício de sua atividade;

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

20.2.11. Indicar profissional com certificação PMP (Project Management Professional) que atuará desde o início da execução do contrato até a conclusão da implantação da solução como Gerente de Projeto;

20.2.12. Guardar inteiro sigilo dos dados que vier a ter acesso, reconhecendo serem estes de propriedade exclusiva do **CONTRATANTE**;

20.2.13. Substituir imediatamente, a critério do **CONTRATANTE**, a qualquer tempo, e sem nenhum ônus adicional, qualquer profissional do seu corpo técnico cuja presença seja considerada indesejável ou inconveniente, em virtude de comportamento inadequado devidamente justificado;

20.2.14. Arcar com todas as despesas relativas ao fornecimento e todos os tributos incidentes, devendo efetuar os respectivos pagamentos na forma e nos prazos previstos em Lei;

20.2.15. Providenciar a substituição no prazo de 05 (cinco) dias úteis, dos materiais que apresentarem problemas, sob pena de aplicação das penalidades previstas na legislação vigente;

20.2.16. Prestar todos os esclarecimentos que lhe forem solicitados pela SEDUC no concernente ao objeto do presente termo de referência, inclusive documentação e atos praticados até o recebimento definitivo e cujas reclamações formalmente realizadas obriga-se a atender prontamente;

20.2.17. Responder, integralmente, por perdas e danos que vier a causar á Contratante ou a terceiros, em razão de ação ou omissão dolosa ou culpa, sua ou dos seus prepostos, independentemente de outras cominações contratuais ou legais a que estiver sujeita;

20.2.18. Não efetuar, sob nenhum pretexto, a transferência de responsabilidade para outros, sejam fabricantes, técnicos ou quaisquer outros;

20.2.19. Prover todos os meios necessários à garantia da plena operacionalidade do fornecimento, inclusive considerados os casos de greve ou paralisação de qualquer natureza;

20.2.20. Ficam vedadas a subcontratação total ou parcial do objeto, pela contratada à outra empresa, a cessão ou transferência total ou parcial do objeto licitado;

20.2.21. Indenizar terceiros e/ou a SEDUC, mesmo em caso de ausência ou omissão de fiscalização de sua parte, pelos danos causados por sua culpa ou dolo, devendo a CONTRATADA adotar todas as medidas preventivas, com fiel observância às exigências das autoridades competentes e às disposições legais vigentes;

20.2.22. Quando nas dependências da SEDUC, manter seu pessoal identificado através de crachás, com fotografia recente;

20.2.23. O licitante vencedor se obriga a informar, para fins de recebimento de citações, intimações, ordem de serviço, e outras comunicações oficiais com a Secretaria de Estado da Educação, o nome do seu preposto, seu endereço comercial, E-mail (endereço eletrônico) e nº de telefone móvel e fixo para contato;

20.2.24. O licitante se obriga a acompanhar, permanentemente, os meios de comunicação informados e responder as comunicações encaminhadas, sob pena de revelia;

20.2.25. Manter durante toda a execução do contrato, em compatibilidade com as obrigações por ela (contratada) assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

21. DAS SANÇÕES

21.1. Além daquelas determinadas por leis, decretos, regulamentos e demais dispositivos legais, a CONTRATADA estará sujeita as sanções definidas neste Termo de Referência.

21.2. Sem prejuízo das sanções cominadas no art. 87, I, III e IV, da Lei nº 8.666/93, pela inexecução total ou parcial do instrumento de contrato, a Contratante poderá, garantida a prévia e ampla defesa, aplicar à Contratada multa (Tabela – Item 19.11), sobre a parcela inadimplida do contrato.

21.3. Se a adjudicatária recusar-se a retirar o instrumento contratual injustificadamente ou se não apresentar situação regular na ocasião dos recebimentos, garantida a prévia e ampla defesa, aplicar à Contratada **multa de até 10% (dez por cento) sobre o valor adjudicado**.

21.4. A licitante, adjudicatária ou contratada que, convocada dentro do prazo de validade de sua proposta, não celebrar o instrumento contratual, deixar de entregar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução de seu objeto, não mantiver a proposta, falhar ou fraudar na execução do instrumento contratual, comportar-se de modo inidôneo ou cometer fraude fiscal, garantida a prévia e ampla defesa, **ficará impedida de licitar e contratar com o Estado, e será descredenciado no Cadastro de Fornecedores Estadual, pelo prazo de até 05 (cinco) anos**, sem prejuízo das multas previstas no Edital e das demais cominações legais, devendo ser incluída a penalidade no SICAFI e no CAGEFIMP. (Cadastro de Fornecedores Impedidos de Licitar e Contratar com a Administração Pública Estadual).

21.5. A multa, eventualmente imposta à Contratada, será automaticamente descontada da fatura a que fizer jus, acrescida de juros moratórios de 1% (um por cento) ao mês. Caso a contratada não tenha nenhum valor a receber do Estado, ser-lhe-á concedido o prazo de 05 (cinco) dia úteis, contados de sua intimação, para efetuar o pagamento da multa. Após esse prazo, não sendo efetuado o pagamento, serão deduzidos da garantia, **caso houver**. Mantendo-se o insucesso, seus

dados serão encaminhados ao órgão competente para que seja inscrita na dívida ativa, podendo, ainda a Administração proceder à cobrança judicial.

21.6. As multas previstas nesta seção não eximem a adjudicatária ou contratada da reparação dos eventuais danos, perdas ou prejuízos que seu ato punível venha causar à Administração.

21.7. De acordo com a gravidade do descumprimento, poderá ainda a licitante se sujeitar à Declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que o contratado ressarcir a Administração pelos prejuízos resultantes e depois de decorrido o prazo da sanção aplicada com base na legislação vigente.

21.8. A sanção denominada "Advertência" só terá lugar se emitida por escrito e quando se tratar de faltas leves, assim entendidas como aquelas que não acarretarem prejuízos significativos ao objeto da contratação, cabível somente até a segunda aplicação (reincidência) para a mesma infração, caso não se verifique a adequação da conduta por parte da Contratada, após o que deverão ser aplicadas sanções de grau mais significativo.

21.9. São exemplos de infração administrativa penalizáveis, nos termos da Lei nº 8.666, de 1993, da Lei nº 10.520, de 2002, **dos Decretos Estaduais nº 12.205/06, 12.234/06 (Pregão Eletrônico e Presencial):**

a) Inexecução total ou parcial do contrato;

b) Apresentação de documentação falsa;

c) Comportamento inidôneo;

d) Fraude fiscal;

e) Descumprimento de qualquer dos deveres elencados no Edital ou no Contrato.

21.10. As sanções serão aplicadas sem prejuízo da responsabilidade civil e criminal que possa ser acionada em desfavor da Contratada, conforme infração cometida e prejuízos causados à administração ou a terceiros.

21.11. Para efeito de aplicação de multas, às infrações são atribuídos graus, com percentuais de multa conforme a tabela a seguir, que elenca apenas as principais situações previstas, não eximindo de outras equivalentes que surgirem, conforme o caso:

ITEM	DESCRIÇÃO DA INFRAÇÃO	GRAU	MULTA*
1	Permitir situação que crie a possibilidade ou cause danos físico, lesão corporal ou consequências letais; por ocorrência.	06	4,0% por dia
2	Suspender ou interromper, salvo por motivo de força maior ou caso fortuito, os fornecimentos dos bens adquiridos, por dia e por unidade de atendimento;	05	3,2% por dia
3	Recusar-se a executar as determinações feitas pela FISCALIZAÇÃO, sem motivo justificado; por ocorrência;	04	1,6% por dia
4	Destruir ou danificar documentos por culpa ou dolo de seus agentes; por ocorrência.	05	3,2% por dia
5	Executar a entrega incompleta, paliativo substitutivo como por caráter permanente, ou deixar de providenciar recomposição complementar; por ocorrência.	02	0,4% por dia

6	Inexecução total do contrato;	10	10 %
Para os itens a seguir, deixar de:			
7	Cumprir quaisquer dos itens do Termo de Referência e seus anexos, mesmo que não previstos nesta tabela de multas, após reincidência formalmente notificada pela FISCALIZAÇÃO; por ocorrência.	03	0,8% por dia
8	Cumprir determinação formal ou instrução complementar da FISCALIZAÇÃO, por ocorrência;	03	0,8% por dia
9	Iniciar a entrega nos prazos estabelecidos, observados os limites mínimos estabelecidos por este Contrato; por item, por ocorrência.	02	0,2% por dia
10	Ressarcir o órgão por eventuais danos causados por sua culpa;	02	0,4% por dia
11	Manter a documentação de habilitação atualizada; por item, por ocorrência.	01	0,2% por dia
12	Atraso na entrega do Plano de Implantação	1	0,05% por dia
13	Atraso na entrega de todos os equipamentos e acessórios da solução	1	0,1% por dia
14	Atraso na conclusão da etapa de instalação e configuração da solução.	1	0,15% por dia
15	Atraso na conclusão do serviço de transferência de conhecimento.	4	1% por dia

*** Incidente sobre a parcela inadimplida.**

21.12. As sanções aqui previstas poderão ser aplicadas concomitantemente, facultada a defesa prévia do interessado, no respectivo processo, no prazo de 05 (cinco) dias úteis.

21.13. Após 30 (trinta) dias da falta de execução do objeto, será considerada inexecução total do contrato, o que ensejará a rescisão contratual.

21.14. As sanções de natureza pecuniária serão diretamente descontadas de créditos que eventualmente detenha a CONTRATADA ou efetuada a sua cobrança na forma prevista em lei.

21.15. As sanções previstas não poderão ser relevadas, salvo ficar comprovada a ocorrência de situações que se enquadrem no conceito jurídico de força maior ou casos fortuitos, devidos e formalmente justificados e comprovados, e sempre a critério da autoridade competente, conforme prejuízo auferido.

21.16. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

21.17. A sanção será obrigatoriamente registrada no Sistema de Cadastramento Unificado de Fornecedores – SICAF, bem como em sistemas Estaduais.

21.18. Também ficam sujeitas às penalidades de suspensão de licitar e impedimento de contratar com o órgão licitante e de declaração de inidoneidade, previstas no subitem anterior, as empresas ou profissionais que, em razão do contrato decorrente desta licitação:

a) tenham sofrido condenações definitivas por praticarem, por meio dolosos, fraude fiscal no recolhimento de tributos;

b) tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

c) demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

21.19. A recusa injustificada do adjudicatário em assinar o contrato, aceitar ou retirar o instrumento equivalente, (Nota de Empenho) dentro do prazo estabelecido pela Administração, caracteriza o descumprimento total da obrigação assumida, sujeitando-se às penalidades aqui estabelecidas, além das previstas no Termo de Referência.

21.20. Na hipótese de apresentar documentação inverossímil ou de cometer fraude, o licitante poderá sofrer sem prejuízo da comunicação do ocorrido ao Ministério Público, quaisquer das sanções previstas, que poderão ser aplicadas cumulativamente.

21.21. Nenhuma sanção será aplicada sem o devido processo administrativo, que prevê defesa prévia do interessado e recurso nos prazos definidos em Lei, sendo-lhe franqueada vista ao processo.

22. APLICAÇÃO DO DECRETO ESTADUAL N°. 21.264/2016

22.1. No fornecimento do objeto, a empresa contratada deverá adotar os critérios de sustentabilidade ambiental, conforme disposições constantes no Art. 6º do Decreto Estadual nº. 21.264/2016.

23. DA APLICAÇÃO DO ART. 8º DO DECRETO ESTADUAL 21.675/2017 – COTA ME/EPP

23.1. Neste certame, para evitar a possibilidade de perda de conjunto do objeto, não serão concedidos os benefícios de até 25% (vinte e cinco por cento), para pequenas empresas, conforme Art. 8º e parágrafos, do Decreto Estadual 21.675/2017, constantes deste Termo de Referência.

24. DA ESTIMATIVA DA DESPESA

24.1. A pesquisa de mercado visando estimativa de preços será oportunamente juntada aos autos pela Superintendência Estadual de Compras e Licitações, em atendimento a competência designativa do Decreto Estadual nº 10.538, de 11/06/2003.

25. DOS CRITÉRIOS DE JULGAMENTO DAS PROPOSTAS (Lei 8.666/93, art. 40, VII)

25.1.O critério de julgamento das propostas será de **MENOR PREÇO (GLOBAL)**, em conformidade com o estabelecido no ato convocatório pela Comissão de Licitação, de acordo com a Lei nº 8.666, de 21 de junho de 1993 e suas alterações.

25.2. A empresa interessada deverá apresentar a proposta detalhada, contendo o valor individual do produto.

25.3. A empresa deverá apresentar, **juntamente com a proposta comercial**, se possível, catálogos ou folders ou prospectos e/ou folhetos em português, ofertados com descrição detalhada do modelo, marca, características, especificações técnicas e outras informações que possibilitem a avaliação ou ficha técnica do produto, contendo no mínimo as especificações constantes no item 3.3. **Das Especificações Técnicas e Quantidades Estimadas**.

25.4. A Licitante deverá apresentar ficha técnica descritiva do item e deverá conter, inclusive, a afirmação do compromisso de entrega dos produtos nas características e especificações descritas. Ficando ressalvado que a descrição a ser ofertada deverá ser o da realidade do objeto, não podendo ser cópia fiel do contido no presente aviso Especifico, salvo se este corresponder em sua integralidade às especificações requisitadas.

25.6. Demais condições conforme o Termo de Referência.

26. DO USO DO REGISTRO DE PREÇOS

Quanto à forma de contratação a que se pretende realizar, cabe-nos verificar a legislação específica acerca do Sistema de Registro de preços, sendo esta, a metodologia adotada para a pretendida contratação. A Lei 8.666/93, especificamente em seu artigo 15, diz que:

> *"§ 4º A existência de preços registrados* ***não obriga a Administração a firmar as contratações que deles poderão advir,*** *ficando-lhe facultada a utilização de outros meios, respeitada a legislação relativa às licitações, sendo assegurado ao beneficiário do registro preferência em igualdade de condições."*

Marçal Justen Filho, comentando o tema, assevera que:

> *"O sistema de Registro de Preços (SRP) é uma das mais úteis e interessantes alternativas de gestão de contratações colocada à disposição da Administração Pública. (...) A sistemática do registro de preços possibilita uma atuação rápida e imediata da Administração Pública, com observância ao princípio da isonomia e garantindo a persecução objetiva da contratação mais vantajosa."*[1]

O procedimento de registro de preços tem vistas à reduzir os custos procedimentais da aquisição, por meio da racionalização da aquisição. Salutar, neste momento, renovar a consulta à sede doutrinária, quando expressa:

> *"Consiste num procedimento especial a ser adotado, que agiliza as aquisições na área pública, permitindo que os fornecimentos sejam feitos sem grandes entraves burocráticos, adaptados às contingências da vida moderna, eliminando uma série de medidas supérfluas e desnecessárias.*
>
> *A licitação, nesse caso, destina-se a selecionar fornecedor e proposta para contratações não específicas, seriadas, que poderão ser realizadas durante certo período, por repetidas vezes, quantas vezes a administração o desejar."*[2]

Dentre os diversos argumentos que justificam a adoção dessa estratégia de compras, ressalta-se a redução do esforço administrativo para a realização de diversos processos licitatórios, sendo que a execução conjunta culmina em um único certame. Tal fato implica, **diretamente,** redução dos custos operacionais da Administração e na redução dos custos operacionais dos sistemas de controle da administração, sem prejuízo dos ditames do ordenamento acerca das contratações públicas, tal qual o sistema *just in time*, utilizado por grandes empresas e fábricas e recomendada pela Administração.

Além disso, cumpre propor menção especial ao ganho de economia de escala, que retorna em economia de recursos para os cofres públicos. Ao prospectar grandes volumes licitados, a Administração Pública amplia seu poder de compra junto aos fornecedores e consegue reduções

consideráveis de preços, fato que certamente não ocorreria se o certamente fosse de forma isolada.

Em nosso Estado, por força dos incisos I a V e § 1º, do art. 3º, do Decreto nº 18.340/2013, o Registro de Preços deve ser utilizado de forma preferencial em relação ao rito tradicional das contratações, sempre que:

> *I - quando, pelas características do bem ou serviço, houver necessidade de contratações frequentes, com maior celeridade e transparência;*
>
> *II - quando for conveniente a aquisição de bens com previsão de entregas parceladas...;*
>
> *III - quando for conveniente a aquisição de bens ou a contratação de serviços para atendimento a mais de um órgão ou entidade a programas de governo;"*
>
> *IV - quando pela natureza do objeto não for possível definir previamente o quantitativo a ser demandado pela Administração;*
>
> *V – houver expectativa futura de crédito orçamentário.*

Evidenciadas as hipóteses acima, **a não utilização** do Registro de Preços como forma de contratação, **deverá ser justificada** nos autos do processo como condição de validade dos atos (§2º, do art. 3º, do Decreto nº 18.340/2013), ou seja, **utilizar o sistema é a obrigação legal.**

Isso posto, a forma legal e mais eficiente para a presente contratação se dará mediante a formação de Registro de Preços para futura e eventual contratação do objeto.

27. VIGÊNCIA DA ATA DE REGISTRO DE PREÇOS

27.1. A Vigência da Ata de Registro de Preços será de até 12 (doze) meses, contados a partir da data de sua publicação no Diário Oficial do Estado, sendo vedada sua prorrogação.

28. GERENCIAMENTO DA ATA DE REGISTRO DE PREÇOS

28.1. A Superintendência Estadual de Compras e Licitações – SUPEL, será o órgão responsável pelos atos de administração, controle e gerenciamento da Ata de Registro de Preços, conforme Decreto Estadual nº. 18.340 de 06/11/2013.

29. UTILIZAÇÃO DA ATA E DO FORNECIMENTO ADICIONAL "CARONAS"

29.1. Poderá nos termos do artigo 26 do Decreto Estadual 18.340/13, está Ata de Registro de Preços, durante a sua vigência, poderá ser utilizada por qualquer órgão ou entidade da Administração Pública Estadual que não tenha participado do certame licitatório, mediante anuência do órgão gerenciador.

29.2. É facultada aos órgãos ou entidades municipais, distritais ou estaduais a adesão a ata de registro de preços da Administração Pública Estadual.

29.3. Caberá ao fornecedor beneficiário da Ata de Registro de Preços, observadas as condições nela estabelecidas, optar pela aceitação ou não do fornecimento decorrente da adesão, desde que não prejudique as obrigações presentes e futuras da ata, assumidas com o órgão gerenciador e órgãos participantes.

29.4. As aquisições ou contratações adicionais não poderão exceder, por órgão ou entidade, a 50% dos quantitativos dos itens do instrumento convocatório e registrados na ata de registro de preços para o órgão gerenciador e órgãos participantes.

29.5. A adesão à ata de registro de preços não poderá exceder, na totalidade, ao **DOBRO** do quantitativo de cada item registrado na ata de registro de preços para o órgão gerenciador e órgãos participantes, independentemente do número de órgãos não participantes que aderirem.

29.6. Caberá ao órgão que se utilizar da ata, verificar a vantagem econômica da adesão a este Registro de Preço.

29.7. Além das condições e as regras estabelecidas no termo do Artigo 26 do Decreto nº 18.340/2013, as adesões ao presente Registro de Preços fica condicionada ao atendimento das determinações do Tribunal de Contas do Estado de Rondônia, consolidadas no Parecer Prévio nº 07/2014 do TCE/RO, caberá ao órgão ou entidade da Administração interessado, verificar se está enquadrado nas regras do item 3.2 do PP nº 07/2014.

29.8. O cumprimento das demais determinações para fornecimentos adicionais (caronas) do Parecer Prévio Nº 07/2014/TCE-RO (comprovação da viabilidade operacional, econômica e financeira e verificação da capacitação técnica e econômica complementares) devem ser documentadas nos autos da adesão e são de responsabilidade do requisitante.

30. ALTERAÇÃO DA ATA DE REGISTRO DE PREÇOS

30.1. Os preços registrados poderão ser revistos nos termos dos Art. 21 e 22 do Decreto Estadual nº. 18.340 de 06/11/2013, observadas as disposições contidas na alínea "d" do inciso II do caput do artigo 65 da Lei 8.666/93.

31. DO SIGILO E DA INVIOLABILIDADE DAS INFORMAÇÕES

31.1. A contratada deverá manter o sigilo e a inviolabilidade, sob pena de responsabilidade, das informações de interesse da CONTRATANTE ou de terceiros de que tomar conhecimento em razão da execução contratual, devendo orientar seus empregados neste sentido. A contratada deverá observar Termo de Compromisso e Confidencialidade constante do Anexo E deste termo de referência.

32. VISTORIA

32.1. A vistoria é de caráter **facultativo,** as empresas licitantes **deverão** vistoriar as instalações da CONTRATANTE, das 9 às 12 horas, com o objetivo de conhecer todos os aspectos e características inerentes aos equipamentos, serviços e materiais necessários à perfeita execução do objeto deste Termo de Referência, bem como para o correto dimensionamento e cumprimento das obrigações e formulações e suas propostas, caso julguem conveniente. Não serão admitidas, em hipótese alguma, alegações posteriores de desconhecimento dos serviços e de dificuldades técnicas não previstas.

32.2. A vistoria técnica deverá ocorrer por horário marcado, e será agendada por meio do telefone (69) 3216-5333, junto da Gerência de Infraestrutura e Suporte - SEDUC-GIS .

32.3. A vistoria deverá ser previamente agendada com a Equipe Técnica da Coordenadoria de Tecnologia da Informação e Comunicação -CTIC, por meio de contato dos telefones

(69) 3216-5333/5367, o agendamento de vistoria deverá ocorrer **até 48 (quarenta e oito)** horas antes da data e horário de abertura do processo licitatório.

32.4. A vistoria técnica deverá ser realizada em até, no máximo, 24 (vinte e quatro) horas da abertura do processo licitatório

33. DA MARGEM DE PREFERÊNCIA PARA PRODUTOS MANUFATURADOS NACIONAIS

Será assegurada margem de preferência normal e adicional de 10%, de acordo com o disposto no Decreto n. 8.184, de 17 de janeiro de 2014, para os produtos manufaturados nacionais, nos termos do disposto no art. 3º da Lei nº 8.666, de 21 de junho de 1993, cujos cálculos partirão da seguinte fórmula:

PM = PE x (1+M), sendo:

PM = preço com margem;

PE = menor preço ofertado do produto manufaturado estrangeiro;

M = margem de preferência em percentual

As margens de preferências normal e adicional serão aplicadas para os produtos manufaturados nacionais, conforme Processo Produtivo Básico aprovado nos termos do Decreto-Lei nº 288, de 28 de fevereiro de 1967 e da Lei nº 8.248 de 23 de outubro de 1991 e que atendam os requisitos e os critérios definidos na Portaria Interministerial MDIC/MCTI nº 383, de 26 de abril de 2013.

As margens de preferência não serão aplicadas caso o preço mais baixo ofertado seja de produto manufaturado nacional e sua aplicação fica condicionada ao cumprimento do disposto no § 9º do art. 3º da Lei n. 8.666, de 1993.

Caso a licitante da proposta classificada em primeiro lugar seja inabilitado, haverá a reclassificação das propostas, para fins de aplicação da margem de preferência.

A aplicação da margem de preferência não excluirá o direito de preferência das microempresas e empresas de pequeno porte, de que tratam os artigos 44 e 45 da Lei complementar n° 123 de 14 de dezembro de 2006.

34. DAS CONDIÇÕES GERAIS

34.1. A contratante poderá realizar acréscimo ou supressões nas quantidades inicialmente previstas respeitados os limites do artigo 65, § 1º, da Lei 8.666/93 e suas alterações, tendo como base os preços constantes da (s) proposta (s) da (s) Contratada (s).

35. DOS ANEXOS

35.1. ANEXO I - Minuta do Contrato

ANEXO I DO TERMO DE REFERÊNCIA

MINUTA DO CONTRATO

CONTRATO Nº _____/PGE_____.

CONTRATO QUE ENTRE SI CELEBRAM A SECRETARIA DE EDUCAÇÃO DO ESTADO DE RONDÔNIA E A EMPRESA _____(nome)_____, PARA OS FINS QUE SE ESPECIFICA

Aos ___ dias do mês de _____ do ano de _____, **A Secretaria de Estado da Educação – SEDUC/RO, situado na Rua: Pe. Chiquinho S/N, Bairro Pedrinhas, no PALÁCIO RIO MADEIRA, Edifício Rio Guaporé – Reto 1, CEP: 76.801-468, Porto Velho/RO,** doravante denominada apenas CONTRATANTE, neste ato representado pelo _____, RG n.º ___(***número***)___, CPF ___(***número***)___, e a firma _____, CNPJ/MF n.º ___, estabelecida no ___, em ___, doravante denominada **CONTRATADA**, neste ato representada pelo Sr. _____, (***nacionalidade***), RG ___, CPF _____, residente e domiciliado na _____, celebram o presente Contrato, decorrente do **PROCESSO ADMINISTRATIVO Nº**. _____ que deu origem ao **Pregão,** na forma **Eletrônica,** de **Nº.** _____, homologado pela Autoridade Competente, regido pela Lei Federal nº. 10.520/2002, Decreto Estadual nº. 12.205, de 02/06/2006, aplicando-se, subsidiariamente, no que couber, a Lei Federal nº. 8.666/93, com suas alterações e legislação correlata, sujeitando-se às normas dos supramencionados diplomas legais, mediante as cláusulas e condições a seguir estabelecidas:

1. CLÁUSULA PRIMEIRA - DO OBJETO

Constitui o objeto do presente Termo de Referência, Aquisição de Equipamentos e Materiais Permanentes e Serviços – Solução unificada de segurança para proteção de *e-mail*, proteção de *endpoint* e proteção contra ataques avançados, com garantia de **36** meses, contemplando pacote de instalação e configuração, **treinamento (hands-on)** e **operação assistida**, por meio de formação de registro de preços, para futuras e eventuais aquisições, conforme condições, quantidades e exigências estabelecidas neste instrumento.

1.2. As **especificações e quantidade estimadas do** objeto desse contrato, estão previstas no **Item 3.3 do Termo de Referência**

ITEM	DESCRIÇÃO DO OBJETO	UNIDADE DE MEDIDA	QUANTIDADE SOLICITADA
1	SOLUÇÃO DE SEGURANÇA	UNIDADE	4.300

MARIA DO CARMO DO PRADO
Pregoeiro (a) SUPEL-RO
Mat. 300131839

	PARA DESKTOPS (ENDPOINT), com garantia de 36 meses.		
2	**SOLUÇÃO DE SEGURANÇA COMPLETA PARA DESKTOPS (COMPLETA),** com garantia de 36 Meses.	**UNIDADE**	4.300
3	**SOLUÇÃO DE SEGURANÇA PARA AMBIENTE VIRTUALIZADO, DATACENTER E NUVEM,** com garantia de 36 Meses.	**UNIDADE**	150
4	**SOLUÇÃO DE PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS,** com garantia de 36 meses.	**UNIDADE**	02
5	**SOLUÇÃO DE SANDBOX (ANÁLISE DE DIA ZERO),** com garantia de 36 meses.	**UNIDADE**	02
6	**SOLUÇÃO DE ANTI-SPAM (GATEWAY DE E-MAIL) ,** com garantia de 36 meses.	**UNIDADE**	4.300
7	**SOLUÇÃO DE PROTEÇÃO WEB(FILTROWEB) ,** com garantia de 36 meses.	**UNIDADE**	4.300
8	**SOLUÇÃO DE PREVENÇÃO DE INTRUSÃO DE PROXIMA GERAÇÃO (NGIPS) - 1 GB,** com garantia de 36 meses.	**UNIDADE**	02
9	**NGIPS EXPANÇÃO DE LICENÇA 2 Gbps(Upgrade 1,5Gbps IPS + 500Mbps SSL) - REFERENTE AO ITEM NGIPS,** com garantia de 36 meses.	**UNIDADE**	02
10	**PACOTES DE INSTALAÇÃO E CONFIGURAÇÃO (serviços)**	**UNIDADE**	20
11	**TREINAMENTO (HANDS-ON) - 30 HORAS CADA**	**UNIDADE**	03
12	**OPERAÇÃO ASSISTIDA/HORAS (suporte técnico)**	**HORAS**	2.000

1.3. O detalhamento do objeto é apresentado no **subitem 3.4.** e seguintes – Termo de Referência e seus anexos, os quais aderem a este contrato e dele fazem parte, independentemente de transcrição.

2. CLÁUSULA SEGUNDA – DA JUSTIFICATIVA DAS QUANTIDADES

2.1. As informações quanto as quantidades estimadas do objeto do presente contrato, estão previstas no **item 5, subitem 5.2 do Termo de Referência, Anexo I do Edital**

3. CLÁUSULA TERCEIRA– DO LOCAL E PRAZO DE EXECUÇÃO DE RECEBIMENTO

3.1. As informações do Local de Entrega/Execução estão previstas no **item 6, subitem 6.1 do Termo de Referência, Anexo I do Edital.**

3.2. As informações do Prazo de Entrega/Cronograma de Execução estão previstas no **item 6, subitem 6.2 do Termo de Referência, Anexo I do Edital.**

3.3. As informações das Condições de Recebimento estão previstas no **Item 6, subitem 6.3 do Termo de Referência, Anexo I do Edital.**

4. CLÁUSULA QUARTA – DA DOTAÇÃO ORÇAMENTÁRIA

4.1. As despesas do presente processo correrão por conta das Atividades abaixo detalhada**,** conforme o Plano Plurianual, PPA 2016-2019 e a LOA 2019 nº 4.454, de 07 de janeiro de 2019:

PROGRAMA	AÇÃO	ESPECIFICAÇÃO	FONTE	NATUREZA DA DESPEZA
12.126.1076.	**2204**	Modernizar a Infraestrutura Tecnológica de TI na Educação	**112 Tesouro Estadual**	**33.90.39**. – Outros Serviços de Terceiros – Pessoa Jurídica. **44.90.40**. – Aquisição de Software
12.122.1015.	**2087**	Assegurar a Manutenção Administrativa da Unidade		

5. CLÁUSULA QUINTA – DAS CONDIÇÕES DE PAGAMENTO

5.1. As condições de pagamento estão previstas no **item 10 do Termo de Referência, Anexo I do Edital.**

6. CLÁUSULA SEXTA – DAS CONDIÇÕES CONTRATUAIS

6.1. A formalização da contratação se dará através de Contrato Administrativo, conforme disposto no Art. 62 da Lei nº. 8.666/93.

6.2. A Administração convocará regularmente o interessado para aceitar ou retirar o instrumento equivalente, no prazo de 05 (cinco) dias úteis, contado da data da ciência ao chamamento, para no local indicado, firmar o instrumento de Contrato, nas condições estabelecidas no respectivo Termo de Referência e Edital de licitação sob pena de decair o direito à contratação, sem prejuízo das sanções previstas no art. 81 da Lei n. º 8.666/93.

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

6.4. É facultado à Administração, quando o convocado não assinar o termo de contrato ou não aceitar ou retirar o instrumento equivalente no prazo e condições estabelecidos, convocar os licitantes remanescentes, na ordem de classificação, para fazê-lo obedecida a ordem de classificação e examinada a aceitabilidade da proposta classificada quanto ao objeto, valor ofertado e habilitação, podendo inclusive negociar diretamente com o proponente para que seja obtido melhor preço, independentemente da cominação prevista no art. 81 da Lei n.º 8.666/93.

6.5. A recusa injustificada do licitante vencedor em receber o documento de contração, ou aceitar/retirar o instrumento equivalente dentro do prazo estabelecido pela Administração, caracteriza o descumprimento total da obrigação assumida, sujeitando-o às penalidades legalmente estabelecidas na Lei. 8.666/93 e art. 7º da Lei Federal 10.520/2002.

6.6. A(s) licitantes vencedora(s) deverão apresentar:

a) Certificado CERTICS válido, na forma do §3º do art. 8º da Portaria n. 555, de 2013, do Ministério da Ciência, Tecnologia e Inovação;

b) Portaria Interministerial que atesta a habilitação aos incentivos da Lei n. 8.248, de 1991 ou Resolução do Conselho de Administração da Superintendência da Zona Franca de Manaus – Suframa que atesta a habilitação aos incentivos do Decreto-Lei n. 288, de 1967;

Nota: A documentação elencada nesta alínea "f" ou "g" somente será exigida da licitante que declarar, durante a fase de cadastramento da proposta, que o produto ofertado atende ao Processo Produtivo Básico aprovado nos termos das legislações supramencionadas.

c) Declaração comprometendo-se a prestar garantia e suporte técnico de, no mínimo, 36 (trinta e seis) meses a contar da data de recebimento do Termo de Recebimento Definitivo.

6.7. Toda e qualquer modificação, redução ou acréscimo nas disposições do Contrato será formalizada através de Termo Aditivo, exceto as previstas no § 8, do art. 65 da Lei 8.666/93.

6.8. O contratado fica obrigado a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

6.9. É obrigação do contratado de manter, durante toda execução do contrato, em compatibilidade com as obrigações por ele assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

7. CLÁUSULA SÉTIMA – DO PRAZO DE VIGÊNCIA CONTRATUAL

7.1. O prazo de vigência do contrato será de até 36 (trinta e seis) meses contados da data de assinatura do contrato, podendo ser prorrogado na forma do art. 57, § 1º, da Lei nº. 8.666/93.

8. CLÁUSULA OITAVA – DA GARANTIA CONTRATUAL

8.1. Para o integral cumprimento de todas as obrigações contratuais assumidas, inclusive indenização a terceiros e multas eventualmente aplicadas, será exigida garantia correspondente a 5% (cinco porcento) do valor total contratado, nos 20 (vinte) dias subsequentes à emissão da ordem de Serviço, em uma das modalidades do art. 56, §1º da Lei n. 8.666/93, nos termos constantes da Minuta de Contrato.

8.1.1. A CONTRATADA ficará obrigada a apresentar nova garantia sempre que necessário, seja por expirar o vencimento, alteração por aumento no valor do contrato ou outra necessidade indispensável.

8.2. Não serão aceitos instrumentos de garantia que contenham cláusulas conflitantes com dispositivos contratuais ao até mesmo restrinjam-lhe a cobertura ou a sua eficácia.

8.3. O termo de garantia será restituído à empresa licitante, após o cumprimento integral de todas as obrigações contratuais.

9. CLÁUSULA NONA – DO REAJUSTE CONTRATUAL

9.1. Os valores contratados serão fixos e irreajustáveis pelo período de 12 (doze) meses, de acordo com o art. 2º, da Lei Federal nº 10.192/01 contados da assinatura inicial do termo, ou do último reajuste.

10. CLÁUSULA DÉCIMA - DA RESCISÃO CONTRATUAL

10.1. O Termo de Contrato poderá ser rescindido nas hipóteses previstas no art. 78 da Lei nº 8.666, de 1993, com as consequências indicadas no art. 80 da mesma Lei, sem prejuízo das sanções aplicáveis.

10.2. Os casos de rescisão contratual serão formalmente motivados, assegurado-se à CONTRATADA o direito à prévia e ampla defesa.

10.3. A CONTRATADA reconhece os direitos da CONTRATANTE em caso de rescisão administrativa prevista no art. 77 da Lei nº 8.666, de 1993.

11. CLÁUSULA DÉCIMA PRIMEIRA – DO ACOMPANHAMENTO E FISCALIZAÇÃO

11.1. A Secretaria de Estado da Educação, conforme os termos do art. 67, § 1º e 2º, da Lei nº. 8.666/93, designará um representante para acompanhar e fiscalizar a execução do contrato, anotando em registro próprio todas as ocorrências relacionadas a execução do contrato, determinando o que for necessário à regularização das faltas ou defeitos observados. As decisões e providências que ultrapassarem a sua competência deverão ser solicitadas a seus superiores em tempo hábil para a adoção das medidas conveniente.

11.2. O exercício da fiscalização pela CONTRATANTE, não excluirá ou reduzirá a responsabilidade da CONTRATADA.

12. CLÁUSULA DÉCIMA SEGUNDA – DA SUBCONTRATAÇÃO CESSÃO E/OU TRANSFERÊNCIA

12.1. É vedada a subcontratação, cessão e/ou transferência total ou parcial do objeto deste termo.

13. CLÁUSULA DÉCIMA TERCEIRA – DAS OBRIGAÇÕES DAS PARTES

13.1. As obrigações da Contratante, são aquelas estabelecidas no I**tem 20, subitem 20.1, do Termo de Referência, Anexo I do Edital.**

13.2. As obrigações da Contratada, são aquelas estabelecidas no I**tem 20, subitem 20.2 do Termo de Referência, Anexo I do Edital.**

14. CLÁUSULA DÉCIMA QUARTA – DAS SANÇÕES

14.1. As sanções aplicáveis na execução do contrato são aquelas estabelecidas no **item 21 do Termo de Referência, Anexo I do Edital.**

15. CLÁUSULA DÉCIMA QUINTA –DO PREÇO

15.1. O valor total da contratação é de R$ 0,00 (VALOR POR EXTENSO), que corresponde à nota de empenho, a servir de lastro, para efetuar o pagamento dos bens/materiais referidos na cláusula primeira, tudo depois de recebidos, testados e aprovados pela CONTRATANTE. Sob nenhuma hipótese o valor mencionado será reajustado;

15.2. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

16. CLÁUSULA DÉCIMA SEXTA – DAS ALTERAÇÕES

16.1. Eventuais alterações contratuais reger-se-ão pela disciplina do art. 65 da Lei nº 8.666, de 1993.

16.2. A CONTRATADA é obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do Contrato.

16.3. As supressões resultantes de acordo celebrado entre as partes contratantes poderão exceder o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do Contrato.

16.4. O descumprimento de qualquer Cláusula ou de simples condição deste Contrato, assim como a execução do seu objeto em desacordo com o estabelecido em suas Cláusulas e Condições, dará direito à CONTRATANTE de rescindi-lo mediante notificação expressa, sem que caiba à CONTRATADA qualquer direito, exceto o de receber o estrito valor correspondente ao fornecimento realizado, desde que estejam de acordo com as prescrições ora pactuadas, assegurada a defesa prévia.

16.5. Este Contrato poderá, ainda, ser rescindido nos seguintes casos:

16.5.1. Decretação de falência, pedido de concordata ou dissolução da CONTRATADA;

16.5.2. Alteração do Contrato Social ou a modificação da finalidade ou da estrutura da CONTRATADA, que, a juízo da CONTRATANTE, prejudique a execução deste pacto;

16.5.3. Transferência dos direitos e/ou obrigações pertinentes a este Contrato, sem prévia e expressa autorização da CONTRATANTE;

16.5.4. Cometimento reiterado de faltas, devidamente anotadas;

16.5.5. No interesse da CONTRATANTE, mediante comunicação com antecedência de 05 (cinco) dias corridos, com o pagamento dos serviços adquiridos até a data comunicada no aviso de rescisão;

16.5.6. No caso de descumprimento da legislação sobre trabalho de menores, nos termos do disposto no inciso XXXIII do Art. 7º da Constituição Federal.

17. CLÁUSULA DÉCIMA SÉTIMA - DA FRAUDE E CORRUPÇÃO

17.1. A CONTRATADA deverá observar os mais altos padrões éticos durante a execução do Contrato, estando sujeitas às sanções previstas na legislação brasileira.

18. CLÁUSULA DÉCIMA OITAVA - DOS CASOS OMISSOS

18.1. Rege-se este instrumento pelas normas e diretrizes estabelecidas na Lei Federal n° 8.666/93, e outros preceitos de direito público, aplicando-se supletivamente os princípios da teoria geral dos contratos e disposições de direito privado.

19. CLÁUSULA DÉCIMA NONA – DAS RESPONSABILIDADES

19.1. A CONTRATADA assume como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução das obrigações contratadas. Responsabiliza-se, também, pela idoneidade e pelo comportamento de seus empregados, prepostos ou subordinados, e, ainda, por quaisquer prejuízos que sejam causados à CONTRATANTE ou terceiros.

19.2. A CONTRATANTE não responderá por quaisquer ônus, direitos ou obrigações vinculadas à legislação tributária, trabalhista, previdenciária ou securitária, e decorrentes da execução do presente Contrato, cujo cumprimento e responsabilidade caberão, exclusivamente, à CONTRATADA.

19.3. A CONTRATANTE não responderá por quaisquer compromissos assumidos pela CONTRATADA com terceiros, ainda que vinculados à execução do presente Contrato, bem como por qualquer dano causado a terceiros em decorrência de ato da CONTRATADA, de seus empregados, prepostos ou subordinados.

19.4. A CONTRATADA manterá, durante toda a execução do Contrato, as condições de habilitação e qualificação que lhe foram exigidas na contratação.

20. CLÁUSULA VIGÉSIMA – DA PUBLICAÇÃO

20.1. Após as assinaturas deste Contrato a Procuradoria Geral do Estado providenciará a publicação de resumo no Diário Oficial do Estado, sem prejuízo de outras publicações que a CONTRATANTE tenha como necessárias.

21. CLÁUSULA VIGÉSIMA PRIMEIRA - DO FORO

21.1. As questões decorrentes da execução deste Instrumento que não possam ser dirimidas administrativamente serão processadas e julgadas no Foro de Porto Velho, capital do Estado de Rondônia, que prevalecerá sobre qualquer outro, por mais privilegiado que seja para dirimir quaisquer dúvidas oriundas do presente Contrato.

22. CLÁUSULA VIGÉSIMA SEGUNDA – DAS DISPOSIÇÕES FINAIS

22.1. Declaram as partes que este Contrato corresponde à manifestação final, completa e exclusiva do acordo entre elas celebrado.

Para firmeza e como prova do acordado, o presente Contrato foi lavrado em 02 (duas) vias de igual teor, que constitui o documento de fls. _____/_____, do Livro Especial nº _____/ Contrato, o qual, depois de lido e achado conforme, vai assinado pelas partes, dele sendo extraídas as cópias que se fizerem necessárias para sua publicação e execução, devidamente certificadas pela Procuradoria Geral do Estado. Porto Velho-RO, _____ de _____ de _____.

_____ Representante / Contratada		_____ Representante / Contratante

MARIA DO CARMO DO PRADO
Pregoeiro (a) SUPEL-RO
Mat. 300131839

ANEXO II DO EDITAL – QUADRO ESTIMATIVO DE PREÇOS

SUBITEM	DESCRIÇÃO	UNID	QUANT.	SUBTOTAL GERAL
1	SOLUÇÃO DE SEGURANÇA PARA DESKTOPS (ENDPOINT), com garantia de 36 meses.	**UNID**	**4.300**	**R$ 1.095.382,00**
2	SOLUÇÃO DE SEGURANÇA COMPLETA PARA DESKTOPS (COMPLETA), com garantia de 36 Meses.	**UNID**	**4.300**	**R$ 2.119.298,00**
3	SOLUÇÃO DE SEGURANÇA PARA AMBIENTE VIRTUALIZADO, DATACENTER E NUVEM, com garantia de 36 Meses.	**UNID**	**150**	**R$ 781.902,00**
4	SOLUÇÃO DE PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS, com garantia de 36 meses.	**UNID**	**2**	**R$ 1.077.550,00**
5	SOLUÇÃO DE SANDBOX (ANÁLISE DE DIA ZERO), com garantia de 36 meses.	**UNID**	**2**	**R$ 1.050.290,00**
6	SOLUÇÃO DE ANTI-SPAM (GATEWAY DE E-MAIL) , com garantia de 36 meses.	**UNID**	**4.300**	**R$ 567.600,00**
7	SOLUÇÃO DE PROTEÇÃO WEB(FILTROWEB) , com garantia de 36 meses.	**UNID**	**4.300**	**R$ 369.671,00**
8	SOLUÇÃO DE PREVENÇÃO DE INTRUSÃO DE PROXIMA GERAÇÃO (NGIPS) - 1 GB, com garantia de 36 meses.	**UNID**	**2**	**R$ 1.859.519,34**
9	NGIPS EXPANÇÃO DE LICENÇA 2 Gbps(Upgrade 1,5Gbps IPS + 500Mbps SSL) - REFERENTE AO ITEM NGIPS, com garantia de 36 meses.	**UNID**	**2**	**R$ 1.016.339,34**
10	PACOTES DE INSTALAÇÃO E CONFIGURAÇÃO (serviços)	**UNID**	**20**	**R$ 497.130,00**
11	TREINAMENTO (HANDS-ON) - 30 HORAS CADA	**UNID**	**3**	**R$ 36.000,00**
12	OPERAÇÃO ASSISTIDA/HORAS (suporte técnico)	**HORAS**	**2.000**	**R$ 300.000,00**
VALOR TOTAL				**R$ 10.770.681,68**

MARIA DO CARMO DO PRADO
Pregoeiro (a) SUPEL-RO
Mat. 300131839

ANEXO III DO EDITAL
MINUTA DA ATA DE REGISTRO DE PREÇOS

MINUTA DA ATA DE REGISTRO DE PREÇOS PARA AQUISIÇÃO DE EQUIPAMENTOS E MATERIAIS PERMANENTES E SERVIÇOS – SOLUÇÃO UNIFICADA DE SEGURANÇA PARA PROTEÇÃO DE E-MAIL, PROTEÇÃO DE ENDPOINT E PROTEÇÃO CONTRA ATAQUES AVANÇADOS, COM GARANTIA DE 36 MESES, CONTEMPLANDO PACOTE DE INSTALAÇÃO E CONFIGURAÇÃO, TREINAMENTO (HANDS-ON) E OPERAÇÃO ASSISTIDA.

ATA DE REGISTRO DE PREÇOS: N° ____/2019/SUPEL

PREGÃO ELETRÔNICO: Nº 290/2019/SUPEL/RO.
PROCESSO: Nº 0029.173574/2019-04

Pelo presente instrumento, o Estado de Rondônia, através da SUPERINTENDÊNCIA ESTADUAL DE COMPRAS E LICITAÇÕES – SUPEL situada à AVENIDA FARQUAR, S/N – BAIRRO PEDRINHAS – COMPLEXO RIO MADEIRA, Ed. Curvo 3 – Rio Jamari 1º Andar, Porto Velho/RO, neste ato representado pelo **Superintendente da SUPEL**, Senhor Márcio Rogério Gabriel e a empresa qualificada no Anexo Único desta Ata, resolvem **REGISTRAR O PREÇO** nas quantidades estimadas no Anexo Único desta ata, atendendo as condições previstas no instrumento convocatório e as constantes nesta Ata de Registro de Preços, sujeitando-se as partes às normas constantes da Lei nº. 8.666/93 e suas alterações, Decreto Estadual nº 18.340/13 e suas alterações e em conformidade com as disposições a seguir:

1. DO OBJETO

Registro de preço de aquisição de equipamentos e materiais permanentes e serviços – solução unificada de segurança para proteção de e-mail, proteção de endpoint e proteção contra ataques avançados, com garantia de 36 meses, contemplando pacote de instalação e configuração, treinamento (hands-on) e operação assistida, conforme especificação completa do Termo de Referência – Anexo I deste Edital.

2. DA VIGÊNCIA

2.1. O presente Registro de Preços terá validade de 12 (doze) meses, contados a partir de sua publicação no Diário Oficial do Estado.

2.1.1. A vigência dos contratos decorrentes do Sistema de Registro de Preços será definida nos instrumentos convocatórios, observado o artigo 57 da Lei 8.666, de 1993, conforme Decreto Estadual nº 18.340/13.

3. DA GERÊNCIA DA PRESENTE ATA DE REGISTRO DE PREÇOS

3.1. Caberá à Superintendência Estadual de Compras e Licitações – SUPEL a condução do conjunto de procedimentos do certame para registro de preços e gerenciamento da Ata dele recorrente (Decreto 18.340/13 artigo 5º, incisos VII e VIII). No entanto, a alocação de recursos, empenhamento, análise do mérito das quantidades adquiridas, bem como a finalidade pública na utilização dos materiais e serviços são de responsabilidade exclusiva do ordenador de despesas do órgão requisitante.

4. DA ESPECIFICAÇÃO, QUANTIDADE E PREÇO

4.1. O preço, a quantidade, o fornecedor e a especificação do item registrado nesta Ata, encontram-se indicados no Anexo I deste instrumento.

5. PRAZOS E CONDIÇÕES DE FORNECIMENTO

A DETENTORA do registro de preços se obriga, nos termos do Edital e deste instrumento, a:

5.1. Retirar a Nota de Empenho junto ao órgão solicitante no prazo de até 05 (cinco) dias, contados da convocação;

5.2. Iniciar o fornecimento do objeto dessa Ata, conforme prazo estabelecido no Termo de Referência e edital de licitações.

5.3. Não será admitida a entrega pela detentora do registro, de qualquer item, sem que esta esteja de posse da respectiva nota de empenho, liberação de fornecimento, ou documento equivalente.

5.4. O objeto e/ou serviço desta ata deverá ser fornecido parcialmente durante a vigência da ata ou contrato, de acordo com as necessidades dos órgãos requerentes, nas quantidades solicitadas pelos mesmos.

6. DO PRAZO E LOCAL DE ENTREGA

6.1. No recebimento e aceitação de qualquer item, objeto desta Ata de Registro de Preços, serão observadas as especificações contidas no instrumento convocatório.

6.2. Expedida a Nota de Empenho, o recebimento de seu objeto ficará condicionado a observância das normas contidas no art. 40, inciso XVI, c/c o art. 73 inciso II, “a” e “b”, da Lei 8.666/93 e alterações.

6.3. PRAZO DE ENTREGA: O prazo de entrega dos equipamentos deverá ser de até **60 (sessenta) dias**, contados a partir do primeiro dia útil após o recebimento da Nota de Empenho – NE, conforme subitem 8.2.1 do Termo de Referência – Anexo I do Edital.

6.4. LOCAL/EXECUÇÃO/HORÁRIOS: Os materiais, objeto da presente Licitação, deverão ser entregues com frete CIF, no (s) seguinte (s) local (is): Deverão ser entregues na Diretoria de Almoxarifado e Patrimônio da Secretaria de Estado da Educação – DAP/SEDUC, na Rua dos Imigrantes, nº 1699, Bairro São Sebastião II, ao lado do IDARON, em Porto Velho-RO, de segunda à sexta-feira, no horário das 07h30m às 13h30min, **mediante prévio agendamento** junto ao DAP/SEDUC, pelos telefones: (69) 3216-5901 e (69) 3216-5923, A **EXECUÇÃO** dos Serviços de Instalação, Configuração e demais necessários, descritos ou não, neste termo deverão ser realizados na sede do CONTRATANTE, na Secretaria de Estado da Educação, situada na Rua Padre Chiquinho s/n, Bairro Pedrinhas, palácio Rio Madeira, Edifício Reto 1, CEP: 76.801-468 – Porto Velho/RO, aos cuidados da Coordenadoria de Tecnologia da Informação e Comunicação – CTIC/SEDUC, nos dias e horários definidos em programação específica, conforme subitem 8.1 do Termo de Referência – Anexo I do Edital.

7. DAS CONDIÇÕES DE PAGAMENTO

7.1. A empresa detentora da Ata apresentará a Gerência Financeira do Órgão requisitante a nota fiscal referente ao fornecimento efetuado.

7.2. O respectivo Órgão terá o prazo de 10 (dez) dias úteis, a contar da apresentação da nota fiscal para aceitá-la ou rejeitá-la.

7.3. A nota fiscal não aprovada será devolvida à empresa detentora da Ata para as necessárias correções, com as informações que motivaram sua rejeição, contando-se o prazo estabelecido no subitem 7.2. a partir da data de sua reapresentação.

7.4. A devolução da nota fiscal não aprovada, em hipótese alguma, servirá de pretexto para que a empresa detentora da Ata suspenda quaisquer fornecimentos.

7.5. O Estado de Rondônia, através dos órgãos requisitantes, providenciará o pagamento no prazo de até 30 (trinta) dias corridos, contada da data do aceite da nota fiscal.

8. DA DOTAÇÃO ORÇAMENTÁRIA

8.1. A despesa correrá à conta dos orçamentos informados no Termo de Referência e edital de licitações. Os órgãos participantes poderão celebrar contratos, emitir notas de empenho ou instrumento equivalente, dependendo dos valores envolvidos, conforme previsto no artigo 62 da Lei 8.666/93.

9. DAS SANÇÕES NO CASO DE INADIMPLÊNCIA E DO CANCELAMENTO DO REGISTRO DE PREÇOS

9.1. Cobrança pelo Estado, por via administrativa ou judicial, de multa equivalente a 1% (um por cento) do valor estimado pelo item ofertado.

9.2. Suspensão temporária ao direito de licitar e impedimento de contratar com o Estado de Rondônia e cancelamento de seu Certificado de Registro Cadastral no Cadastro de Fornecedores do

Estado de Rondônia, conforme período determinado na Lei 8.666/93 e 10.520/00, de acordo com a modalidade de licitação.

9.3. Salvo ocorrência de caso fortuito ou de força maior, devidamente justificada e comprovada, o não cumprimento, por parte da empresa detentora da Ata, das obrigações assumidas, ou a infringência de preceitos legais pertinentes, ensejará a aplicação, segundo a gravidade da falta, das seguintes penalidades:

9.3.1. Advertência, sempre que for constatada irregularidade de pouca gravidade, para as quais tenha a Contratada concorrida diretamente, ocorrência que será registrada no Cadastro de Fornecedores do Estado de Rondônia;

9.3.2. Multa de 0,2% (dois décimos por cento) ao dia, por atraso no fornecimento e por entrega em desacordo com as especificações estabelecidas neste Edital, até o décimo dia corrido;

9.3.3. Multa de 10% (dez por cento), na hipótese de inexecução parcial ou total de cada Nota de Empenho, calculada sobre o valor total da inadimplência ou na hipótese do não cumprimento de qualquer das obrigações assumidas;

9.4. As multas serão, após regular processo administrativo, descontadas dos créditos da empresa detentora da Ata ou, se for o caso, cobrada administrativa ou judicialmente.

9.5. As penalidades previstas neste item têm caráter de sanção administrativa, conseqüentemente, a sua aplicação não exime a empresa detentora da Ata da reparação das eventuais perdas e danos que seu ato venha acarretar ao Estado de Rondônia.

9.6. As penalidades são independentes e a aplicação de uma não exclui a das demais, quando cabíveis.

9.7. Na hipótese de apresentar documentação inverossímil ou de cometer fraude, o licitante poderá sofrer, sem prejuízo da comunicação do ocorrido ao Ministério Público, quaisquer das sanções adiante previstas, que poderão ser aplicadas cumulativamente:

9.8. Desclassificação, se a seleção se encontrar em fase de julgamento;

9.9. Cancelamento do preço registrado, procedendo-se à paralisação do fornecimento.

9.10. O preço registrado poderá ser cancelado pela Administração Pública, nos termos do Artigo 24 e 25 do Decreto 18.340/13, quando:

9.10.1. A Detentora do Registro deixar de cumprir total ou parcial as condições da Ata de Registro de Preços.

9.10.2. A Detentora do Registro não retirar a nota de empenho ou instrumento equivalente no prazo estabelecido, sem justificativa aceita pela Administração;

9.10.3. A detentora incorrer reiteradamente em infrações previstas no Edital;

9.10.4. A Detentora do Registro que praticar atos fraudulentos no intuito de auferir vantagem ilícita;

9.10.5. Não aceitar reduzir o seu preço registrado, na hipótese deste se tornar superior aqueles praticados no mercador ou sofrer sanção prevista nos incisos III ou IV do caput do artigo 87 da Lei 8.666/93 ou no artigo 7º da Lei 10.520/02.

9.10.6. Por razões de interesse público, mediante despacho motivado, devidamente justificado.

9.10.7. O cancelamento do registro nas hipóteses nos sub itens 9.11.1, 9.11.2, 9.11.5 será formalizado por despacho do órgão gerenciador, assegurado o contraditório e a ampla defesa.

9.10.8. O cancelamento do registro nas hipóteses dos sub itens 9.11.1 e 9.11.2 acarretará ainda a aplicação das penalidades cabíveis, assegurado o contraditório e a ampla defesa.

9.10.9. O cancelamento do registro de preços poderá ocorrer por fato superveniente, decorrente de caso fortuito ou força maior, que prejudique o cumprimento da ata, devidamente comprovados e justificados:

9.10.9.1 por razões de interesse público ou

9.10.9.2 a pedido do fornecedor.

10. UTILIZAÇÃO DA ATA

10.1. Nos termos do Artigo 26 do Decreto Estadual 18.340/13, esta Ata de Registro de Preços, durante a sua vigência, poderá ser utilizada por qualquer órgão ou entidade da Administração Pública Estadual que não tenha participado do certame licitatório, mediante anuência do órgão gerenciador.

10.2. É facultada aos órgãos s ou entidades municipais, distritais ou estaduais a adesão a ata de registro de preços da Administração Pública Estadual.

10.3. Caberá ao fornecedor beneficiário da Ata de Registro de Preços, observadas as condições nela estabelecidas, optar pela aceitação ou não do fornecimento decorrente da adesão, desde que não prejudique as obrigações presentes e futuras da ata, assumidas com o órgão gerenciador e órgãos participantes.

10.4. As aquisições ou contratações adicionais não poderão exceder, por órgão ou entidade, a 50% dos quantitativos dos itens do instrumento convocatório e registrados na ata de registro de preços para o órgão gerenciador e órgãos participantes.

10.5. As adesões à ata de registro de preços não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na ata de registro de preços para o órgão gerenciador e órgãos participantes, independentemente do número de órgãos não participantes que aderirem.

10.6. Caberá ao órgão que se utilizar da ata, verificar a vantagem econômica da adesão a este Registro de Preço."

11. DA ALTERAÇÃO DA ATA DE REGISTRO DE PREÇOS

11.1. De acordo com artigo 21 e 22 do Decreto Estadual 18.340/2013 os preços registrados poderão ser revistos em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos serviços ou bens registrados, cabendo ao órgão gerenciador promover as negociações junto aos fornecedores, observadas as disposições contidas na alínea "d" do inciso II do caput do artigo 65 da Lei 8.666/93.

11.2. Quando o preço registrado tornar-se superior ao preço praticado no mercado por motivo superveniente, o órgão gerenciador convocará os fornecedores para negociarem a redução dos preços aos valores praticados pelo mercado.

11.3. Os fornecedores que não aceitarem reduzir seus preços aos valores praticados pelo mercado serão liberados do compromisso assumido, sem aplicação de penalidade.

11.4. A ordem de classificação dos fornecedores que aceitarem reduzir seus preços aos valores de mercado observará a classificação original.

11.5. Quando o preço de mercado tornar-se superior aos preços registrados, e o fornecedor não puder cumprir o compromisso, o órgão gerenciador poderá:

11.5.1.liberar o fornecedor do compromisso assumido, caso a comunicação ocorra antes do pedido de fornecimento, sem aplicação de penalidade se confirmada a veracidade dos motivos e comprovantes;

11.5.2. Convocar os demais fornecedores para assegurar igual oportunidade de negociação;

11.5.3. Não havendo êxito nas negociações, o órgão gerenciador deverá proceder a revogação do item da ata de registro de preços, adotando as medidas cabíveis para obtenção da contratação mais vantajosa.

12. DAS OBRIGAÇÕES DA DETENTORA DOREGISTRO

12.1. Substituir em qualquer tempo e sem qualquer Ônus para o Órgão/Entidade toda ou parte da remessa devolvida pela mesma, no prazo de 05 (cinco) dias úteis, caso constatada divergência na especificação;

12.2. Dispor-se a toda e qualquer fiscalização, no tocante ao fornecimento do produto, assim como ao cumprimento das obrigações previstas na ATA;

12.3. Prover todos os meios necessários à garantia da plena operacionalidade do fornecimento, inclusive considerados os casos de greve ou paralisação de qualquer natureza;

12.4. A falta de quaisquer dos produtos cujo fornecimento incumbe ao detentor do preço registrado, não poderá ser alegada como motivo de força maior para o atraso, má execução ou inexecução dos serviços objeto deste contrato e não a eximirá das penalidades a que está sujeita pelo não cumprimento dos prazos e demais condições estabelecidas;

12.5. Comunicar imediatamente à Administração Pública qualquer alteração ocorrida no endereço, conta bancária e outros julgáveis necessários para recebimento de correspondência;

12.6. Respeitar e fazer cumprir a legislação de segurança e saúde no trabalho, previstas nas normas regulamentadoras pertinentes;

12.7. Fiscalizar o perfeito cumprimento do fornecimento a que se obrigou, cabendo-lhe, integralmente, os ônus decorrentes. Tal fiscalização dar-se-á independentemente da que será exercida pela Administração Pública.

12.8. Indenizar terceiros e/ou ao Órgão/Entidade, mesmo em caso de ausência ou omissão de fiscalização de sua parte, pelos danos causados por sua culpa ou dolo, devendo a contratada adotar todas as medidas preventivas, com fiel observância às exigências das autoridades competentes e às disposições legais vigentes;

12.9. Toda e qualquer tipo de autuação ou ação que venha a sofre em decorrência do fornecimento em questão, bem como pelos contratos de trabalho de seus empregados, mesmo nos casos que envolvam eventuais decisões judiciais, eximindo o Órgão/Entidade de qualquer solidariedade ou responsabilidade;

12.10. Todos os impostos e taxas que forem devidos em decorrência das contratações do objeto do Edital correrão por conta exclusiva da contratada;

13. DAS OBRIGAÇÕES DOS ÓRGÃOS REQUISITANTES

13.1. Proporcionar todas as facilidades indispensáveis à boa execução das obrigações contratuais;

13.2. Rejeitar, no todo ou em parte, os objetos desta Ata entregues em desacordo com as obrigações assumidas pelo fornecedor;

13.3. Notificar a CONTRATADA de qualquer irregularidade encontrada no fornecimento dos objetos desta Ata;

13.4. Efetuar o pagamento à(s) contratada(s) de acordo com as condições de preços e prazos estabelecidos no edital e ata de registro de preços

13.5. Nenhum pagamento será efetuado à empresa adjudicatária, enquanto pendente de liquidação qualquer obrigação. Esse fato não será gerador de direito a reajustamento de preços ou a atualização monetária.

13.6. Não haverá, sob hipótese alguma, pagamento antecipado.

14. DOS ÓRGÃOS PARTICIPANTES:

14.1. É participante desta ata o seguinte órgão pertencente à Administração Pública do Estado de Rondônia:

15. DISPOSIÇÕES GERAIS

15.1. A existência de preços registrados não obriga a Administração a firmar as contratações de que deles poderão advir, facultada a realização de licitação específica para a aquisição pretendida, sendo assegurada à Detentora do registro de preços a preferência em igualdade de condições.

15.2. Fica a Detentora ciente que a publicidade da ata de registro de preços na imprensa oficial terá efeito de compromisso nas condições ofertadas e pactuadas na proposta apresentada à licitação.

15.3. A Ata de Registro de Preços, os ajustes dela decorrentes, suas alterações e rescisões obedecerão ao Decreto Estadual 18.340/13, Lei Federal nº 8.666/93, demais normas complementares e disposições desta Ata e do Edital que a precedeu, aplicáveis à execução e especialmente aos casos omissos.

15.4. Fazem parte integrante desta Ata, para todos os efeitos legais: o Edital de Licitação e seus anexos, bem como, o ANEXO ÚNICO desta ata que contém os preços registrados e respectivos detentores.

15.5. Fica eleito o foro do Município de Porto Velho/RO para dirimir as eventuais controvérsias decorrentes do presente ajuste.

ÓRGÃO GERENCIADOR:

MÁRCIO ROGÉRIO GABRIEL
Superintendente Estadual de Compras e Licitações

GENEAN PRESTES DOS SANTOS
Gerente do Sistema de Registro de Preços

EMPRESA(S) DETENTORA(S):

Qualificada(s) no Anexo Único desta Ata

SUPERINTENDÊNCIA ESTADUAL DE LICITAÇÕES - SUPEL/RO
Equipe de licitação ÔMEGA

AVISO DE LICITAÇÃO
PREGÃO ELETRÔNICO Nº290/2019/ÔMEGA/SUPEL/RO

A SUPERINTENDÊNCIA ESTADUAL DE LICITAÇÕES, por meio de suo(a) Pregoeiro(a) e Equipe de Apoio, nomeada por força das disposições contidas na Portaria nº 081/GAB/SUPEL, publicada no DOE do dia 23/04/2019, torna público que se encontra autorizada a realização da licitação na modalidade de **PREGÃO,** na forma **ELETRÔNICA,** sob o nº**290/2019/ÔMEGA/SUPEL/RO,** do tipo **MENOR PREÇO LOTE,** tendo por finalidade a qualificação de empresas e a seleção da proposta mais vantajosa, conforme disposições descritas neste edital e seus anexos, em conformidade com as Leis Federais nº 10.520/02 e nº 8.666/93 e suas alterações a qual se aplica subsidiariamente a modalidade de Pregão, com os Decretos Estaduais nº 12.205/06, n° 16.089/2011 e n° 21.675/2017, Decreto Federal n° 5.450/05, com a Lei Complementar nº 123/06 e suas alterações, com a Lei Estadual n° 2.414/2011, e demais legislações vigentes, tendo como interessada a Coordenadoria de Tecnologia da Informação e Comunicação - CTIC/SEDUC**.**

PROCESSO ADMINISTRATIVO Nº0029.173574/2019-04
OBJETO: Registro de preço de aquisição de equipamentos e materiais permanentes e serviços – solução unificada de segurança para proteção de e-mail, proteção de endpoint e proteção contra ataques avançados, com garantia de 36 meses, contemplando pacote de instalação e configuração, treinamento (hands-on) e operação assistida.

PROGRAMA DE TRABALHO:12.126.1076/12.122.1015**.**

ELEMENTO DE DESPESA:33.90.39/44.90.40**.**

FONTE DE RECURSOS:112 – Tesouro Estadual.

VALOR ESTIMADO PARA CONTRATAÇÃO: R$ 10.770.681,68.
DATA DE ABERTURA: 08 de Outubro de 2019, às 10h00min.(HORÁRIO DE BRASÍLIA - DF)
ENDEREÇO ELETRÔNICO: https://www.comprasgovernamentais.gov.br/
CÓDIGO DA UASG:925373

LOCAL: O Pregão Eletrônico será realizado por meio do endereço eletrônico acima mencionado, por meio do(a) Pregoeiro(a) e equipe de apoio.

EDITAL: O Instrumento Convocatório e todos os elementos integrantes encontram-se disponíveis para consulta e retirada no endereço eletrônico acima mencionado, e, ainda, no site **www.supel.ro.gov.br**. Maiores informações e esclarecimentos sobre o certame serão prestados pelo(a) Pregoeiro(a) e Equipe de Apoio, na Superintendência Estadual Licitações, pelo telefone (69) 3212-9270, ou no endereço sito a Av. Farquar, S/N, Bairro: Pedrinhas, Complexo Rio Madeira, Ed. Pacaás Novos, 2º Andar, em Porto Velho/RO - CEP: 76.903-036.

Porto Velho-RO, 31 de Julho de 2019.

MARIA DO CARMO DO PRADO
Pregoeiro(a) SUPEL-RO
Mat. 300131839

MARIA DO CARMO DO PRADO
Pregoeiro (a) SUPEL-RO
Mat. 300131839