SEGUE ABAIXO A TABELA DE RESULTADO:

Candidato	Município	Foto	Posição
Maysa Regina Dias da Silva	Ariquemes	Maquinas Museu	1º Lugar
Rômulo Cândido Fagá	Cacoal	Cacoal Nosso Lar	1º Lugar
José Gustavo Rodrigues	Campo Novo de Rondônia	Praça Augusto Lira	1º Lugar
Rodrigo Húngaro Lemes Gonçalves	Costa Marques	Costa Marques Vida Aquática	1º Lugar
Maysa Regina Dias da Silva	Costa Marques	Parede Forte Príncipe	2º Lugar
Maysa Regina Dias da Silva	Guajará-Mirim	Balneário do Célio	1º Lugar
Daniel Celano Guimarães Santos	Guajará-Mirim	Guajará-Mirim Museu	2º Lugar
Daniel Celano Guimarães Santos	Nova Mamoré	Pedra da Memória	1º Lugar
Maysa Regina Dias da Silva	Nova Mamoré	Ponte Ribeirão	2º Lugar
Rodrigo Húngaro Lemes Gonçalves	Ouro Preto do Oeste	Portal	1º Lugar
Anderson de Paula Guizolpe	Pimenta Bueno	Espelho do Céu	1º Lugar
Karoline dos Santos Nava	Pimenta Bueno	Estrada Loteamento	2º Lugar
Fábio Santos Guimarães	Pimenta Bueno	Véu da Noiva	3º Lugar
Pedro Augusto da Costa Silva	Porto Velho	Ponte do Amor - Cadeado	1º Lugar
Maysa Regina Dias da Silva	Porto Velho	Acesso Passarela	2º Lugar
Rodrigo Húngaro Lemes Gonçalves	Vilhena	Bola de Fogo	1º Lugar

Informamos que está aberto o prazo para interposição de recursos a contar da data de publicação deste Aviso. Dessa forma a licitante poderá apresentar peça recursal até o dia 06/12/2022 até às 23h:59min (horário de Rondônia) exclusivamente através do e-mail: concursos.setur.ro@gmail.com, indicado no Item 9.1 do TR. Não havendo manifestação, o presente resultado será homologado pela SETUR. Informações poderão ser solicitadas no horário das 07h:30min às 13h:30min. (horário de Rondônia), de segunda a sexta-feira, na Sede da SUPEL, ou, através do endereço eletrônico www.rondonia.ro.gov.br/supel e telefone: (0XX) 69.3212-9269.

Porto Velho, 06 de dezembro de 2022.

BRUNA GONÇALVES APOLINÁRIO

Presidente - SUPEL/RO

Protocolo 0034177154

Portaria nº 186 de 28 de novembro de 2022

Designa membros para compor a Comissão de Processamento e Apoio para suporte aos servidores responsáveis pela condução técnica da modalidade pregão, bem como conjunto de pregoeiros com o fito de proporcionar o processamento dos certames no âmbito da Superintendência Estadual de Compras e Licitações - SUPEL/RO.

O **SUPERINTENDENTE DE COMPRAS E LICITAÇÕES DO ESTADO DE RONDÔNIA** , no uso das atribuições legais e regimentais previstas nos termos do art. 17, inciso VIII, do Decreto nº 8978, de 31 de janeiro de 2000 e do art. 43 da Lei Complementar n. 965, de 20 de dezembro de 2017;

CONSIDERANDO o art. 13, inciso I, do Decreto Estadual nº 26.182, de 24 de junho de 2021, que atribui à autoridade competente do órgão promotor da licitação o direito de designar pregoeiros e membros da equipe de apoio; e

CONSIDERANDO o art. 7º da Portaria nº 184 de 24 de novembro de 2022 (id. 0033911142), que institui a Comissão de Processamento e Apoio para suporte aos servidores responsáveis pela condução técnica da modalidade pregão, e estabelece suas competências, com o fito de proporcionar o processamento dos certames no âmbito da Superintendência Estadual de Compras e Licitações – SUPEL/RO,

RESOLVE:

Art. 1º Designar os servidores abaixo para desempenhar a função de Pregoeiro(a), conduzindo os certames

dos pregões:

I - Bruna Gonçalves Apolinário, matrícula n.º 300141033;

II - Camila Caroline Rocha Peres, matrícula n.º 300145454;

III - Fabíola Menegasso Dias, matrícula n.º 300148746;

IV - Graziela Genoveva Ketes, matrícula n.º 300118300;

V - Izaura Taufmann Ferreira, matrícula n.º 300094012;

VI - Jader Chaplin Bernardo de Oliveira, matrícula n.º 300130075;

VII - Maria do Carmo do Prado, matrícula n.º 300131839;

VIII - Marina Dias de Moraes Taufmann, matrícula n.º 300114886;

IX - Nilséia Ketes Costa, matrícula n.º 300061141;

X - Rogério Pereira Santana, matrícula n.º 300109135.

Parágrafo único. Ficam designados à função de Pregoeiro(a) Substituto(a) os servidores abaixo, que desempenharão as atividades de estilo nas ausências e impedimentos de quaisquer titulares:

I - Aline Lopes Espíndola, matrícula n.º 300131588;

II - Ana Viana de Souza, matrícula n.º 300138121;

III - Bianca Matias de Souza, matrícula n.º 300109123;

IV - Bruna Karen Borges Rodrigues, matrícula n.º 3001768695;

V - Ivanir Barreira de Jesus, matrícula n.º 300138122;

VI - Luciana Pereira de Souza, matrícula n.º 300137520;

VII - Maíza Braga Barbeto, matrícula n.º 300134844;

VIII - Nathalia Veronezi Rodrigues da Silva, matrícula n.º 300167750;

IX - Ronaldo Alves dos Santos, matrícula n.º 200006353;

X - Yago da Silva Teixeira, matrícula n.º 300172800.

Art. 2º Designar os seguintes membros para compor a Comissão de Processamento e Apoio:

I - Adriana de Oliveira da Silva, matrícula n.º 300116763;

II - Aline Cruz de Oliveira, matrícula n.º 300130696;

III - Anikelle Lima Rodrigues, matrícula n.º 300178779;

IV - Anna Cecilia Enes Costa, matrícula n.º 300184530;

V - Ayanne Carmencita Ramos Dias, matrícula n.º 300180964;

VI - Dhandara França Hotong Siqueira, matrícula n.º 300179012;

VII - Harrisson Lucas Oliveira Rodrigues, matrícula n.º 300132731;

VIII - Janaina Muniz Lobato, matrícula n.º 300130481;

IX - Jenilson Reis de Azevedo, matrícula n.º 300102002;

X - Jéssica Bazán Padilha Graciliano, matrícula n.º 300130071;

XI - João Vitor Rodrigues de Souza, matrícula n.º 300178886;

XII - Jonattas Afonso Oliveira Pacheco, matrícula n.º 300169993;

XIII - Josélia Pagani Ferreira, matrícula n.º 300151627;

XIV - Josineide Barbosa Leite Anastácio Ferreira, matrícula n.º 300138255;

XV - Letícia Carpina Farias Casara, matrícula n.º 300178797;

XVI - Lucas Antonio Aires da Silva, matrícula n.º 300127160;

XVII - Marcos Felipe Santos Silva, matrícula n.º 300173049;

XVIII - Marcos Silva Almeida Júnior, matrícula n.º 300170429;

XIX - Maria Adriana Reis de Menezes, matrícula n.º 300178810;

XX - Maria Carolina de Carvalho, matrícula n.º 300121196;

XXI - Roberta Arroio, matrícula n.º 300178701;

XXII - Rodrigo Zschornack Gomes, matrícula n.º 300178750;

XXIII - Roseanna Nascimento Alves da Silva, matrícula n.º 300171478.§ 1º

Parágrafo único. Os servidores indicados no parágrafo único, do Art. 1º, desempenharão a função de membro de Comissão de Processamento e Apoio quando não estiverem representando a função de Pregoeiros Substitutos.

Art. 3º Esta portaria entra em vigor na data de sua publicação.

Dê-se ciência. Publique-se. Cumpra-se.

Israel Evangelista da Silva

GOVERNO DO ESTADO DE RONDÔNIA
Superintendência Estadual de Compras e Licitações - SUPEL

INSTRUMENTO CONVOCATÓRIO

PREGÃO ELETRÔNICO N°: 161/2023/SUPEL/RO

AVISO DE LICITAÇÃO	
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 186/GAB/SUPEL, publicada no DOE na data de 07 de dezembro de 2022,** torna público que se encontra autorizada a realização da licitação na modalidade de **PREGÃO,** na forma **ELETRÔNICA,** sob o **nº 161/2023/SUPEL/RO,** do tipo **MENOR PREÇO POR LOTE. PARA O LOTE ÚNICO, aplica-se a ampla participação sem reserva de cota no total de até 25% às empresas ME/EPP**, método de disputa: **ABERTO**, 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 26.182/2021, n°16.089/2011 e n°18.340/13 n°24.082/2019, n°25.969/2021, n°25.829/2021, e n°21.675/2017, com a Lei Complementar nº 123/06 e suas alterações, com a Lei Estadual n°2414/2011, e demais legislações vigentes, tendo como interessada a **Secretaria de Estado da Educação – SEDUC/RO**.	
PROCESSO ADMINISTRATIVO Nº	0029.102870/2022-18
OBJETO:	Registro de Preços para futuras e eventuais Contratações, SOB DEMANDA, de empresa especializada e habilitada para fornecimento de Solução Unificada de Segurança para proteção de *e-mail*, proteção d e *endpoint* e proteção contra-ataques avançados, contemplando os serviços de instalação e configuração, transferência de conhecimento e suporte técnico, para atendimento das necessidades da Secretaria de Estado da Educação, conforme condições, quantidades e exigências estabelecidas neste instrumento.
PROGRAMA DE TRABALHO:	12.126.2125.2387-Modernizar a Infraestrutura Tecnológica de TI
ELEMENTO DE DESPESA:	4.4.90.40 - Aquisição de Software Pronto
FONTE DE RECURSOS:	0112 - Recursos Destinados à Manutenção e Desenvolvimento de Ensino
VALOR ESTIMADO PARA CONTRATAÇÃO:	**R$ 15.678.830,98**

DATA DE ABERTURA:	04 de agosto de 2023 as 09h00min. (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.rondonia.ro.gov.br/supel. Maiores informações e esclarecimentos sobre o certame serão prestados pelo(a) Pregoeiro(a) e Equipe de Apoio, na Superintendência Estadual Licitações, pelo telefone (69) 3212-9243, ou no endereço sito a Av. Farquar, 2986, Bairro: Pedrinhas, Complexo Rio Madeira, Ed. Pacaás Novos, 2º Andar, em Porto Velho/RO - CEP: 76.801-470	

NOTA

INFORMAMOS AOS LICITANTES QUE MEDIANTE A AUSÊNCIA DE DESCRIÇÕES IDÊNTICAS DE ALGUNS ITENS POR OCASIÃO DO CADASTRAMENTO JUNTO AO SISTEMA COMPRAS DO GOVERNO FEDERAL, OS MESMOS FORAM CADASTRADOS COM DESCRITIVOS SIMILARES. TODAVIA, PARA CADASTRAMENTO DAS PROPOSTAS, DEVE-SE OBSERVAR E ATENDER OS DESCRITIVOS INFORMADOS NA SAMS - ANEXO I DO EDITAL, A QUAL CONTÊM AS DESCRIÇÕES FIDEDÍGNAS DOS ITENS.

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 186/GAB/SUPEL, publicada no DOE na data de 07 de dezembro de 2022 (0038356765),** torna público que se encontra autorizada a realização da licitação na modalidade de **PREGÃO,** na forma **ELETRÔNICA,** sob o **nº 161/2023/SUPEL/RO,** do tipo **MENOR PREÇO POR LOTE. PARA O LOTE ÚNICO - ITEM 30 DO TERMO DE REFERÊNCIA, aplica-se a ampla participação sem reserva de cota no total de até 25% às empresas ME/EPP**, método de disputa: **ABERTO**, 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 26.182/2021, nº 16.089/2011 e nº 18.340/13 nº 24.082/2019, nº 25.969/2021, nº 25.829/2021, e nº 21.675/2017, com a Lei Complementar nº 123/06 e suas alterações, com a Lei Estadual nº 2414/2011, e demais legislações vigentes, tendo como interessada a Secretaria de Estado da Educação – SEDUC/RO

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: 04 de agosto de 2023

HORÁRIO: 09h00min. (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 nº **0029.102870/2022-18,** 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

Do Objeto: Registro de Preços para futuras e eventuais Contratações, SOB DEMANDA, de empresa especializada e habilitada para fornecimento de Solução Unificada de Segurança para proteção d e *e-mail*, proteção de *endpoint* e proteção contra-ataques avançados, contemplando os serviços de instalação e configuração, transferência de conhecimento e suporte técnico, para atendimento das necessidades da Secretaria de Estado da Educação, conforme condições, quantidades e exigências estabelecidas neste instrumento.

Em caso de discordância existente entre as especificações deste objeto descritas no endereço eletrônico – COMPRAS.GOV.BR/CATMAT, e as especificações constantes no ANEXO III deste Edital – SAMS, prevalecerão as últimas;

2.1. Da Descrição e Quantidades Estimadas: Ficam aquelas estabelecidas no subitem 3.3 do Anexo I – Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

2.2. Da Garantia do Produto: Ficam aquelas estabelecidas no item 3.4. e subitens do Anexo I – Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

2.3. Da Característica do Objeto: Ficam aquelas estabelecidas no item 3.5. do Anexo I – Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão

requerente.

2.4. Do Local/Horário/Prazo e Condições de Entrega/Recebimento: Ficam aquelas estabelecidas no item 6. do Anexo I – Termo de Referência, os quais foram devidamente aprovados pelo ordenador de despesa do órgão requerente.

2.5. Do Acompanhamento e Fiscalização: Ficam aquelas estabelecidas no item 15 do Anexo I – Termo de Referência, os quais foram devidamente aprovados pelo ordenador de despesa do órgão requerente.

2.6. Da Garantia Contratual: Ficam aquelas estabelecidas no item 12 do Anexo I – Termo de Referência, os quais foram devidamente aprovados pelo ordenador de despesa do órgão requerente.

3. DA IMPUGNAÇÃO AO EDITAL

3.1. Até 03 (três) dias úteis que anteceder a abertura da sessão pública, qualquer pessoa poderá IMPUGNAR o instrumento convocatório deste PREGÃO ELETRÔNICO, conforme art. 24 do Decreto Estadual nº 26.182/2021, devendo o licitante mencionar o número do pregão, o ano e o número do processo licitatório, manifestando-se PREFERENCIALMENTE via e- mail**:** atendimentosupel@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) 3212-9243,** 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: (069) 3212-9242.

3.1.1. A impugnação não possui efeito suspensivo. A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo pregoeiro, nos Autos do processo de licitação.

3.1.2. Caberá ao pregoeiro, auxiliado pelos responsáveis pela elaboração do edital e dos anexos, decidir sobre a impugnação no prazo de **até 1 (um) dia útil antecedente à data marcada para a abertura da licitação.**

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 Compras.gov.br,** ficando o licitante obrigado a acessá-lo para obtenção das informações prestadas pelo (a) Pregoeiro (a).

3.1.3. A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo pregoeiro, nos Autos do processo de licitação.

3.1.4. 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.

4. DO PEDIDO DE ESCLARECIMENTO E 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 previsto no art. 23 Decreto Estadual n.º 26.182/2021, manifestando-se PREFERENCIALMENTE via e-mail: atendimentosupel@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) 3212-9243** 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: (69) 3212-9242, devendo o licitante mencionar o número do Pregão, o ano e o número do

processo licitatório.

4.1.1. O pregoeiro responderá aos pedidos de esclarecimentos até a data definida para a sessão inaugural e poderá requisitar subsídios formais aos responsáveis pela elaboração do edital e dos anexos. 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.

4.1.2. **As respostas aos pedidos de esclarecimentos serão divulgadas pelo sistema e vincularão os participantes e a administração.**

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 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 certame o Licitante deverá declarar, em campo próprio do Sistema Eletrônico: Ciência as regras do edital, assumindo 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 falsidade das declarações, sujeitará o licitante às sanções previstas no Decreto Estadual nº 26.182, DE 24 DE JUNHO DE 2021, Edital e nas demais cominações legais.

5.2.2. Os licitantes interessados em usufruir dos benefícios estabelecidos pela Lei Complementar nº 123/2006 e suas alterações, deverão atender às regras de identificação, atos e manifestação de interesse, bem como aos demais avisos emitidos pelo Pregoeiro ou pelo sistema eletrônico, nos momentos e tempos adequados.

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 site www.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.

5.4. 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; conforme motivação exposta no item 20.8 do Anexo I – Termo de Referência;

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;

5.4.4. 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 o Órgão e/ou Entidade contratante, durante o prazo de sanção;**

5.4.5.1. Conforme Informação nº 28/2021/PGE-ASSESADM, a Administração não poderá inabilitar o licitante que tiver sofrido sanção de suspensão temporária de participação em licitação por entidade ou unidade administrativa distinta da que promover o certame, tendo em vista o teor do Acórdão nº 2.218/211-Plenário, Acordão nº 902/2012-Plenário, Acordão nº 3243/2012- Plenário e Acordão nº 842/2013-Plenário, todos do Tribunal de Contas da União.

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.

6.2. O licitante enquadrado como microempresa ou empresa de pequeno porte deverá declarar, em campo próprio do Sistema, que atende aos requisitos do art. 3º da LC nº 123/2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 e 49 da mesma Lei, para fazer jus aos benefícios previstos.

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.

7.2. O lance será realizado considerando o VALOR TOTAL do lote.

8. DO REGISTRO (INSERÇÃO) DA PROPOSTA DE PREÇOS E DOCUMENTOS DE HABILITAÇÃO NO SISTEMA ELETRÔNICO

8.1. A participação no Pregão Eletrônico dar-se-á por meio da digitação da senha privativa do Licitante 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, devendo ser encaminhado, exclusivamente por meio do sistema, **concomitantemente os *documentos de habilitação* e *proposta,*** conforme Decreto Estadual nº 26.182/2021 e as exigências do edital.

8.1.1. Os licitantes que não anexarem o documento disposto **no item 8.1** serão desclassificados, não podendo alegar desconhecimento da exigência acima.

8.1.2. As Microempresas e Empresas de Pequeno Porte deverão encaminhar a documentação de habilitação, ainda que haja alguma restrição de regularidade fiscal e trabalhista, nos termos do art. 43, § 1º da LC nº 123, de 2006 e alterações.

8.1.3. Não será estabelecida, nessa etapa do certame, ordem de classificação entre as propostas apresentadas, o que somente ocorrerá após a realização dos procedimentos de negociação e julgamento da proposta.

8.1.4. Os documentos que compõem a proposta e a habilitação do licitante melhor classificado somente serão disponibilizados para avaliação do pregoeiro e para acesso público após o encerramento da fase de lances.

8.1.5. 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, 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.

8.1.6. As propostas de preços e documentos de habilitação registradas no Sistema Compras.gov.br, 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 COMPRAS.GOV.BR),** 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 **COMPRAS.GOV.BR NÃO 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 vedação de identificação que trata o subitem 8.2.1 refere-se ao *cadastramento* da proposta no sistema eletrônico de compras.

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 COMPRAS.GOV.BR 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.

8.6. O prazo de validade da proposta não poderá ser inferior a 90 (noventa) dias.

8.7. Decorridos 90 (noventa) dias da data da entrega das propostas, sem convocação para a contratação, ficam os licitantes liberados dos compromissos assumidos.

9. DA FORMULAÇÃO DE LANCES, CONVOCAÇÃO DAS ME/EPP E CRITÉRIOS

9.1. A partir da data e horário estabelecido no subitem 1.1.4 de 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 **Item 8.2** 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 o **LOTE** 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. O lance será realizado considerando o VALOR TOTAL DE CADA LOTE.

9.5.2. 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. As licitantes poderão oferecer lances menores e sucessivos, observado o horário fixado

e as regras de sua aceitação;

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

9.8. O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser:

a) **2% (dois por cento)** quando o item licitado possuir valor estimado de até R$ 1.000.000,00 (um milhão de reais).

b) **1% (um por cento)** quando o item licitado possuir valor estimado acima de R$ 1.000.000,00 (um milhão de reais).

9.9. Será adotado para o envio de lances no pregão eletrônico o modo de disputa “aberto”, em que os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

9.10. A etapa de lances da sessão pública terá duração de dez minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos dois minutos do período de duração da sessão pública.

9.11. A prorrogação automática da etapa de lances, de que trata o item anterior, será de dois minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

9.12. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente.

9.13. Encerrada a fase competitiva sem que haja a prorrogação automática pelo sistema, poderá o pregoeiro, assessorado pela equipe de apoio, justificadamente, admitir o reinício da sessão pública de lances, em prol da consecução do melhor preço.

9.14. 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;

9.15. 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;

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

9.15.2. 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;

9.16. 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;

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

9.16.2. 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/

9.16.2.1. Por outro lado, caberá ao licitante acessar o Portal de Compras Governamentais e manter-se atualizado diariamente quanto ao reinício e/ou continuidade de sessão licitatória, não podendo alegar qualquer prejuízo caso assim não o faça.

9.17. 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;

9.18. 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;

9.19. 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 COMPRAS.GOV.BR;

9.20. 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 Compras.gov.br **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 Compras.gov.br, 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.

10.1.2.1. Caso seja encerrada a fase de lances, e a licitante divergir com o exigido no item 10.1.2, 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, ficando desde já os licitantes cientes.

10.2. O pregoeiro **poderá** solicitar ao licitante melhor classificado que, no prazo de até 2 (duas) horas, envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

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.

11.2.1.2 Quando 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.

11.2.1.3. Se, no curso da licitação, depreender indício de que o levantamento prévio de preços padece de fragilidade, a Pregoeira poderá diligenciar a disparidade dos preços ofertados pelos participantes em razão da estimativa inicial.

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 da proposta, o (a) Pregoeiro (a) e equipe de apoio analisará a proposta anexada ao sistema quanto à conformidade do objeto proposto com o solicitado no Edital. O Pregoeiro poderá convocar o licitante para enviar documento digital complementar relacionado à proposta, bem como a proposta ajustada ao valor do último lance ofertado e/ou valor negociado, por meio de funcionalidade disponível no sistema, no prazo de até 120 (cento e vinte) minutos se outro prazo não for fixado, para enviar:**

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

11.5.2. 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;.

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

11.4. 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.

11.5. 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.

11.6. 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;

11.7. 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. Os licitantes poderão deixar de apresentar os documentos de habilitação que constem do SICAF e/ou Cadastro Geral de Fornecedores – CAGEFOR da SUPEL, assegurado aos demais licitantes o direito de acesso aos dados constantes dos sistemas.

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. Ressalvado o disposto no item 13.1.2, os licitantes **deverão** encaminhar concomitantemente com a proposta de preços, nos termos deste Edital, a documentação relacionada nos itens a seguir, para fins de habilitação:

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.

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 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;

f) No caso de agricultor familiar: Declaração de Aptidão ao Pronaf – DAP ou DAP-P válida, ou, ainda, outros documentos definidos pelo Ministério do Desenvolvimento Social, nos termos do art. 4º, §2º do Decreto n° 11.476/2023.

g) No caso de produtor rural: matrícula no Cadastro Específico do INSS – CEI, que comprove a qualificação como produtor rural pessoa física, nos termos da Instrução Normativa RFB nº 971, de 2009 (arts. 17 a 19 e 165).

h) 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 há mais de um ano) ou Capital Social (licitantes constituídas há menos de um ano), de 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. <u>RELATIVOS À QUALIFICAÇÃO TÉCNICA</u>

13.8.1. Considerando a Orientação Técnica nº 001/2017/GAB/SUPEL, de 14 de fevereiro de 2017, que em seu art. 3º define que os termos de referência, projetos básicos e editais relativos à aquisição de bens e materiais de consumo comuns, considerando o valor estimado da contratação, devem observar o seguinte:

Art. 3º Os Termos de Referência, Projetos Básicos e Editais relativos à aquisição de bens e materiais de consumo comuns, considerando o valor estimado da contratação, devem observar o seguinte:

I – Até 80.000,00 (oitenta mil reais) - fica dispensada a apresentação de Atestado de Capacidade Técnica;

II - de 80.000,00 (oitenta mil reais) a 650.000,00 (seiscentos e cinquenta mil reais) - apresentar Atestado de Capacidade Técnica que comprove ter fornecido anteriormente materiais compatíveis em características;

III – acima de 650.000,00 (seiscentos e cinquenta mil reais) – apresentar Atestado de Capacidade Técnica compatível em características e quantidades, limitados a parcela de maior relevância e valor significativo;

Parágrafo único. Não se aplica a regra do inc. I, aplicando-se a regra do inc. II deste artigo, quando tratar da aquisição de bens e materiais de natureza mais complexas tais como equipamentos médicos, odontológicos, de segurança, eletrônicos, computacionais.

a) Entende-se por pertinente e compatível em **<u>características</u>** o(s) atestado(s) que em sua individualidade ou soma de atestados, contemplem a parcela de maior relevância do objeto desta licitação, **quais sejam pelo fornecimento de software**;

b) Entende-se por pertinente e compatível em **<u>quantidades</u>** o (s) atestado (s) que em sua individualidade ou soma de atestados, demonstrem que a licitante forneceu o objeto do presentes processo, na quantidade correspondente a no mínimo **2% (dois por cento) do quantitativo total previsto no presente Termo.**

O (s) Atestado (s) emitido (s) por pessoa de direito privado, bem como o (s) atestado (s) emitido (s) por pessoa de direito público deverá (rão) constar órgão, cargo e matrícula do emitente (razão social, CNPJ, endereço, telefone, fax, data de emissão) e dos signatários do documento (nome, função, telefone, etc.), além da descrição do objeto, quantidades e prazos de prestação dos serviços, vale ressaltar, que a ausência das informações do órgão, cargo e matrícula do emitente nos atestados de capacidade técnica, não ensejará a imediata inabilitação do licitante, cabendo a promoção de diligência para averiguar a veracidade do documento, conforme previsto no art. 6º, parágrafo único, da Orientação Técnica n° 001/2017/GAB/SUPEL, incluído pela Orientação Técnica n° 002/2017/GAB/SUPEL;

As exigências quanto aos atestados de capacidade técnica estão estabelecidas conforme art. 3º 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.

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

13.9.1. A DOCUMENTAÇÃO DE HABILITAÇÃO ANEXADA NO SISTEMA COMPRAS.GOV.BR TERÁ EFEITO PARA TODOS OS ITENS, OS QUAIS A EMPRESA ENCONTRA-SE CLASSIFICADA.

13.9.2. O ENVIO DE TODA DOCUMENTAÇÃO SOLICITADA, DEVERÁ SER ANEXADA CORRETAMENTE NO SISTEMA COMPRAS.GOV.BR, 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.

13.9.3. **TODOS OS DOCUMENTOS DE HABILITAÇÃO DEVEM SER ANEXADOS NO SISTEMA COMPRASNET CONCONMITANTEMENTE COM A PROPOSTA DE PREÇOS – ART. 26, I, DO DECRETO ESTADUAL N. 26.182/21.**

13.10. 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;

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

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

13.13. 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.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, EM RESPEITO AO PRINCÍPIO DA ISONOMIA E VINCULAÇÃO AO INSTRUMENTO CONVOCATÓRIO, DISPOSTOS NO ART. 3º, DA LEI 8.666/93, E NO ART. 5º. DO DECRETO ESTADUAL Nº 26.182/21.

13.15.1. EM SEDE DE DILIGÊNCIA, QUE SE DESTINA UNICAMENTE A ESCLARECER E COMPLEMENTAR A INSTRUÇÃO PROCESSUAL, **NÃO SERÁ ADMITIDA A INCLUSÃO DE DOCUMENTO NOVO**, CONFORME ART. 43, §3º Lei nº 8.666/93.

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 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.

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 Compras.gov.br), 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/LOTES ADJUDICANDO-OS.

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 REGISTRO DE PREÇOS

16.1. Homologada a licitação pela Autoridade Competente, a Ata de Registro de Preços será publicada na imprensa Oficial, momento em que terá efeito de compromisso nas condições ofertadas e pactuadas na proposta apresentada à licitação.

16.2. A Ata de Registro e Preços terá validade de 12 (doze) meses, contados a partir da publicação no Diário Oficial do Estado.

16.3. Os contratos decorrentes da Ata de Registro de Preços terão sua vigência em conforme as disposições contidas no art. 57, da Lei n° 8.666/93.

16.4. 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.

16.5. 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.

16.6. A ata de registro de preços, os ajustes dela decorrentes, suas alterações e rescisões

obedecerão a Decreto Estadual n° 18.340/2013, Lei Federal n° 8.666/93, demais normas complementares e disposições desta Ata e do Edital que a precedeu, aplicáveis à execução e especialmente aos casos omissos.

16.7. Nos termos do Decreto Estadual 18.340/13 e suas alterações, a Ata de Registro de Preços, durante a sua vigência, poderá ser utilizada por qualquer órgão ou entidade da Administração Pública que não tenha participado do certame licitatório, mediante anuência do órgão gerenciador.

16.8. **Após a homologação da licitação para o registro de preços, d**everá ser observado **o art. 14 do Decreto n° 18.340/2013.**

16.9. Em atendimento ao Art.14, I, do Decreto n. 18.340, de 2013, poderão ser incluídas na Ata de Registro de Preços, o registro dos licitantes que aceitarem preços iguais ao do licitante vencedor na sequência da classificação do certame.

16.10.Para o cadastro reserva disposto no item 16.9 o Pregoeiro realizará as convocações no chat de mensagens durante o transcurso da sessão pública.

16.11. CRITÉRIO DE REVISÃO DA ATA DE REGISTRO DE PREÇOS

16.11.1. Os preços registrados poderão ser revistos nos termos dos art. 21 e 22 do Decreto Estadual nº. 18.340 de 06/11/2013, Art. 23–A do Decreto Estadual nº. 18.871/2014, e Art. 23-B do Decreto Estadual nº 25.969/2021:

> Art. 21. 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 nº 8.666, de 1993.
>
> Art. 22. Quando o preço registrado se tornar 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.
>
> § 1º Os fornecedores que não aceitarem reduzir seus preços aos valores praticados pelo mercado serão liberados do compromisso assumido, sem aplicação de penalidade.
>
> § 2º A ordem de classificação dos fornecedores que aceitarem reduzir seus preços aos valores de mercado observará a classificação original.
>
> Art. 23. Quando o preço de mercado tornar-se superior aos preços registrados, e o fornecedor não puder cumprir o compromisso, o órgão gerenciador poderá:
>
> I - liberar o fornecedor do compromisso assumido, caso a comunicação ocorra antes do pedido de fornecimento, e sem aplicação da penalidade se confirmada a veracidade dos motivos e comprovantes apresentados; e
>
> II - convocar os demais fornecedores para assegurar igual oportunidade de negociação.
>
> Parágrafo único: Não havendo êxito nas negociações, o órgão gerenciador deverá proceder à revogação do item da ata de registro de preços, adotando as medidas cabíveis para obtenção da contratação mais vantajosa.
>
> Art. 23-A. Será admitida solicitação de revisão de preços de que trata o artigo 23, quando tratar -se de produtos cujo preço médio de mercado for obtido em tabelas oficiais publicamente reconhecidas ou de preços regulamentados pelo poder público, depois de cumprido o disposto no inciso II, do artigo 23, deste Decreto.
>
> Parágrafo único: A revisão de preços prevista no caput poderá ser efetivada mediante requerimento do detento da ata, que deverá fazê-lo antes do pedido de fornecimento e, deverá instruir o pedido com a documentação probatória de majoração do preço do mercado e a oneração de custos.

16.11.2. O Decreto Estadual nº 25.969/2021, acresceu o artigo 23-B no Decreto Estadual nº 18.340/2013, dispositivo este que acrescentou à normativa retro a possibilidade de se promover à revisão de preços registrados em ARPs, para majorar ou minorar os preços registrados, em casos excepcionais, nas hipóteses legais e considerando os preços vigentes de mercado:

> Art. 23-B. Os preços registrados serão mantidos inalterados por todo o período de vigência da Ata de Registro de Preços - ARP, admitida sua revisão, para majorar ou minorar os preços registrados, em casos excepcionais, nas hipóteses legais e considerando os preços vigentes de mercado. **(Artigo**

acrescido pelo Decreto n°25.969, de 7/4/2021)

§ 1°. A revisão de preços prevista no **caput** precederá de requerimento: **(Parágrafo acrescido pelo Decreto n°25.969, de 7/4/2021)**

I - Do detentor da ata, que deverá fazê-la antes do pedido de fornecimento e, instruindo seu pedido com documentação probatória de majoração de preço do mercado e a oneração de custos; ou **(Inciso acrescido pelo Decreto n° 25.969, de 7/4/2021)**

II - Pelo órgão participante ou órgão interessado, comprovando por meio de pesquisas de preços que há minoração do valor originalmente registrado. **(Inciso acrescido pelo Decreto n°25.969, de 7/4/2021)**

§ 2°. Comprovada a majoração dos valores de mercado nas hipóteses da alínea "d" do inciso II do artigo 65 da Lei n° 8.666, de 1993, o órgão gerenciador da Ata convocará, antes da efetiva alteração de preços, as demais licitantes na ordem de classificação original para que manifestem interesse em manter o preço original registrado em ata, de modo que, inexistindo interessados dispostos em manter o valor da ARP; os preços poderão ser revisados conforme disposto no **caput** deste artigo. **(Parágrafo acrescido pelo Decreto n°25.969, de 7/4/2021)**

§ 3°. Comprovada a minoração dos valores de mercado, o órgão gerenciador da ata convocará os licitantes na ordem de classificação original para que manifestem interesse em adequar o preço registrado em ata, de modo que o órgão, mediante análise de vantajosidade e probidade das licitantes, poderá realizar, a seu critério técnico, os trâmites administrativos cabíveis para o cancelamento do beneficiário da ata. **(Parágrafo acrescido pelo Decreto n°25.969, de 7/4/2021)**

§ 4°. A revisão aprovada não poderá ultrapassar o preço praticado no mercado e deverá manter a diferença percentual apurada entre o preço originalmente constante da proposta e o preço de mercado vigente à época do registro. **(Parágrafo acrescido pelo Decreto n°25.969, de 7/4/2021)**

§ 5°. Para fins deste Decreto e do Sistema de Registro de Preços - SRP, por ele regulamentado, o órgão gerenciador do registro de preços, fixará por meio de Portaria, a forma de apuração do preço de mercado para efetivação de ajustes decorrentes das Atas de Registro de Preços. **(Parágrafo acrescido pelo Decreto n°25.969, de 7/4/2021).**

17. DO TERMO DE CONTRATO OU INSTRUMENTO EQUIVALENTE

17.1 A vigência será de 12 meses, podendo a duração estender-se pelo prazo de até 48 (quarenta e oito) meses após o início da vigência do contrato, conforme art. 57, IV, da Lei Federal n. 8.666/93.

17.2 A assinatura do termo de contrato após 60 (sessenta) dias da data de apresentação da proposta ou da data da licitação, precluirá o direito ao reajuste contratual, passando a ser contado o interregno mínimo para concessão de reajuste a para a data da assinatura do contrato.

17.3. CRITÉRIO DE REAJUSTE E REEQUILÍBRIO CONTRATUAL

17.3.1. Os valores contratados serão fixos e irreajustáveis pelo período inferior a um ano, de acordo com o art. 2º, §1º da Lei nº 10.192, de 14 de fevereiro de 2001.

17.3.2. Ocorrendo às hipóteses previstas no Art. 2º, Inciso XIII, Decreto Estadual nº 25.829/2021, será concedido **reequilíbrio econômico-financeiro** do contrato, requerido pela contratada, desde que documentalmente e suficientemente comprovado a desarmonia contratual, podendo ser concedido utilizando algum índice oficial de inflação tais como: IPCA/IBGE, bem como, outro índice que vier a substituí-los..

17.3.3. Igualmente será admitido sua revisão para majorar ou minorar os preços registrados, em casos excepcionais, nas hipóteses legais e considerando os preços vigentes de mercado, em conformidade com o artigo 23-B no Decreto Estadual nº 18.340/2013, acrescido pelo Decreto nº 25.969/2021

17.3.4. Em caso de reajuste superior a um ano, dever-se-á seguir os tramites previstos nos artigos 4º, 5 e 6 do DECRETO Nº 25.829, DE 11 DE FEVEREIRO DE 2021:

Art. 4º O reajuste em sentido estrito, espécie de reajuste nos contratos de obra, fornecimento ou serviço continuado sem dedicação exclusiva de mão de obra, consiste na aplicação de índice de correção monetária estabelecido no contrato, que retratará a variação efetiva do custo de produção, admitida a adoção de índices específicos ou setoriais.

§ 1º É nula de pleno direito qualquer estipulação de reajuste com periodicidade inferior a 1 (um) ano.

§ 2º A periodicidade anual nos contratos de que trata o § 1º será contada a partir da data limite para apresentação da proposta ou do orçamento a que essa se referir.

§ 3º Nas hipóteses em que o valor dos contratos de serviços continuados seja preponderantemente formado pelos custos dos insumos, poderá ser adotado o reajuste de que trata este artigo.

Art. 5º Para fins de adoção de índices pré-fixados de reajuste, os gestores observarão o critério da especialidade e da setorialidade, analisando se para o objeto contratual há índice específico de reajuste.

§ 1º Na falta de índice de reajuste específico para o objeto, poderá ser utilizado os índices oficiais que estabelecem a inflação.

§ 2º Para itens de contrato que necessitem ser reajustados por mais de um índice, as parcelas que compõem esses itens deverão ser desmembrados, passando cada parcela a ser corrigida pelo seu respectivo índice.

§ 3º Em caso de paralisação ou aditamento de prazo em obras públicas, que venha a ultrapassar o prazo previsto em contrato para a execução, ter-se-á que as parcelas contratuais excedentes ao prazo original serão reajustadas pelo índice previsto no instrumento convocatório, desde que devidamente justificado pela contratante e que o contratado não tenha dado causa ao atraso na execução, respeitando a periodicidade anual prevista no art. 4º. Art. 6º O pedido de reajuste do contrato deverá ser instruído, observado o art.15, com os seguintes documentos:

I - requerimento da contratada devidamente assinado pelo seu responsável;

II - planilha de custos demonstrando a equação inicial do contrato; e

III - planilha de custos demonstrando a equação atual do contrato, a qual deverá demonstrar a variação do preço, levando em consideração o índice de reajuste pré-fixado no instrumento convocatório e no contrato.

§ 1º O reajuste poderá ser formalizado por meio de apostilamento, exceto quando coincidirem com a prorrogação contratual, em que deverá ser formalizado por termo aditivo.

§ 2º Os reajustes a que o contratado fizer jus e que não forem solicitadas durante a vigência do contrato serão objeto de preclusão com a assinatura da prorrogação contratual ou com o encerramento do contrato, salvo se, no caso de prorrogação contratual, constar cláusula específica resguardando o direito do contratado.

17.3.5. As alterações decorrentes de solicitação de reequilíbrio seguirão o disposto no Decreto n. 25.829/21, na Lei nº 8.666/93 e demais normas correlatas.

18. DO PAGAMENTO

Conforme estabelecido no item 8. do Termo de Referência – Anexo I deste Edital.

19. DAS SANÇÕES ADMINISTRATIVAS

Conforme estabelecido no item 19. do Termo de Referência – Anexo I deste Edital.

20. DAS OBRIGAÇÕES DA CONTRATADA

Conforme estabelecido no item 18.2 do Termo de Referência – Anexo I deste Edital.

21. DAS OBRIGAÇÕES DA CONTRATANTE

Conforme estabelecido no item 18.1. do Termo de Referência – Anexo I deste Edital.

22. DA TRANSFERÊNCIA/CESSÃO OU SUBCONTRATAÇÃO

Conforme estabelecido no item 16 do Termo de Referência – Anexo I deste Edital.

23. DA DOTAÇÃO ORÇAMENTÁRIA

Programa de Trabalho: 12.126.2125.2387

Elemento de Despesa 4.4.90.40, 3.3.90.40 e 4.4.90.52.

Fonte de Recurso: 0112

24. DAS CONDIÇÕES GERAIS

24.1 A Administração Pública se reserva no direito de:

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

24.3 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.

24.4 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.

24.5 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.

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

24.7 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).

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

24.9 *O 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 descredenciada 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(s) penalidade(s) no SICAF*** *e no* ***CAGEFIMP (Cadastro de Fornecedores Impedidos de Licitar e Contratar com a Administração Pública Estadual – CAGEFIMP, nos termos da Lei nº. 2.414, de 18, de fevereiro de 2011 e Decreto nº. 16089, DE 28 DE JULHO DE 2011)***

24.10 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.

24.11 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.

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

24.13 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.

24.14. Art. 15, § 1º, do Decreto Estadual n. 18.340/13 , § 1º é vedado efetuar acréscimos nos quantitativos fixados pela ata de registro de preços, inclusive o acréscimo de que trata o § 1º do artigo 65 da Lei nº 8.666 , de 21 de junho de 1993. (Redação do parágrafo dada pelo Decreto Nº 24082 DE 22/07/2019).

24.15. Com relação às supressões, conforme previsto no § 1°, do Art. 65, da Lei Federal nº. 8.666/93, o objeto da presente licitação poderá sofrer supressões.

24.16. 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.

24.17. 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;

24.18. 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.

24.19. 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.

24.20. 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. 26.182/2021, 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.

24.21. 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.

24.21.1. 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;

24.21.2. 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 na Lei n° 8.666/93.

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

24.23. 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.

24.24. Quaisquer informações complementares sobre o presente Edital e seus Anexos poderão ser obtidas pelo telefone/fax **(069) 3212-9243,** ou na sede SUPERINTENDÊNCIA ESTADUAL DE LICITAÇÕES – SUPEL/RO.

24.25. O Foro para dirimir os possíveis litígios que decorrerem do presente procedimento licitatório será o da Comarca da Capital do Estado de Rondônia.

25. ANEXOS

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

ANEXO I – Termo de Referência; 0039695603, SAMS id, 0038158624 e Minuta do Contrato id, 0037236535

ANEXO II – Quadro Estimativo de Preços; 0038716240

ANEXO III – Modelo de Minuta da Ata de Registro de Preço; 0039069040

ANEXO IV– Modelo de Solicitação de Adesão à Ata de Registro de Preço; 0039069213

Porto Velho-RO, 18 de julho de 2023.

Elaborado por:

Josélia Pagani Ferreira
Membro - Núcleo de ProcesSamento - SUPEL/RO

Conferido por:

Yago da Silva Teixeira
Assessor VI-Nível III - SUPEL/NP

Conferido/Aprovado por:

Bianca Matias de Souza
Pregoeira Substituta - SUPEL/RO

Documento assinado eletronicamente por **Bianca Matias de Souza**, **Assessor(a)**, em 18/07/2023, às 09:15, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.

A autenticidade deste documento pode ser conferida no site portal do SEI, informando o código verificador **0039050616** e o código CRC **E15A9C98**.

GOVERNO DO ESTADO DE RONDÔNIA
Secretaria de Estado da Educação - SEDUC

TERMO DE REFERÊNCIA

Nº 131/2022

SISTEMA DE REGISTRO DE PREÇOS

1. IDENTIFICAÇÃO

Unidade Orçamentária: 16.001 – Secretaria de Estado da Educação – SEDUC

Unidade Administrativa: Diretoria Administrativa e Financeira – SEDUC-DAF

Unidade Solicitante: Coordenadoria de Tecnologia da Informação e Comunicação - COTIC/SEDUC

2. INTRODUÇÃO E BASE LEGAL

O presente Termo de Referência foi elaborado em atendimento as regras pautadas nos princípios estabelecidos na Constituição Federal, art. 37, *caput*, nas Leis Federais nº 8.666/93 (**Lei Geral de Licitação**) e 10.520/02 (**Lei do Pregão)**, no Decreto Estadual nº 26.182/2021 (**Pregão Eletrônico**), e nos Decretos Estaduais nº 18.340/2013 e 24.082/2019 (**Registro de Preços**), e tem a finalidade de instruir procedimento licitatório a ser deflagrado para contratação de Serviços de Tecnologia da Informação e Aquisição de Software Pronto.

No que se refere ao objeto pretendido, os presentes Termos têm como base as informações definidas pelo setor demandante, conforme Solicitação de Compra e demais anexos, por ser este o detentor dos conhecimentos técnicos, demanda e sua real destinação, consequentemente, responsável competente pelas definições, eventuais correções, adequações e esclarecimentos.

3. OBJETO E OBJETIVO

3.1. Do Objeto

Constitui objeto do presente Termo de Referência a formação de Registro de Preços para futuras e eventuais Contratações, SOB DEMANDA, de empresa especializada e habilitada para fornecimento de Solução Unificada de Segurança para proteção de *e-mail*, proteção de *endpoint* e proteção contra-ataques avançados, contemplando os serviços de instalação e configuração, transferência de conhecimento e suporte técnico, para atendimento das necessidades da Secretaria de Estado da Educação, conforme condições, quantidades e exigências estabelecidas neste instrumento.

3.2. Do Objetivo

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 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. <u>Da Descrição e Quantidades Estimadas</u>

3.3.1. Os itens e descrições foram apresentados pela Coordenadoria de Tecnologia da Informação e Comunicação - COTIC/SEDUC, conforme apresentado na Solicitação de Compra - Aquisição de Material 0030898123.

3.3.2. Quanto a quantidade mínima a ser cotada, não será facultado para o objeto em tela, conforme previsto no art. 10, inciso V, do Decreto Estadual nº 18.340/2013, a cotação de quantidade inferior ao total estabelecido na tabela abaixo, por entender que não há viabilidade técnica.

LOTE ÚNICO			
Item	**Descrição do Objeto**	**Unid. de Medida**	**Quant**
1	Contratações, SOB DEMANDA, de empresa especializada e habilitada para fornecimento de Solução Unificada de Segurança para proteção de *e-mail*, proteção de *endpoint* e proteção contra-ataques avançados, contemplando os serviços de instalação e configuração, transferência de conhecimento e suporte técnico, **contemplando**:		01
1.1	Trend Micro Smart Protection Complete	Unidade	4300
1.2	Trend Micro Smart Protection for Endpoints	Unidade	628
1.3	Software de segurança para usuário final, com visibilidade completa para estações de trabalho com detecção e resposta, incluindo garantia e atualização por 12 (doze) meses	Unidade	24.873
1.4	Solução de segurança para cargas de trabalho híbridas com detecção e resposta, incluindo garantia e atualização de versão por 12 (doze) meses	Unidade	390
1.5	Módulo de investigação, correlação e resposta à incidentes em endpoints e servidores por 12 (doze) meses	Unidade	5000
1.6	Módulo de investigação, correlação e resposta à incidentes em email por 12 (doze) meses	Unidade	4300
1.7	Solução de segurança contra ameaças avançadas com detecção e resposta, incluindo garantia e atualização de versão por 12 (doze) meses	Unidade	2
1.8	Solução de prevenção de intrusão de próxima geração (NGIPS) – 3Gbps	Unidade	4
1.9	Serviço Especializado de Instalação e configuração, Pacote de 40 horas.	Unidade	20
1.10	Serviço Especializado de Treinamento Hands-on, Pacote de 40 horas.	Unidade	18
1.11	Serviço Especializado de Suportes corretivo e preventivo para 12 (doze) meses por solução de segurança.	Unidade	06

3.4. <u>Da Garantia do Produto</u>

3.4.1. Todos os materiais ofertados deverão atender à Lei nº 8.078/1990 (Código de Defesa do Consumidor) e às demais legislações pertinentes;

3.4.2. No caso de vícios ou de quaisquer outras irregularidades constatadas, a Administração fornecerá à Contratado relatório concernente a essas ocorrências, expondo seus motivos, a fim de que as mesmas sejam corrigidas;

3.5. <u>Da Característica do Objeto (0030898123)</u>

SOFTWARE DE SEGURANÇA PARA USUÁRIO FINAL, COM VISIBILIDADE COMPLETA PARA ESTAÇÕES DE TRABALHO COM DETECÇÃO E RESPOSTA, INCLUINDO GARANTIA E ATUALIZAÇÃO POR 12 (DOZE) MESES.

Características gerais

A solução deverá ser entregue na modalidade como um serviço (em nuvem);

Possuir console Web para gerenciamento e administração da ferramenta;

A solução deverá ser toda de um único fabricante;

A proteção para estações de trabalho deverá prover Anti-Malware, Firewall, Host IPS, Controle de Aplicações e Controle de dispositivos em um único agente.

Módulo de Proteção Anti-Malware

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

Windows 8.1 (x86/x64);

Windows 10 (x86/x64);

Windows 11 (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 detectar, analisar e eliminar programas maliciosos, tais como vírus, spyware, worms, cavalos de tróia, keyloggers, 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, 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;

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 possuir capacidade de escaneamento de arquivos compactados e, em caso de identificação de um arquivo malicioso, apenas este deve ser removido, mantendo os demais intactos

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 obfuscação 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 metadados, bem como, o porquê do veredito emitido pela Machine Learning;

Deve bloquear processos comuns associados a ransomware;

Em casos de ataques de ransomware, a solução deve ter a capacidade de interromper o processo de criptografia e restaurar os arquivos originais aos seus respectivos diretórios

Deve possuir funcionalidade de detecção de malwares conhecidos e desconhecidos por comportamento;

Deve permitir a integração com solução de análise de artefatos suspeitos (sandbox) do próprio fabricante.

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 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 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 permitir a deleção dos arquivos quarentenados;

Deve permitir remoção automática de clientes inativos por determinado período;

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

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 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 criptografia 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 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

As configurações da funcionalidade de controle de dispositivos devem ser aplicadas por usuário;

Deve permitir políticas e ações diferentes para dispositivos conectados à rede interna e aqueles utilizados na rede externa (conectado à Internet, por exemplo);

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 CD-ROM, 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;

Para ação de restrição como o bloqueio, a solução deve permitir adicionais dispositivos USB autorizados, bem como apontar executáveis específicos como exceção ao bloqueio;

Deve ter a capacidade de bloquear a função de Autorun nos dispositivos;

Deve permitir controle de permissão ou bloqueio para dispositivos que não armazenam dados tendo, pelo menos, os seguintes tipos de dispositivos: adaptadores bluetooth, dispositivos de imagem, modems, interfaces wireless externas, cartões PCMCIA, dispositivos infravermelhos e portas COM/LPT.

Módulo de Proteção Anti-Malware para estações MacOS

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

macOS 12 (Monterey);

macOS 11 (Big Sur)

macOS 10.15 (Catalina);

macOS 10.14 (Mojave);

macOS 10.13 (High Sierra);

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:

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 detecção/proteção contra exploração de vulnerabilidades nos seguintes sistemas operacionais:

Windows 8.1 (x86/x64);

Windows 10 (x86/x64);

Windows 11 (x64).

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

As regras de vulnerabilidades deverão possuir a opção de desativar a regra de forma individual;

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 que o usuário altere as configurações de níveis de segurança e exceções;

Deverá possuir a possibilidade de configurar níveis diferentes de segurança podendo ser eles alto, médio e baixo;

O modulo de HIPS deverá possuir perfis pré-determinados baseados em performance e segurança;

O modulo de HIPS deverá possuir regras pra proteger contra ameaças do tipo Ransomware;

O modulo de HIPS deverá conter regras contra exploit, vulnerabilidades e genericas protegendo contra ameaças conhecidas ou desconhecidas;

O módulo de HIPS deverá permitir que o administrador monitore apenas ou realize o bloqueio das tentativas de exploração de vulnerabilidades;

Deve suportar configuração de parâmetros de pacotes como quantidade máxima de conexões TCP e timeout para pacotes UDP;

Deve ter a capacidade de proteção contra exploração de vulnerabilidades do sistema operacional e de aplicações terceiras instaladas na estação de trabalho;

A lista de regras deve permitir que o administrador realize buscas e tenha rápida visibilidade do tipo da aplicação, em que modo a regra encontra-se (bloqueio ou monitoramento), CVE, CVSS score, quando aplicável.

Módulo para Controle De Aplicações

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

Windows 8.1 (x86/x64);

Windows 10 (x64);

Windows 11 (x64).

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

Permissão de execução;

Bloqueio de execução;

Bloqueio de novas instalações.

A regra de liberação para o controle de aplicação deverá permitir que o programa liberado efetue ou não a execução de outros processos,

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 e SHA-256 do executável;

Atributos do certificado utilizado para assinatura digital do executável;

Caminho lógico do executável;

Base de assinaturas de cortiçados digitais válidos e seguros.

As regras de controle de aplicação devem possuir categorias pré-determinadas de aplicações;

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

O módulo de controle de aplicativos deve possuir uma lista de aplicações mal-intencionados para bloqueio e monitoramento tendo, pelo menos, as categorias de KeyLoggers, anonimizadores de proxy, P2P, crackers de senhas;

Deve permitir a busca por aplicações ou fabricante destas;

Deve possuir ferramenta para extrair o hash de um ou um grupo de executáveis, permitindo a importação destes hashes através de arquivo CSV.

Módulo de Detecção e Resposta

A solução deve ser compatível com os sistemas operacionais Windows, Linux e MacOS;

O fabricante deve implementar e organizar os ataques baseados no framework MITRE ATT&CK®, identificando técnicas e táticas dos ataques;

A solução deve possuir módulo de investigação e detecção integrados;

Deve fazer uso de inteligência artificial e inteligência de ameaças do fabricante da solução para analisar e correlacionar as atividades dos sensores do ambiente;

Possuir painéis que apresentem visualização executiva dos principais incidentes e atividades no ambiente com base nos usuários, aplicações acessadas e estações de trabalho;

Utilizar bases de inteligência de ameaças integrando relatórios de inteligência do fabricante e de terceiros para ajudar a identificar ameaças no ambiente;

Apresentar os alertas consolidados e correlacionados de ameaças para melhor investigação e resposta;

Fornece a capacidade de realizar buscas avançadas para localizar dados ou objetos no ambiente para análise avançada de atividades ou detecções;

Capacidade de construir sequências de buscas poderosas para localizar os dados ou objetos em seu ambiente que você deseja examinar;

Deve prover diferentes métodos de pesquisa, filtros e uma linguagem de consulta do tipo *Kibana* para identificar, categorizar e recuperar os resultados da pesquisa;

Deve ser possível realizar buscas através de *strings* parciais, exatas, valores nulos, *wildcards* e caracteres especiais;

Permitir investigar os alertas gerados pelos modelos de detecção por meio de uma análise impacto e análise de causa-raiz;

Deve consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento;

Deve permitir que as detecções sejam correlacionadas com módulos de servidores, rede e e-mail do próprio fabricante através de console dedicada. Não serão aceitas consoles de correlação de terceiros;

A console de correlação deve estar disponível na nuvem do próprio fabricante, o qual deve ser responsável pelas manutenções, atualizações e disponibilidade;

Deve possuir capacidade de encaminhar as atividades suspeitas identificadas nos servidores para a console de correlação centralizada;

O módulo de EDR deve atuar baseado em modelos de detecção de ataques avançados e furtivos;

Os logs de detecções devem estar disponíveis na console por, pelo menos, 30 dias;

A console de correlação centralizada deve possuir informações a respeito dos principais ataques que estão ocorrendo no mundo, quais plataformas e países são afetados, além de links para obter mais informações;

A console deve permitir o Single Sign-On através de SAML ou padrão equivalente;

Permitir investigar os alertas gerados pelos modelos de detecção por meio de uma análise impacto e análise de causa-raiz;

Deve consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento;

Deve exibir os eventos de forma a priorizar os alertas mais críticos para que o analista realize a investigação, como pontuações ou níveis de prioridade;

Deve ser possível criar usuários com permissões distintas, contendo no mínimo, permissão total e permissão para realizar investigações;

Deve permitir habilitar ou desabilitar um determinado usuário sem excluí-lo da console;

Deve ser possível interagir com cada um dos objetos relacionados ao evento para análise avançada e resposta;

Deve destacar e organizar as atividades relacionadas a cada modelo de detecção por ordem cronológica, permitindo identificar a relação de cada atividade com os modelos de detecção;

Deve permitir o envio de notificações para os administradores através de email, API e integrações com SIEMs;

Deve prover visualização em linha do tempo com informações dos eventos monitorados em cada estação de trabalho;

Deve permitir a visualização entre usuários, servidores, processos/comandos, arquivos e demais componentes correlacionados em determinado ataque;

Deverá informar com qual técnica e tática do MITRE ATT&CK framework o ataque está relacionado, além de possuir link direto para o site da organização;

A solução deve mostrar, pelo menos, o timestamp, objetos envolvidos (comandos, processos, usuários, servidores);

Ao clicar em quaisquer dos objetos, a solução deve permitir realizar buscar específicas pelo objeto ou ainda executar ações como executar investigações mais aprofundadas;

Deve informar qual o escopo de impacto ou dimensionar o impacto em servidores, estações de trabalho e usuários, indicando a quantidade de componentes afetados no ataque;

Deve permitir que o analista possa alterar o status dos incidentes de acordo com seu tratamento e indicar falsos positivos para a plataforma;

Deve permitir adicionar arquivos SHA-1, URLs, IPs ou domínios a lista de bloqueio dos sensores;

Deve permitir remover arquivos SHA-1, URLs, IPs ou domínios a lista de bloqueio dos sensores;

Deve permitir terminar processos ativos executados nas estações de trabalhos e servidores;

Permitir coletar e fazer o *download* de um arquivo para investigação local detalhada;

Isolar a estação de trabalho desconectando-a da rede e permitindo se comunicar exclusivamente com a

console de gerenciamento do fabricante;

Restaurar a conectividade da estação de trabalho com a rede;

Iniciar uma sessão de *shell* remoto na estação de trabalho selecionada para execução de comandos remotos para investigação;

Deve ser possível fazer o download do histórico da sessão após finalizar a sessão remota do *shell* na estação de trabalho para fins de auditoria.

SOLUÇÃO DE SEGURANÇA PARA CARGAS DE TRABALHO HÍBRIDAS COM DETECÇÃO E RESPOSTA, INCLUINDO GARANTIA E ATUALIZAÇÃO DE VERSÃO POR 12 (DOZE) MESES

Características Gerais Da Solução

A solução deverá ser compatível com pelo menos os seguintes sistemas operacionais:

Windows Server 2000;

Windows Server 2003 SP1 e 2003 R2 SP2;

Windows Server 2008 e 2008 R2;

Windows Server 2012 e 2012 R2;

Windows Server 2016;

Windows Server 2019;

Windows Server 2022;

Red Hat Enterprise 5, 6, 7 e 8;

CentOS 5, 6, 7 e 8;

AIX 6.1, 7.1 e 7.2;

Oracle Linux 5, 6, 7 e 8;

SUSE Linux Enterprise Server 10, 11, 12 e 15;

Ubuntu 10, 12, 14, 16, 18 e 20;

Debian 6, 7, 8, 9 e 10;

Rocky Linux 8;

AlmaLinux 8;

Cloud Linux 5, 6, 7 e 8;

Solaris 10 1/13 Sparc;

Solaris 10 1/13 (x86/x64);

Solaris 11.2/ 11.3 Sparc;

Solaris 11.2/ 11.3 (x86/x64);

Solaris 11.4 (x86, x64 ou SPARC)

Amazon Linux e Amazon Linux 2 (x64).

A solução deverá ser totalmente compatível e homologada com o ambiente Vmware;

A console de gerenciamento deverá ser em nuvem, permitindo o gerenciamento das políticas de segurança através da Internet;

A solução deverá ser gerenciada por console Web, compatível com pelo menos os browsers Internet Explorer, Google Chrome e Firefox. Deve ainda suportar certificado digital para gerenciamento;

A solução deverá permitir a integração com pelo menos as seguintes plataformas de nuvem: Vmware vCloud, MS Azure e AWS;

Precisa ter a capacidade de controlar e gerenciar a segurança de múltiplas plataformas e sistemas operacionais, incluindo máquinas em nuvens externas a partir de uma console única e centralizada do próprio fabricante;

A solução deverá 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;

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;

A solução deverá possuir a funcionalidade tags para identificar falsos positivos ou facilitar a visualização de determinados alertas;

A solução deverá permitir a criação de widgets para facilitar a administração e visualização dos eventos;

A solução deverá permitir que a distribuição de patterns e novos componentes possa ser efetuada por agentes de atualização espalhados pelo 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;

A solução deverá fornecer pelo menos dois tipos de relatórios nos seguintes formatos PDF, CSV, XLS e RTF;

A solução precisa permitir que relatórios no formato PDF, possam ser enviados com uma senha única para cada destinatário;

A solução deverá prover relatórios contendo no mínimo as seguintes informações; malware, regras de IPS aplicadas e Firewall;

Em caso de solução e nuvem, o ambiente do fabricante deverá fornecer alta disponibilidade;

A solução de segurança ter a capacidade de identificar ataques entre conteineres;

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/TLS 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, ou de forma automatizada através de script PowerShell;

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, ou de forma automatizada através de bash script;

Em servidores Windows e Linux, a solução deverá permitir a atualização automática dos agentes após sua ativação;

Para servidores Linux, a solução deverá possibilitar a atualização automática da versão quando o agente reiniciar;

Para efeito de administração, a solução deverá avisar quando um agente se encontrar não conectado a sua console de gerenciamento;

Deve permitir a remoção automática de agentes inativos, definindo o período para, pelo menos 1 semana, 1 mês e 12 meses;

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;

A solução deverá vir com perfis pré-definidos e aptos a funcionarem de acordo com sua denominação;

A solução deverá 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;

A solução deverá permitir a configuração de componentes de integração com o vCenter, a fim de permitir a sincronização das máquinas virtuais conectadas a ele;

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;

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;

A solução deverá ser capaz de aplicar políticas diferentes para placas de redes diferentes em um mesmo servidor;

A solução deverá ser capaz de executar bypass completo de rastreamento de tráfego de forma que os módulos não atuem em determinado tipo de conexão ou pacote;

A solução deverá ter a capacidade de se integrar com o Amazon SNS e os principais softwares de SIEMs contemplando, no mínimo: Splunk, IBMQradar e HPArcSight de modo a permitir enviar os seus logs para essas soluções;

A solução deverá ter a possibilidade de enviar logs para SYSLOG servers;

Solução deverá permitir criar relatórios customizados de todas as suas funcionalidades;

Deve permitir enviar os relatórios para uma lista de contatos independente de login na console de administração;

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;

A solução deverá ter capacidade de gerar pacote de autodiagnóstico 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;

Deverá possibilitar colocar etiquetas em eventos para que se possam visualizar apenas os eventos desejados;

O fabricante deverá participar do 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 vCloud, de modo a importar e sincronizar os objetos (hosts vmware e guests vm) para a console de gerenciamento da solução;

O fabricante da solução deverá manter programa de pesquisa em vulnerabilidades há, pelo menos, 5 anos;

A solução deve possuir API documentada para integração na esteira de automação;

A documentação da API deve conter exemplos prontos para implementação de determinadas funcionalidades, como cookbooks;

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;

A solução deve permitir desabilitar os módulos individualmente;

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.

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 possuir listas de exclusão separadas por módulo da proteção antimalware como exclusão das detecções por comportamento, exclusão por machine learning e exclusão por assinatura;

Em plataforma Windows, a solução deve permitir criar exclusões de escaneamento a partir do certificado digital das aplicações;

A solução deve possibilitar a verificação de ameaças dentro de arquivos compactados, efetuando a limpeza apenas de arquivos maliciosos em casos de detecção. A limpeza deve ocorrer sem a descompactação do arquivo;

Em servidores Windows, deve identificar e bloquear ameaças através de métodos de Machine Learning, quarentenando arquivos identificados;

A solução deverá possuir a funcionalidade de Monitoramento de Comportamento para detectar mudanças e atividades suspeitas não autorizadas;

A solução deverá oferecer escanear 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 mínimo 20 camadas de compressão;

Para servidores Windows, a solução deverá permitir que o escaneamento agendado ocorra, ainda que o agente esteja offline na console de gerenciamento;

A solução deverá possuir ações pré-configuradas para cada tipo de ameaça detectada ou tomar uma ação baseada na configuração padrão da ferramenta;

Em servidores Windows, a solução deverá integrar-se com interface AMSI (Antimalware Scan Interface);

A solução deverá 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;

Deve possuir cache dos arquivos verificados de modo a evitar a redundância da varredura;

Deve possibilitar o controle do consumo de memória durante as varreduras a fim de minimizar os impactos de desempenho no servidor;

A solução deve possuir opção para forçar a comunicação com o agente e coletar os respectivos logs;

Em servidores Windows, deve possuir capacidade de detectar ameaças por comportamento;

Deverá ter a possibilidade de escanear drivers de rede mapeados nos servidores.

Proteção Contra URLs Maliciosas

Deve permitir a proteção contra acesso a websites ou URLs 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;

A solução deve permitir alterar o nível de sensibilidade para detecção de URLs maliciosas tendo, pelo menos, os níveis Alto, médio e baixo;

Deve permitir a criação de listas de exclusão, permitindo que usuários acessem determinadas URLs especificadas pelo administrador do sistema;

Deve permitir configurar notificações personalizadas para detecções desse módulo, deixando a cargo do administrador exibir ou não tais notificações;

Deverá ter capacidade de identificar acessos a URLs maliciosas além das portas padrão 80 e 443;

A solução deve permitir que o administrador reclassifique uma URL através do site do fabricante para evitar falsos positivos;

A proteção deve possibilitar proteção através da instalação de agente de segurança do fabricante da solução de segurança.

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;

A solução deverá 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;

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;

Deverá identificar escaneamentos ativos de porta ou da rede, bloqueando o IP ofensor por um período de tempo configurado pelo administrador;

Deverá permitir criar lista de exceções para identificar os Ips autorizados a realizar varreduras de portas ou da rede;

Poderá atuar no modo em linha para proteção contra-ataques ou modo escuta para monitoração e alertas.

Proteção De Vulnerabilidades de SO e Aplicações

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;

A solução deverá conter regras pré-definidas para detecções de ransomware para as principais famílias deste tipo de malware;

Precisa ter a capacidade de detectar uma conexão maliciosa, com a possibilidade de bloquear esta conexão;

Precisa conter regras de defesa para blindagem de vulnerabilidades e ataques que explorem os seguintes sistemas operacionais: Windows 2003, 2008, 2012, 2016, 2019, Linux Red Hat, Suse, CentOS, Ubuntu, Debian, Solaris, AIX 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 criptografado de entrada;

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

A solução deverá permitir a implantação nas plataformas Linux, Microsoft, Solaris, HP-UX, AIX, através da instalação de agentes;

Precisa ter a capacidade de detectar mudanças de integridade em arquivos e diretórios do SO e aplicações terceiras;

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 tempo real ou utilizando de scans periódicos para detectar mudanças de integridade;

Deverá alertar toda vez que uma modificação ocorrer em tempo real para ambiente Windows e pseudo real-time para ambiente Linux;

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

A solução deverá 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

A solução deverá 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;

A solução deverá possuir um mecanismo ao qual permita a execução de aplicações e scripts

automaticamente, sem intervenção manual, por um determinado período que deve ser no máximo 10 horas;

A solução deverá possuir no mínimo as funcionalidades de bloquear o que não for permitido explicitamente e permitir o que não for bloqueado explicitamente.

Detecção e Resposta

A solução deve ser compatível com Linux e Windows Server 2008 R2 e superiores;

A solução deve possuir módulo de investigação, detecção integrados;

Deve permitir que as detecções sejam correlacionadas com módulos de endpoint, rede e e-mail do próprio fabricante através de console dedicada. Não serão aceitas consoles de correlação de terceiros;

A console de correlação deve estar disponível na nuvem do próprio fabricante, o qual deve ser responsável pelas manutenções, atualizações e disponibilidade;

Deve possuir capacidade de encaminhar as atividades suspeitas identificadas nos servidores para a console de correlação centralizada;

O módulo de EDR deve atuar baseado em modelos de detecção de ataques avançados e furtivos;

Os logs de detecções devem estar disponíveis na console por, pelo menos, 30 dias;

A console de correlação centralizada deve possuir informações a respeito dos principais ataques que estão ocorrendo no mundo, quais plataformas e países são afetados, além de links para obter mais informações;

A solução deve permitir realizar buscas em todos os dados de atividades enviadas pelos servidores e demais sensores que estejam conectados na console, ainda que estas não sejam detectadas como maliciosas;

A console deve permitir o Single Sign-On através de SAML ou padrão equivalente;

Deve ser possível criar usuários com permissões distintas, contendo no mínimo, permissão total e permissão para realizar investigações;

Deve permitir habilitar ou desabilitar um determinado usuário sem excluí-lo da console;

Deve permitir o envio de notificações para os administradores através de email, API e integrações com SIEMs;

Deve prover visualização em linha do tempo com informações dos eventos monitorados em cada servidor;

Deve permitir a visualização entre usuários, servidores, processos/comandos, arquivos e demais componentes correlacionados em determinado ataque;

Deverá informar com qual técnica e tática do MITRE ATT&CK framework o ataque está relacionado, além de possuir link direto para o site da organização;

A solução deve mostrar, pelo menos, o timestamp, objetos envolvidos (comandos, processos, usuários, servidores);

Ao clicar em quaisquer dos objetos, a solução deve permitir realizar buscar específicas pelo objeto ou ainda executar ações como executar investigações mais aprofundadas.

SOLUÇÃO DE SEGURANÇA CONTRA AMEAÇAS AVANÇADAS COM DETECÇÃO E RESPOSTA, INCLUINDO GARANTIA E ATUALIZAÇÃO DE VERSÃO POR 12 (DOZE) MESES

Características gerais

A solução deverá ser instalada de modo a detectar ameaças avançadas no ambiente da CONTRATANTE, inspecionando o tráfego de rede, independente de agentes instalados;

Deve ser dimensionada para inspecionar 04Gbps de throughput;

A solução deve permitir que o administrador escolha uma implementação em modo inline ou em modo de

monitoramento através de tráfego espelhado;

Caso seja implementada no modo inline, a solução deverá permitir criar um by-pass para casos de falhas de interface;

Quando inline, a solução deverá ter a capacidade de analisar tráfego TLS;

Funcionalidades e Requisitos específicos:

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.

Esta solução deverá 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 poderá ser realizada em uma solução separada do sensor de HTTP e demais protocolos;

A capacidade de análise de artefatos em sandbox pode ser realizada através de no mesmo equipamento de análise;

A solução deverá 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 inspecionar o tráfego de rede de throughput de 04Gbps 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;

O ambiente controlado de sandbox deve contemplar, pelo menos, os sistemas operacionais CentOS, Windows 10, Windows 7, Windows Server 2003, 2008, 2012 R2, 2016 e 2019;

Deve possuir possibilidade de habilitação e desabilitação de regras de inspeção, individualmente, através de interface de gerenciamento web;

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 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;

A solução de análise em sandbox deve ter a capacidade de analisar, de forma estática e dinâmica, ameaças com características de autoinicialização ou alteração de arquivos de sistema, rootkits/cloakings, arquivos mal-formados, engenharia social, dentre outros;

A análise de sandbox deve identificar e analisar ameaças que tenham características de evitar a segurança e análise em sandbox, e auto-preservação;

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;

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 analise;

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, Google Chrome 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 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.

A solução deverá 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.

A solução deverá 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 transito 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.

A solução deverá 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.

Módulo de Detecção e Resposta

A solução deve ter a capacidade de integrar-se com a plataforma de investigação e resposta centralizada, a fim de enviar objetos suspeitos e metadados das detecções locais para correlação com as demais soluções de segurança do ambiente;

A funcionalidade deve ser licenciada para analisar o throughput total do appliance;

A solução deve permitir a integração dos eventos ocorridos em outros segmentos de rede e outros appliances com objetivo de correlacionar os ataques na rede;

Deve permitir a análise em linha de tempo gráfica, representando a sequência da comunicação dos ativos, bem como seu protocolo e direção;

Deve identificar tentativas de ataques avançados na rede da CONTRATANTE e correlacionar com eventos das soluções de estação de trabalho, servidores e e-mail, a fim de rastrear o passo-a-passo do ataque na rede;

Caso necessário, a CONTRATANTE pode optar em direcionar parte do licenciamento deste módulo para outros módulos da plataforma de Detecção e Resposta, como o monitoramento do email, endpoint ou servidores, sem acréscimos ou mudanças de licenciamento;

Ao clicar em um dos objetos identificados pela solução de inspeção de rede, a plataforma deverá informar um resumo do ataque em questão, contendo o IP/hostname envolvido, quais protocolos, atividades maliciosas, severidade do incidente, fases do ataque;

Deve exibir de forma e em tabela, as transações identificadas contendo detalhes do ataque, bem como os Indicadores de Comprometimento (IOCs).

SOLUÇÃO DE PREVENÇÃO DE INTRUSÃO DE PRÓXIMA GERAÇÃO (NGIPS) – 3GBPS

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 interfaces de rede modularizadas com, pelo menos, 2 slots para inserção de módulos;

Os módulos disponíveis para a solução NGIPS devem contemplar, pelo menos, expansão até 20 interfaces 10/100/1000Gbps, expansão até 20 interfaces 1Gbps SFP, expansão até 16 interfaces 10Gbps SFP+ e expansão até 4 interfaces 40Gbps QSFP+ (os transceivers necessários deverão ser entregues em conjunto da solução);

Para atendimento do bypass das interfaces cobre, não serão aceitos dispositivos externos. Nas interfaces de fibra óptica deverá ser ofertado módulo de bypass, que poderá ser embutido ou externo;

A solução NGIPS deverá usar discos de estado sólido (SSD), não sendo aceitos equipamentos com discos mecânicos;

Deverá ser entregue equipamento NGIPS que atenda às seguintes especificações:

IPS com throughput de inspeção de 3Gbps, podendo ser expandido até 5Gbps sem necessitar trocar o equipamento;

Deverá gerar latência igual ou inferior a 40 Microsegundos;

Deverá suportar pelo menos 390.000 novas conexões por segundo;

Deverá suportar pelo menos 29 milhões de sessões concorrentes;

Deverá suportar pelo menos 3.300 novas conexões SSL por segundo;

Deverá suportar inspeção de tráfego SSL de até 3,5Gbps;

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%.

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);

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 ou unidirecional (permitindo ativar a política de segurança nos sentidos de comunicação de A > B e de B > A [na mesma politica de segurança]. Ou com política de segurança dedicada de A > B 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 bypass total forçado;

A solução NGIPS deverá possuir 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

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;

A solução deverá 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

A solução de NGIPS deve suportar a operação de forma redundante, com possíveis cenários de operação Ativo-Passivo e Ativo-Ativo;

A gerência da solução deve permanecer ativa em caso de indisponibilidade dos NGIPS e possui cenários de alta disponibilidade;

A solução NGIPS ofertada deverá suportar fontes do tipo hot-swappable;

A solução NGIPS deverá suportar software bypass;

Em caso de atualizações ou reinicializações do NGIPS, a solução não deverá gerar nenhuma interrupção de rede.

Gerenciamento Centralizado

A solução NGIPS precisa suportar ser gerenciada de maneira centralizada por solução fornecida pelo mesmo fabricante;

A solução de gerenciamento centralizado entregue deverá permitir o gerenciamento de pelo menos 4 equipamentos NGIPS, sendo possível efetuar os mesmos níveis de configuração existentes na solução NGIPS;

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 possuir 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 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 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;

A solução deverá possuir suporte nativo a pelo menos as seguintes ferramentas: Qualys, Nessus e Nexpose;

A solução de gerenciamento centralizado deverá possuir 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 4 IPS. A solução ofertada deverá estar dimensionada para atender o exigido neste edital, com crescimento suportado previsto para até 20 NGIPS;

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);

A solução deverá ser fornecida em modo de alta disponibilidade, tendo pelo menos 2 nós de redundância;

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 rollback, além de capacidade de importação e exportação de configurações.

MÓDULO DE INVESTIGAÇÃO, CORRELAÇÃO E RESPOSTA À INCIDENTES EM ENDPOINTS E SERVIDORES POR 12 (DOZE) MESES

Características gerais

Plataforma de investigação e correlação de incidentes hospedada em nuvem do próprio fabricante, com *data lake* próprio para detecção e investigação de atividades maliciosas ou suspeitas para os seguintes contextos:

Estações de trabalho e servidores;

Dispositivos móveis (iOS e Android);

E-mails hospedados no Microsoft Office 365;

Sensores de rede.

Possuir console Web para gerenciamento e administração da ferramenta;

A solução deverá integrar-se aos sensores em uso pela CONTRATANTE;

O fabricante da solução deve dispor de laboratório próprio para desenvolvimento de vacinas e *engines* e possuir analista dedicado a desenvolvimento de defesas contra ameaças e malwares originados no Brasil. Esta informação deve ser comprovada pelo Fabricante através de documentação oficial.

Deve fazer uso de inteligência artificial e inteligência de ameaças do fabricante da solução para analisar e correlacionar as atividades dos sensores do ambiente;

A solução deverá permitir configuração de *Single Sign-On (SSO)* com suporte a SAML 2.0;

A solução deve prover diferentes níveis de administração e acesso a ferramenta para os usuários em pelo menos: Master Administrator, Administrator, Senior Analyst, Analyst e Auditor;

Deve permitir configuração de duplo fator de autenticação para acesso dos usuários à console de gerenciamento;

Deve registrar os logs de atividades realizados na console de gerência para fins de auditoria;

Ter capacidade de enviar os eventos e detecções para aplicações de *SIEM* e *SOAR*;

Deve permitir configuração de notificações por e-mail (SMTP) para envio de alertas e notificações;

Possuir painéis que apresentem visualização executiva dos principais incidentes e atividades no ambiente com base nos usuários, aplicações em nuvem acessadas, estações de trabalho e contas de e-mail;

Possuir modelos pré-definidos pelo fabricante de atividades suspeitas e/ou maliciosas para identificação e categorização de ameaças no ambiente;

A solução deve ser capaz de associar diferentes modelos de ameaças e associá-los a um único incidente/evento;

Deve ter capacidade de apresentar informações relacionadas ao MITRE para cada um dos eventos detectados no ambiente, caso possuam;

A visualização das técnicas e táticas deve ser feita através de matriz clicável para detalhamento do item selecionado;

Utilizar bases de inteligência de ameaças integrando relatórios de inteligência do fabricante e de terceiros para ajudar a identificar ameaças no ambiente;

Apresentar os alertas consolidados e correlacionados de ameaças para melhor investigação e resposta;

Permitir tomar diferentes ações de resposta no ambiente e monitorar cada ação tomada, com opção de desfazê-la;

Fornecer a capacidade de realizar buscas avançadas para localizar dados ou objetos no ambiente para análise avançada de atividades ou detecções;

Deve suportar a integração com serviço de gerenciamento de incidentes do próprio fabricante através da plataforma de investigação.

Deve permitir monitorar os status dos produtos integrados à plataforma de resposta à incidentes através da console de gerência.

Modelos de Detecção de Ameaça

A solução deve apresentar uma lista com todos os modelos de detecção pré-definidos que a solução possui;

Cada modelo deve possuir uma descrição e um *score* para auxiliar na identificação do risco e impacto de cada modelo;

Deve permitir ativar ou desativar qualquer modelo de detecção caso necessário;

Permitir criação de listas de exceção de objetos para redução de falso-positivo.

Os modelos de detecção deverão possuir níveis de severidade (*score)* individuais para cada modelo em pelo menos os seguintes níveis:

Crítico;

Alto;

Médio;

Baixo.

Threat Intelligence

Deve prover relatórios de inteligência de ameaças avançadas mais recentes e indicadores de comprometimento para ajudar a organização a se defender proativamente contra ameaças;

Deve integrar relatórios de inteligência criados por especialistas em ameaças do fabricante e terceiros para ajudar na identificação de ameaças;

Os relatórios de ameaças do fabricante deverão gerar alertas de detecção caso sejam identificadas

atividades presentes nos relatórios dentro do ambiente;

Deve ser possível identificar individualmente cada relatório de ameaça;

Cada relatório deverá possuir informações como, região/país alvo, plataforma alvo e campanha de ataques relacionadas a estes relatórios;

Deve permitir adicionar bases de inteligência terceiras de forma manual, por API, importando arquivos com base CSV ou STIX através de assinatura de feeds de inteligência de ameaças terceiros;

Deve permitir adicionar no mínimo os seguintes indicativos de comprometimento (IOCs) à base de inteligência:

Arquivos SHA-1;

URLs;

IPs;

Domínios;

Deve permitir configurar as ações dos indicativos de comprometimento (IOCs) adicionados à console em pelo menos:

Log;

Bloquear/Enviar à quarentena;

A base de inteligência terceira deve ser integrada através dos protocolos TAXII 2.0 ou TAXII 2.1.

Características para o sensor de Endpoint

A solução deve ser compatível com os sistemas operacionais Windows, Linux e MacOS;

O fabricante deve implementar e organizar os ataques baseados no framework MITRE ATT&CK®, identificando técnicas e táticas dos ataques;

A solução deve possuir módulo de investigação e detecção integrados;

Deve fazer uso de inteligência artificial e inteligência de ameaças do fabricante da solução para analisar e correlacionar as atividades dos sensores do ambiente;

Possuir painéis que apresentem visualização executiva dos principais incidentes e atividades no ambiente com base nos usuários, aplicações acessadas e estações de trabalho;

Utilizar bases de inteligência de ameaças integrando relatórios de inteligência do fabricante e de terceiros para ajudar a identificar ameaças no ambiente;

Apresentar os alertas consolidados e correlacionados de ameaças para melhor investigação e resposta;

Fornecer a capacidade de realizar buscas avançadas para localizar dados ou objetos no ambiente para análise avançada de atividades ou detecções;

Capacidade de construir sequências de buscas poderosas para localizar os dados ou objetos em seu ambiente que você deseja examinar;

Deve prover diferentes métodos de pesquisa, filtros e uma linguagem de consulta do tipo *Kibana* para identificar, categorizar e recuperar os resultados da pesquisa;

Deve ser possível realizar buscas através de *strings* parciais, exatas, valores nulos, *wildcards* e caracteres especiais;

Permitir investigar os alertas gerados pelos modelos de detecção por meio de uma análise impacto e análise de causa-raiz;

Deve consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento;

Deve permitir que as detecções sejam correlacionadas com módulos de servidores, rede e e-mail do próprio fabricante através de console dedicada. Não serão aceitas consoles de correlação de terceiros;

A console de correlação deve estar disponível na nuvem do próprio fabricante, o qual deve ser responsável

pelas manutenções, atualizações e disponibilidade;

Deve possuir capacidade de encaminhar as atividades suspeitas identificadas nos servidores para a console de correlação centralizada;

O módulo de EDR deve atuar baseado em modelos de detecção de ataques avançados e furtivos;

Os logs de detecções devem estar disponíveis na console por, pelo menos, 30 dias;

A console de correlação centralizada deve possuir informações a respeito dos principais ataques que estão ocorrendo no mundo, quais plataformas e países são afetados, além de links para obter mais informações;

A console deve permitir o Single Sign-On através de SAML ou padrão equivalente;

Permitir investigar os alertas gerados pelos modelos de detecção por meio de uma análise impacto e análise de causa-raiz;

Deve consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento;

Deve exibir os eventos de forma a priorizar os alertas mais críticos para que o analista realize a investigação, como pontuações ou níveis de prioridade;

Deve ser possível criar usuários com permissões distintas, contendo no mínimo, permissão total e permissão para realizar investigações;

Deve permitir habilitar ou desabilitar um determinado usuário sem excluí-lo da console;

Deve ser possível interagir com cada um dos objetos relacionados ao evento para análise avançada e resposta;

Deve destacar e organizar as atividades relacionadas a cada modelo de detecção por ordem cronológica, permitindo identificar a relação de cada atividade com os modelos de detecção;

Deve permitir o envio de notificações para os administradores através de email, API e integrações com SIEMs;

Deve prover visualização em linha do tempo com informações dos eventos monitorados em cada estação de trabalho;

Deve permitir a visualização entre usuários, servidores, processos/comandos, arquivos e demais componentes correlacionados em determinado ataque;

Deverá informar com qual técnica e tática do MITRE ATT&CK framework o ataque está relacionado, além de possuir link direto para o site da organização;

A solução deve mostrar, pelo menos, o timestamp, objetos envolvidos (comandos, processos, usuários, servidores);

Ao clicar em quaisquer dos objetos, a solução deve permitir realizar buscar específicas pelo objeto ou ainda executar ações como executar investigações mais aprofundadas;

Deve informar qual o escopo de impacto ou dimensionar o impacto em servidores, estações de trabalho e usuários, indicando a quantidade de componentes afetados no ataque;

Deve permitir que o analista possa alterar o status dos incidentes de acordo com seu tratamento e indicar falsos positivos para a plataforma;

Deve permitir adicionar arquivos SHA-1, URLs, IPs ou domínios a lista de bloqueio dos sensores;

Deve permitir remover arquivos SHA-1, URLs, IPs ou domínios a lista de bloqueio dos sensores;

Deve permitir terminar processos ativos executados nas estações de trabalhos e servidores;

Permitir coletar e fazer o *download* de um arquivo para investigação local detalhada;

Isolar a estação de trabalho desconectando-a da rede e permitindo se comunicar exclusivamente com a console de gerenciamento do fabricante;

Restaurar a conectividade da estação de trabalho com a rede;

Iniciar uma sessão de *shell* remoto na estação de trabalho selecionada para execução de comandos remotos para investigação;

Deve ser possível fazer o download do histórico da sessão após finalizar a sessão remota do *shell* na estação de trabalho para fins de auditoria.

Características para o sensor de cargas de trabalho

A solução deve ser compatível com Linux e Windows Server 2008 R2 e superiores;

A solução deve possuir módulo de investigação, detecção integrados;

Deve permitir que as detecções sejam correlacionadas com módulos de endpoint, rede e e-mail do próprio fabricante através de console dedicada. Não serão aceitas consoles de correlação de terceiros;

A console de correlação deve estar disponível na nuvem do próprio fabricante, o qual deve ser responsável pelas manutenções, atualizações e disponibilidade;

Deve possuir capacidade de encaminhar as atividades suspeitas identificadas nos servidores para a console de correlação centralizada;

O módulo de EDR deve atuar baseado em modelos de detecção de ataques avançados e furtivos;

Os logs de detecções devem estar disponíveis na console por, pelo menos, 30 dias;

A console de correlação centralizada deve possuir informações a respeito dos principais ataques que estão ocorrendo no mundo, quais plataformas e países são afetados, além de links para obter mais informações;

A solução deve permitir realizar buscas em todos os dados de atividades enviadas pelos servidores e demais sensores que estejam conectados na console, ainda que estas não sejam detectadas como maliciosas;

A console deve permitir o Single Sign-On através de SAML ou padrão equivalente;

Deve ser possível criar usuários com permissões distintas, contendo no mínimo, permissão total e permissão para realizar investigações;

Deve permitir habilitar ou desabilitar um determinado usuário sem excluí-lo da console;

Deve permitir o envio de notificações para os administradores através de email, API e integrações com SIEMs;

Deve prover visualização em linha do tempo com informações dos eventos monitorados em cada servidor;

Deve permitir a visualização entre usuários, servidores, processos/comandos, arquivos e demais componentes correlacionados em determinado ataque;

Deverá informar com qual técnica e tática do MITRE ATT&CK framework o ataque está relacionado, além de possuir link direto para o site da organização;

A solução deve mostrar, pelo menos, o timestamp, objetos envolvidos (comandos, processos, usuários, servidores);

Ao clicar em quaisquer dos objetos, a solução deve permitir realizar buscar específicas pelo objeto ou ainda executar ações como executar investigações mais aprofundadas.

MÓDULO DE INVESTIGAÇÃO, CORRELAÇÃO E RESPOSTA À INCIDENTES EM EMAIL POR 12 (DOZE) MESES

Características gerais

Plataforma de investigação e correlação de incidentes hospedada em nuvem do próprio fabricante, com *data lake* próprio para detecção e investigação de atividades maliciosas ou suspeitas para os seguintes contextos:

Estações de trabalho e servidores;

Dispositivos móveis (iOS e Android);

E-mails hospedados no Microsoft Office 365;

Sensores de rede.

Possuir console Web para gerenciamento e administração da ferramenta;

A solução deverá integrar-se aos sensores em uso pela CONTRATANTE;

O fabricante da solução deve dispor de laboratório próprio para desenvolvimento de vacinas e *engines* e possuir analista dedicado a desenvolvimento de defesas contra ameaças e malwares originados no Brasil. Esta informação deve ser comprovada pelo Fabricante através de documentação oficial.

Deve fazer uso de inteligência artificial e inteligência de ameaças do fabricante da solução para analisar e correlacionar as atividades dos sensores do ambiente;

A solução deverá permitir configuração de *Single Sign-On (SSO)* com suporte a SAML 2.0;

A solução deve prover diferentes níveis de administração e acesso a ferramenta para os usuários em pelo menos: Master Administrator, Administrator, Senior Analyst, Analyst e Auditor;

Deve permitir configuração de duplo fator de autenticação para acesso dos usuários à console de gerenciamento;

Deve registrar os logs de atividades realizados na console de gerência para fins de auditoria;

Ter capacidade de enviar os eventos e detecções para aplicações de *SIEM* e *SOAR*;

Deve permitir configuração de notificações por e-mail (SMTP) para envio de alertas e notificações;

Possuir painéis que apresentem visualização executiva dos principais incidentes e atividades no ambiente com base nos usuários, aplicações em nuvem acessadas, estações de trabalho e contas de e-mail;

Possuir modelos pré-definidos pelo fabricante de atividades suspeitas e/ou maliciosas para identificação e categorização de ameaças no ambiente;

A solução deve ser capaz de associar diferentes modelos de ameaças e associá-los a um único incidente/evento;

Deve ter capacidade de apresentar informações relacionadas ao MITRE para cada um dos eventos detectados no ambiente, caso possuam;

A visualização das técnicas e táticas deve ser feita através de matriz clicável para detalhamento do item selecionado;

Utilizar bases de inteligência de ameaças integrando relatórios de inteligência do fabricante e de terceiros para ajudar a identificar ameaças no ambiente;

Apresentar os alertas consolidados e correlacionados de ameaças para melhor investigação e resposta;

Permitir tomar diferentes ações de resposta no ambiente e monitorar cada ação tomada, com opção de desfazê-la;

Fornecer a capacidade de realizar buscas avançadas para localizar dados ou objetos no ambiente para análise avançada de atividades ou detecções;

Deve suportar a integração com serviço de gerenciamento de incidentes do próprio fabricante através da plataforma de investigação.

Deve permitir monitorar os status dos produtos integrados à plataforma de resposta à incidentes através da console de gerência.

Modelos de Detecção de Ameaça

A solução deve apresentar uma lista com todos os modelos de detecção pré-definidos que a solução possui;

Cada modelo deve possuir uma descrição e um *score* para auxiliar na identificação do risco e impacto de cada modelo;

Deve permitir ativar ou desativar qualquer modelo de detecção caso necessário;

Permitir criação de listas de exceção de objetos para redução de falso-positivo.

Os modelos de detecção deverão possuir níveis de severidade (*score)* individuais para cada modelo em pelo menos os seguintes níveis:

Crítico;

Alto;

Médio;

Baixo.

Threat Intelligence

Deve prover relatórios de inteligência de ameaças avançadas mais recentes e indicadores de comprometimento para ajudar a organização a se defender proativamente contra ameaças;

Deve integrar relatórios de inteligência criados por especialistas em ameaças do fabricante e terceiros para ajudar na identificação de ameaças;

Os relatórios de ameaças do fabricante deverão gerar alertas de detecção caso sejam identificadas atividades presentes nos relatórios dentro do ambiente;

Deve ser possível identificar individualmente cada relatório de ameaça;

Cada relatório deverá possuir informações como, região/país alvo, plataforma alvo e campanha de ataques relacionadas a estes relatórios;

Deve permitir adicionar bases de inteligência terceiras de forma manual, por API, importando arquivos com base CSV ou STIX através de assinatura de feeds de inteligência de ameaças terceiros;

Deve permitir adicionar no mínimo os seguintes indicativos de comprometimento (IOCs) à base de inteligência:

Arquivos SHA-1;

URLs;

IPs;

Domínios;

Deve permitir configurar as ações dos indicativos de comprometimento (IOCs) adicionados à console em pelo menos:

Log;

Bloquear/Enviar à quarentena;

A base de inteligência terceira deve ser integrada através dos protocolos TAXII 2.0 ou TAXII 2.1.

Características para o sensor de Email

Deve suportar a integração com serviço de gerenciamento de incidentes do próprio fabricante através da plataforma de investigação.

O recurso de detecção e resposta para e-mails deverá ser integrado à solução da Microsoft Office 365 sem a necessidade de alterar configurações dos serviços de e-mail, ou configurações dos usuários;

Possuir modelos pré-definidos pelo fabricante de atividades suspeitas e/ou maliciosas para identificação e categorização de ameaças no ambiente;

A solução deve ser capaz de associar diferentes modelos de ameaças e associá-los a um único incidente/evento;

Deve ter capacidade de apresentar informações relacionadas ao MITRE para cada um dos eventos detectados no ambiente, caso possuam;

Utilizar bases de inteligência de ameaças integrando relatórios de inteligência do fabricante e de terceiros para ajudar a identificar ameaças no ambiente;

Em caso de ameaça avançada por email, a solução deve permitir tomar diferentes ações de resposta no ambiente, contemplando, no mínimo:

Permitir adicionar o remetente (sender) de um e-mail na lista de bloqueio, impedindo o mesmo de enviar novos e-mails os usuários internos;

Mover o e-mail selecionado para a área de quarentena de um específico usuário ou todos os usuários que contenham este e-mail em suas caixas;

Deletar o e-mail selecionado das caixas selecionadas.

Serviço Especializado de Treinamento Hands-on, Pacote de 40 horas:

Serviço Especializado de Suportes corretivo e preventivo para 12 (doze) meses.

Serviço de Suporte especializado para ajustes, configurações, migrações e implementação da solução a ser fornecida.

Neste serviço deverá estar incluso todo tipo de suporte para funcionamento da solução, seja este corretivo ou preventivo.

Serviço especializado de suporte corretivo e preventivo para 12 (Doze) meses, prestados diretamente pelo fabricante da solução ou parceiro autorizado.

Serviço especializado de suporte para ajustes, configurações, migrações e implementação da solução a ser fornecida, a serem prestados pelo fabricante ou parceiro autorizado.

Neste serviço deverá estar incluso todo tipo de suporte para funcionamento da solução, seja este corretivo ou preventivo.

Considerando que esta SEDUC/RO não dispõe de um corpo técnico suficiente em número de profissionais para absorver atividades e atender demandas relativas ao escopo, o que nos obriga a contratar serviços técnicos especializados para tais necessidades, para que haja a garantia de prestação eficiente destes serviços, a contratada deverá empregar funcionários devidamente qualificados na utilização desse tipo de ferramenta, a ser comprovado através de apresentação de certificados emitidos pelo próprio fabricante, ou instituições por ele autorizados. Os profissionais certificados alocados podem ser do fabricante ou parceiro autorizado do fabricante.

4. CLASSIFICAÇÃO DOS BENS (LEI Nº. 10.520/02, ART. 1º)

4.1. Os bens 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.

5. JUSTIFICATIVA/MOTIVAÇÃO (LEI 10.520 ART. 3º, I; E LEI 8.666/93, ART. 3º, § 1º, I)

5.1. Do Interesse Público 0030898123

A Secretaria de Estado da Educação de Rondônia – SEDUC/RO, alinhada as evoluções tecnológicas realizou investimento em infraestrutura de DATACENTER com o foco em hiperconvergência e proteção de dados “fria”, os quais hoje sustentam os sistemas corporativos e os serviços de tecnologia da informação ofertados à população e aos servidores públicos através da Coordenadoria de Tecnologia da Informação e Comunicação - COTIC/SEDUC, que tem como principal atribuição prover e manter os meios tecnológicos da SEDUC/RO e, portanto, vem fazendo ao longo dos últimos anos a inovação necessária para a melhoria do ensino público ofertado para a população do Estado por meio do uso de tecnologia com os sistemas de Diário Eletrônico, CODISE (Monitoramento das medições corporais dos alunos da rede estadual), JOER (Sistema de acompanha as etapas Municipais, Regionais e Estaduais dos jogos escolares de Rondônia), Sistema de Chamada Escolar, Matricula Online, Sistema Administrativo e Pedagógico (SIAP), Sistema de Gestão Escolar (SIGE), Sistema de Modulação de Servidores (MDL) e Sistemas de Reordenamento de Matricula (SRMN), Ambiente Virtual de Aprendizagem (AVA), apenas

para citar alguns dos sistemas implementados ao longo dos últimos anos.

Atualmente a SEDUC/RO possui um parque computacional em seu DATACENTER formado por plataforma de processamento e armazenamento de dados “vivos” hiperconvergente distribuídos em duas localidades separadas geograficamente, comutadores de rede de alto desempenho e baixa latência com velocidades predominantes de 20Gbps, em média 260 (duzentas e sessenta) máquinas virtuais instaladas nos dois ambientes em modelo de replicação, que podemos estimar em torno de 36TB de volumetria de conteúdo em uso. Este ambiente usa o software Acropolis Hypervisor como virtualizadores e possui diversas aplicações cruciais ao funcionamento orgânico desta Secretaria de Educação do Estado de Rondônia, como por exemplo, Servidores de Arquivos, Servidores de Banco de Dados, Sistemas de Monitoramento de Ativos de Redes, Administração centralizada de ativos de rede (Access Point e Firewalls), entre outras tecnologias.

Além do ambiente de DATACENTER, esta Secretaria de Estado da Educação vem, desde início da atual gestão, fazendo investimentos na modernização dos seu parque computacional no ambiente coorporativo e educacional na sede desta SEDUC/RO, nas Coordenadorias Regionais de Ensino - CREs e em todas as unidades administrativas e escolares, renovando e criando novos laboratórios de informática, sala de professores, ambiente administrativos e alcançando inclusive os estudantes e professores em sala de aula, com a aquisição de notebooks aos professores da rede estadual de ensino e tablets para os alunos da rede pública de ensino. O próprio ambiente de sala de aula está sendo modernizado com a aquisição de lousas digitais para enriquecer o ensino e aumentar o interesse dos nossos alunos com um ambiente escolar moderno.

Só para se ter exemplo, apenas par atender as necessidades dos professores da rede estadual de ensino, foram adquiridos 7.824 notebooks através do processo 0029.386866/2021-11, e temos que considerar que o investimento feito no parque de computadores novos foi de 24.873 unidades com a finalidade de atender diversos setores no âmbito desta Secretaria de Estado da Educação e das unidades administrativas e escolares a ela vinculadas.

Considerando que possuímos em nossos sistemas de cadastro dados de alunos, alunos menores de idade, dados de pais e/ou responsáveis e dados dos servidores públicos vinculados a esta SEDUC/RO, sendo imensurável a quantidade de dados pessoais, que se encontram atualmente distribuídos em vários servidores de banco de dados e aplicações distintas.

Com o exposto, esclarecemos que a área de estudos da Segurança da Informação, corroborada pela família de Norma ISO 27000 e frameworks internacionais como NIST (americano), apresentam 3 grandes pilares para fundamentar todas as ações de segurança cibernética: Disponibilidade, Integridade e Confidencialidade, onde todas as ações, estratégias e justificativas se apoiam.

A Disponibilidade se trata de manter os dados e ativos funcionais e operacionais o máximo de tempo possível. A Integridade é sobre os dados inalterados por terceiros que não possuam permissão para tal. Por último a Confidencialidade diz respeito a manter acessível os dados apenas a quem é de direito.

Dito isto, o arcabouço jurídico brasileiro vem, nos últimos anos, evoluindo e se modernizando para abarcar a segurança da informação como parte fundamental da sociedade brasileira, como sociedade e nação, criando leis como a lei nº 12.965, de 2014 (Marco Civil da Internet), lei nº 13.709, de 2018 (Lei Geral de Proteção de Dados), e até mesmo decretos, como o decreto nº 9.637, de 2018 que estipulou a Política De Nacional De Segurança Da Informação.

Foi constatado que no início de 2021 as notificações referentes a ataques cibernéticos cresceram 220% em relação ao mesmo período em 2020. Alguns ataques recentes foram amplamente noticiados, como o caso do Superior Tribunal de Justiça, que ocorreu em 4 de novembro de 2020. Com esse ataque, os ministros e servidores não conseguiam acessar seus próprios arquivos e e-mails por dez dias, quando os sistemas foram restaurados. Outro caso de ataque cibernético que ficou bem conhecido foi o da empresa de processamento de carne JBS, que teve as redes de computadores *hackeadas*, fazendo com que algumas operações em diferentes localidades fossem temporariamente fechadas. Este ataque foi detectado no dia 30 de maio de 2021, quando ocorreram anormalidades no funcionamento de alguns servidores e foi encontrada uma mensagem que exigia o pagamento de um resgate para liberação do sistema da empresa. A empresa só restabeleceu o funcionamento normal após o pagamento de uma vultosa quantia financeira.

Um caso mais atual é o da rede de lojas varejistas Renner que sofreu um ataque no dia 19 de agosto de

2021, afetando diretamente seu funcionamento, onde o site da rede ficou indisponível, seu comércio online e presencial inoperante. Estes ataques influenciam diretamente na produção da empresa, causando prejuízo em tempo de produção ou na busca do resgate dos dados.

Diante de todo o exposto, esta Secretaria de Estado da Educação - SEDUC/RO, vem tentando, por meio de uma série de aquisições, modernizar e aprimorar suas camadas de segurança cibernética, de modo a oferecer aos seus usuários, a tranquilidade de poder trabalhar tentando minimizar as preocupações com incidentes, e à sociedade rondoniense a certeza que suas informações estão guardadas e seguras contra vazamentos, roubos e extorsão.

Estas aquisições visam, por meio de uma estratégia complexa de defesa em camadas que se completam e complementam em profundidade defender não apenas os ativos, mas a organização e seus usuários.

As violações de dados estão ocorrendo em uma taxa cada vez maior. Cada vez mais as organizações estão sentindo os impactos devido a essas violações. Empresas de pesquisa de mercado que prestam assessoria sobre o impacto existente e potencial da tecnologia estimam que pelo menos 80% das violações de dados têm conexão com credenciais privilegiadas e identidades comprometidas como: senhas, tokens, chaves e certificados.

O Plano Diretor de Tecnologia da Informação do Estado de Rondônia PDTI 2016-2019, atualizado para o biênio 2021-2022, possui no seu arcabouço a diretriz de número 14 trata especificamente de segurança da informação física e lógica, ou seja, as estratégias de proteção e salvaguarda de dados são premissas e elemento intrínseco a qualquer modelo serviço de TIC provido por qualquer entidade do estado, bem como Normas Internacionais de Segurança da Informação, cito ABNT NBR ISO/IEC 27001 e 27002. E estar em acordo com essas normatizações, é estar preparado para atender aos requisitos de excelência em qualidade na prestação de serviços para a população do Estado de Rondônia.

Considerando que compete a esta Coordenadoria de Tecnologia da Informação e Comunicação - COTIC/SEDUC, planejar, implementar, acompanhar e executar as ações de tecnologia da informação nesta SEDUC, nas Coordenadorias Regionais de Educação – CREs e nas Escolas da Rede Pública Estadual, por meio do desenvolvimento e atualização de programas e sistemas da informação, visando o atendimento de demandas operacionais e administrativas desses órgãos educacionais, assegurando a disponibilidade, a qualidade e a confiabilidade dos serviços de tecnologia da informação e dados na Educação Pública Estadual.

Considerando que desde o ano de 2019, a SEDUC/RO vem adquirindo e implementando tecnologias de segurança em múltiplas camadas para aumentar sua maturidade na proteção dos dados armazenados em sua rede, o que tem demonstrado eficiência através dos indicadores de segurança digital, porém, estudos recentes apontam a necessidade de detectar ataques além do endpoint, tendo uma visão holística, principalmente nos servidores, email e na rede. Esse conceito está alinhado ao que o mercado chama de XDR (Extended Detection and Response), que vai além da detecção e resposta nos endpoints (EDR), dando maior visibilidade sobre os ataques e correlacionando os eventos relevantes a serem tratados. O XDR, com seu serviço de resposta a incidentes agregado, permite ainda aumentar a velocidade de análise em caso de incidentes de segurança, o que é reforçado pelo Gartner, ao definir essa estratégia como um dos principais projetos de segurança cibernética para os próximos anos.

Considerando os recentes relatos de ciberataques e violações de dados em ambientes com dados pessoais e dados pessoais sensíveis no cenário nacional, está COTIC/SEDUC busca consolidar e manter atualizadas as camadas de proteção existentes que estão em utilização desde o ano de 2019, adquiridas através do processo administrativo 0029.484700/2019-45. As licenças adquiridas estão em período de vencimento próximo e, portanto, dado a sua importância no contexto de segurança cibernetica, precisam ser renovadas e ter ampliadas o seu escopo de atendimento no âmbito desta secretaria, que conforme demonstrado, vem se modernizando e instalando novos equipamentos de TI no seu parque computacional.

Considerando que recentemente várias empresas públicas e privadas têm sido afetadas por ataques do tipo Ransonware (ferramentas de sequestro de dados), como já mencionado, que requerem uma nova abordagem de segurança.

Essa nova abordagem começa pela revisão das funcionalidades de segurança das estações de trabalho. Outra situação que necessitamos priorizar é a proteção dos arquivos transitados com a nuvem da Google dado ao uso da solução de armazenamento ilimitado que esta secretaria dispõe junto a este fornecedor.

Atualmente está COTIC/SEDUC gerencia 192.046 contas de alunos e professores cadastrados no Google Drive. Neste sentido necessitamos de uma solução de segurança que seja capaz de atuar protegendo os usuários contra ameaças avançadas que possam entrar na corporação vindas através de e-mail com conteúdo malicioso e também de possíveis arquivos maliciosos que possam ser compartilhados entre os usuários através do serviço de compartilhamento de arquivos e e-mails, além de ser possível ainda o controle de informações confidenciais que podem ser manipuladas dentro desses compartilhamentos.

É extremamente urgente adotar mecanismos e recursos tecnológicos que possuam a capacidade de inspeção avançada deste tráfego, assim como a simulação do comportamento das ameaças em ambiente controlado (SANDBOX) visando o tratamento e resposta aos incidentes de segurança. Notadamente no que diz respeito à segurança de dados, é consenso de que não existe uma única bala de prata capaz de oferecer proteção contra todos os tipos de ameaças cibernéticas existentes atualmente. A estratégia de proteção integrada em camadas visa adotar mecanismos de detecção e bloqueio de ameaças em cada ponto de fragilidade da infraestrutura de tecnologia, porém de forma a propiciar a visão integrada do ambiente, facilitando a gestão e agilizando o tempo de resposta aos incidentes.

Considerando também o aumento das demandas da área de TIC, e considerando a velocidade de surgimento de novas ameaças e dado o surgimento e a evolução de ameaças massivas, robustas e danosas, tais como o ataque com o ransomware WannaCry e Petya, que criptografam os dados e solicitam resgates em Bitcoins, moeda virtual e principalmente devido aos recentes ataques avançados à infraestrutura de servidores e sistemas no cenário nacional, os quais geraram impactos negativos a alguns entes públicos. Verifica-se então a necessidade de expansão da segurança em outras camadas e ambientes, não se limitando a proteger apenas os endpoints e o serviço de e-mail, mas também o ambiente de data center virtualizado (servidores e sistemas) com solução específica para a dinâmica destes ambientes com a finalidade de minimizar que tais incidentes gerem impactos para a área de negócios desta SEDUC/RO e para a sociedade que se utiliza do serviço público por ela prestado. Do mesmo modo que as ameaças estão em constante evolução, as camadas de proteção precisam ser adaptadas e melhoradas para garantir a segurança do ambiente. Aumentar a segurança pode tornar-se um desafio ao mesclar fabricantes em uso, bem como treinar as equipes para utilizarem as tecnologias da melhor maneira possível. Dessa maneira, a busca pela unificação e padronização, além do apoio dos serviços de especialistas, referem-se a requisitos de segurança.

Diante da importância de criar essa estratégia de defesa conectada de ameaças, atendendo aos padrões do Cybersecurity Framework do NIST, o qual recomenda tecnologias e procedimentos para Identificar, Proteger, Detectar, Responder e Recuperar; a SEDUC/RO busca acrescentar camadas de Detecção e Resposta aos seus endpoints e servidores – visto que já possui o módulo para email e rede do fabricante atual – além do serviço especializado do fabricante para monitorar o ambiente 24x7, identificando, reportando e atuando nos incidentes ainda no início.

Pesquisas de mercado mostraram que para compor esse requisito seriam necessárias 2 ou mais tecnologias de fabricantes distintos, o que torna mais complexo o gerenciamento da solução, além de elevar o custo global e pode representar falhas de segurança. Essa estratégia técnica de unificar as soluções segue também a recomendação do Gartner para o XDR, a qual visa melhorar a proteção, detecção e resposta, aumentar a produtividade geral da equipe e reduzir o custo total de propriedade (TCO).

Ademais, outros fatores que impactam na decisão de padronização:

1. Aproveitamento do conhecimento técnico das equipes para extrair o máximo das tecnologias contratadas ao reduzir a curva de aprendizado;

2. Gestão centralizada das tecnologias de visibilidade, proteção, detecção e resposta;

3. A integração nativa entre as soluções de segurança contratadas permitirá ter uma visão completa e unificada do ambiente de tecnologia da informação contra as ameaças cibernéticas. No caso de multifornecedores, a integração nem sempre ocorre, reduzindo, consideravelmente, a visibilidade para detecção das ameaças cibernéticas, impactando diretamente no tempo de resposta e proteção;

4. A visão unificada por meio de console única trará para a SEDUC-RO um ganho considerável no tempo de detecção, bem como no nível de classificação das ameaças, sejam elas reais ou aquelas consideradas como falso positivo. Todas as tecnologias a serem contratadas têm integração nativa com a solução atual

de gestão e inteligência de ameaças, trazendo uma maior qualidade na detecção e aumentando o nível de proteção contra as ameaças cibernéticas no ambiente da SEDUC-RO.

Implantada no ambiente da SEDUC/RO desde o ano de 2019 e atendendo adequadamente, a opção pela Trend Micro se dá pela reconhecida e relevante posição de liderança nas principais tecnologias de segurança digital. A Forrester reconheceu recentemente a Trend Micro como líder em detecção e resposta empresarial. Esse relatório é corroborado com a posição de destaque na avaliação APT29, FIN7 e Carbanak do MITRE para tecnologias de EDR. A Trend Micro está categorizada ainda como líder nas categorias de Endpoint Protection Platform do Gartner desde 2002, em Email Security e Endpoint Protection do Forrester; além da liderança em Breach Detection System (BDS) pelo NSS Labs. Sendo destacada, portanto, como o parceiro mais adequado para apoiar na estratégia de XDR da SEDUC-RO.

A renovação e ampliação em si, 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.

Por fim, o processo em questão trará maior maturidade de segurança da informação e atualização das capacidades desta Secretaria de Estado da Educação para defender-se das ameaças digitais mais avançadas, as tecnologias propostas estão alinhadas aos requisitos da Lei Geral de Proteção de Dados (LGPD), aumentando a visibilidade sobre os ataques e possíveis roubos de dados pessoais.

5.2. Do Quantitativo Estimado0030898123

As quantidades presentes no item 3.3 do presente Termo de Referência foram apresentadas pela Coordenadoria de Tecnologia da Informação e Comunicação - COTIC/SEDUC, conforme Solicitação de Compra - Aquisição de Material 0030898123.

6. PRAZO E CONDIÇÕES DE ENTREGA/INSTALAÇÃO E RECEBIMENTO

6.1. Do Prazo e Condições de Entrega

6.1.1. A entrega dos produtos/início dos serviços, se dará no prazo de até 30 (trinta) dias uteis, contados da emissão da Nota de Empenho e/ou Assinatura do Contrato, através da disponibilização da Subscrição de Licença de Uso, com efetiva ativação.

6.1.2. A Secretaria de Estado da Educação encaminhará à contratada, a Ordem de Serviços, juntamente com o (s) endereço (s) da (s) unidade (s) administrativa (s), em conformidade com o cronograma da SEDUC-COTIC.

6.1.3. O prazo início dos serviços poderá ser prorrogado por períodos sucessivos, mediante o cumprimento, pela Contratada, dos seguintes requisitos cumulativos:

a) Solicitação de prorrogação protocolada dentro do prazo de início dos serviços;

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.

6.1.3.1. Não se admitirá prorrogação se:

a) O atraso ocorrer por culpa da contratada;

b) Se não cumprir os requisitos do item 6.1.4; ou

c) Houver interesse público devidamente justificado nos autos que demonstre ser a escolha mais vantajosa para a administração.

6.1.3.2. Ocorrendo recusa ou atraso na execução total ou parcial dos serviços, 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".

6.1.4. 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.

6.2. Das Condições de Recebimento

6.2.1. O recebimento do (s) material (is) se dará da seguinte forma:

a) Provisoriamente no prazo de até 05 (cinco) 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 do recebimento provisório, pelo responsável pelo acompanhamento e fiscalização do contrato, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo circunstanciado.

6.2.2. O recebimento provisório NÃO líquida a despesa e NÃO se presta para autorizar o pagamento dos materiais/bens.

6.2.3. O recebimento provisório ou definitivo não exclui a responsabilidade civil do CONTRATADO em face da eventual existência de vícios redibitórios.

6.2.4. 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 05 (cinco) 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.

6.2.5. 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.

6.2.6. 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.

6.2.7. O recebimento provisório ou definitivo não exclui a responsabilidade da Contratada pelos prejuízos resultantes da incorreta execução do contrato.

7. DOTAÇÃO ORÇAMENTÁRIA

7.1. As despesas do presente processo correrão por conta das Atividades abaixo detalhada**,** conforme o Plano Plurianual, e a Lei 5.533, de 14 de março 2023 - LOA, conforme a seguinte classificação:

Função Programática: 12.126.2125.2387-Modernizar a Infraestrutura Tecnológica de TI	
Fonte: 0112 - Recursos Destinados à Manutenção e Desenvolvimento de Ensino	
Natureza da Despesa: 4.4.90.40 - Aquisição de Software Pronto	
1.1	Trend Micro Smart Protection Complete
1.2	Trend Micro Smart Protection for Endpoints
1.3	Software de segurança para usuário final, com visibilidade completa para estações de trabalho com detecção e resposta, incluindo garantia e atualização por 12 (doze) meses
1.4	Solução de segurança para cargas de trabalho híbridas com detecção e resposta, incluindo garantia e atualização de versão por 12 (doze) meses
1.5	Módulo de investigação, correlação e resposta à incidentes em endpoints e servidores por 12 (doze) meses
1.6	Módulo de investigação, correlação e resposta à incidentes em email por 12 (doze) meses
Natureza da Despesa: 4.4.90.52 - Aquisição de Material Permanente e 4.4.90.40 - Aquisição de Software Pronto	
1.7	Solução de segurança contra ameaças avançadas com detecção e resposta, incluindo garantia e atualização de versão por 12 (doze) meses.

1.8	Solução de prevenção de intrusão de próxima geração (NGIPS) – 3Gbps
Natureza da Despesa: 3.3.90.40 - Serviços de Tecnologia da Informação e Comunicação	
1.9	Serviço Especializado de Instalação e configuração, Pacote de 40 horas.
1.10	Serviço Especializado de Treinamento Hands-on, Pacote de 40 horas.
1.11	Serviço Especializado de Suportes corretivo e preventivo para 12 (doze) meses por solução de segurança.

8. CONDIÇÕES DE PAGAMENTO

8.1. 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;

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).

8.1.1. As certidões elencadas nas alíneas de "c" a “g”, acima, serão aceitas se apresentada na forma "Negativa" ou "Positiva com efeito Negativa".

8.2. As Notas Fiscais/Faturas, emitidas em 2 (duas) vias, devendo conter no corpo da Nota Fiscal/Fatura, a descrição dos serviços, o número do empenho e o número da Conta Bancária da CONTRATADA, para depósito do pagamento.

8.3. O pagamento será efetuado através de Ordem Bancária - OB e depósito em conta corrente, indicada pela Contratada.

8.4. 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.

8.5. Na hipótese de a Nota Fiscal/Fatura apresentar 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 8.1.

8.6. Quando da ocorrência de eventuais atrasos de pagamento provocados exclusivamente pela Administração, o valor devido deverá ser acrescido de atualização financeira, e sua apuração se fará desde a data de seu vencimento até a data do efetivo pagamento, em que os juros de mora serão calculados à taxa de 0,5% (meio por cento) ao mês, ou 6% (seis por cento) ao ano, mediante aplicação das seguintes fórmulas:

$$I = \frac{(TX/100)}{365}$$

EM = I x N x VP, onde:

I = Índice de atualização financeira;

TX = Percentual da taxa de juros de mora anual;

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela em atraso.

8.7. Na hipótese de pagamento de juros de mora e demais encargos por atraso, os autos deverão ser instruídos com as justificativas e motivos e, ser submetidos à apreciação da autoridade superior competente, que adotará as providências para verificar se é ou não caso de apuração de responsabilidade, identificação dos envolvidos e imputação de ônus a quem deu causa.

8.8. O prazo para pagamento da Nota Fiscal só será contado da data de sua validação, considerando o trâmite administrativo. Considerar-se-á como sendo a data do pagamento a data da emissão da respectiva ordem bancária.

8.9. A Contratante não se responsabilizará por qualquer despesa que venha a ser efetuada pela Contratada, que porventura não tenha sido acordada no contrato. Os eventuais encargos financeiros, processuais e outros, decorrentes da inobservância, pela Contratada, de prazo de pagamento, serão de sua exclusiva responsabilidade.

9. DOCUMENTOS DE HABILITAÇÃO

9.1. Da 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 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;

f) No caso de agricultor familiar: Declaração de Aptidão ao Pronaf – DAP ou DAP-P válida, ou, ainda, outros documentos definidos pelo Ministério do Desenvolvimento Social, nos termos do art. 4º, §2º do Decreto n° 7.775, de 2012.

g) No caso de produtor rural: matrícula no Cadastro Específico do INSS – CEI, que comprove a qualificação como produtor rural pessoa física, nos termos da Instrução Normativa RFB nº 971, de 2009 (arts. 17 a 19 e 165).

h) 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.

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

9.2. 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;

9.2.1. Poderão ser aceitas certidão (ões) positiva (s) com efeito de negativa.

9.3. Seguridade 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

9.4. <u>Da Qualificação Econômico-Financeira</u>

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 há mais de um ano) ou Capital Social (licitantes constituídas há menos de um ano), de no mínimo 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).

9.5. <u>Da Qualificação Técnica</u>

9.5.1. O (s) Atestado (s) de Capacidade Técnica (declaração ou certidão), fornecido por pessoa jurídica de direito público e privado, comprovando o desempenho da licitante pelo fornecimento de bem pertinente e compatível em características e quantidades com o objeto da licitação, será conforme indicado abaixo.

9.5.2. O (s) Atestado (s) emitido (s) por pessoa de direito privado, bem como o (s) atestado (s) emitido (s)

por pessoa de direito público deverá (rão) constar órgão, cargo e matrícula do emitente (razão social, CNPJ, endereço, telefone, fax, data de emissão) e dos signatários do documento (nome, função, telefone, etc.), além da descrição do objeto, quantidades e prazos de prestação dos serviços, vale ressaltar, que a ausência das informações do órgão, cargo e matrícula do emitente nos atestados de capacidade técnica, não ensejará a imediata inabilitação do licitante, cabendo a promoção de diligência para averiguar a veracidade do documento, conforme previsto no art. 6º, parágrafo único, da Orientação Técnica n° 001/2017/GAB/SUPEL, incluído pela Orientação Técnica n° 002/2017/GAB/SUPEL;

> *"Art. 3º Os Termos de Referência, Projetos Básicos e Editais relativos à aquisição de bens e materiais de consumo comuns, considerando o valor estimado da contratação, devem observar o seguinte:*
>
> *I – até 80.000,00 (oitenta mil reais) - fica dispensada a apresentação de Atestado de Capacidade Técnica;*
>
> *II - de 80.000,00 (oitenta mil reais) a 650.000,00 (seiscentos e cinquenta mil reais) - apresentar Atestado de Capacidade Técnica que comprove ter fornecido anteriormente materiais compatíveis em características;*
>
> *III – acima de 650.000,00 (seiscentos e cinquenta mil reais) – apresentar Atestado de Capacidade Técnica compatível em características e quantidades, limitados a parcela de maior relevância e valor significativo;"*
>
> *Parágrafo único. Não se aplica a regra do inc. I, aplicando-se a regra do inc. II deste artigo, quando tratar da aquisição de bens e materiais de natureza mais complexas tais como equipamentos médicos, odontológicos, de segurança, eletrônicos, computacionais."*

a) Entende-se por pertinente e compatível em **<u>características</u>** o(s) atestado(s) que em sua individualidade ou soma de atestados, contemplem a parcela de maior relevância do objeto desta licitação, **quais sejam pelo fornecimento de software**;

b) Entende-se por pertinente e compatível em **<u>quantidades</u>** o (s) atestado (s) que em sua individualidade ou soma de atestados, demonstrem que a licitante forneceu o objeto do presentes processo, na quantidade correspondente a no mínimo **2% (dois por cento) do quantitativo total previsto no presente Termo.**

9.5.3. As exigências quanto aos atestados de capacidade técnica estão estabelecidas conforme art. 3º 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.

9.5.4. 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.

9.6. <u>Do Cumprimento do Disposto no Inciso XXXIII do Art. 7º da Constituição Federal:</u>

a) **Declaração** de cumprimento do inciso XXXIII do art. 7º da Constituição Federal**.**

9.7. <u>Da Certidão de "Nada Consta", referente a</u>:

a) CNIA - Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa e Inelegibilidade

b) Cadastro Nacional de Empresas Inidôneas e Suspensas

9.8. As regras definidas acima, relativas à habilitação, fundamenta-se no disposto na Lei de Licitações nº 8.666/93 e objetiva promover condições de mínimas, no entanto, suficientes, que possibilitem a verificação das condições de legalidade e capacidade técnico-financeira das empresas participantes, condições estas que atendidas, atenuam os possíveis riscos na execução contratual.

10. CONDIÇÕES CONTRATUAIS

10.1. A formalização da contratação se dará através de Contrato Administrativo, conforme disposto no Art. 62 da Lei nº. 8.666/93.

10.2. 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.

10.3. 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.

10.4. 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.

10.5. 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.

10.6. 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.

10.7. O contratado fica obrigado a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, com base no valor inicial atualizado do contrato, respeitando os limites do art. 65 da Lei nº 8.666/93 e suas alterações e ainda, em conformidade com o Art. 15, § 3º, do Decreto Estadual nº 18.340/2013..

10.8. 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.

11. PRAZO DE VIGÊNCIA CONTRATUAL

11.1. O Contrato terá vigência de 12 (doze) meses, podendo a duração estender-se pelo prazo de até 48 (quarenta e oito) meses após o início da vigência do contrato, conforme art. 57, IV, da Lei Federal n. 8.666/93.

11.2. Em havendo prorrogação do contrato, em comum acordo entre as partes, conforme previsto no item 13, o contrato poderá ser reajustado pelo índice oficial utilizado pelo Governo Federal para o cálculo da inflação, índice este acumulado durante o período de vigência do contrato.

11.3. A assinatura do termo de contrato após 60 (sessenta) dias da data de apresentação da proposta ou da data da licitação, precluirá o direito ao reajuste contratual, passando a ser contado o interregno mínimo para concessão de reajuste a parr da data da assinatura do contrato.

12. GARANTIA CONTRATUAL

12.1. Nos moldes do art. 56 da Lei 8.666/1993, o fornecedor será convocado a apresentar, na Coordenadoria de Tecnologia da Informação e Comunicação - COTIC/SEDUC desta Secretaria, no ato da assinatura do Contrato, comprovante de garana para sua execução, com validade durante todo período de vigência contratual, correspondente a 5% (cinco por cento) de seu valor global.

13. REAJUSTE CONTRATUAL

13.1. 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, bem como, observará as disposições constantes no Decreto Estadual nº 25.829/2021.

13.2. Ocorrendo às hipóteses previstas no Art. 2º, Inciso XIII, Decreto Estadual nº 25.829/2021, será concedido **reequilíbrio econômico-financeiro** do contrato, requerido pela contratada, desde que documentalmente e suficientemente comprovado a desarmonia contratual, podendo ser concedido utilizando algum índice oficial de inflação tais como: IPCA/IBGE, bem como, outro índice que vier a substituí-los.

13.3. Igualmente será admitido sua revisão para majorar ou minorar os preços registrados, em casos excepcionais, nas hipóteses legais e considerando os preços vigentes de mercado, em conformidade com o artigo 23-B no Decreto Estadual nº 18.340/2013, acrescido pelo Decreto nº 25.969/2021

§ 1°. A revisão de preços prevista no **caput** precederá de requerimento: **(Parágrafo acrescido pelo Decreto n° 25.969, de 7/4/2021)**

I - do detentor da ata, que deverá fazê-la antes do pedido de fornecimento e, instruindo seu pedido com documentação probatória de majoração de preço do mercado e a oneração de custos; ou **(Inciso acrescido pelo Decreto n° 25.969, de 7/4/2021)**

II - pelo órgão participante ou órgão interessado, comprovando por meio de pesquisas de preços que há minoração do valor originalmente registrado. **(Inciso acrescido pelo Decreto n° 25.969, de 7/4/2021)**

§ 2°. Comprovada a majoração dos valores de mercado nas hipóteses da alínea "d" do inciso II do artigo 65 da Lei n° 8.666, de 1993, o órgão gerenciador da Ata convocará, antes da efetiva alteração de preços, as demais licitantes na ordem de classificação original para que manifestem interesse em manter o preço original registrado em ata, de modo que, inexistindo interessados dispostos em manter o valor da ARP; os preços poderão ser revisados conforme disposto no **caput** deste artigo. **(Parágrafo acrescido pelo Decreto n° 25.969, de 7/4/2021)**

§ 3°. Comprovada a minoração dos valores de mercado, o órgão gerenciador da ata convocará os licitantes na ordem de classificação original para que manifestem interesse em adequar o preço registrado em ata, de modo que o órgão, mediante análise de vantajosidade e probidade das licitantes, poderá realizar, a seu critério técnico, os trâmites administrativos cabíveis para o cancelamento do beneficiário da ata. **(Parágrafo acrescido pelo Decreto n° 25.969, de 7/4/2021)**

§ 4°. A revisão aprovada não poderá ultrapassar o preço praticado no mercado e deverá manter a diferença percentual apurada entre o preço originalmente constante da proposta e o preço de mercado vigente à época do registro. **(Parágrafo acrescido pelo Decreto n° 25.969, de 7/4/2021)**

§ 5°. Para fins deste Decreto e do Sistema de Registro de Preços - SRP, por ele regulamentado, o órgão gerenciador do registro de preços, fixará por meio de Portaria, a forma de apuração do preço de mercado para efetivação de ajustes decorrentes das Atas de Registro de Preços. **(Parágrafo acrescido pelo Decreto n° 25.969, de 7/4/2021)**

14. RESCISÃO CONTRATUAL

14.1. 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.

14.2. Os casos de rescisão contratual serão formalmente motivados, assegurando-se à CONTRATADA o direito à prévia e ampla defesa.

14.3. A CONTRATADA reconhece os direitos da CONTRATANTE em caso de rescisão administrativa prevista no art. 77 da Lei nº 8.666, de 1993.

15. ACOMPANHAMENTO E FISCALIZAÇÃO

15.1. 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 convenientes;

15.2. O exercício da fiscalização pela CONTRATANTE, não excluirá ou reduzirá a responsabilidade da contratada;

16. SUBCONTRATAÇÃO, CESSÃO E/OU TRANSFERÊNCIA

16.1. É vedada a subcontratação, cessão e/ou transferência total ou parcial do objeto deste.

17. PARTICIPAÇÃO DE EMPRESAS REUNIDAS SOB A FORMA DE CONSÓRCIO

17.1. 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.

17.2. 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.

18. OBRIGAÇÕES das partes

18.1. <u>Da Contratante</u>

18.1.1. Receber o objeto no prazo e condições estabelecidas neste Termo de Referência;

18.1.2. Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento definitivo;

18.1.3. Comunicar à Contratada, por escrito, no prazo de 24 (vinte e quatro) horas úteis, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido;

18.1.4. Acompanhar e fiscalizar cumprimento das obrigações da Contratada, através de comissão/servidor especialmente designado;

18.1.5. Efetuar o pagamento à Contratada no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos no Edital e seus anexos;

18.1.6. Notificar previamente à Contratada, quando da aplicação de sanções administrativas; e,

18.1.7. 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.

18.2. <u>Da Contratada</u>

18.2.1. Cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto e, ainda:

18.2.1.1. Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes no Termo de Referência, acompanhado da respectiva nota fiscal, na qual constarão, conforme o caso, as indicações referentes a: marca, fabricante, modelo, procedência e prazo de garantia ou validade;

18.2.1.2. O produto deverá ser entregue contendo as informações precisas, corretas, claras, em língua portuguesa sobre suas características, quais sejam: qualidade, quantidade, composição, garantia, prazo de validade e origem;

18.2.1.3. O material entregue deverá ser original, não se admitindo, em hipótese alguma, o fornecimento

de material alternativo;

18.2.1.4. A Administração poderá solicitar testes dos materiais junto aos seus fabricantes, para verificar a legitimidade do produto. Se verificada a inadequação do produto ou sua falsidade, será feita notificação da empresa para que se proceda a substituição, no prazo máximo de 05 (cinco) dias úteis. Caso não seja realizada a substituição, a empresa ficará sujeita às penalidades previstas no Termo de Referência e em Contrato. Se a falsidade for declarada pelo fabricante, independente de substituição, os produtos ficarão retidos, para que se proceda a responsabilidade criminal, prevista no art. 96, da Lei nº 8.666/93;

18.2.1.5. Fornecer os produtos, objeto da licitação, de acordo com os preços, formas e prazos estipulados na proposta, responsabilizando-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 12, 13 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);

18.2.1.6. Reparar, corrigir, remover, refazer ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verifiquem imperfeições, vícios, defeitos ou incorreções decorrentes de fabricação, no prazo de 5 (cinco) dias úteis.

18.2.1.7. Comunicar à Contratante, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;

18.2.1.8. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

18.2.1.9. 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;

18.2.1.10. Responsabilizar-se por todas as despesas decorrentes da execução do contrato, inclusive locomoção, quaisquer outras que forem devidas, quer em relação à execução do fornecimento, quer em relação aos empregados;

18.2.1.11. 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;

18.2.1.12. 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;

18.2.1.13. 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;

18.2.1.14. Não efetuar, sob nenhum pretexto, a transferência de responsabilidade para outros, sejam fabricantes, técnicos ou quaisquer outros;

18.2.1.15. Prover todos os meios necessários à garantia da plena operacionalidade do fornecimento, inclusive considerados os casos de greve ou paralisação de qualquer natureza;

18.2.1.16. 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;

18.2.1.17. Permitirá e oferecerá condições para a mais ampla e completa fiscalização, durante o período de realização do Evento, fornecendo informações, propiciando o acesso à documentação pertinente e atendendo às observações e exigências apresentadas pela fiscalização;

18.2.1.18. 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;

18.2.1.20. O licitante se obriga a acompanhar, permanentemente, os meios de comunicação informados e responder as comunicações encaminhadas, sob pena de revelia; e,

18.2.1.21. Respeitar rigorosamente, no que se refere a todos os seus empregados utilizados na obra, a legislação vigente sobre trabalho, tributos, previdência social, acidentes de trabalho e outros, por cujo ônus

e encargos responderá unilateralmente em toda a sua plenitude.

19. SANÇÕES

19.1. Além daquelas determinadas por leis, decretos, regulamentos e demais dispositivos legais, a CONTRATADA estará sujeita as sanções definidas neste Termo de Referência.

19.2. 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.

19.3. Se a adjudicatária se recusar 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.

19.4. 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 Estadual de Fornecedores Impedidos de Licitar).

19.5. 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.

19.6. 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.

19.7. 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.

19.8. 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.

19.9. São exemplos de infração administrativa penalizáveis, nos termos da Lei nº 8.666, de 1993, da Lei nº 10.520, de 2002, do Decreto Estadual nº 26.182/2021 (**Pregão Eletrônico**):

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.

19.10. 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.

19.11. 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	Executar os serviços incompleto, paliativo substitutivo como por caráter permanente, ou deixar de providenciar recomposição complementar; por ocorrência.	02	0,4% por dia
2	Recusar-se a executar as determinações feitas pela FISCALIZAÇÃO, sem motivo justificado; por ocorrência;	04	1,6% por dia
3	Suspender ou interromper, salvo por motivo de força maior ou caso fortuito, a execução do serviço/fornecimento, por dia e por unidade de atendimento;	05	3,2% por dia
4	Destruir ou danificar documentos por culpa ou dolo de seus agentes; por ocorrência.	05	3,2% por dia
5	Permitir situação que crie a possibilidade ou cause danos físico, lesão corporal ou consequências letais; por ocorrência.	06	4,0% por dia
6	Recusar prestar os serviços nos locais indicados pela Administração, multa de 6% (seis) do valor total do Contrato;	07	6%
7	Inexecução total do contrato;	10	10 %
Para os itens a seguir, deixar de:			
8	Manter a documentação de habilitação atualizada; por item, por ocorrência.	01	0,2% por dia
10	Substituir funcionário que se conduza de modo inconveniente ou não atenda às necessidades do Órgão, por funcionário e por dia;	01	0,2% por dia
11	Iniciar a execução nos prazos estabelecidos, observados os limites mínimos estabelecidos por este Contrato; por item, por ocorrência.	02	0,2% por dia
12	Ressarcir o órgão por eventuais danos causados por sua culpa;	02	0,4% por dia
13	Prestar os serviços especificados no Termo de Referência, com a disponibilização de materiais e utensílios, que se fizerem necessários à execução do objeto, bem como, pessoal devidamente qualificado, com capacidade para atender as quantidades informadas neste Termo de Referência.	02	0,4 % por dia
14	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
15	Cumprir determinação formal ou instrução complementar da FISCALIZAÇÃO, por ocorrência;	03	0,8% por dia
16	Efetuar o pagamento de seguros, encargos fiscais e sociais, assim como quaisquer despesas diretas e/ou indiretas relacionadas à execução deste contrato; por dia e por ocorrência;	05	3,2% por dia

**** Incide sobre a parte inadimplida.***

19.12. As sanções aqui previstas poderão ser aplicadas concomitantemente, facultada a defesa prévia do interessado, no respectivo processo, no prazo de 05 (cinco) dias úteis.

19.13. Após 30 (trinta) dias da falta de execução do objeto, será considerada inexecução total do contrato, o que ensejará a rescisão contratual.

19.14. 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.

19.15. 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.

19.16. 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.

19.17. A sanção será obrigatoriamente registrada no Sistema de Cadastramento Unificado de Fornecedores - SICAF, bem como em sistemas Estaduais.

19.18. 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.

19.19. 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.

19.20. 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.

19.21. 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.

19.22. 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.

20. 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:

"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 a 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, alterado pelo Decreto Estadual n. 24.082, de 22/07/2019, 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.

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, e suas alterações por meio do Decreto nº 24.082/2019), ou seja, **utilizar o sistema é a obrigação legal.**

No presente caso, a Contratação de Solução Unificada de Segurança para proteção de *e-mail*, proteção de *endpoint* e proteção contra-ataques avançados, contemplando os serviços de instalação e configuração, transferência de conhecimento e suporte técnico, de que trata o presente instrumento, relaciona-se com a **necessidade de atendimento a mais de uma unidade escolar (inciso III)**, ensejando várias contratações, por isso, caso a aquisição não se prover via registro de preços, teríamos que reprisá-la várias vezes ao ano, o que demonstraria ineficiência na eleição da forma de contratação em afronta ao princípio da eficiência **(inciso I).** Além do que, o quantitativo solicitado é apenas uma estimativa, não se sabe exatamente o quantitativo a ser utilizado, pois **pela natureza do objeto e sua destinação, em razão do número de inclusão e/ou evasão escolar, não é possível definir previamente o quantitativo a ser demandado (inciso IV)**, é essa indefinição que faz que a contratação via registro de preço seja a mais vantajosa pois permite que a aquisição seja de **forma parcelada (inciso II)**, somente quando surgir a necessidade real, até porque, não temos estrutura física para armazenamento e estocagem dos produtos.

Dessa forma, o registro de preços confere flexibilidade às contratações públicas uma vez que a aquisição dele decorrente não é obrigatória, bem como pelo fato de que, a administração não precisa repetir os procedimentos de seleção do mesmo objeto durante o ano e poder decidir com curto espaço para resposta (abastecimento) o melhor momento da contratação; razão pela qual a SEDUC opta pela formação de registro de preços.

---

[1] MARÇAL, Justen Filho. Comentários à lei de licitações e contratos administrativos. 15° Edição. fls. 223/224;

[2] BONAFÉ, Marici Abreu. Pregão e Registro de Preços. In: CARDOZO, José Eduardo Martins (Coord.) Et. Al. Direito Administrativo Econômico. Atlas: São Paulo, 2011. Pág. 1251.

21. VIGÊNCIA DE ATA DE REGISTRO DE PREÇOS

21.1. O prazo de 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.

22. GERENCIAMENTO DA ATA DE REGISTRO DE PREÇOS CASO

22.1. 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.

23. UTILIZAÇÃO DA ATA E DO FORNECIMENTO ADICIONAL "CARONAS"

23.1. 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;

23.2. É facultada aos órgãos ou entidades municipais, distritais ou estaduais, a adesão a ata de registro de preços da Administração Pública Estadual, desde que está disponha do caráter anômalo, excepcional e não-obrigatório.

23.3. 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;

23.4. As aquisições ou contratações adicionais não poderão exceder, por órgão ou entidade, **a 50% (cinquenta por cento)** dos quantitativos dos itens do instrumento convocatório e registrados na ata de registro de preços para o órgão gerenciador e órgãos participantes;

23.5. 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;

23.6. Caberá ao órgão que se utilizar da ata, verificar a vantagem econômica da adesão a este Registro de Preço;

23.7. 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 ficam condicionadas 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; e,

23.8. 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.

23.9. Não será autorizada adesão a Ata de Registro de Preços para aquisição separada, de itens adjudicados por preço global para os quais a licitante vencedora não tenha apresentado o menor preço, conforme Decisão do Acórdão 7243/2017-Segunda Câmara.

24. ALTERAÇÃO DA ATA DE REGISTRO DE PREÇOS

24.1. Os preços registrados serão mantidos inalterados por todo o período de vigência da Ata de Registro de Preços - ARP, admitida sua revisão, para majorar ou minorar os preços registrados, em casos excepcionais, nas hipóteses legais e considerando os preços vigentes de mercado, nos termos do Decreto Estadual nº. 18.340 de 06/11/2013 (alterado pelos decretos Nº 24.082 DE 22/07/2019 e nº 25.969, DE 7 DE ABRIL DE 2021), observadas as disposições contidas na alínea "d" do inciso II do caput do artigo 65 da Lei 8.666/93.

25.2. Conforme disposto no Art. 15, § 1º, do Decreto nº 18.340/2013, alterado pelo Decreto nº 24.082/2019, é vedado efetuar acréscimos nos quantitativos fixados pela ata de registro de preços, inclusive o acréscimo de que trata o § 1º do artigo 65 da Lei nº 8.666, de 21 de junho de 1993.

25. APLICAÇÃO DO DECRETO ESTADUAL N°. 21.264/2016

25.1. Na execução dos serviços, a empresa contratada deverá adotar as práticas de sustentabilidade, conforme disposições constantes no Art. 7º do Decreto Estadual nº. 21.264/2016.

26. APLICAÇÃO DO DECRETO ESTADUAL N°. 21.675/2017

26.1. Não poderão ser concedidos o Tratamento Favorecido, Diferenciado e Simplificado às Microempresas – ME, Empresas de Pequeno Porte – EPP e Microempreendedores Individuais – MEI, conforme disposições estabelecidas no Decreto Estadual nº. 21.675/2017, considerando a justificativa disposta no item 27 – Agrupamento em Lote.

27. AGRUPAMENTO DOS LOTES

A Lei Geral de Licitações admite a contratação integral ou dividida em tantas parcelas quantas se demonstrem técnica e economicamente viáveis, com vistas ao melhor aproveitamento dos recursos disponíveis no mercado e à ampliação da competitividade, contudo, sem fugir da modalidade licitatória cabível para o total do objeto (§§1º e 2º, do art. 23, da Lei Federal nº 8.666/93).

Nesse sentido, dispõe o Tribunal de Contas da União - TCU (Acórdão 5301/2013-Segunda Câmara):

"É legítima a adoção da licitação por lotes/polos, quando a licitação por itens isolados exigir elevado número de processos licitatórios, onerando o trabalho da administração pública, sob o ponto de vista do emprego de recursos humanos e da dificuldade de controle, colocando em risco a economia de escala e a celeridade processual e comprometendo a seleção da proposta mais vantajosa para a administração. Não obstante, a licitação por itens poderia exigir a realização de igual número de contratações, o que, como já ressaltado, constituiria ônus aos servidores encarregados do acompanhamento desses instrumentos, o que possivelmente oneraria a Administração".

Ainda sobre o tema, a Corte de Contas Federal, através do Acórdão 861/2013-Plenário, trouxe o seguinte entendimento:

"É lícito o agrupamento em lotes de itens a serem adquiridos por meio de pregão, desde que possuam mesma natureza e que guardem relação entre si".

Nos mesmos moldes, o Tribunal de Contas do Estado de Rondônia se manifestou sobre o tema (Súmula 8/2014 –TCE/RO):

"A Administração Pública em geral deverá restringir a utilização do critério de julgamento menor preço por lote, reservando-a àquelas situações em que a fragmentação em itens acarretar a perda do conjunto; perda da economia de escala; redundar em prejuízo à celeridade da licitação; ocasionar a excessiva pulverização de contratos ou resultar em contratos de pequena expressão econômica".

A ampliação da competitividade não está diretamente relacionada com a formulação, pelo órgão contratante, do maior número de itens possíveis. Deve-se observar que em determinados seguimentos de mercado (produtos de alta e média tecnologia, ou que possam ser vendidos diretamente pelo fabricante e serviços) a contratação do objeto por item, ou sua distribuição em pequenos lotes possibilitarão a participação de um maior número de empresas regionalizadas, contudo, sem poder econômico para fomentar a disputa pelo melhor preço, prejudicando a economia de escala.

A divisão em Lotes visa atender ao Acórdão 3185/2016 do egrégio Tribunal de Contas do Estado – TCE/RO, buscando "*aumentaria da competitividade" entre as empresas do ramo.*

Contudo, o agrupamento dos itens do objeto do presente Instrumento em um lote único, se justifica em razão da sua separação não ser recomentada, conforme demostrado no Despacho da SEDUC-COTIC 0037798093, conforme descrito abaixo:

"...a separação entre serviço e soluções não é recomendada uma vez que existe a possibilidade de conflitos quanto à responsabilidade entre a empresa que vendeu a licença/subscrição e a prestadora do serviço, comprometendo a qualidade da entrega e causando prejuízo para a administração pública na prestação de um serviço crítico.

Considerando que a proteção do ambiente está unificada e administrada de modo centralizado, seria um risco separar os lotes e permitir que outras soluções sejam adquiridas. Isso traria uma possibilidade de conflito entre as soluções, causando problemas de desempenho, instabilidade e até mesmo falha da detecção de ameaças. Além disso, dificultaria a gestão das ferramentas, tornando complexa uma integração e visão centralizada. Por fim, isso poderia representar custos adicionais com gestão de ambiente, treinamento e curva de aprendizado da equipe. O descritivo cumpre boas práticas de mercado e normas como o CIS (Center of Internet Security Controls), que recomenda o uso de apenas uma solução de antimalware em endpoints para evitar conflitos, maximizar a eficiência e eficácia. Como complemento, a norma NBR ISO/IEC 27001:2013 prevê que a organização defina e implemente medidas de proteção adequadas para proteção contra software malicioso, destacando a importância de manter processos de avaliação de risco e evitando exposições desnecessárias."

Nesse diapasão, as vantagens seriam o maior nível de controle pela Administração na execução da prestação de serviços, a maior facilidade no cumprimento do cronograma preestabelecido, a observância dos prazos de entrega do objeto, concentração da responsabilidade pela execução a cargo de um fornecedor e melhor garana no acompanhamento dos resultados, para o objeto estabelecido neste Termo de Referência.

Portanto, consideramos os itens do lote único como sendo interdependentes e complementares na composição de uma solução de Tecnologia, devendo, portanto, serem licitados em um único grupo e entregues por uma única empresa de forma a garanr uma única entrega; minimizando o risco de fornecimento apenas parcial da solução, ou ainda o risco de comparlhamento de responsabilidades entre diferentes fornecedores, o que comprometeria o seu correto funcionamento.

Isso posto, entendemos que a formulação de único lote para disputa resultará na obtenção da proposta mais vantajosa para a Administração e em maior eficiência administrativa.

28. ESTIMATIVA DA DESPESA

28.1. 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.

29. DA AMOSTRA

29.1. Para o objeto deste TR, a aceitação das propostas não está condicionada a apresentação de amostras, sendo que a avaliação do produto será verificada por ocasião da entrega, estando tais produtos sujeitos a recusa de recebimento definitivo, caso não corresponda às especificações mínimas definidas nos autos.

30. CRITÉRIOS DE JULGAMENTO DAS PROPOSTAS

30.1. O critério de julgamento das propostas será de **MENOR PREÇO POR LOTE,** 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;

30.2. Caberá ao pregoeiro diligenciar, se, no curso da licitação, depreender indício de que o levantamento prévio de preços padece de fragilidade, a exemplo da disparidade entre o preço inicialmente previsto e o preço ofertado pelos parcipantes;

30.3.Na proposta deverão constar o preço unitário de cada item que compoe o lote, e preço global do lote, expressos e moeda corrente nacional, nele incluídas todas as despesas com a confecção, impostos, taxas,

seguro, frete e serviços, depreciação, emolumentos e quaisquer outros custos que, direta ou indiretamente venham a ocorrer.

31. CONDIÇÕES GERAIS

31.1. O presente instrumento objetiva apresentar regramento acerca da aquisição proposta pela Coordenadoria de Tecnologia da Informação e Comunicação - COTIC/SEDUC, restando preservados na íntegra, aspectos relativos à definição técnica, quantitativos, destinação e outras informações relativas ao objeto, sendo de competência desta SEDUC-CCOM, tão somente os aspectos relativos às normas de enquadramento da modalidade, para orientar a modalidade licitatória.

31.2. Para solução de prováveis controvérsias da contratação, ficou definido como cláusula compromissória, a forma estatal, conforme consta em cláusula na Minuta de Contrato 0037237259, anexo do Termo de Referência.

32. ANEXOS

32.1. Anexo I - Estudo Técnico 0031911199

32.2. Anexo II - Minuta de Contrato 0037236535

32.3. Anexo III - SAMS 0038158624

Na forma do que dispõe o Art. 7° § 2°, incisos I, II e III da Lei nº. 8.666/93, ***autorizo, aprovo, declaro e dou fé as laudas do presente Termo de Referência e Anexos***

Documento assinado eletronicamente por **Adriana Marques Ramos**, **Coordenador(a)**, em 05/07/2023, às 09:27, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.

Documento assinado eletronicamente por **Wanderlei Ferreira Leite**, **Coordenador(a)**, em 05/07/2023, às 09:38, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.

Documento assinado eletronicamente por **DÉBORA LÚCIA RAPOSO DA SILVA** , **Secretário(a) Adjunto(a)**, em 11/07/2023, às 16:57, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.

A autenticidade deste documento pode ser conferida no site portal do SEI, informando o código verificador **0039695603** e o código CRC **EA584837**.

GOVERNO DO ESTADO DE RONDÔNIA
Secretaria de Estado da Educação - SEDUC

SAMS

SOLICITAÇÃO E AQUISIÇÃO DE MATERIAIS/SERVIÇOS – SAMS

Unidade Orçamentária: 16.001 – Secretaria de Estado da Educação – SEDUC	**Unidade Administrativa:** Diretoria Administrativa e Financeira – SEDUC-DAF	**Unidade Solicitante:** Coordenadoria de Tecnologia da Informação e Comunicação - COTIC/SEDUC
Objeto: Constitui objeto do presente Termo de Referência a formação de Registro de Preços para futuras e eventuais Contratações, SOB DEMANDA, de empresa especializada e habilitada para fornecimento de Solução Unificada de Segurança para proteção de *e-mail*, proteção de *endpoint* e proteção contra-ataques avançados, contemplando os serviços de instalação e configuração, transferência de conhecimento e suporte técnico, para atendimento das necessidades da Secretaria de Estado da Educação, , conforme condições, quantidades e exigências estabelecidas neste instrumento.		

LOTE ÚNICO						
Item	**Descrição do Objeto**	**Unid. de Medida**	**Quant**	**Marca**	**Valor Unitário**	**Valor Total por item**
1	**Contratações, SOB DEMANDA, de empresa especializada e habilitada para fornecimento de Solução Unificada de Segurança para proteção de *e-mail*, proteção de *endpoint* e proteção contra-ataques avançados, contemplando os serviços de instalação e configuração, transferência de conhecimento e suporte técnico, contemplando:**		**01**			
1.1	Trend Micro Smart Protection Complete	Unidade	4300			
1.2	Trend Micro Smart Protection for Endpoints	Unidade	628			
1.3	Software de segurança para usuário final, com visibilidade completa para estações de trabalho com detecção e resposta, incluindo garantia e atualização por 12 (doze) meses	Unidade	24.873			
1.4	Solução de segurança para cargas de trabalho híbridas com detecção e resposta, incluindo garantia e atualização de versão por 12 (doze) meses	Unidade	390			

1.5	Módulo de investigação, correlação e resposta à incidentes em endpoints e servidores por 12 (doze) meses	Unidade	5000			
1.6	Módulo de investigação, correlação e resposta à incidentes em email por 12 (doze) meses	Unidade	4300			
1.7	Solução de segurança contra ameaças avançadas com detecção e resposta, incluindo garantia e atualização de versão por 12 (doze) meses	Unidade	2			
1.8	Solução de prevenção de intrusão de próxima geração (NGIPS) – 3Gbps	Unidade	4			
1.9	Serviço Especializado de Instalação e configuração, Pacote de 40 horas.	Unidade	20			
1.10	Serviço Especializado de Treinamento Hands-on, Pacote de 40 horas.	Unidade	18			
1.11	Serviço Especializado de Suportes corretivo e preventivo para 12 (doze) meses por solução de segurança.	Unidade	06			
					Valor Total do Lote:	

VALOR DA PROPOSTA EM R$:	VALIDADE DA PROPOSTA:	PRAZO DE ENTREGA:
LOCAL:	DATA:	TELEFONE DE CONTATO:
BANCO:	AGÊNCIA:	C/C:
ASSINATURA (QUANDO RUBRICADO, NOME POR EXTENSO OU CARIMBO DO RESPONSÁVEL PELA COTAÇÃO DA EMPRESA):		
CARIMBO DO CNPJ/CPF-ME	USO EXCLUSIVO DA SC/SUPEL	

Documento assinado eletronicamente por **Ana Lucia da Silva Silvino Pacini**, **Secretário(a)**, em 20/05/2023, às 21:09, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.

A autenticidade deste documento pode ser conferida no site portal do SEI, informando o código verificador **0038158624** e o código CRC **B2207A3C**.

GOVERNO DO ESTADO DE RONDÔNIA
Secretaria de Estado da Educação - SEDUC

MINUTA DE CONTRATO

ANEXO II

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. 26.182/2021, 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 objeto do presente Termo de Referência a formação de Registro de Preços para futuras e eventuais Contratações, SOB DEMANDA, de empresa especializada e habilitada para fornecimento de Solução Unificada de Segurança para proteção de *e-mail*, proteção de *endpoint* e proteção contra-ataques avançados, contemplando os serviços de instalação e configuração, transferência de conhecimento e suporte técnico, para atendimento das necessidades da Secretaria de Estado da Educação, conforme condições, quantidades e exigências estabelecidas no Termo de Referência e seus anexos.

1.1. Vinculação: Integram este Contrato além do Termo de Referência, as normas do (IDENTIFICAÇÃO DA MODALIDADE), o disposto na proposta da CONTRATADA e demais elementos que sirvam à exata definição do objeto descrito na cláusula primeira.

1.2. As informações quanto a **especificações e quantidade estimadas do** objeto desse contrato, estão previstas no **Item 3.3 do Termo de Referência, Anexo I do Edital.**

1.3. As informações quanto a **garantia do produto do** objeto desse contrato, estão previstas no **subitem 3.4 do Termo de Referência, Anexo I do Edital**.

1.3. As informações quanto a **caracteristica do objeto** objeto desse contrato, estão previstas no **subitem 3.5 do Termo de Referência, Anexo I do Edital**.

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 – PRAZO E CONDIÇÕES DE ENTREGA/INSTALAÇÃO E RECEBIMENTO

3.1. As informações do Prazo e Condições de Entrega estão previstas no **Item 6, subitem 6.1 do Termo de Referência, Anexo I do Edital.**

3.2. As informações das Condições de Recebimento estão previstas no **Item 6, subitem 6.2 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, e a Lei 5.533, de 14 de março 2023 - LOA, conforme a seguinte classificação:

Função Programática: 12.126.2125.2387-Modernizar a Infraestrutura Tecnológica de TI	
Fonte: 0112 - Recursos Destinados à Manutenção e Desenvolvimento de Ensino	
Natureza da Despesa: 4.4.90.40 - Aquisição de Software Pronto	
1.1	Trend Micro Smart Protection Complete
1.2	Trend Micro Smart Protection for Endpoints
1.3	Software de segurança para usuário final, com visibilidade completa para estações de trabalho com detecção e resposta, incluindo garantia e atualização por 12 (doze) meses
1.4	Solução de segurança para cargas de trabalho híbridas com detecção e resposta, incluindo garantia e atualização de versão por 12 (doze) meses
1.5	Módulo de investigação, correlação e resposta à incidentes em endpoints e servidores por 12 (doze) meses
1.6	Módulo de investigação, correlação e resposta à incidentes em email por 12 (doze) meses
Natureza da Despesa: 4.4.90.52 - Aquisição de Material Permanente e 4.4.90.40 - Aquisição de Software Pronto	
1.7	Solução de segurança contra ameaças avançadas com detecção e resposta, incluindo garantia e atualização de versão por 12 (doze) meses.
1.8	Solução de prevenção de intrusão de próxima geração (NGIPS) – 3Gbps
Natureza da Despesa: 3.3.90.40 - Serviços de Tecnologia da Informação e Comunicação	
1.9	Serviço Especializado de Instalação e configuração, Pacote de 40 horas.
1.10	Serviço Especializado de Treinamento Hands-on, Pacote de 40 horas.
1.11	Serviço Especializado de Suportes corretivo e preventivo para 12 (doze) meses por solução de segurança.

5. CLÁUSULA QUINTA – DO PREÇO

5.1. 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;

5.2. 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.

6. CLÁUSULA SEXTA – DAS CONDIÇÕES DE PAGAMENTO

6.1. As condições de pagamento estão previstas no **item 8 do Termo de Referência, Anexo I do Edital.**

7. CLÁUSULA SÉTIMA – DAS CONDIÇÕES CONTRATUAIS

7.1. A formalização da contratação se dará através de Contrato Administrativo, conforme disposto no Art. 62 da Lei nº. 8.666/93.

7.2. 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.

7.3. 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.

7.4. 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.

7.5. 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.

7.6. 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.

7.7. 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) com base no valor inicial atualizado do contrato, respeitando os limites do art. 65 da Lei nº 8.666/93.

7.8. 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.

8. CLÁUSULA OITAVA – DO PRAZO DE VIGÊNCIA CONTRATUAL

8.1. O Contrato terá vigência de 12 (doze) meses, podendo a duração estender-se pelo prazo de até 48 (quarenta e oito) meses após o início da vigência do contrato, conforme art. 57, IV, da Lei Federal n. 8.666/93.

8.2. Em havendo prorrogação do contrato, em comum acordo entre as partes, conforme previsto no item 13, o contrato poderá ser reajustado pelo índice oficial ulizado pelo Governo Federal para o cálculo da inflação, índice este acumulado durante o período de vigência do contrato.

8.3. A assinatura do termo de contrato após 60 (sessenta) dias da data de apresentação da proposta ou da

data da licitação, precluirá o direito ao reajuste contratual, passando a ser contado o interregno mínimo para concessão de reajuste a parr da data da assinatura do contrato.

9. CLÁUSULA NONA – DA GARANTIA CONTRATUAL

9.1. Nos moldes do art. 56 da Lei 8.666/1993, o fornecedor será convocado a apresentar, na Coordenadoria de Tecnologia da Informação e Comunicação - COTIC/SEDUC desta Secretaria, no ato da assinatura do Contrato, comprovante de garana para sua execução, com validade durante todo período de vigência contratual, correspondente a 5% (cinco por cento) de seu valor global.

10. CLÁUSULA DÉCIMA - DO REAJUSTE CONTRATUAL

10.1. 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, bem como, observará as disposições constantes no Decreto Estadual nº 25.829/2021.

10.2. Ocorrendo às hipóteses previstas no Art. 2º, Inciso XIII, Decreto Estadual nº 25.829/2021, será concedido **reequilíbrio econômico-financeiro** do contrato, requerido pela contratada, desde que documentalmente e suficientemente comprovado a desarmonia contratual, podendo ser concedido utilizando algum índice oficial de inflação tais como: IPCA/IBGE, bem como, outro índice que vier a substituí-los.

10.3. Igualmente será admitido sua revisão para majorar ou minorar os preços registrados, em casos excepcionais, nas hipóteses legais e considerando os preços vigentes de mercado, em conformidade com o artigo 23-B no Decreto Estadual nº 18.340/2013, acrescido pelo Decreto nº 25.969/2021

§ 1°. A revisão de preços prevista no **caput** precederá de requerimento: **(Parágrafo acrescido pelo Decreto n° 25.969, de 7/4/2021)**

I - do detentor da ata, que deverá fazê-la antes do pedido de fornecimento e, instruindo seu pedido com documentação probatória de majoração de preço do mercado e a oneração de custos; ou **(Inciso acrescido pelo Decreto n° 25.969, de 7/4/2021)**

II - pelo órgão participante ou órgão interessado, comprovando por meio de pesquisas de preços que há minoração do valor originalmente registrado. **(Inciso acrescido pelo Decreto n° 25.969, de 7/4/2021)**

§ 2°. Comprovada a majoração dos valores de mercado nas hipóteses da alínea "d" do inciso II do artigo 65 da Lei n° 8.666, de 1993, o órgão gerenciador da Ata convocará, antes da efetiva alteração de preços, as demais licitantes na ordem de classificação original para que manifestem interesse em manter o preço original registrado em ata, de modo que, inexistindo interessados dispostos em manter o valor da ARP; os preços poderão ser revisados conforme disposto no **caput** deste artigo. **(Parágrafo acrescido pelo Decreto n° 25.969, de 7/4/2021)**

§ 3°. Comprovada a minoração dos valores de mercado, o órgão gerenciador da ata convocará os licitantes na ordem de classificação original para que manifestem interesse em adequar o preço registrado em ata, de modo que o órgão, mediante análise de vantajosidade e probidade das licitantes, poderá realizar, a seu critério técnico, os trâmites administrativos cabíveis para o cancelamento do beneficiário da ata. **(Parágrafo acrescido pelo Decreto n° 25.969, de 7/4/2021)**

§ 4°. A revisão aprovada não poderá ultrapassar o preço praticado no mercado e deverá manter a diferença percentual apurada entre o preço originalmente constante da proposta e o preço de mercado vigente à época do registro. **(Parágrafo acrescido pelo Decreto n° 25.969, de 7/4/2021)**

§ 5°. Para fins deste Decreto e do Sistema de Registro de Preços - SRP, por ele regulamentado, o órgão gerenciador do registro de preços, fixará por meio de Portaria, a forma de apuração do preço de mercado para efetivação de ajustes decorrentes das Atas de Registro de Preços. **(Parágrafo acrescido pelo Decreto n° 25.969, de 7/4/2021).**

11. CLÁUSULA DÉCIMA PRIMEIRA – DA RESCISÃO CONTRATUAL

11.1. 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.

11.2. Os casos de rescisão contratual serão formalmente motivados, assegurado-se à CONTRATADA o direito à prévia e ampla defesa.

11.3. A CONTRATADA reconhece os direitos da CONTRATANTE em caso de rescisão administrativa prevista no art. 77 da Lei nº 8.666, de 1993.

12. CLÁUSULA DÉCIMA SEGUNDA – DO ACOMPANHAMENTO E FISCALIZAÇÃO

12.1. Conforme os termos do art. 67, § 1º e 2º, da Lei nº. 8.666/93, será designado 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

12.2. O exercício da fiscalização pela Contratante, não excluirá ou reduzirá a responsabilidade da Contratada.

13. CLÁUSULA DÉCIMA TERCEIRA – DA SUBCONTRATAÇÃO CESSÃO E/OU TRANSFERÊNCIA

13.1. É vedada a subcontratação, cessão e/ou transferência total ou parcial do objeto deste termo.

14. CLÁUSULA DÉCIMA QUARTA– DAS OBRIGAÇÕES DAS PARTES

14.1. As obrigações da Contratante, são aquelas estabelecidas no I**tem 18, subitem 18.1, do Termo de Referência, Anexo I do Edital.**

14.2. As obrigações da Contratada, são aquelas estabelecidas no I**tem 18, subitem 18.2 do Termo de Referência, Anexo I do Edital**

15. CLÁUSULA DÉCIMA QUINTA– DAS SANÇÕES

15.1. As sanções aplicáveis na execução do contrato são aquelas estabelecidas no **item 19 do Termo de Referência, Anexo I do Edital.**

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 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

Documento assinado eletronicamente por **Ana Lucia da Silva Silvino Pacini**, **Secretário(a)**, em 20/05/2023, às 21:09, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.

A autenticidade deste documento pode ser conferida no site portal do SEI, informando o código verificador **0037236535** e o código CRC **D068EBC6**.

Referência: Caso responda este(a) Minuta de Contrato, indicar expressamente o Processo nº 0029.102870/2022-18 SEI nº 0037236535

Governo do Estado de RONDÔNIA

Superintendência Estadual de Compras e Licitações
Coordenadoria de Pesquisa e Análise de Preços

ITEM	DESCRIÇÃO	UNID	QUANT.(A)	EMP 1	EMP 2	EMP 3	EMP 4	PREÇO MÍNIMO (D)	PREÇO MÉDIO (E)	DESVIO PADRÃO	COEFICIENTE DE VARIAÇÃO	PARAMETRO UTILIZADO (MÍNIMO/MÉDIO)	SUBTOTAL GERAL [F + G]
LOTE ÚNICO													
Cabeçalho referente ao lote único: Contratações, SOB DEMANDA, de empresa especializada e habilitada para fornecimento de Solução Unificada de Segurança para proteção de e-mail, proteção de endpoint e proteção contra-ataques avançados, contemplando os serviços de instalação e configuração, transferência de conhecimento e suporte técnico, contemplando:													
1.1	Trend Micro Smart Protection Complete	Unidade	4300	100,00	111,55	120,32	110,83	R$ 100,00	**R$ 110,68**	**8,32**	**7,52%**	**MÉDIO**	**R$ 475.924,00**
1.2	Trend Micro Smart Protection for Endpoints	Unidade	628	290,00	223,45	241,02	217,07	R$ 217,07	**R$ 242,89**	**33,00**	**13,59%**	**MÉDIO**	**R$ 152.534,92**
1.3	Software de segurança para usuário final, com visibilidade completa para estações de trabalho com detecção e resposta, incluindo garantia e atualização por 12 (doze) meses	Unidade	24.873	N/C	212,00	228,67	204,08	R$ 204,08	**R$ 214,92**	**12,55**	**5,84%**	**MÉDIO**	**R$ 5.345.705,16**
1.4	Solução de segurança para cargas de trabalho híbridas com detecção e resposta, incluindo garantia e atualização de versão por 12 (doze) meses	Unidade	390	1.102,00	1.456,00	1.570,51	1.324,58	R$ 1.102,00	**R$ 1.363,27**	**201,09**	**14,75%**	**MÉDIO**	**R$ 531.675,30**
1.5	Módulo de investigação, correlação e resposta à incidentes em endpoints e servidores por 12 (doze) meses	Unidade	5000	N/C	101,00	108,94	93,25	R$ 93,25	**R$ 101,06**	**7,85**	**7,76%**	**MÉDIO**	**R$ 505.300,00**
1.6	Módulo de investigação, correlação e resposta à incidentes em email por 12 (doze) meses	Unidade	4300	N/C	21,00	22,65	13,99	R$ 13,99	**R$ 19,21**	**4,60**	**23,94%**	**MÉDIO**	**R$ 82.603,00**
1.7	Solução de segurança contra ameaças avançadas com detecção e resposta, incluindo garantia e atualização de versão por 12 (doze) meses	Unidade	2	N/C	1.750.000,00	1.887.637,50	1.531.817,35	R$ 1.531.817,35	**R$ 1.723.151,62**	**179.423,02**	**10,41%**	**MÉDIO**	**R$ 3.446.303,24**
1.8	Solução de prevenção de intrusão de próxima geração (NGIPS) – 3Gbps	Unidade	4	N/C	920.333,00	992.717,19	902.376,94	R$ 902.376,94	**R$ 938.475,71**	**47.824,77**	**5,10%**	**MÉDIO**	**R$ 3.753.902,84**

1.9	Serviço Especializado de Instalação e configuração, Pacote de 40 horas.	Unidade	20	N/C	35.000,00	37.752,75	30.550,08	R$ 30.550,08	**R$ 34.434,28**	**3.634,51**	**10,55%**	**MÉDIO**	**R$ 688.685,60**
1.10	Serviço Especializado de Treinamento Hands-on, Pacote de 40 horas.	Unidade	18	19.000,00	25.000,00	26.966,25	23.144,00	R$ 19.000,00	**R$ 23.527,56**	**3.397,97**	**14,44%**	**MÉDIO**	**R$ 423.496,08**
1.11	Serviço Especializado de Suportes corretivo e preventivo para 12 (doze) meses por solução de segurança.	Unidade	6	37.800,00	50.000,00	53.932,50	40.068,05	R$ 37.800,00	**R$ 45.450,14**	**7.749,05**	**17,05%**	**MÉDIO**	**R$ 272.700,84**
VALOR DO LOTE 1													**R$ 15.678.830,98**

VALOR TOTAL	**R$ 15.678.830,98**

VALOR DO LOTE 1	**R$ 15.678.830,98**

LEGENDA:
NC = Não encontrado
* = Valores excluídos por elevar a taxa de desvio padrão acima de 20% conforme estipulado na Portaria nº 238/2019/SUPEL-CI

NOTA EXPLICATIVA:

IDENTIFICAÇÃO DAS COTAÇÕES	**EMP1**	**BANCO DE PREÇOS**
	EMP2	**BANCO DE PREÇOS**
	EMP3	**BANCO DE PREÇOS**
	EMP4	
	EMP5	
	EMP6	

1) NC
2) As descrições foram reduzidas neste quadro comparativo, porém se encontra completas no termo de referência ().

MODELO DE MINUTA DA ATA DE REGISTRO DE PREÇOS

ATA DE REGISTRO DE PREÇOS Nº XXXX/20XX/SUPEL_RO			
Origem:	Pregão Eletrônico nº 161/2023		
Data da Publicação no DOE:	XX/XX/XXXX	Processo nº	0029.102870/2022-18
Órgão Participante:	Secretaria de Estado da Seduc/RO		
Órgão gerenciador:	Superintendência Estadual de Compras e Licitações - SUPEL		

1. CLÁUSULA I – IDENTIFICAÇÃO DO(S) FORNECEDOR(S) REGISTRADO(S).

1.1. A identificação dos detentores está inserida no anexo único desta ata.

2. CLÁUSULA II – DO OBJETO

Registro de Preços para futuras e eventuais Contratações, SOB DEMANDA, de empresa especializada e habilitada para fornecimento de Solução Unificada de Segurança para proteção de *e-mail*, proteção de *endpoint* e proteção contra-ataques avançados, contemplando os serviços de instalação e configuração, transferência de conhecimento e suporte técnico, para atendimento das necessidades da Secretaria de Estado da Educação, conforme condições, quantidades e exigências estabelecidas neste instrumento

3. CLÁUSULA III – DA VALIDADE DA ATA DE REGISTRO DE PREÇOS

3.1. A validade desta ata de registro de preços será de 12 (doze) meses, contados a partir dapublicação no Diário Oficial do Estado.

4. CLÁUSULA IV – DA UTILIZAÇÃO DESTA ATA DE REGISTRO DE PREÇOS POR ÓRGÃO NÃO

4.1. A Adesão ao presente Registro de Preços fica condicionada ao atendimento das determinações do Estado de Rondônia, após autorização expressa do órgão gerenciador – Superintendência Estadual de Compras e Licitações – SUPEL.

4.2. A adesão fica ainda condicionada às exigências dispostas no Art. 26 do Decreto Estadual nº18.340/2013.

4.3. As aquisições ou as contratações adicionais (caronas) não poderão exceder, por órgão ou entidade, a 50% (cinquenta por cento) dos quantitativos dos itens registrados na ata de registro de preços.

4.4. O quantitativo decorrente das adesões à ata de registro dos preços não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na ata de registro de preços, independentemente do número de órgãos não participantes que aderirem.

5. CLÁUSULA V – DA REVISÃO E CANCELAMENTO DO REGISTRO

5.1. De acordo com artigo 21 e 22 do Decreto Estadual 18.340/2013 os preços registrados

oderão 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

5.2. Nos termos do Decreto Estadual 25.969 de 07 de abril de 2021, os preços registrados serão mantidos inalterados por todo o período de vigência da Ata de Registro de Preços - ARP, admitida sua revisão, para majorar ou minorar os preços registrados, em casos excepcionais, nas hipóteses legais e considerando os preços vigentes de mercado.

5.3. A revisão de preços prevista no caput do artigo 23B do Decreto Estadual 25.969 precederá de requerimento: I - do detentor da ata, que deverá fazê-la antes do pedido de fornecimento e, instruindo seu pedido com documentação probatória de majoração de preço do mercado e a oneração de custos; ou II

- pelo órgão participante ou órgão interessado, comprovando por meio de pesquisas de preços que há minoração do valor originalmente registrado.

5.4. Nos termos do § 2° do Decreto 25.969/2021, se comprovada a majoração dos valores de mercado nas hipóteses da alínea "d" do inciso II do artigo 65 da Lei n° 8.666, de 1993, o órgãogerenciador da Ata convocará, antes da efetiva alteração de preços, as demais licitantes na ordem de classificação original para que manifestem interesse em manter o preço original registrado em ata, de modo que, inexistindo interessados dispostos em manter o valor da ARP; os preços poderão ser revisados conforme disposto no caput artigo 23B.

5.5. Conforme disposto no § 4°do Decreto 25.969/2021. a revisão aprovada não poderá ultrapassar o preço praticado no mercado e deverá manter a diferença percentual apurada entre o preço originalmente constante da proposta e o preço de mercado vigente à época do registro.

5.5.1. O Decreto Estadual 18.340/2013 dispõe ainda no artigo 25, sobre as hipóteses do cancelamento do preço registrado, que poderá ocorrer por fato superveniente, decorrente de caso fortuito ou força maior, que prejudique o cumprimento da ata, **devidamente comprovados e justificados, por** razão de interesse público; ou II - a pedido do fornecedor

5.5.2. O preço registrado também poderá ser cancelado nas hipóteses do artigo 24 do Decreto Estadual 18.340/2013, quando o fornecedor descumprir total ou parcialmente as condições da ata de registro de preços; não retirar a nota de empenho ou instrumento equivalente no prazo estabelecido pela Administração, não aceitar reduzir o seu preço registrado, na hipótese deste se tornar superior aqueles praticados no mercado, ou sofrer sanção prevista na forma do artigo 87 da Lei 8.666/93.

6. CLÁUSULA VI - DA FORMAÇÃO DE CADASTRO RESERVA

6.1. A apresentação de novas propostas para compor o cadastro de reserva não prejudicará o resultado do certame em relação ao licitante melhor classificado.

6.2. Esta ordem de classificação dos licitantes registrados deverá ser respeitada nas contratações e somente será utilizada caso o melhor colocado no certame tenha seu registro cancelado ou revogado, nas hipóteses previstas no Decreto Estadual 18.340/2013.

6.3. Para o registro do preço dos demais licitantes será exigida a análise da habilitação.

7.CLÁUSULA VII - DAS CONDIÇÕES A SEREM OBSERVADAS NAS FUTURASCONTRATAÇÕE

7.1. As condições gerais referentes ao fornecimento, tais como prazo e local de entrega e recebimento do objeto, obrigações da Administração e do fornecedor detentor do registro e penalidades, encontram-se definidas no Termo de Referência e Edital da licitação, partes integrantes da presente Ata.

7.2. É **vedado** o aditamento dos quantitativos consignados na Ata de Registro de Preços, conforme o disposto no §1° do artigo 15 do Decreto Estadual nº 18.340/2013.

7.3. A detentora do registro fica obrigada a atender a todas as ordens de fornecimento efetuadas pelo órgão participante, durante a vigência desta ata.

8. CLÁUSULA VIII – DAS DISPOSIÇÕES FINAIS

8.1. 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.

8.2. Fica a empresa 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.

8.3. 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 casosomissos.

8.4. 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.

9. CLÁUSULA IX - DO FORO

9.1. Para dirimir eventuais conflitos oriundos desta Ata, é competente o Foro da Comarca de Porto Velho/RO, excluindo-se qualquer outro, por mais privilegiado que seja.

ANEXO ÚNICO

EMPRESA(S) DETENTORA(S):

ALCINEY SOARES DE LIMA JÚNIOR
Coordenador do Sistema de Registro de Preços/SUPEL

FABIOLA MENEGASSO DIAS
Diretora Executiva/SUPEL

ISRAEL EVANGELISTA DA SILVA
Superintendente Estadual de Compras e Licitações

SUPERINTENDÊNCIA ESTADUAL DE LICITAÇÕES - SUPEL/RO
PREGÃO ELETRÔNICO N°: 161/2023/SUPEL/RO

ANEXO ÚNICO.

[UNIDADE CONTRATANTE SOLICITANTE]

OFÍCIO Nº_____/_____ , [DATA DA EMISSÃO]

Prezado Gestor da Ata nº [Nº DA ATA] do(a) [ÓRGÃO GESTOR DA ATA]

Nos termos do art. 26 do Decreto Estadual nº 18.340/2013, solicito autorização para ADERIR à Ata de Registro de Preços em epígrafe visando adquirir os itens e quantitativos relacionados na tabela abaixo.

Ressalto que o(s) fornecedor(es), detentor(es) do(s) preço(s) registrado(s), já se manifestou(ram) pela aceitação, conforme previsto no Decreto 18.340/2013

Nº ITEM DA ATA	**ESPECIFICAÇÃO**	**QUANT. ADESÃO**

ASSINATURA DO GESTOR DA UNIDADE SOLICITANTE