RECIBO DE RETIRADA DE EDITAL VIA INTERNET
PREGÃO PRESENCIAL Nº. 057/2020
PROCESSO LICITATÓRIO Nº. 083/2020

OBJETO: CONTRATAÇÃO DE EMPRESA ESPECIALIZADA EM FORNECIMENTO DE HARDWARE (SERVIDOR DE DADOS, SWITCH E STORAGE) E SOFTWARE, A SEREM UTILIZADOS NA SEDE ADMINISTRATIVA DO SERVIÇO AUTÔNOMO DE SANEAMENTO BÁSICO DE ITABIRITO – MG, CONFORME ESPECIFICAÇÕES DO ANEXO I.

O SERVIÇO AUTÔNOMO DE SANEAMENTO BÁSICO DE ITABIRITO - MG, TORNA PÚBLICO, NA PRESENÇA E CIÊNCIA DO (A) PREGOEIRO (A) DESIGNADO (A) PELA PORTARIA - Nº. SAAE 084/2020 DE 10 DE AGOSTO DE 2020, QUE ÀS **09:00 HORAS DO DIA 10/09/2020**, NA SALA DE REUNIÕES DO SAAE, LOCALIZADA À RUA RIO BRANCO, Nº. 99, CENTRO, ITABIRITO/MG, SERÁ REALIZADA LICITAÇÃO NA MODALIDADE **PREGÃO PRESENCIAL,** DO TIPO **"MENOR PREÇO GLOBAL".**

Razão Social			
CNPJ			
Endereço:			
e-mail:			
Cidade:		Estado:	
Telefone:		Fax:	

Obtivemos através do acesso à página www.saaeita.mg.gov.br nesta data, cópia do instrumento convocatório da licitação acima identificada.

Local: _____, _____ de _____ de 2020.

_____
Assinatura

Sr. Licitante,
Visando comunicação futura entre o SAAE – Serviço Autônomo de Saneamento Básico de Itabirito e essa empresa, solicitamos preencher o recibo de retirada do edital e remeter ao setor de Licitações, via fax (31) 3562-4102 ou através do e-mail compras@saaeita.mg.gov.br.

A não remessa do recibo exime o SAAE da responsabilidade de comunicação de eventuais esclarecimentos e retificações ocorridas no instrumento convocatório, bem como de quaisquer informações adicionais, não cabendo posteriormente qualquer reclamação.

EDITAL DE PREGÃO PRESENCIAL Nº.: 057/2020

PROCESSO LICITATORIO Nº.: 083/2020

MODALIDADE: PREGÃO PRESENCIAL **Nº.: 057/2020**

TIPO: MENOR PREÇO GLOBAL

SETOR: ADMINISTRAÇÃO – TECNOLOGIA DA INFORMAÇÃO - CPD

RECEBIMENTO DE ENVELOPES DE DOCUMENTAÇÃO E DAS PROPOSTAS: Dia **10/09/2020** até as **09:00 horas**, em sua sede na Rua Rio Branco nº. 99 – Centro – Itabirito – MG.

CREDENCIAMENTO: **10/09/2020** até as 09h00min.

INÍCIO DA SESSÃO PÚBLICA DO PREGÃO PRESENCIAL: **10/09/2020 às 09h00min**.

LEGISLAÇÃO APLICÁVEL: Regido pela Lei Federal nº. 10.520/02, retificada em 18 de julho de 2002 e Lei nº. 8.666/93, de 21 de junho de 1993, com suas posteriores alterações, pela Lei Complementar nº. 123/2006, alterada pela Lei Complementar 147/2014 e Decreto Municipal 7.191/2005 de 28 de Março de 2005.

RECURSO ORÇAMENTÁRIO: a saber:

PROJ. CONSTR. AMPL. OBRAS INFRAEST. GESTÃO DA ADM GERAL SAAE.
17 512 1711 3.030 44.90.52.00

OP. MANUT. AÇÕES DE GESTÃO ADM GERAL SAAE.
17 512 1711 4.030 33.90.40.00

OBJETO: **CONTRATAÇÃO DE EMPRESA ESPECIALIZADA EM FORNECIMENTO DE HARDWARE (SERVIDOR DE DADOS, SWITCH E STORAGE) E SOFTWARE, A SEREM UTILIZADOS NA SEDE ADMINISTRATIVA DO SERVIÇO AUTÔNOMO DE SANEAMENTO BÁSICO DE ITABIRITO – MG, CONFORME ESPECIFICAÇÕES DO ANEXO I.**

PREGÃO PRESENCIAL

O Serviço Autônomo de Saneamento Básico de Itabirito, na presença e ciência do (a) Pregoeiro (a) designado (a) pela Portaria - nº. SAAE 084/2020 de 10 de Agosto de 2020, tornam pública a abertura do **Processo Licitatório nº. 083/2020**, na modalidade **PREGÃO PRESENCIAL Nº. 057/2020**, **DO TIPO MENOR PREÇO GLOBAL,** regido pelas Leis Federais nº. 10.520/2002 e nº. 8.666/1993 pela Lei Complementar nº. 123/2006 e pelo Decreto Municipal no 7.191/2005.

A SESSÃO PARA RECEBIMENTO E ABERTURA DOS ENVELOPES CONTENDO A PROPOSTA COMERCIAL E DOCUMENTAÇÃO DE HABILITAÇÃO INICIAR-SE-Á ÀS **09:00 HORAS** DO DIA **10/09/2020**, NA SALA DE REUNIÕES do SAAE, localizada à Rua Rio Branco nº. 99, Centro, no município de Itabirito/MG.

I – DO OBJETO

O presente procedimento licitatório tem por objeto a contratação de empresa especializada em fornecimento de Hardware (Servidor de Dados, Switch e Storage) e Software, a serem utilizados na Sede Administrativa do Serviço Autônomo de Saneamento Básico de Itabirito – MG, conforme especificações do anexo I.

JUSTIFICATIVA PARA AQUISIÇÃO EM MENOR PREÇO GLOBAL

Inicialmente, cabe reforçar que a pretensão deste processo licitatório não é apenas aquisição de uma solução ou hardware. O que se pretende é adquirir todo um ambiente de hiper-disponibilidade, por isso é necessária a expertise do licitante nesta área com a solução de recuperação de desastres e alta disponibilidade com a ferramenta ofertada.

"A concepção da solução integrada relaciona-se com a proposta de identificar um fornecedor, que se obrigue a produzir um resultado eficiente, satisfatório e adequado para atender determinada necessidade. Assim, o fornecedor assumirá o dever de produzir a conjugação de equipamentos e soluções, implementando os serviços correspondentes à necessidade do Contratante. Nesse caso, o dever do fornecedor não reside na mera tradição de equipamentos, nem no fornecimento de soluções. Cabe-lhe entregar um conjunto de bens e serviços em perfeita operação..." (Marçal Justen Filho, Comentários à lei de licitações e contratos administrativos. 11ª ed. São Paulo: Dialética, 2005. p.217).

A compra de um pacote em fornecimento global garante a Autarquia a aquisição de equipamentos e software com trabalho em perfeito sincronismo evitando problemas com compatibilidade e acionamento de assistência técnica ou suporte desnecessariamente.

Assim, levando em consideração todos os eventos inesperados e que acarretaram grandes prejuízos citados neste edital, faz-se necessário otimizar o custo e o prazo de implantação prevendo para este projeto a entrega de uma solução global.

II - DAS CONDIÇÕES DE PARTICIPAÇÃO

2.1. Poderão participar da presente licitação, observada as subcondições abaixo, os interessados que atenderem a todas as exigências constantes deste Edital e seus anexos.

2.1.1 Participarão exclusivamente as microempresas e empresas de pequeno porte, em cumprimento ao art. 48, inciso I, da Lei Complementar nº 123/2006, desde que se enquadrem nas disposições abaixo estabelecidas.

2.1.2 Não será aplicado o disposto no item 2.1.1, previsto no art. 48 da Lei Complementar 123/2006, quando:

II - não houver um mínimo de 03 (três) fornecedores competitivos enquadrados como microempresas ou empresas de pequeno porte sediado local ou regionalmente e capazes de cumprir as exigências estabelecidas no instrumento convocatório;

III - o tratamento diferenciado e simplificado para as microempresas e empresas de pequeno porte não for vantajoso para a administração pública ou representar prejuízo ao conjunto ou complexo do objeto a ser contratado;

2.1.3 Para fins do art. 49, inciso II, da Lei Complementar nº 123/06 o alcance da expressão "regionalmente", será delimitado aos municípios de Itabirito/MG, Ouro Preto/MG e Mariana/MG.

2.1.4 A definição da regionalidade objetiva a promoção do desenvolvimento econômico e social, bem como, a ampliação da eficiência das políticas públicas e o incentivo à inovação tecnológica nos termos do artigo 47 da Lei Complementar nº 123/06.

2.2. Não poderão participar deste pregão os interessados que se encontrarem em processo de falência, de dissolução, de fusão, de cisão, de incorporação, que estejam cumprindo suspensão temporária de participação de licitação ou impedidos de contratar com a Administração Pública, ou que tenham sido declarados inidôneos para licitar ou contratar com a Administração Pública; bem como as licitantes que se apresentem constituídas na forma de empresa em consórcio e ainda os interessados que se enquadrem nas hipóteses do art. 9º da Lei nº. 8.666/93.

2.3. A simples participação neste certame implica a aceitação de todas as condições estabelecidas neste instrumento convocatório.

2.4. Com relação aos itens: 01 e 02, poderão participar da presente licitação os interessados que atenderem a todas as exigências constantes deste Edital e seus anexos.

2.5. Poderão participar desta licitação pessoas jurídicas que forneçam objetos de natureza relacionada com o presente edital.
2.6 - Comunicamos a todas as licitantes que a **VISITA TÉCNICA** ao local é **OPCIONAL** e poderá ser realizada em até 03(três) dias antes da realização do Certame e poderá ser agendada com o servidor Sérgio Pereira dos Santos, através dos telefones: (31) 3562-4113 e (31) 9 8699-2756.

2.7. Cópia deste edital permanecerá afixada no quadro de avisos localizado no *hall* de entrada do Edifício-Sede do Serviço Autônomo de Saneamento Básico de Itabirito-MG e poderá ser obtida junto ao Setor de Compras/Licitações, em dias úteis, no horário das 08:00h às 12:00 horas e das 13:30h às 16:30 horas; no site do SAAE através do endereço www.saaeita.mg.gov.br/licitacoes; ou solicitado através do e-mail: compras@saaeita.mg.gov.br. Deverão ser atendidas as condições abaixo relacionadas, sendo que o não atendimento de qualquer das condições, independentemente de sua magnitude, implicará a inabilitação do licitante ou a desclassificação de sua proposta.

III – IMPUGNAÇÃO AO EDITAL

3.1. Qualquer pessoa poderá solicitar esclarecimentos, providências ou impugnar o presente instrumento convocatório do Pregão em epígrafe, protocolando o pedido em até 02 (dois) dias úteis antes da data fixada para recebimento das propostas.

3.2. A apresentação de impugnação contra o presente edital será processada e julgada na forma e prazos previstos no regulamento da licitação na modalidade de "Pregão" devendo ser dirigida ao Pregoeiro (a) e protocolada no Setor de Compras/Licitação do SAAE localizado na Rua Rio Branco nº. 99 – Centro – Itabirito/MG.

3.3. Acolhida a petição contra o ato convocatório, e caso não seja esta reconhecida manifestadamente improcedente, será designada nova data para a realização do certame.

3.4. A entrega da proposta, sem que tenha sido tempestivamente impugnado o presente Edital, implicará na plena aceitação, por parte dos interessados, das condições nele estabelecidas.

IV – REGULAMENTO OPERACIONAL DO CERTAME

4.1. O certame será conduzido pelo (a) Pregoeiro (a), que terá em especial, as seguintes atribuições:
a) acompanhar os trabalhos da equipe de apoio;
b) responder as questões formuladas pelos fornecedores, relativas ao certame;
c) abrir as propostas de preços;
d) analisar a aceitabilidade das propostas;
e) desclassificar as propostas indicando os motivos;
f) conduzir os procedimentos relativos aos lances e à escolha da proposta do lance de menor preço por item;
g) verificar os documentos de habilitação do proponente classificado em primeiro lugar.
h) declarar o vencedor;
i) receber, examinar e decidir sobre a pertinência dos recursos;
j) elaborar a ata da sessão;
k) adjudicar o objeto dessa licitação à licitante vencedora.
l) encaminhar o processo à autoridade superior para homologar e autorizar a contratação;
m) convocar o vencedor para assinar o contrato ou retirar o instrumento equivalente no prazo estabelecido;
n) abrir processo administrativo para apuração de irregularidades visando à aplicação de penalidades previstas na legislação;

V – DO CREDENCIAMENTO DA EMPRESA E DOS REPRESENTANTES

5.1. O credenciamento se dará junto ao Pregoeiro (a) por um sócio ou por um representante munido de Procuração/Carta de Credenciamento – Modelo - Anexo II, em ambos os casos com a apresentação conjunta dos seguintes documentos, ***fora de envelopes***:

I- Documento oficial de identidade do sócio/representante;
II- Estatuto ou Contrato Social e a última alteração contratual ou Registro Comercial, devidamente registrado;
III- Declaração dando ciência de que cumprem plenamente os requisitos de habilitação, de acordo com o modelo constante do Anexo III, deste Edital;
IV- Declaração para Micro Empresas e Empresas de Pequeno Porte (Anexo VI), se for o caso.

5.2. O Contrato Social/Estatuto/Registro Comercial do licitante poderá ser apresentado em original ou por qualquer processo de cópia autenticada, conforme o disposto no art. 32 da Lei nº. 8.666/93.

5.3. Se o licitante não credenciar um representante estará abdicando do direito de fazer lance e, principalmente, de recorrer dos atos do (a) Pregoeiro (a).

5.4. Nenhuma pessoa, ainda que munida de procuração, poderá representar mais de uma empresa licitante neste PREGÃO, sob pena de exclusão sumária dos representados.

5.5. A outorga de poderes para efetuar lances deverá estar expressa na carta de credenciamento ou procuração, caso contrário os credenciados ou procuradores não poderão ofertar lances.

5.6. Após o encerramento do credenciamento, identificação dos representantes das empresas proponentes e entrega dos envelopes contendo as propostas e a documentação, será declarada a abertura da sessão pública pelo (a) pregoeiro (a), e não mais serão admitidos novos proponentes.

VI – DO RECEBIMENTO DAS PROPOSTAS E DOCUMENTAÇÃO DE HABILITAÇÃO

6.1. A Proposta Comercial e a Documentação de Habilitação exigidas neste edital deverão ser apresentadas em envelopes distintos, indevassáveis, colados e rubricados nos fechos, sob pena de desclassificação, até o dia, horário e local fixado neste Edital, contendo em sua parte externa, as seguintes informações:

ENVELOPE Nº 01 **RAZÃO SOCIAL E ENDEREÇO DO LICITANTE** **"PROPOSTA DE PREÇO"** **PROCESSO LICITATÓRIO Nº 083/2020** **MODALIDADE: PREGÃO Nº 057/2020**

ENVELOPE Nº 02 **RAZÃO SOCIAL E ENDEREÇO DO LICITANTE** **"DOCUMENTOS PARA HABILITAÇÃO"** **PROCESSO LICITATÓRIO Nº 083/2020** **MODALIDADE: PREGÃO Nº 057/2020**

6.2. A entrega dos envelopes poderá ser realizada via postal ou através de protocolo no Setor de Compras/Licitação do SAAE localizado na Rua Rio Branco, nº. 99, Bairro Centro, Itabirito/MG, CEP: 35.450-000, até a data e horários previstos no preâmbulo deste instrumento convocatório ou entregues na sala de licitações do SAAE até a hora da abertura.

6.3. O SAAE não se responsabilizará por envelopes endereçados via postal ou por outras formas, entregues em local diverso do Setor de Compras/Licitação do SAAE, e que, por isso, não cheguem até a data e horário previstos.

VII – DA FORMA DE APRESENTAÇÃO DA PROPOSTA COMERCIAL – ENVELOPE Nº 01

7.1. São requisitos da proposta:
7.1.1. Apresentar a Planilha de Especificações e Preços – Anexo I, devidamente preenchida, contendo as especificações e o valor em moeda corrente brasileira em duas casas decimais, explicitado unitariamente e globalmente, no qual já deverão estar incluídos todos os custos para a entrega dos materiais/equipamentos

ora licitados, inclusive impostos diretos e indiretos, obrigações trabalhistas e previdenciárias, taxas, transportes e seguros incidentes ou que venham a incidir sobre o objeto desta licitação;
7.1.2. Ser impressa em língua portuguesa, contendo o número e a modalidade da licitação deste Edital, devendo, preferencialmente conter: razão social, CNPJ, endereço, número de telefone, número de fax da empresa licitante e dados bancários;
7.1.3. Conter a assinatura do representante legal do licitante em todas as suas páginas;
7.1.4. Conter o prazo de validade da proposta, não inferior a 60 (sessenta) dias, a contar do dia da sessão de recebimento dos envelopes. No caso de omissão desse prazo, será entendido como válida por 60 (sessenta) dias.

7.2. Os preços desta proposta deverão ser fixos e irreajustáveis, admitidas à repactuação, nos termos e condições previstos neste edital.

7.3. Não se admitirá proposta que apresente valores simbólicos, ou irrisórios, de valor zero, excessivos ou manifestamente inexequíveis.

7.4. Não serão aceitas propostas enviadas via fax, e-mail ou em envelopes abertos/grampeados.

7.5. Deverá ser especificada a marca dos materiais/equipamentos, seu fabricante, se importado, o seu país de origem e demais elementos que permitam identificá-lo com clareza.

7.6. Deverá conter especificações e características detalhadas dos materiais/equipamentos e outros elementos, de modo a ser atendido o disposto no art. 31 da Lei nº. 8.078/90 – Código do Consumidor, que identifiquem os materiais/equipamentos ofertados, a fim de que o (a) pregoeiro (a) possa facilmente constatar se as especificações deste edital foram ou não atendidas.

7.7. Deverá ser apresentado no envelope junto à proposta comercial, marca, modelo, catálogo, folder ou folheto, de todos os equipamentos e soluções propostas onde conste de maneira clara as características dos equipamentos cotados. NÃO SERÃO ACEITOS PROSPECTOS MONTADOS.

7.8. Após a entrega das propostas, não será admitida a sua retirada ou o descumprimento das condições estabelecidas neste edital, ficando o licitante sujeito à suspensão ou cancelamento de seu registro no cadastro de fornecedores do SAAE, sem prejuízo da aplicação das penalidades previstas no título XIV deste Edital.

VIII – DO JULGAMENTO DAS PROPOSTAS

8.1. Os envelopes de Propostas Comerciais serão abertos pelo (a) Pregoeiro (a) que, após a rubrica por todos os presentes, verificará sua conformidade com os requisitos do edital e seus anexos, examinará a aceitabilidade quanto aos preços apresentados e procederá à classificação daquelas que estiverem de acordo com o edital e apresentem o MENOR PREÇO GLOBAL ou valores sucessivos e superiores em até 10% (dez por cento), relativamente ao menor preço, para participarem dos lances verbais.

8.2. Para fins do que dispõe o art. 48, inciso II da Lei nº. 8.666/93, o (a) Pregoeiro (a) poderá exigir a apresentação da planilha de custos na abertura das propostas bem como após a fase de lances, na própria Sessão.

8.3. Caso não haja no mínimo 03 (três) propostas de preços nas condições definidas no item 8.1., o (a) Pregoeiro (a) classificará as melhores propostas subsequentes, até o máximo de 03 (três), neste número já incluso a de **menor preço global**, para que seus autores participem dos lances verbais, quaisquer que sejam os preços oferecidos nas propostas apresentadas.

8.4. Na ocorrência de empate dentre os classificados para participarem dos lances verbais, a ordem para esses lances será definida através de sorteio.

8.5. Aos licitantes classificados conforme os itens 8.1. e 8.3. serão dados a oportunidade para nova disputa, por meio de lances verbais e sucessivos, de valores distintos e decrescentes.
8.5.1. Caberá ao Pregoeiro (a) a definição e/ou alteração de valores mínimos na fase de lances verbais.

8.6. Caso não se realize lances verbais, verificada a conformidade entre a proposta de **menor preço global**, as exigências do Edital e ainda, o preço estimado para a contratação, o (a) Pregoeiro (a) negociará diretamente com o proponente para que seja obtido preço melhor.

8.7. Não poderá haver desistência dos lances ofertados, sujeitando-se o proponente desistente às penalidades do previstas no título XIV deste Edital.

8.8. Quando não houver mais lances, será encerrada a etapa competitiva e ordenadas as ofertas exclusivamente pelo critério do menor preço por item.

8.9. O (a) Pregoeiro (a) examinará a aceitabilidade, quanto ao preço apresentado pela primeira classificada, conforme definido neste Edital e anexo.

8.10. Sendo aceitável a oferta, será verificado o atendimento das condições habilitatórias do proponente. Se não aceitável, o (a) Pregoeiro (a) examinará as ofertas subsequentes, na ordem de classificação, até a apuração de uma proposta que atenda a todas as exigências, prosseguindo-se o certame.

8.11. Ocorrendo qualquer das hipóteses do item 8.10., será lícito ao Pregoeiro (a) negociar diretamente com o proponente para obtenção de melhor preço.

8.12. Ainda durante a sessão pública do pregão, o licitante declarado vencedor deverá readequar seu preço, com as modificações necessárias para sua adaptação ao novo preço proposto, se for o caso.

8.13. Será assegurada, como critério de desempate, preferência de contratação para as microempresas e empresas de pequeno porte.
8.13.1. Entende-se por empate aquelas situações em que as propostas apresentadas pelas microempresas e empresas de pequeno porte sejam iguais ou até 5% (cinco por cento) superiores ao melhor preço.

8.14. Ocorrendo o empate, proceder-se-á da seguinte forma:
8.14.1. A microempresa ou empresa de pequeno porte mais bem classificada poderá apresentar proposta de preço inferior àquela considerada vencedora do certame, situação em que será adjudicado em seu favor o objeto licitado;
8.14.2. Não ocorrendo à contratação da microempresa ou empresa de pequeno porte, na forma do subitem 8.14.1. será convocadas as remanescentes que porventura se enquadrem na hipótese do subitem 8.13.1, na ordem classificatória, para o exercício do mesmo direito;
8.14.3. No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem no intervalo estabelecido no subitem 8.13.1., será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.

8.15. Na hipótese da não-contratação nos termos previstos no subitem 8.14.1., o objeto licitado será adjudicado em favor da proposta originalmente vencedora do certame.

8.16. O disposto no item 8.13. somente se aplicará quando a melhor oferta inicial não tiver sido apresentada por microempresa ou empresa de pequeno porte.

8.17. Não serão aceitos lances verbais com valores irrisórios, incompatíveis com o valor orçado.

8.18. Serão realizadas tantas rodadas de lances verbais quantas se façam necessárias.

8.19. A microempresa ou empresa de pequeno porte mais bem classificada será convocada para apresentar nova proposta no prazo máximo de 05 (cinco) minutos após o encerramento dos lances, sob pena de preclusão.

8.20. Caso não mais se realize lance verbal, será verificada a conformidade entre a proposta escrita de menor preço e o valor estimado da contratação.

8.21. O encerramento da etapa competitiva dar-se-á quando convocados pelo (a) pregoeiro (a), os licitantes manifestaram seu desinteresse em apresentar novos lances.

8.22. A desistência em apresentar lance verbal, quando convocado pelo (a) pregoeiro (a), não implicará a exclusão imediata do licitante da etapa de lances verbais, mas sim a manutenção do último preço por ele apresentado, impossibilitando-o de efetuar novos lances, salvo nas hipóteses previstas no inciso XVII do artigo 4º da Lei Federal nº. 10.520/02.

8.23. Será desclassificada a proposta que:
8.23.1. Contiver cotação de objeto diverso daquele requerido nesta licitação;
8.23.2. Não atender aos requisitos deste instrumento convocatório;
8.23.3. Apresentar preço unitário ou global simbólico, de valor zero, superestimado ou manifestamente inexeqüível, incompatível com os preços e insumos de mercado, assim considerados nos termos do disposto no § 3º do art. 44 e nos incisos I e II do art. 48, da Lei Federal nº. 8.666/93;
8.23.4. Contiver alternativas, condições ou que em seu texto contenha rasuras, emendas, borrões, entrelinhas, defeitos de linguagem ou outras irregularidades que impossibilitem o julgamento;
8.23.5. Não se referir à integralidade do objeto.

8.24. Em caso de divergência entre o preço unitário e o total, prevalecerá o primeiro, do mesmo modo que prevalecerá o valor expresso por extenso sobre o valor numérico.

8.25. Na análise das propostas não serão consideradas ofertas e outras informações não solicitadas neste instrumento ou em diligências.

8.26. O (a) Pregoeiro (a) poderá desconsiderar eventuais falhas formais sanáveis e que não afetem o seu conteúdo.

IX – DA FORMA DE APRESENTAÇÃO DOS DOCUMENTOS DE HABILITAÇÃO ENVELOPE Nº 02

9.1. Para habilitar-se a esta licitação, a proponente deverá apresentar os seguintes documentos, com vigência plena até a data fixada para abertura dos envelopes “Documentos de Habilitação”:
a) Cópia do Cartão de Cadastro Nacional de Pessoas Jurídica **CNPJ** do estabelecimento que participará da licitação;
b) Certidão Negativa de Débito Relativa aos Tributos Federais e á Divida Ativa da União.
c) Certificado de Regularidade (**CRF**) Relativo ao Fundo de Garantia por Tempo de Serviço – FGTS, emitido pela Caixa Econômica Federal;
d) Certidão Negativa ou Certidão Positiva com Efeito de Negativa com a Fazenda Municipal sede da Licitante;
e) Certidão Negativa ou Certidão Positiva com Efeito de Negativa com a Fazenda Estadual sede da Licitante;
f) Certidão Negativa de Débitos Trabalhistas (**CNDT**);
g) Declaração (*conforme modelo do Anexo IV*) da empresa participante sob as penas da Lei de que não está suspensa, nem é impedida de licitar com Órgão Público, conforme Inciso III e IV Artigo 87 da Lei nº. 8.666/93 com suas posteriores alterações;
h) Declaração (*conforme modelo do Anexo V*) do Empregador Pessoa Jurídica em cumprimento ao Disposto no Inciso XXXIII do art. 7 da Constituição Federal;
i) Declaração (*conforme modelo do Anexo VII*) somente para Microempresas ou Empresas de Pequeno Porte, quanto à restrição em Documentação de Regularidade Fiscal, se for o caso;
j) Declaração (*conforme modelo do Anexo VIII*) de Elaboração Independente de Proposta;

k) Ato constitutivo: estatuto acompanhado do documento de eleição de seus administradores ou contrato social e a última alteração ou Registro Comercial, devidamente registrados
l) Apresentar ATESTADO DE CAPACIDADE TÉCNICA emitido por pessoa jurídica de direito público ou privado, que comprove o fornecimento de materiais compatíveis com o objeto licitado. Será permitido a apresentação de mais de um atestado de capacidade técnica.

9.2. Os documentos acima poderão ser apresentados em originais ou cópias reprográficas legíveis, devidamente autenticados em cartório ou pelo (a) Pregoeiro (a) ou pela sua equipe de apoio, sendo reservado a estes o direito de exigir a apresentação do original para conferência, no ato da abertura da habilitação, conforme disposto no art. 32 da Lei nº. 8.666/93. A documentação acima citada, quando extraída da internet, terá o seu aceite condicionado à consulta, via internet, no ato da abertura da habilitação.

9.3. Para certidões emitidas que não tenham de forma explícita o prazo de validade, será considerado o prazo máximo de 90 (noventa) dias contados a partir de suas emissões, devendo estar válidas na data de abertura dos envelopes de documentos de habilitação.

X – DAS CONDIÇÕES GERAIS DE HABILITAÇÃO

10.1. Concluída a fase de classificação das propostas, será aberto o Envelope nº. 02 – Habilitação da proponente cuja proposta tenha sido classificada em primeiro lugar.

10.2. Sendo inabilitada a proponente cuja proposta tenha sido classificada em primeiro lugar, o (a) Pregoeiro (a) prosseguirá com a abertura do envelope de documentação da proponente classificada em segundo lugar, assim sucessivamente, até a apuração de uma proposta que atenda ao Edital, sendo a respectiva licitante declarada vencedora e a ela adjudicada o objeto do certame.

10.3. Para Micro Empresas e Empresas de Pequeno Porte, havendo alguma restrição na comprovação da regularidade fiscal, será assegurado o prazo de 05 (cinco) dias úteis, cujo termo inicial corresponderá ao momento em que o proponente for declarado o vencedor do certame, prorrogáveis por igual período, a critério do SAAE, para a regularização da documentação, pagamento ou parcelamento do débito e emissão de eventuais certidões negativas ou positivas com efeito de certidão negativa.
10.3.1. A não-regularização da documentação, no prazo previsto no item 10.3., implicará decadência do direito à contratação, sendo facultado à Administração convocar os licitantes remanescentes, conforme item 10.2., ou revogar a licitação, sem prejuízo das penalidades cabíveis aos licitantes.

10.4. Ocorrendo a hipótese contida no item 10.3., o juízo de habilitação referente à micro empresa e a empresa de pequeno porte será suspenso até a apresentação da documentação necessária ou a expiração do prazo.

10.4.1. A sessão será suspensa e o (a) pregoeiro (a) definirá e comunicará aos licitantes a data na qual será dada continuidade ao pregão.

XI – DA ADJUDICAÇÃO E HOMOLOGAÇÃO

11.1. Constatado o atendimento pleno às exigências do Edital, será declarada a licitante vencedora, sendo-lhe adjudicado pelo (a) pregoeiro (a) o objeto da presente licitação.

11.2. Da sessão pública do pregão será lavrada ata circunstanciada com o registro dos licitantes credenciados, das propostas escritas e verbais apresentadas, na ordem de classificação, dos preços a serem registrados, da análise dos documentos de habilitação dos recursos interpostos, além de ocorrências relevantes.
11.3. Inexistindo manifestação recursal, o (a) pregoeiro (a) adjudicará o objeto da licitação ao licitante vencedor, com a posterior homologação do resultado pela autoridade superior.

11.4. Havendo a interposição de recurso, após o julgamento e seu trânsito em julgado, a autoridade superior adjudicará e homologará o procedimento licitatório ao licitante vencedor.

XII – INSTRUÇÕES E NORMAS PARA INTERPOSIÇÃO DOS RECURSOS

12.1. Declarado o vencedor, qualquer licitante poderá manifestar imediata e motivadamente a intenção de interpor recurso, desde que devidamente registrada a síntese de suas razões em ata, quando lhe será concedido o prazo de 03 (três) dias para apresentar razões de recurso, facultando-se aos demais licitantes a oportunidade de apresentar contra-razões em igual número de dias, que começarão a correr do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos autos.
12.1.1. O recurso contra decisão do (a) Pregoeiro (a) terá efeito suspensivo.

12.2. A falta de manifestação imediata e motivada do licitante importará na decadência do direito de recurso e na adjudicação do objeto da licitação pelo (a) Pregoeiro (a) ao vencedor.

12.3. O acolhimento de recurso ou a reconsideração de decisão pelo (a) Pregoeiro (a) importará a invalidação apenas dos atos insuscetíveis de aproveitamento.

12.4. As razões e contra-razões do Recurso poderão ser apresentadas de forma oral reduzida a termo em ata da sessão ou apresentadas através de memoriais devendo ser protocoladas no Setor de Compras/Licitação do SAAE situado à Rua Rio Branco nº. 99 - Centro – Itabirito/MG, no prazo estabelecido no item 12.1.

12.5. Decidido(s) o(s) recurso(s) e constatada a regularidade dos atos procedimentais, a Autoridade competente homologará o resultado da licitação.

12.6. Dos demais atos da Administração, após a Adjudicação, decorrentes da aplicação da Lei nº. 8.666/93, caberá:
a) recurso dirigido à autoridade superior por intermédio do (a) pregoeiro (a), interposto no prazo de 05 (cinco) dias úteis, a contar da intimação do ato, a ser protocolizado no endereço referido no preâmbulo deste Edital, nos casos de: anulação ou revogação da licitação; rescisão de contrato, a que se refere o inciso I do art. 79 da Lei nº. 8.666/93 aplicação das penas de advertência, suspensão temporária ou multa;
b) representação, no prazo de 05 (cinco) dias úteis da intimação da decisão relacionada com o objeto da licitação ou do contrato, de que não caiba recurso hierárquico;
c) pedido de reconsideração, no caso de declaração de inidoneidade para licitar ou contratar com a Administração Pública, no prazo de 10 (dez) dias úteis da intimação do ato.
12.6.1. O recurso será dirigido à autoridade superior, por intermédio da que praticou o ato recorrido, a qual poderá reconsiderar sua decisão, no prazo de 05 (cinco) dias úteis, ou, nesse mesmo prazo, encaminhá-lo devidamente informado àquela autoridade. Neste caso, a decisão deverá ser proferida dentro de 05 (cinco) dias úteis, contados do recebimento do recurso, sob pena de responsabilidade (§ 4º do art. 109 da Lei nº. 8.666/93).

12.6.2. A intimação da decisão referida no item 12.6.1. deste edital, excluindo-se as penas de advertência e multa de mora, será feita mediante publicação na imprensa local.

12.7. Os recursos e impugnações interpostos fora dos prazos não serão conhecidos.

XIII – PRAZOS E CONDIÇÕES PARA RETIRADA DA NOTA DE EMPENHO

13.1. Depois de homologado o resultado desta licitação, a empresa adjudicatária será convocada para retirar a respectiva nota de empenho.

13.2. A convocação de que trata o item anterior deverá ser atendida no prazo máximo de 02 (dois) dias úteis, prorrogável apenas 01 (uma) única vez, por igual período a critério da Administração, sob pena de decair o direito à contratação, sem prejuízo das sanções previstas no Título XIV.

13.3. Ao retirar a nota de empenho, a empresa adjudicatária obriga-se a fornecer os materiais/equipamentos a ela adjudicados, conforme especificações e condições contidas neste edital, em seus anexos, e também na proposta apresentada, prevalecendo, no caso de divergência, as especificações e condições do edital.

13.4. Quando o proponente vencedor não apresentar situação regular no ato da emissão da Nota de Empenho ou recusar-se a retirá-la no prazo estipulado, é facultativo à Administração não emitir a respectiva Nota de Empenho e convocar os licitantes remanescentes, na ordem de classificação, para fazê-lo em igual prazo, ou revogar a licitação, independentemente da aplicação das sanções previstas neste edital.

XIV – DAS SANÇÕES ADMINISTRATIVAS

14.1. Ao licitante que, ensejar o retardamento da execução do certame, não mantiver a proposta, falhar na execução do contrato, se comportar de modo inidôneo, fizer declaração falsa ou cometer qualquer espécie de fraude, não executar total ou parcialmente o fornecimento do material; serão aplicadas, conforme o caso, as seguintes sanções, sem prejuízo da reparação dos danos causados à Administração Pública:
14.1.1. Advertência;
14.1.2. Multa de 10% (dez por cento) sobre o valor do contrato;
14.1.3. Suspensão do direito de licitar e impedimento de contratar com o SAAE, pelo prazo de até 02 (dois) anos.

14.2. As sanções previstas nos itens 14.1.1. e 14.1.3. poderão ser aplicadas juntamente com a do item 14.1.2.

14.3. O atraso injustificado no fornecimento do material/equipamento, consoante §1º do art. 86 da Lei nº. 8.666/93 sujeitará o licitante adjudicatário à multa de mora de 0,5% (cinco décimos por cento) por dia de atraso, calculada sobre o valor da obrigação não cumprida.
14.3.1. O atraso superior a 30 (trinta) dias, caracteriza não execução parcial ou total, conforme o caso, aplicando-se o disposto no item 14.1.

14.4. O material/equipamento fornecido em desacordo com o estipulado deverá ser substituído no prazo máximo de 48 (quarenta e oito) horas, contados do recebimento da notificação da recusa.
14.4.1. A não ocorrência da substituição do material/equipamento ensejará a aplicação da multa estabelecida no item 14.3., considerando-se a mora a partir do primeiro dia útil seguinte ao término do prazo fixado no item 14.4.

14.5. A aplicação das penalidades será precedida da concessão da oportunidade de defesa prévia do Licitante, no prazo de 05 (cinco) dias, contados do recebimento da notificação.

14.6. A defesa deverá ser encaminhada ao Pregoeiro (a) do Setor de Compras do SAAE que em conjunto com o Setor Requisitante e amparada em Parecer Jurídico, decidirá, motivadamente, sobre o acolhimento ou rejeição das razões apresentadas, para concluir pela imposição ou não da penalidade.

14.7. Da aplicação das penalidades caberá recurso administrativo ao Diretor do SAAE, que poderá ser interposto através de protocolo no Setor de Compras, nos termos do § 4º do artigo 109 da Lei Federal nº. 8.666, de 21 de junho de 1993 e suas alterações, no prazo de 05 (cinco) dias a contar de sua notificação.

14.8. As multas quando for o caso, serão calculadas sobre os valores contratuais reajustados, e serão:
I. Descontadas da garantia prestada quando da assinatura do contrato ou instrumento equivalente;
II. Descontadas de pagamentos eventualmente devidos pelo SAAE, quando não houver garantia ou esta for insuficiente.

14.9. Na hipótese do pagamento das multas não ocorrer integralmente na forma prevista no item anterior, a CONTRATADA terá o prazo de 10 (dez) dias, a contar da notificação da decisão definitiva de aplicação da multa, para quitá-la, fazendo-o através de depósito em conta bancária do SAAE.

14.10. Além das sanções previstas no item 14.4., poderá ser aplicada pelo Diretor Presidente do SAAE a penalidade de declaração de inidoneidade para licitar ou contratar com o SAAE, nos termos do art. 87 Incisos IV da Lei nº. 8.666/1993, assegurada a defesa prévia do Licitante no prazo de 10 (dez) dias, contados da notificação.

XV – DO RECEBIMENTO E FORNECIMENTO DOS SOFTWARE E EQUIPAMENTOS

15.1. Os software/equipamentos a serem fornecidos pela licitante adjudicatária incluirão as condições e especificações estabelecidas neste instrumento convocatório e seus anexos, necessárias à fiel execução do objeto desta licitação.

15.2. O objeto da presente licitação será recebido na sede do SAAE, situado à Rua Rio Branco, nº. 99, Bairro Centro, em Itabirito/MG, com todos os encargos para entrega, **no horário de 08:00 horas às 11:00 horas e das 13:00 horas às 15:30 horas, em dias úteis**, em dias úteis, onde a Comissão designada para recepção procederá a conferência e recebimento dos materiais.

15.3. Todos software/equipamentos deverão ser obrigatoriamente novos, originais, genuínos, de 1ª linha e 1ª qualidade.

15.4. O Serviço Autônomo de Saneamento Básico de Itabirito – MG reserva-se o direito de não receber os software/equipamentos em desacordo com o previsto neste instrumento convocatório, podendo rescindir o contrato e aplicar o disposto no art. 24, inciso XI da Lei Federal nº. 8.666/93, com suas posteriores alterações.

15.5. Todos os itens de que trata esta licitação deverão obedecer às especificações constantes do Edital e seus anexos, sendo a CONTRATADA obrigada a substituir de imediato e às suas expensas, materiais/equipamentos em que se verifiquem irregularidades.

15.6. A entrega dos software/equipamentos será realizada **em até 45 (quarenta e cinco) dias corridos**, após o recebimento da Nota de Empenho. **Deverá a Nota fiscal Eletrônica estar em conformidade com a Nota de Empenho emitida.** A Nota Fiscal deverá ser emitida eletronicamente, cumprindo o disposto pelos protocolos ICMS 42/2009 e 19/2011. Deverá vir acompanhada de arquivos digitais contendo cópia da Certidão Negativa de Débitos (***CND***) Relativos aos Tributos Federais e á Divida Ativa da União e Certificado de Regularidade do FGTS (***CRF***) da CONTRATADA, e todas as incidências fiscais que sobre elas possam recair deverão vir destacadas, condições estas indispensáveis para efetuar-se o pagamento.

15.7. O SAAE poderá autorizar, quando reconhecer a ocorrência de força maior ou de conveniência administrativa, alteração contratual de que decorra variação do valor do contrato ou modificação no prazo de sua execução, nos limites estabelecidos no parágrafo 1° do artigo 65 da Lei nº. 8.666/93, a qual se formalizará através de Termo Aditivo. As ordens de fornecimento expedidas serão circunstanciadas e pormenorizadas, especialmente em caso de possível aditamento.

15.7.1. A CONTRATADA obriga-se a manter, durante toda a vigência do processo, em compatibilidade com as obrigações por ela assumidas, todas as condições de habilitação e qualificação exigidas na licitação, devendo comunicar, imediatamente, qualquer alteração que possa comprometer a manutenção do contrato.

15.8. O empenho da despesa firmado com o SAAE não poderá ser objeto de cessão, transferência ou subcontratação sem autorização deste por escrito, sob pena de aplicação de sanção, inclusive rescisão.
15.8.1. Tais situações só poderão ser autorizadas na ocorrência de caso fortuito ou força maior que inviabilize a prestação pessoal pela CONTRATADA.

15.9. A tolerância do SAAE com qualquer atraso ou inadimplemento por parte da CONTRATADA não importará, de forma alguma, em alteração contratual ou novação, podendo o SAAE, exercer seus direitos a qualquer tempo.
15.9.1. A licitante deverá ser responsável pelo pagamento de todo os encargos, tributos e quaisquer outras contribuições que sejam exigidas para o fornecimento dos materiais/equipamentos que constituem o objeto desta licitação.

15.10. A licitante assumirá inteira responsabilidade pelas obrigações decorrentes da legislação trabalhista, previdenciária de acidentes de trabalho e quaisquer outras relativas a danos a terceiros, que decorram da prestação do objeto desta licitação.

15.11. A licitante fica responsável pela entrega dos software/equipamentos na sede do SAAE, situado à Rua Rio Branco, nº. 99, Bairro Centro, Itabirito/MG.

XVI – CONDIÇÕES DE PAGAMENTO

16.1. O pagamento decorrente da concretização do objeto desta licitação será efetuado pelo Setor Contábil do SAAE.
16.1.1. Em caso de irregularidade na emissão dos documentos fiscais, o prazo de pagamento será contado a partir de sua reapresentação, desde que devidamente regularizados.

16.2. Para a efetivação do pagamento, os documentos comprobatórios de situação regular em relação ao INSS (CND) e ao FGTS (CRF), deverão ser apresentados. Caso não o faça, o pagamento ficará retido até a apresentação de novos documentos, dentro do prazo de validade.

16.3. O pagamento será efetuado da seguinte forma: em até **10 (dez) dias corridos** do recebimento e aceite da Nota Fiscal Eletrônica, onde serão discriminados os equipamentos e os materiais adquiridos, o preço unitário e o preço total. Ressalte que a Nota Fiscal Eletrônica deverá estar acompanhada de arquivos digitais contendo cópia da Certidão Negativa de Débitos (***CND***) Relativos aos Tributos Federais e á Divida Ativa da União e o Certificado de Regularidade do FGTS (***CRF***), de acordo com o item 16.2.

16.4. A nota fiscal eletrônica deverá ser emitida pela própria CONTRATADA, em respeito ao disposto no item 15.6, posteriormente a emissão do Empenho Prévio, obrigatoriamente com o número de inscrição no CNPJ apresentado nos documentos de habilitação e de proposta de preço não se admitindo notas fiscais eletrônicas emitidas com outro CNPJ, mesmo que aquele de filial ou da matriz.

16.5. Para qualquer alteração nos dados da empresa, a CONTRATADA deverá comunicar o CONTRATANTE por escrito, acompanhado esta comunicação dos documentos alterados, no prazo de 30 (trinta) dias antes da emissão da Nota Fiscal Eletrônica.

XVII - DA REVISÃO DE PREÇOS

17.1. Havendo alterações na conjuntura econômica do País ou do Estado, que resulte em desequilíbrio financeiro permanente, nas condições do contrato e nas hipóteses autorizadas pela Lei de Licitações, a CONTRATADA poderá pleitear revisão de preços.

17.2. A revisão será aprovada conforme apresentação das Planilhas de Custo dos materiais/equipamentos e/ou Nota Fiscal anterior ao processo do qual baseou o preço da proposta apresentada e a Nota Fiscal atual comprovando o preço a ser revisado. O preço poderá sofrer acréscimo a decréscimo de acordo com o preço praticado no mercado

17.3. A cada pedido de revisão de preço deverão ser comprovadas as suas alterações justificadoras, demonstrando-se novamente a composição do preço, através de notas fiscais que comprovem o seu aumento.

17.4. É VEDADO À CONTRATADA INTERROMPER A ENTREGA DOS MATERIAIS/EQUIPAMENTOS, ENQUANTO AGUARDA O TRÂMITE DO PROCESSO DE REVISÃO DE PREÇOS, ESTANDO SUJEITA ÀS PENALIDADES PREVISTAS NESTE EDITAL E NA LEGISLAÇÃO APLICÁVEL NO CASO DE DESCUMPRIMENTO DESTA CLÁUSULA.

17.5. A revisão levará em consideração preponderantemente as normas legais federais, estaduais e municipais.

17.6. Deverá ser entregue uma planilha que comprove por item licitado o preço ofertado, sob pena de impossibilitar revisões de preço, se legalmente possíveis, em dia e prazo definidos pelo Setor Responsável.

17.7. Considerando o prazo de cumprimento do objeto esta licitação, em atendimento ao § 1º, do artigo 28, da Lei Federal nº. 9.069/95, e demais legislações pertinentes, fica vedado qualquer reajustamento de preços.

XVIII - DA RESCISÃO

18.1. A CONTRATANTE poderá declarar rescindido o Contrato, independentemente de qualquer procedimento judicial ou extrajudicial, sem que assista à CONTRATADA direito a qualquer indenização nos seguintes casos:

a) O descumprimento ou o cumprimento irregular de cláusulas contratuais, especificações, projetos ou prazos;
b) A lentidão no cumprimento do contrato, que impossibilite a conclusão da entrega do produto Licitado, no prazo estipulado;
c) Atraso injustificado da entrega do material/equipamento;
d) Se a CONTRATADA não mantiver os padrões de qualidade exigidos;
e) A subcontratação total ou parcial do seu objeto, fora das hipóteses permissivas contidas no item 15.9 e seu sub-item;
f) Desatendimento das determinações regulares da autoridade designada para acompanhar e fiscalizar a sua execução, assim como a de seus superiores;
g) Decretação de falência, instauração de insolvência civil, dissolução da sociedade ou o falecimento do CONTRATADO;
h) Alteração social ou modificação da finalidade ou da estrutura da CONTRATADA que, a Juízo do SAAE de Itabirito, prejudique a execução do Contrato;
i) O valor das multas atingir 10% (dez por cento) do valor global contratado ou após o trigésimo dia de atraso no cumprimento da obrigação assumida;
j) Razões de interesse público, de alta relevância e amplo conhecimento, justificado e determinado pelo Diretor Presidente do SAAE, exaradas no processo administrativo a que se refere o Contrato;
k) O descumprimento do disposto no inciso V do art.27 da Lei nº. 8.666/93, com a redação conferida pela Lei 9.854/99;
l) Nos demais casos elencados no art. 78 da Lei nº. 8.666/93, com suas posteriores alterações.

18.2. Na extinção da relação contratual o pagamento será efetuado de forma proporcional, retratando-se os materiais/equipamentos fornecidos e que efetivamente não foram compreendidos na última quitação.

18.3. O Contrato conterá cláusula de rescisão, que poderá ser judicial ou extrajudicial, podendo esta ser por ato unilateral e escrito da Administração, nos casos enumerados nos incisos I a XII e XVII do art. 78 da Lei nº. 8.666/93.

18.4. Nos casos de rescisão extrajudicial por ato unilateral, a CONTRATADA será notificada, em observância aos princípios do contraditório e da ampla defesa.

18.5. Além das hipóteses previstas no item acima, o Contrato poderá ser rescindindo sempre que a CONTRATADA agir dolosamente.

18.6. O Contrato poderá ser alterado mediante termo aditivo nas hipóteses previstas no art. 65 da Lei nº. 8.666/93.

18.7. No caso de rescisão do Contrato, é facultado à Administração convocar as licitantes remanescentes na ordem de classificação e nos moldes do art. 24, XI, da Lei nº. 8.666/93, ou ainda revogar a licitação.

18.8. O presente contrato poderá ser rescindido, quer pela inexecução das obrigações pactuadas, quer pela superveniência de norma legal que torne formal ou materialmente inexigível, ou desde que ocorra qualquer das hipóteses previstas no artigo 78 da Lei nº. 8.666/93, com suas posteriores alterações, à qual das partes expressamente se submetem, podendo a rescisão ser determinada:

a) mediante a denúncia da parte interessada, com antecedência de 30 (trinta) dias da data para a extinção de sua vigência.

b) por ato unilateral e escrito do CONTRATANTE nos casos enumerados nos incisos I a XII e XVII do supracitado artigo, quando nenhuma indenização será devida à CONTRATADA.

c) judicialmente, nos termos da Lei.

PARÁGRAFO PRIMEIRO

As partes contratantes poderão, observada a conveniência do CONTRATANTE, promover a rescisão amigável deste contrato, mediante termo próprio de distrato.

PARÁGRAFO SEGUNDO

Na hipótese de rescisão não amigável do contrato, não vinculada a ato ou fato da CONTRATADA, ser-lhe-á dado prévio aviso, com no mínimo 30 (trinta) dias de antecedência.

PARÁGRAFO TERCEIRO

Permanecem garantidos os diretos do CONTRATANTE no caso de Rescisão Administrativa, prevista no art. 77 da Lei nº. 8.666/93, com suas posteriores alterações.

XIX - DA FISCALIZAÇÃO

19.1. O setor competente para autorizar e fiscalizar o fornecimento do objeto desta licitação será **Tecnologia da Informação**, juntamente com o Chefe do Setor da Tecnologia da Informação, servidor Sérgio Pereira dos Santos, observado os artigos 73 a 76 da Lei Federal nº. 8.666/93.

19.2. O SAAE através do Setor de **Tecnologia da Informação** reserva-se no direito de não aceitar os materiais/equipamentos em desacordo com o previsto neste instrumento convocatório, podendo rescindir o contrato nos termos do art. 78, inciso I e aplicar o disposto no art. 24, inciso XI, ambos da Lei Federal nº. 8.666/93.

XX - DAS CONDIÇÕES GERAIS

20.1. O SAAE reserva-se o direito de, por despacho fundamentado de seu diretor, e sem que caiba em qualquer dos casos à licitante interessada, direito a indenização:

a) Revogar a licitação, em razão de conveniência administrativa;
b) Anular, total ou parcialmente o procedimento em razão de ilegalidade ocorrida em seu curso;
c) Homologar a licitação optando pela aquisição total ou parcial dos materiais/equipamentos a serem adquiridos.

20.2. A licitação não implica proposta de contrato por parte do SAAE. Até a entrega da nota de empenho poderá o licitante vencedor ser excluído da licitação, sem direito à indenização ou ressarcimento e sem prejuízo de outras sanções cabíveis, se a Administração tiver conhecimento de qualquer fato ou circunstância superveniente, anterior ou posterior ao julgamento desta licitação, que desabone a sua idoneidade ou capacidade financeira, técnica ou administrativa.

20.3. As despesas decorrentes da presente licitação correrão à conta dos orçamentos próprios sendo seus elementos as classificações orçamentárias, a saber:

PROJ. CONSTR. AMPL. OBRAS INFRAEST. GESTÃO DA ADM GERAL SAAE.
17 512 1711 3.030 44.90.52.00

OP. MANUT. AÇÕES DE GESTÃO ADM GERAL SAAE.
17 512 1711 4.030 33.90.40.00

20.4. É facultado ao Pregoeiro (a) ou à autoridade superior, em qualquer fase da licitação, a promoção de diligência com a suspensão da sessão, destinada a esclarecer ou complementar a instrução do processo, sendo vedada a inclusão posterior de documento ou informação que deveria constar no ato da sessão pública.

20.5. Toda a documentação apresentada no Instrumento Convocatório e seus Anexos são complementares entre si, de modo que qualquer detalhe que se mencione em um documento e se omita em outro, será considerado especificado e válido.

20.6. As decisões do (a) Diretor (a) e do Pregoeiro (a) e o extrato de contrato serão publicados no órgão de Imprensa Local, conforme artigo 78 da Lei orgânica e artigo 6º, XIII da Lei nº. 8.666/93, podendo ser aplicado o disposto no § 1º, do art. 109, da Lei nº. 8.666/93.

20.7. Maiores esclarecimentos serão prestados na sede do Serviço Autônomo de Saneamento Básico, situado na Rua Rio Branco, Nº. 99 – Bairro Centro – Itabirito/MG, Tel.: (31) 3562-4100 Fax.: (31) 3562-4102, pelo (a) Pregoeiro (a) e equipe de apoio, no horário de 08:00 horas às 12:00 horas e das 13:30 horas às 16:30 horas, em dias úteis.

20.8. Os casos omissos serão submetidos à apreciação da autoridade competente superior do Serviço Autônomo de Saneamento Básico de Itabirito/MG.

20.9. Fica eleito o foro da comarca de Itabirito/MG, com renúncia expressa a qualquer outro, por mais especial que seja para a solução de qualquer pendência atinente a este processo licitatório.

XXI - DAS PARTES QUE INTEGRAM O EDITAL

21.1. Constituem anexos deste instrumento convocatório, dele fazendo parte integrante:
ANEXO I – Planilha de Especificações e Preços/Proposta Comercial;
ANEXO II – Modelo de Carta de Credenciamento;
ANEXO III – Modelo de Declaração Habilitação;
ANEXO IV – Modelo de Declaração da empresa participante sob as penas da Lei de que não está suspensa nem é impedida de licitar com Órgão Público, conforme Incisos III e IV Artigo 87 da Lei nº. 8.666/93 com suas posteriores alterações;
ANEXO V – Modelo de Declaração do Empregador Pessoa Jurídica em cumprimento ao Disposto no Inciso XXXIII do art. 7 da Constituição Federal;
ANEXO VI – Modelo de Declaração somente para as Microempresas e Empresas de Pequeno Porte;
ANEXO VII – Declaração para Microempresas ou Empresas de Pequeno Porte, quanto à restrição em Documentação de Regularidade Fiscal;
ANEXO VIII – Modelo de Declaração de Elaboração Independente da Proposta.
ANEXO IX – Termo de Referencia.

Itabirito – MG, 20 de Agosto de 2020.

ROGÉRIO EDUARDO DE OLIVEIRA
Diretor Presidente do SAAE

Atesto que conferi o edital referente ao Processo Licitatório N° 083/2020, na modalidade Pregão Presencial N° 057/2020 referente à contratação de empresa especializada em fornecimento de Hardware (Servidor de Dados, Switch e Storage) e Software, a serem utilizados na Sede Administrativa do Serviço Autônomo de Saneamento Básico de Itabirito – MG, conforme especificações do anexo I, deste edital, e que o mesmo encontra-se em conformidade com o Termo de Referência.

Em _____/_____/2020

_____

SÉRGIO PEREIRA DOS SANTOS
Chefe do Setor de Tecnologia da Informação.

AVISO DE LICITAÇÃO

PREGÃO PRESENCIAL Nº. 057/2020

Encontra-se aberto na sede do Serviço Autônomo de Saneamento Básico de Itabirito à Rua Rio Branco, nº. 99, Centro, em Itabirito - MG, o Processo Licitatório **nº. 083/2020**, na Modalidade de PREGÃO PRESENCIAL **nº. 057/2020**, para contratação de empresa especializada em fornecimento de Hardware (Servidor de Dados, Switch e Storage) e Software, a serem utilizados na Sede Administrativa do Serviço Autônomo de Saneamento Básico de Itabirito – MG, conforme especificações do anexo I**,** no dia **10/09/2020 às 09:00** horas, na sala de reuniões do SAAE, sito à Rua Rio Branco, nº. 99 – Centro, em Itabirito - MG – CEP: 35.450-000. – Site www.saaeita.mg.gov.br - E-mail: compras@saaeita.mg.gov.br.

Detalhes do Pregão encontram-se à disposição dos interessados, no endereço acima, ou pelo telefone (31) 3562-4100 ou Fax (31) 3562-4102.

_____

ROGÉRIO EDUARDO DE OLIVEIRA

Diretor Presidente do SAAE

ANEXO I

PLANILHA DE ESPECIFICAÇÕES E PREÇOS

PROCESSO LICITATÓRIO Nº.: 083/2020

PREGÃO PRESENCIAL Nº.: 057/2020

DATA: 10/09/2020

HORÁRIO: 09:00 HORAS

OBJETO: **CONTRATAÇÃO DE EMPRESA ESPECIALIZADA EM FORNECIMENTO DE HARDWARE (SERVIDOR DE DADOS, SWITCH E STORAGE) E SOFTWARE, A SEREM UTILIZADOS NA SEDE ADMINISTRATIVA DO SERVIÇO AUTÔNOMO DE SANEAMENTO BÁSICO DE ITABIRITO – MG, CONFORME ESPECIFICAÇÕES DO ANEXO I.**

EMPRESA: .....

ENDEREÇO: ..... TELEFONE: .....

C. N. P. J.:..... INSC. ESTADUAL: .....

Apresenta cotação de preço para o fornecimento dos software/equipamentos abaixo discriminados, de acordo com as especificações e condições estabelecidas no EDITAL:

PROJ. CONSTR. AMPL. OBRAS INFRAEST. GESTÃO DA ADM GERAL SAAE. 17 512 1711 3.030 44.90.52.00							
ITEM	**ESPECIFICAÇÕES – LOTE 01**	UNID	QTDE	PREÇO UNIT.	PREÇO TOTAL	MARCA/ FABRI-CANTE/ MODELO	SE IMPORTADO PAÍS DE ORIGEM
01	**SERVIDOR TORRE** Servidor torre, possuindo no mínimo 02 processadores instalados, com velocidade mínima de 2,00 ghz – cache mínimo de 18,75mb, com mínimo de 08 cores, e não pode estar descontinuado pelo fabricante. Memória Ram com no mínimo 128gb **tipo** ddr4 – mínimo 2400mhz homologada pelo fabricante. Suporte de no mínimo 600gb de Ram Placa mãe deve ser do mesmo fabricante do equipamento, não sendo aceitas soluções OEM. Energia: Deve possuir redundância de fontes, com no mínimo 02 unidades de 485w cada, 80 PLUS, CERTIFICAÇÃO PLATINUM. Gravador de DVD interno. Chassi: deve ser torre, com no mínimo 4u. Deve possuir chaves para trava de chassi (não sendo aceitas adaptações). O servidor deve vir com o kit original do fabricante para instalação do mesmo em rack. Discos: deve possuir no mínimo: 2 unidades de discos sas 300gb sff 10k e 03 unidades de discos sata 2tb 7.2k sdd. Os discos devem ser originais do fabricante, homologados, não sendo aceitas adaptações ou utilização de discos não originais. Deve ter suporte a raid 5 e 10. O servidor deve ter suporte para no mínimo 24 discos. Rede: deve possuir no mínimo 02 portas de rede gigabit e no mínimo 01 porta rede 10gb sfp plus pci-e homologada do mesmo fabricante do servidor ou processador. O servidor deve vir com no mínimo 02 portas usb 3.0 Garantia: servidor deve possuir no mínimo 36 meses de garantia. **Apresentar catálogo técnico do equipamento, sob pena de desclassificação.**	Unid.	01				

saae Itabirito-MG

02	**STORAGE** Storage para armazenamento e backup Fiber Channel / ISCSI Dual LFF –Deve possuir no mínimo 02 controladoras redundantes Gabinete tipo Rack 2U, suporte a RAID: 0, 1, 3, 5 ,6, 10, Gerenciamento: 1p por controladora 1GbE Memória cache mínimo de 16GB (8GB por controladora), deve suportar um mínimo de 12 baias e discos LFF (3,5) Interface de disco, suportando pelo menos discos NL-SAS/SSD. Deve ter capacidade máxima de armazenamento de, no mínimo, até 1PB em discos SSD (Storage + 4 Expansões). Conectividade: Suporta conexões FC e ISCSI Conectividade: Sem Gbics Inclusos Fonte com no mínimo: 900W (sendo fonte redundante) (100-240 V bivolt automático) garantia mínima do fabricante: 03 anos (suporte 9 x 5). Devem estar inclusos, no mínimo 10 discos com capacidade 4tb, originais, do fabricante do equipamento, não sendo aceitos discos de outro fabricante, evitando assim perda ou não cumprimento da garantia por parte do fabricante. O sistema operacional e software de gestão do mesmo devem ser do mesmo fabricante. **Apresentar catálogo técnico do equipamento e discos, sob pena de desclassificação.**	Unid.	01				
03	STORAGE Especificações mínima do equipamento Processador: Processador com no mínimo 1.5GHz (núcleos) Possuir criptografia embarcada Memória: estática sem possibilidade de expansão, mínimo 1,5GB Deve possuir no mínimo 04 baias internas Deverá suportar no mínimo 48 TB Portas: Deve possuir no mínimo 02 Portas USB 3.1 Deve possuir no mínimo 01 Porta de Rede Gigabit Ethernet Deve possuir no mínimo 01 Rede 10 Gigabit Ethernet Deve ter resfriamento próprio condizente com o equipamento Deve possuir no mínimo 01 Fonte de Alimentação externa: 75W Deve ser bivolt automático Deve possuir no mínimo as certificações: FCC, CE, VCCI, BSMI, C-TICK Deve possuir software próprio e homologado Estar incluso 05 Discos (04 internos + 01 spare) com capacidade mínima de 10 TB cada. Deve possuir garantia mínima de 12 meses Os discos devem ser próprios para Storage, não sendo aceito discos para Desktop ou Sistema de Segurança e devem ser homologados pelo fabricante, novos e sem uso, devem ter garantia diretamente no fabricante, no Brasil e garantia de 60 meses. **Apresentar catálogo técnico do equipamento e discos, sob pena de desclassificação**	Unid.	01				
04	**SWITCH** Especificações mínimas do equipamento Possuir no mínimo 10 portas 10GB SFP+ Suporte IPV4 e IPV6 Layer 2 Possuir Porta console Possuir Porta Usb Capacidade de Switching: mínimo de 188 Mpps Rating: mínimo de 165 Gbps Endereços Mac: mínimo de 30K Buffer de memória: mínimo: 1MB Possuir WEB GUI Arquitetura para RacK (1U)	Unid.	01				

	06 (seis) cabos SFP+ de pelo menos 3 metros homologados pelo fabricante do switch. Garantia: Lifetime (garantia deve ser prestada no Brasil pelo fabricante ou empresa autorizada pelo mesmo) **Apresentar catálogo técnico do equipamento, sob pena de desclassificação.**						
OP. MANUT. AÇÕES DE GESTÃO ADM GERAL SAAE. 17 512 1711 4.030 33.90.40.00							
ITEM	**ESPECIFICAÇÕES – LOTE 02**	UNID	QTDE	PREÇO UNIT.	PREÇO TOTAL	MARCA/ FABRI-CANTE	SE IMPORTADO PAÍS DE ORIGEM
01	**FERRAMENTA DE BACKUP** A solução ofertada deverá, obrigatoriamente, atender as especificações mínimas previstas neste termo quanto às funcionalidades, integrações e compatibilidades com o ambiente virtualizado da CONTRATANTE para criação de backups e recuperação desses ambientes com o mínimo de indisponibilidade e reestruturação da parte física necessária, de forma que recupere, total e/ou granular, qualquer item assegurado por sua funcionalidade de backup e restauração. Deverá ser fornecido licenciamento do software, em caráter de aluguel de licenças, de propriedade e registrado para o SAAE DE ITABIRITO, na modalidade de capacidade por quantidade de instâncias protegidas para o ambiente físico e virtualizado, com suporte para backup e restore de dados. Cada licença de software licenciará UM TOTAL DE 12 VMS, do ambiente virtualizado (provedor/host das máquinas virtuais). Não poderão ser limitadas pelo volume de dados movimentados pelos mesmos. **CARACTERÍSTICAS ESPECÍFICAS** Deverá incluir funcionalidades de proteção (backup) e replicação integradas em uma única solução. Não deverá necessitar de instalação de agentes para poder realizar suas tarefas de proteção, recuperação e replicação das máquinas virtuais. Deverá garantir, no mínimo, a proteção de máquinas virtuais e seus dados, gerenciadas através das soluções de virtualização VMware. Deverá ter a capacidade de replicação de dados armazenados entre storages ou máquinas de configuração e de fabricantes diferentes. Deverá proteger o ambiente, sem interromper a atividade das máquinas virtuais e sem prejudicar sua performance, facilitando as tarefas de proteção (backup) e migrações em conjunto. Deverá ter a capacidade de testar a consistência do backup e replicação (S.O., aplicação, VM), emitindo relatório de auditoria para garantir a capacidade de recuperação. Deverá prover a deduplicação e compressão durante a operação de qualquer backup sem a necessidade de hardware de terceiros (appliance deduplicadora). Deverá possibilitar a cópia de uma máquina virtual completa ou discos virtuais específicos. Deverá ser fornecida com ferramenta de gestão de arquivos para os administradores de máquinas virtuais no console do operador. Deverá ter a capacidade de integração através de API's dos fabricantes de infraestrutura virtualizada para a proteção de dados. Deverá ter a capacidade de realizar proteção (backup) incremental e replicação diferencial, aproveitando a tecnologia de "rastreio de blocos modificados" (CBT – changed block tracking), reduzindo ao mínimo necessário, o tempo de backup e possibilitando proteção (backup e replicação).	Unid.	01				

	Deverá oferecer múltiplas estratégias e opções de transporte de dados para as áreas de proteção (backup), a saber: Diretamente através de Storage Area Network (SAN); Diretamente do storage, através do hypervisor I/O (Virtual Appliance); Mediante uso da rede local (LAN); Deverá manter um backup sintético, eliminando assim a necessidade de realizar backups completos (full) periódicos, incremental permanente, o que permitirá economizar tempo e espaço. Deverá possibilitar a inicialização de uma máquina virtual diretamente do arquivo de backup, inclusive sem necessidade de "hidratação" dos dados "deduplicados" e "comprimidos". Deverá permitir a recuperação de mais de uma máquina virtual e/ou ponto de restauração simultâneo, permitindo assim, ter múltiplos pontos de tempo de uma ou mais máquinas virtuais. Todo serviço de migração das máquinas virtuais do repositório de backup até o armazenamento na produção restabelecida não deverá afetar a disponibilidade e acesso pelo usuário, sem paradas. Deverá prover acesso ao conteúdo das máquinas virtuais, para recuperação de arquivos, pastas ou anexos, diretamente do ambiente protegido (repositório de backup) ou replicados, sem a necessidade de recuperar completamente o backup e inicializar uma máquina virtual. Deverá permitir realizar buscas rápidas mediante os índices dos arquivos que sejam controlados por um sistema operacional Windows, quando este seja o sistema operacional executado dentro da máquina virtual da qual se tenha realizado o backup. Deverá assegurar a consistência de aplicações transacionais de forma automática por meio da integração com Microsoft VSS, dentro de sistemas operacionais Windows. Deverá permitir realizar a truncagem de logs transacionais (transaction logs) para máquinas virtuais com Microsoft Exchange, SQL Server e Oracle. Deverá permitir notificações por correio eletrônico, SNMP ou através dos atributos da máquina virtual do resultado da execução de seus trabalhos. Deverá permitir recuperar no nível de objetos e arquivos de qualquer aplicação virtualizada, em qualquer sistema operacional, utilizando as ferramentas de gestão das aplicações existentes. Deverá incluir ferramentas de recuperação sem a necessidade de agentes, sem a necessidade de recuperar os arquivos da máquina virtual como um todo ou reiniciar a mesma (recuperação granular), para os servidores: Microsoft Exchange 2016, possibilitando recuperar objetos individuais, tais como contatos, mensagens, compromissos, anexos, entre outros; Microsoft Active Directory 2016, possibilitando recuperar objetos individuais, tais como usuários, recuperação de senhas de usuários e computadores, grupos, contas, Objetos de Política de Grupo (GPOs), registros do Microsoft DNS integrados ao Active Directory entre outros sem a necessidade de usar o agente tanto para backup e restauração; Microsoft SQL Server 2014 ou superior, possibilitando recuperar objetos individuais, tais como bases, tabelas, registros, entre outros; Microsoft Sharepoint 2016; Deverá oferecer testes automatizados de recuperação para todas as máquinas virtuais protegidas, garantindo a confiabilidade na execução correta das máquinas virtuais e de suas aplicações (DNS Server, Controlador						

	de domínio, Servidor de e-mail, etc.), no momento da recuperação. Deverá ser possível executar uma ou várias máquinas virtuais a partir do arquivo de backup, em um ambiente isolado de forma automática através de schedule, sem a necessidade de espaço de armazenamento adicional e sem modificar os arquivos de backup (read-only), para criação de ambiente de homologação, teste, etc. Deverá oferecer arquivamento em fita, suportando VTL (Virtual Tape Libraries), biblioteca de fitas e drives LTO5 ou superior, possibilitando a gravação paralela em múltiplos drives, além da criação de pools de mídia globais e pools de mídia GFS, sem a necessidade de licenciamento individual por drive; Deverá oferecer trabalhos de cópia de backup com implementação de políticas de retenção. Deverá operar em ambientes virtualizados através das soluções da Vmware, incluindo: VMware vSphere 7. Deverá garantir a recuperação granular e consistente, sem necessidade de instalação de agentes adicionais para o ambiente virtualizado através das soluções acima, principalmente para os seguintes softwares: Microsoft Active Directory 2016; Microsoft Exchange Server 2016; Microsoft Sharepoint 2013 ou superior Oracle Database 12 ou superior. Deverá ser capaz de realizar réplicas em outros sites ou infraestruturas a partir dos backups realizados. Deverá regular de forma dinâmica e parametrizável, o uso de recursos computacionais, de forma que se possa diminuir o impacto na infraestrutura de produção, durante as atividades de backup. Deverá permitir um método de fácil de recuperação, desde ambientes de contingência, com as ações pré-configuradas para evitar ações manuais em caso de desastre, similar a um botão de emergência. Deverá oferecer a possibilidade de armazenar os arquivos de backup de forma criptografada, com algoritmo mínimo de 256 bits, ativando e desativando tal operação, assim como assegurar o trânsito da informação através desse cenário. Deverá permitir a criação de níveis de delegação de tarefas (perfis) de recuperação no nível de elementos da aplicação, inclusive para outros usuários, de forma a diminuir a carga de atividades executadas pelo administrador da plataforma. Deverá integrar uma solução unificada de monitoração de ambientes virtualizados, com fornecimento de relatórios capazes de apresentar informações do tipo: Relatórios que permitam o planejamento de capacidade; Relatórios que permitam determinar a ineficiência dos recursos em uso; Relatórios que facilitem a visibilidade de tendências negativas e anomalias; Quadros de controle claros, apresentáveis e integráveis em sites web. A licença de software de Backup deverá, nativamente, ser capaz de emitir relatórios com informações completas, conforme subitens: Permitir acesso aos relatórios através de interface gráfica ou web; Suportar a geração de relatórios gráficos customizáveis de atividades de backups/restores, contendo: Horário de início e término dos jobs; Tempo de duração dos jobs; Todos os jobs em execução; Status (situação) de execução dos jobs; Relação e porcentagem de jobs executados por status, como por exemplo: com sucesso e com erros; Logs dos jobs; Volume de dados na origem e no destino, total e por job, por período de tempo, por localidade e por host (físico ou virtual);						

	Tendência de crescimento; Dados históricos de, no mínimo, 24 (vinte e quatro) meses. Suportar a geração de relatórios gráficos customizáveis de atividades de backups, contendo: Identificação da ocupação nos destinos de backups: uso de disco e fita; Porcentagem de dados deduplicados; Taxa de deduplicação e compressão. Permitir a geração de relatórios baseados na utilização de recursos, identificando restrições associadas a aplicativos específicos. Permitir a geração de relatórios baseados em alertas pré-definidos, com o objetivo de reportar eventos ocorridos do ambiente operacional de backup e restore. Deverá correlacionar a execução de trabalhos de backup e réplica com os objetos do ambiente virtual. Deverá oferecer a capacidade de relatar o cumprimento das políticas de proteção de dados e disponibilidade de acordo com parâmetros definidos. Deve suportar múltiplas operações dos componentes/servidores participantes da estrutura de backup, permitindo atividades de backup e recuperação simultâneas; Deve suportar repositório de backup com aumento de escala ilimitado para o armazenamento de dados com suporte aos seguintes sistemas de armazenamento: Microsoft Windows; Linux; Pastas compartilhadas; Appliances de duplicadoras. Storages do tipo SAN e NAS Nuvem (Amazon AWS, Microsoft Azure) Deverá permitir a seleção de um destino de armazenamento do backup em um provedor de serviços em nuvem (BaaS – Backup as a Service); Deverá permitir a seleção de um destino para a réplica dos dados que poderá ser em um provedor de serviços em nuvem (DRaaS – DR as a Service); Possuir integração com armazenamento de objetos compatíveis com S3 como Amazon S3, Azure Blob Storage e qualquer outro dispositivo de armazenamento local compatível com S3; Realizar arquivamento dos dados de backup nos dispositivos e locais de armazenamento de objetos compatíveis com S3; Em caso de desastre, deverá ser possível realizar a recuperação dos dados diretamente do arquivamento em S3; A solução deverá possuir integração com soluções de antivírus de modo a realizar uma varredura de segurança nos dados de backup antes de realizar sua recuperação; Deve possuir a funcionalidade de recuperar dados para servidores diferentes do equipamento de origem; Deve ser ofertada a versão mais atual do software de backup, liberada oficialmente pelo fabricante do software. Caso haja necessidade, por razões de compatibilidade com os demais componentes de hardware e software do ambiente de backup, O SAAE DE ITABIRITO se reserva o direito de utilizar a versão do software imediatamente anterior à versão mais atual, sem nenhum ônus adicional; Deve ser ofertada, junto com a solução, o armazenamento de 6 tb de dados em ambiente de cloud computing com suporte integrado à solução para backup dos dados, com proteção dentro da interface de gerenciamento da solução para evitar “inside atacks” (ataques que objetivam o backup e a deleção dos mesmos). O ambiente de nuvem deve ser integrado para permitir a partir de uma interface única desenvolver tanto o backup quanto o restore de todo o ambiente.						

	Apresentar catálogo técnico da solução, sob pena de desclassificação. **Após aquisição será realizada prova de conceito da solução na Sede do SAAE de ITABIRITO antes do aceite da solução. Não sendo satisfatória, a troca será de total responsabilidade do fornecedor incluindo a mão de obra de instalação.**						
02	**FIREWALL** 1. Especificações Gerais 1.1. Distribuidor deve ter presença nacional de suporte. 1.2. Next-Generation Firewall (NGFW) para proteção de informação perimetral e de rede interna que inclui stateful firewall com capacidade para operar em alta disponibilidade (HA) em modo ativo-passivo para controle de tráfego de dados por identificação de usuários e por camada 7, com controle de aplicação, administração de largura de banda (QoS), VPN IPsec e SSL, IPS, prevenção contra ameaças de vírus, malwares, Filtro de URL, criptografia de email, inspeção de tráfego criptografado e proteção de firewall de aplicação Web. Deverá ser fornecida console de gerenciamento dos equipamentos e centralização de logs em hardware específico e virtualizado. 1.2.1. A solução deve consistir de appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), e console de gerência, monitoração e logs. 1.2.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões. 1.3. Para os itens que representem bens materiais, a CONTRATADA deverá fornecer produtos novos, sem uso anterior. 1.4. O backup e o reestabelecimento de configuração deverão ser feitos localmente, via FTP ou email com frequência diária, semanal ou mensal, podendo também ser realizado por demanda. 1.5. Suportar SNMP e Netflow. 1.6. A solução deverá permitir port-aggregation de interfaces de firewall suportando o protocolo 802.3ad, para escolhas entre aumento de throughput e alta disponibilidade de interfaces 1.7. A solução deverá permitir configurar os serviços de DNS, Dynamic DNS, DHCP e NTP. 1.8. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico. 1.9. Cada appliance deverá ser capaz de executar a totalidade das capacidades exigidas para cada função, não sendo aceitos somatórias para atingir os limites mínimos. 1.10. O hardware e o software fornecidos não podem constar, no momento da apresentação da proposta, em listas de end-of-sale, end-of-support, end-ofengineering-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante. 1.11. O contratante deve possuir a opção de abrir solicitações de suporte diretamente com o fabricante. 1.12. Suporte aos roteamentos estáticos, dinâmico (RIP, BGP e OSPF) e multicast (PIM-SM e IGMP) 1.13. O Appliance proposto deve fornecer logs e relatórios embarcados contendo no mínimo os itens abaixo: 1.13.1. Dashboard com informações do sistema: 1.13.1.1. Informações de CPU 1.13.1.2. Informações do uso da rede. 1.13.1.2. Informações de memória. 1.13.1.3. Informações de sessões ativas. 1.13.1.4. Permitir visualizar número políticas ativas.	Unid.	01				

	1.13.1.5. Visualizar número de access point do fabricante conectados. 1.13.1.6. Visualizar número de usuários conectados remotamente. 1.13.1.7. Visualizar número de usuários conectados localmente. 1.13.2. Relatórios com informações sobre as conexões de origem e destino por países. 1.13.3. Relatórios informando as conexões dos hosts. 1.13.4. Visualizar relatórios por período de tempo, permitindo o agendamento e o envio destes relatórios por email. 1.13.5. Permitir exportar relatórios para as seguintes extensões/plataformas: 1.13.5.1. PDF 1.13.5.2. HTML 1.13.5.3. Excel 1.13.6. Permitir visualizar relatório de políticas ativas associado ao ID da política criada. 1.13.7. Relatório que informe o uso IPSEC por host e usuário. 1.13.8. Relatório que informe o uso L2TP por host e usuário. 1.13.9. Relatório que informe o uso PPTP por usuários. 1.13.10. Relatório abordando eventos de VPN. 1.13.11. Proporcionar sistema de logs em tempo real, com no mínimo as seguintes informações: 1.13.11.1. Logs do sistema. 1.13.11.2. Logs das políticas de segurança 1.13.11.3. Logs de autenticação 1.13.11.4. Logs de administração do appliance. 1.13.12. Permitir ocultar dos relatórios usuários e IPs cadastrados. 1.14. Ter relatórios customizados e em compliance com pelo menos estes órgãos: HIPAA, GLBA, SOX, FISMA, PCI, NERC CIP v3, CIPA. 1.15. Possuir no mínimo 6 interfaces 10/100/1000; 1.16. A solução proposta deve cumprir as normas da CE, FCC Class A, CB, VCCI, CTick, UL, CCC. 1.15. A solução proposta deve corresponder aos seguintes critérios de throughput máximo, considerando o tamanho do pacote UDP sendo 1518 byte: Suportar no mínimo 27.500 (vinte e sete mil e quinhentos) novas conexões por segundo; 1.16. Suportar no mínimo 6.000.000 (seis milhões) conexões simultâneas; 1.17. Possuir no mínimo 3.500 Mbps (três mil e quinhentos) de rendimento (throughput) do Firewall para pacotes UDP; 1.18. No mínimo 900 (novecentos) Mbps de rendimento (throughput) do IPS; 1.18. Possuir no mínimo 350 Mbps de throughput de VPN AES. 1.19. A solução proposta deve corresponder aos seguintes critérios de throughput em mundo real: 1.19.1. Entende-se como mundo real, testes realizados pelo fabricante que tenham sido feitos com o appliance utilizando até 50% da capacidade de processamento, utilizando um mix de protocolos usados no mundo corporativo. 1.19.2. Possuir no mínimo 103 Mbps de rendimento (throughput) de IPS mundo real. 1.19.3. Possuir no mínimo 30 Mbps de rendimento (throughput) de funcionalidades next generation em mundo real; 1.19.4. Possuir no mínimo 90 de rendimento (throughput) de VPN AES mundo real. 1.20. Entende-se como mundo real testes realizados utilizando ambientes e protocolos usados no mundo corporativo. 1.21. A solução proposta deve possuir licenças						

	baseado nos recursos de hardware. 1.22. A solução proposta deve suportar a configuração de políticas baseadas em usuários para segurança e gerenciamento de internet. 1.23. A solução proposta deve fornecer os relatórios diretamente no Appliance, baseados em usuário, não só baseado em endereço IP. 1.24. A solução proposta deve possuir no mínimo 64 GB de espaço em disco SSD para o armazenamento de eventos e relatórios. 1.25. Possuir slot de FleXi Port 1.26. Possuir portas USB 2.0 e 3.0. 1.27. Possuir porta VGA. 1.28. Possuir ao menos uma porta COM (RJ45). 1.29. Número irrestrito de usuários/IP conectados. 1.30. Appliance com 1U para montagem em rack. 2. Especificações da Administração, Autenticação e Configurações em geral 2.1. A solução proposta deve suportar administração via comunicação segura (HTTPS, SSH) e Console. 2.2. A solução proposta deve ser capaz de importar e exportar cópias de segurança (backup) das configurações, incluindo os objetos de usuário. 2.3. O backup pode ser realizado localmente, enviado pela ferramenta para um ou mais emails pré-definidos e via FTP, deve-se também ser feito sob demanda, ou seja, agendar para que este backup seja realizado, por dia, semana, mês e ano. 2.4. A solução proposta deve suportar implementações em modo Router (camada 3) e transparente (camada 2) individualmente ou simultâneos. 2.5. A solução proposta deve suportar integrações com, Active Directory, LDAP, Radius, eDirectory, TACACS+ e Banco de Dados Local para autenticação do usuário. 2.6. A solução proposta deve suportar em modo automático e transparente "Single Sign On" na autenticação dos usuários do active directory e eDirectory. 2.7. Os tipos de autenticação devem ser, modo transparente, por autenticação Kerberus/NTLM e cliente de autenticação nas máquinas. 2.8. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços. 2.9. Deve permitir autenticação em modos: transparente, autenticação proxy (NTLM e Kerberos) e autenticação via clientes nas estações com os sistemas operacionais Windows, MAC OS X e Linux 32/64. 2.10. Certificados de autenticação para iOS e Android. 2.11. A solução proposta deve suportar integração com Dynamic DNS de terceiros 2.12. A solução proposta deve ter gráficos de utilização de banda em modos diários, semanais, mensais ou anuais para os links de forma consolidada ou individual. 2.13. A solução proposta deve suportar Parent Proxy com suporte a IP / FQDN. 2.14. A solução proposta deve suportar NTP. 2.15. A solução proposta deverá suportar a funcionalidade de unir usuário/ip/mac para mapear nome de usuário com o endereço IP e endereço MAC por motivo de segurança. 2.16. A solução proposta deve ter suporte multilíngue para console de administração web. 2.17. A solução proposta deverá suportar fazer um roll back de versão. 2.18. A solução proposta deve suportar a criação de usuário baseada em ACL para fins de administração. 2.19. A solução proposta deve suportar instalação de						

	LAN by-pass no caso do appliance estar configurado no modo transparente. 2.20. A solução proposta deve suportar cliente PPPOE e deve ser capaz de atualizar automaticamente todas as configurações necessárias, sempre que PPPOE trocar. 2.21. A solução proposta deve suportar SNMP v1, v2c e v3. 2.22. A solução proposta deve suportar SSL/TLS para integração com o Active Directory ou LDAP. 2.23. A solução proposta deve possuir serviço de "Host Dynamic DNS" sem custo e com segurança reforçada. 2.24. A solução proposta deve ser baseado em Firmware ao contrário de Software e deve ser capaz de armazenar duas versões de Firmware ao mesmo tempo para facilitar o retorno "rollback" da cópia de segurança. 2.25. A solução proposta deve fornecer uma interface gráfica de administração flexível e granular baseado em perfis de acesso. 2.26. A solução proposta deve fornecer suporte a múltiplos servidores de autenticação para diferentes funcionalidades (Exemplo: Firewall um tipo de autenticação, VPN outro tipo de autenticação) 2.27. A solução proposta deve ter suporte a ambientes de terminais (Microsoft e Citrix) suportando autenticação de usuário de diferentes sessões originando do mesmo endereço IP. 2.28. A solução proposta deve suportar: 2.28.1. Serviço de DHCP/DHCPv6; 2.28.2. Serviço de DHCP/DHCPv6 Relay Agent; 2.28.3. Suporte a DHCP sobre VPN IPSec; 2.29. A solução proposta deve trabalhar como DNS/DNSv6 Proxy. 2.30. Gráficos, relatórios e ferramentas avançadas de apoio para troubleshooting. 2.31. Permitir exportar informações de troubleshooting para arquivo PCAP. 2.32. Permitir o factory reset e troca do idioma via interface gráfica. 2.33. Atualização de firmware de forma automatizada 2.34. Reutilização de definições de objetos de rede, hosts, serviços, período de tempo, usuários, grupos, clientes e servers. 2.35. Portal de acesso exclusivo para usuários poderem realizar atividades administrativas que envolve apenas funcionalidades especificas a ele. 2.36. Controle de acesso e dispositivos por zoneamento. 2.37. Integrar com ferramenta de gerenciamento centralizado disponibilizado pela própria fabricante. 2.38. Opção de habilitar acesso remoto do appliance para suporte diretamente com o fabricante através de um túnel seguro, esta funcionalidade deve estar embarcada dentro do próprio appliance ofertado. 2.39. Traps SNMP ou email para notificações do sistema. 2.40. Suportar envio de informações via Netflow e possuir informações via SNMP. 2.41. Suporte a TAP mode para POCs e trials. 2.42. Ter funcionalidade que permita que o administrador manualmente atribua e/ou desatribua cores do CPU para uma interface em particular, dessa forma, todo trafego que passar por esta interface, será tratado unicamente pelos núcleos definidos. 2.43. Possuir funcionalidade de Fast Path para realizar a otimização no tratamento dos pacotes. 3. Especificações de Balanceamento de Carga e Redundância para Múltiplos Provedores de Internet 3.1. A solução proposta deve suportar o balanceamento de carga e redundância para mais de 2 (dois) links de Internet.						

	3.2. A solução proposta deve suportar o roteamento explícito com base em origem, destino, nome de usuário e aplicação. 3.3. A solução proposta deve suportar algoritmo “Round Robin” para balanceamento de carga. 3.4. A solução proposta deve fornecer opções de condições em caso de falha "Failover" do link de Internet através dos protocolos ICMP, TCP e UDP. 3.5. A solução proposta deve enviar e-mail de alerta ao administrador sobre a mudança do status de gateway. 3.6. A solução proposta deve ter ativo/ativo utilizando algoritmo de "Round Robin" e ativo/passivo para o balanceamento de carga do gateway e suporte a falha (Failover). 3.7. A solução proposta deve fornecer o gerenciamento para múltiplos links de Internet bem como tráfego IPv4 e IPv6. 4. Especificações de Alta Disponibilidade 4.1. A solução proposta deve suportar Alta Disponibilidade (High Availability) ativo/ativo e ativo/passivo. 4.2. A solução proposta deve notificar os administradores sobre o estado (status) dos gateways mantendo a Alta Disponibilidade. 4.3. O tráfego entre os equipamentos em Alta Disponibilidade deverá ser criptografado. 4.4. A solução deverá detectar falha em caso de Link de Internet, Hardware e Sessão. 4.5. A solução proposta deve suportar sincronização automática e manual entre os appliances em "cluster". 4.6. A solução deve suportar Alta Disponibilidade (HA) em "Bridge Mode" e Mixed Mode" (Gateway + Bridge). 5. Proteção básica de firewall 5.1. Especificações do Firewall e roteamento 5.2. A solução deve ser Standalone Appliance e com Sistema Operacional fortalecido "Hardening" para aumentar a segurança. 5.3. Deve suportar controles por: porta e protocolos TCP/UDP, origem/destino e identificação de usuários. 5.4. Suporte a objetos e regras IPV6. 5.5. Suporte a objetos e regras multicast. 5.6. A solução proposta deve suportar “Stateful Inspection” baseado no usuário "one-toone", NAT Dinâmico e PAT. 5.7. A solução proposta deve usar a "Identidade do Usuário" como critério de Origem/Destino, IP/Subnet/Grupo e Porta de Destino na regra do Firewall. 5.8. A solução proposta deve unificar as políticas de ameaças de forma granular como Antivírus/AntiSpam, IPS, Filtro de Conteúdo, Políticas de Largura de Banda e Política de Balanceamento de Carga baseado na mesma regra do Firewall para facilitar de uso. 5.9. A proteção Anti-Malware deverá realizar a proteção com emulação JavaScript. 5.10. Deve permitir o bloqueio de vulnerabilidades. 5.11. Deve permitir o bloqueio de exploits conhecidos. 5.12. A solução proposta deve suportar arquitetura de segurança baseado em Zonas 5.12.1. As zonas deverão ser divididas pelo menos em WAN, LAN e DMZ, sendo necessário que as zonas LAN e DMZ possam ser customizáveis. 5.13. A solução proposta deve ter predefinido aplicações baseadas na "porta/assinatura" e também suporte à criação de aplicativo personalizado baseado na "porta/número de protocolo". 5.14. A solução proposta deve suportar balanceamento de carga de entrada (Inbound NAT) com diferentes métodos de balanceamento como First Alive, Round Robin,						

	Random, Sticky IP e Failover conforme a saúde (Health Check) do servidor por monitoramento (probe) TCP ou ICMP. 5.15. A solução proposta deve suportar 802.1q (suporte a marcação de VLAN). 5.16. A solução proposta deve suportar roteamento dinâmico como RIP1, RIP2, OSPF, BGP4. 5.17. A solução proposta deve possuir uma forma de criar roteamento Estático/Dinâmico via shell. 5.18. O sistema proposto deve prover mensagem de alertas no Dash Board (Painel de Bordo) quando eventos como: a senha padrão não foi alterada, acesso não seguro está permitindo ou a licença irá expirar em breve. 5.19. O sistema proposto deve prover Regras de Firewall através de endereço MAC (MAC Address) para prover segurança na camada de rede 2 até 7 do modelo OSI. 5.20. A solução proposta deve suportar IPv6. 5.20.1. IPv6 deve suportar os tunelamentos 6in4, 6to4, 4in6 e IPv6 Rapid Deployment (6rd) de acordo com a RFC 5969. 5.21. A solução proposta deve suportar implementações de IPv6 Dual Stack. 5.22. A solução proposta deve suportar tuneis 6in4,6to4,4in6,6rd. 5.23. A solução proposta deve suportar toda a configuração de IPv6 através da Interface Gráfica. 5.24. A solução proposta deve suportar DNSv6. 5.25. A solução proposta deve oferecer proteção DoS contra ataques IPv6. 5.26. A solução proposta deve oferecer prevenção contra Spoof em IPv6. 5.27. A solução proposta deve suportar 802.3ad para Link Aggregation. 5.28. A solução proposta deve suportar 3G UMTS e 4G modem via interface USB para VPN e Link Backup "Plano de Continuidade" - Balanceamento de Carga. 5.29. A solução proposta deve suportar gerenciamento de banda baseado em Aplicação que permite administradores criarem políticas de banda de utilização de link baseado por aplicação. 5.30. Flood protection, DoS, DDoS e Portscan. 5.31. Bloqueio de Países baseados em GeoIP. 5.32. Suporte a Upstream proxy. 5.33. Suporte a VLAN DHCP e tagging. 5.34. Suporte a Multiple bridge. 5.35. Funcionalidades do portal do usuário 5.35.1. Autenticação de dois fatores (OTP) para IPSEC e SSL VPN, portal do usuário, e administração web (GUI). 5.35.2. Download dos clientes de autenticação disponibilizados pela ferramenta. 5.35.3. Download do cliente VPN SSL em plataformas Windows. 5.35.4. Download das configurações SSL em outras plataformas. 5.35.5. Informações de hotspot. 5.35.6. Autonomia de troca de senha do usuário. 5.35.7. Visualização do uso de internet do usuário conectado. 5.35.8. Acesso a mensagens quarentena. 5.36. Opções base de VPN 5.36.1. A VPN IPsec deve suportar: DES e 3DES, Autenticação MD5 e SHA-1;Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; Algoritmo Internet Key Exchange (IKE); AES 128, 192 e 256 (Advanced Encryption Standard); SHA 256, 384 e 512; Autenticação via certificado PKI (X.509) e Pre-shared key (PSK). 5.36.2. L2TP e PPTP.						

	5.36.3. VPN SSL, IPSEC. 5.36.4. Proporcionar através do portal do usuário uma forma de conexão via HTML5 de acesso remoto com suporte aos protocolos, RDP, HTTP, HTTPS, SSH, Telnet e VNC. 5.36.5. Suportar autenticação via AD/LDAP, Token e base de usuários local. 5.37. Funcionalidades base de QoS e Quotas 5.37.1. QoS aplicado a redes e usuários de download/Upload em tráfegos baseados em serviços. 5.37.2. Otimização em tempo real do protocolo Voip. 5.37.3. Suporte a marcação DSCP. 5.37.4. Regras associadas por usuário. 5.37.5. Criar regras que limitem e garantam upload e download. Permitir criar regra de QoS individualmente e compartilhada. 6. Proteção Web 7. Filtragem e Segurança Web 7.1. Proporcionar transparência total de autenticação no proxy, provendo segurança antimalware e filtragem web. 7.2. Possuir uma base de dados com mais de 1.000.000 (um milhão) de URLs reconhecidas e categorizadas agregadas a pelo menos 92 categorias oferecidas pela solução. 7.3. Realizar autenticação dos usuários nos modos transparente e padrão. 7.3.1. As autenticações devem ser feitas via NTLM. 7.4. Possuir sistema de quotas aplicado por usuários e grupos. 7.5. Permitir criar politicas por horário aplicado a usuários e grupos. 7.6. Possuir sistema de malware scanning que realize as seguintes ações: 7.6.1. Bloquear toda forma de vírus 7.6.2. Bloquear malwares web 7.6.3. Prevenir infecção de malwares, trojans e spyware em tráfegos HTTPS, HTTP, FTP e emails baseados em acesso web (via navegador). 7.6.4. Proporcionar proteção de web malware avançado com emulação de Javascript. 7.7. Prover proteção em tempo real de todos os acessos web. 7.7.1.A proteção em tempo real deve consultar constantemente a base de dados na nuvem do fabricante que deverá manter-se atualizada prevenindo novas ameaças. 7.8. Prover pelo menos duas engines diferentes de antimalware para auxiliar na detecção de ataques e ameaças realizadas durante os acessos web realizados pelos usuários. 7.9. Fornecer Pharming Protection. 7.10. Possuir pelo menos dois modos diferentes de escaneamento durante o acesso do usuário. 7.11. Permitir criação de regras customizadas baseadas em usuário e hosts. 7.12. Permitir criar exceções de URLs, usuários e hosts para que não sejam verificados pelo proxy. 7.13. Validação de certificado. 7.14. Prover cache de navegação, contribuindo na agilidade dos acessos a internet. 7.15. Realizar filtragem por tipo de arquivo, mime-type, extensão e tipo de conteúdo (exemplo: Activex, applets, cookies, etc.) 7.16. Integração com o youtube for schools. 7.17. Prover funcionalidade que força o uso das principais ferramentas de pesquisa segura (SafeSearch): Google, Bing e Yahoo. 7.18. Permitir alterar a mensagem de bloqueio apresentada pela solução para os usuários finais. 7.19. Permitir alterar a imagem de bloqueio que é						

	apresentado para o usuário quando feito um acesso não permitido. 7.20. Permitir a customização da página HTML que apresenta as mensagens e alertas para os usuários finais. 7.21. Permitir visualizar as alterações feitas nos itens 7.17 e 7.18 antes de salvar as modificações. 7.22. Especificar um tamanho em Kbytes de arquivos que não devem ser escaneados pela proteção web. 7.22.1. Range aceitável de 1 a 25600KB. 7.23. Bloquear trafego que não segue os padrões do protocolo HTTP. 7.24. Permitir criar exceções de sites baseados em URL Regex, tanto para HTTP quanto para HTTPS. 7.25. Nas exceções, permitir definir operadores “AND” e “OR”. 7.26. Permitir definir nas exceções a opção de não realizar escaneamento HTTPS. 7.27. Permitir definir nas exceções a opção de não realizar escaneamento contra malware. 7.28. Permitir definir nas exceções a opção de não realizar escaneamento de critérios especificado por políticas. 7.29. Permitir criar regras de exceções por endereços IPs de origem. 7.30. Permitir criar regras de exceções por endereços IPs de destino 7.31. Permitir criar exceções por grupo de usuários. 7.32. Permitir criar exceções por categorias de sites. 7.33. Permitir a criação de agrupamento de categorias feitas pelo administrador do equipamento. 7.34. Ter grupos de categorias pré-configuradas na solução apresentando nomes sugestivos para tais agrupamentos, por exemplo: “Criminal Activities, Finance & Investing, Games and Gambling”, entre outras. 7.35. Permitir editar grupos de categorias pré-estabelecidos pela solução. 7.36. Deve ter sistema que permita a criação de novas categorias com as seguintes especificações: 7.36.1. Nome da regra; 7.36.2. Permitir criar uma descrição para identificação da regra. 7.36.3. Ter a possibilidade de classificação de pelo menos: 7.36.3.1. Produtivo; 7.36.3.2. Não produtivo; 7.36.3.3. Permitir aplicar Traffic shaping diretamente na categoria. 7.36.3.4. Na especificação das URLs e domínios que farão parte da regra, deve-se permitir cadastrar por domínio e palavra-chave. 7.36.3.5. Deve permitir importar uma base com domínios e palavras chaves na hora da criação da categoria, a base com informações de domínios e palavras chaves deverá aceitar pelo menos as seguintes extensões: .tar, .gz, .bz, .bz2, e .txt. 7.36.3.6. Permitir importar a base citada no item anterior de forma externa, ou seja, especificar uma URL externa que contenha as informações com a lista domínios que poderá ser mantida pelo administrador ou um terceiro. 7.37. Ter função para criar grupos de URLs. 7.38. A base de sites e categorias devem ser atualizadas automaticamente pelo fabricante. 7.39. Permitir ao administrador poder especificar um certificado autoritário próprio para ser utilizado no escaneamento HTTPS. 7.40. Deve permitir que em uma mesma política seja aplicada ações diferentes de acordo com o usuário autenticado. 7.41. Nas configurações das políticas, deve-se existir						

	pelo menos as opções de: Liberar categoria/URL, Bloquear e Alarmar o usuário quando feito acesso a uma categoria não desejada pelo administrador. 7.42. Forçar filtragem diretamente nas imagens apresentadas pelos buscadores, ajudando na redução dos riscos de exposição de conteúdo inapropriado nas imagens. 7.43. Permitir criar cotas de navegação com os seguintes requisitos: 7.43.1. Tipo do ciclo, especificando se o limite será por duração de acesso à internet ou se será especificado uma data limite para o acesso. 8. Controle e Segurança de Aplicações 8.1. Reconhecer pelo menos 2.700 aplicações diferentes, classificadas por nível de risco, características e tecnologia, incluindo, mas não limitado a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, serviços de rede, VoIP, streaming de mídia, proxy e tunelamento, mensageiros instantâneos, compartilhamento de arquivos, web e-mail e update de softwares. 8.2. Reconhecer pelo menos as seguintes aplicações: 4Shared File Transfer, Active Directory/SMB, Citrix ICA, DHCP Protocol, Dropbox Download, Easy Proxy, Facebook Graph API, Firefox Update, Freegate Proxy, FreeVPN Proxy, Gmail Video, Chat Streaming, Gmail WebChat, Gmail WebMail, Gmail-Way2SMS WebMail, Gtalk Messenger, Gtalk Messenger File Transfer, Gtalk-Way2SMS, HTTP Tunnel Proxy, HTTPort Proxy, LogMeIn Remote Access, NTP, Oracle database, RAR File Download, Redtube Streaming, RPC over HTTP Proxy, Skydrive, Skype, Skype Services, skyZIP, SNMP Trap, TeamViewer Conferencing e File Transfer, TOR Proxy, Torrent Clients P2P, Ultrasurf Proxy, UltraVPN, VNC Remote Access, VNC Web Remote Access, WhatsApp, WhatsApp File Transfer e WhatsApp Web. 8.3. Controlar aplicações baseadas em categorias, característica (Ex: Banda e produtividade consumida), tecnologia(Ex:P2P) e risco. 8.4. Permitir criar regras de controle por usuário e hosts. 8.5. Permitir realizar traffic shaping por aplicação e grupo de aplicações. 8.6. Possibilitar que as regras criadas baseadas em aplicação permitam: 8.6.1. Bloquear o trafego para as aplicações 8.6.2. Liberar o trafego para as aplicações 8.6.3. Criar categorização das aplicações por risco: 8.6.3.1. Risco muito baixo 8.6.3.2. Risco baixo 8.6.3.3. Risco médio 8.6.3.4. Risco alto 8.6.3.5. Risco muito alto 8.6.4. Permitir visualizar as aplicações por suas características, por exemplo: aplicações que utilizam banda excessiva, consideradas vulneráveis, que geram perda de produtividade, entre outras. 8.6.5. Permitir selecionar pela tecnologia, por exemplo: p2p, client server, protocolos de redes, entre outros. 8.7. Permitir granularidade na hora da criação da regra baseada em aplicação, como por exemplo: Permitir bloquear anexo dentro de um post do Facebook, bloquear o like do Facebook, permitir acesso ao Youtube mas bloquear o upload de vídeos, e etc. 8.7.1. Deve realizar o escaneamento e controle de micro app incluindo, mas não limitado a: Facebook (Applications, Chat, Commenting, Events, Games, Like Plugin, Message, Pics Download e Upload, Plugin, Post Attachment, Posting, Questions, Status Update, Video Chat, Video Playback, Video Upload, Website), Freegate Proxy, Gmail (Android Application,						

	Attachment), Google Drive (Base, File Download, File Upload), Google Earth Application, Google Plus, LinkedIN (Company Search, Compose Webmail, Job Search, Mail Inbox, Status Update), SkyDrive File Upload e Download, Twitter (Message, Status Update, Upload, Website), Yahoo (WebMail, WebMail File Attach) e Youtube (Video Search, Video Streaming, Upload, Website). 8.7.2.O escaneamento de micro app deverá ser habilitado via console gráfica (GUI) e via comando de linha (CLI). 8.8. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante. 8.9. Permitir agendar um horário e data especifico para a aplicação das regras de controle de aplicativos, podendo ser executadas apenas uma vez como também de forma recursiva. 8.10. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações por assinaturas e camada 7, utilizando portas padrões (80 e 443), portas não padrões, port hopping e túnel através de tráfego SSL encriptado. 8.11. Atualizar a base de assinaturas de aplicações automaticamente. 8.12. Reconhecer aplicações em IPv6. 8.13. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários. 8.14. Deve permitir o uso individual de diferentes aplicativos para usuários que pertencem ao mesmo grupo de usuários, sem que seja necessária a mudança de grupo ou a criação de um novo grupo. Os demais usuários deste mesmo grupo que não possuírem acesso a estes aplicativos devem ter a utilização bloqueada. 9. Suportar no mínimo 82.000 (oitenta e dois mil) novas conexões por segundo; 10. Suportar no mínimo 8.200.000 (oito milhões e duzentos mil) conexões simultâneas; 11. Possuir no mínimo 7.000 Mbps (sete mil) de rendimento (throughput) do Firewall para pacotes UDP; 1.12.4. No mínimo 1.700 (um mil e setecentos) Mbps de rendimento (throughput) do IPS; 12. Possuir no mínimo 950 Mbps de throughput de VPN AES. 13. A solução proposta deve corresponder aos seguintes critérios de throughput em mundo real: 13.1. Entende-se como mundo real, testes realizados pelo fabricante que tenham sido feitos com o appliance utilizando até 50% da capacidade de processamento, utilizando um mix de protocolos usados no mundo corporativo. 13.2. Possuir no mínimo 232 Mbps de rendimento (throughput) de IPS mundo real. 13.3. Possuir no mínimo 75 Mbps de rendimento (throughput) de funcionalidades next generation em mundo real; 13.4. Possuir no mínimo 240 de rendimento (throughput) de VPN AES mundo real. 14. Entende-se como mundo real testes realizados utilizando ambientes e protocolos usados no mundo corporativo. 15. A solução proposta deve possuir licenças baseado nos recursos de hardware. 16. A solução proposta deve suportar a configuração de políticas baseadas em usuários para segurança e gerenciamento de internet.						

	17. A solução proposta deve fornecer os relatórios diretamente no Appliance, baseados em usuário, não só baseado em endereço IP. 18. A solução proposta deve possuir no mínimo 64 GB de espaço em disco SSD para o armazenamento de eventos e relatórios. 19. Possuir portas USB 2.0 e 3.0. 20. Possuir porta VGA. 21. Possuir ao menos uma porta COM (RJ45). 22. Número irrestrito de usuários/IP conectados. Serviços e apoio na implementação Avançado 23. Através de serviços adicionais, a contratante mediante o contrato deste serviço adicional, poderá ter as seguintes opções durante a implementação: 23.1. Configuração de 1 appliance em modo standalone, HA ou cluster. 23.2. Ativação da licença. 23.3. Configuração inicial (hostname, horário, interface WAN e LAN). 23.4. Atualização da versão do firmware. 23.5. Repasse de conhecimentos para: 23.6. Configuração de interfaces adicionais e VLAN. 23.7. Roteamento estático e dinâmico. 23.8. Configuração de DNS e DHCP. 23.9. Configuração de NAT. 23.10. Integração de autenticação via Active Directory, RADIUS, LDAP ou TACACS+. 23.11. Configuração de regra de firewall, IPS, Application Control e QoS. 23.12. Configuração de Web Filter. 23.13. Configuração de Email Filter. 23.14. Configuração de Web Server Protection (WAF). 23.15. Configuração de Wireless Protection (com Access Point da Sophos). 23.16. Configuração do Sophos RED. 23.17. Configuração de VPN. 23.18. Configuração de backup. 23.19. Troubleshooting de erros **Apresentar catálogo técnico da solução, sob pena de desclassificação.**						
03	**ANTIVÍRUS** 1. Aquisição de Licenças e Atualização do Antivírus para o período de 36 meses, 50 (cinquenta) máquinas. 1.1. REQUISITOS MÍNIMOS PARA A SOLUÇÃO DE ANTIVÍRUS 1.2. Possuir uma única console de gerenciamento para gestão e configurações do antivírus, antispyware, firewall, detecção de intrusão, controle de dispositivos, controle de aplicações e criptografia de discos. 1.3. A solução deverá ter a capacidade de remoção do atual antivírus instalado e ser capaz de instalar de forma remota o agente do antivírus pela console de gerenciamento, e caso não tenha a capacidade de realização a remoção completa, a contratada deverá remover a atual solução utilizando scripts, softwares de terceiros, ou mesmo de forma manual; 1.4. O produto deverá possuir no mínimo os seguintes módulos e funcionalidades: 1.5. Console de gerenciamento fornecendo funcionalidades de gestão e configurações de políticas; 1.6. Módulos para estações físicas, notebooks e servidores; 1.7. Módulo para ambientes virtualizados, sendo criado especialmente para ambientes virtuais; 1.8. Módulo para dispositivos móveis no mínimo para tablets e smartphones com sistema operacional iOS e Android; 1.9. Utilizar o conceito de heurística para combate e ações contra possíveis malwares; 1.10. Oferecer tecnologia onde a solução explore	Unid.	01				

	vulnerabilidades de softwares instalados no intuito de reduzir o risco de infecções (anti-exploit); 1.11. Oferecer tecnologia nativa no intuito de eliminar ameaças que sequestram dados, do tipo ransomware; 1.12. Oferecer inventário de softwares; 1.13. Oferecer tecnologia onde a solução teste arquivos potencialmente perigosos em ambiente isolado antes da execução do mesmo no ambiente de produção; 1.14. Oferecer proteção por base de assinaturas (vacinas). 2. CONSOLE DE GERENCIAMENTO 2.1. Instalação e configuração 2.2. Permitir instalação de console local (on-premise) com banco de dados local ou instalação em nuvem (cloud) com banco de dados também em nuvem; 2.3. Para a opção de console local de ser fornecido como um appliance virtual ou executável para instalação em servidores Windows. Deverá suportar no mínimo as seguintes plataformas de virtualização: 2.4. VMWare vSphere; 2.5. Citrix XenServer; XenDesktop, VDI-in-a-Box; 2.6. Microsoft Hyper-V; 2.7. Red hat Enterprise Virtualization; 2.8. Kernel-based Virtual Machine ou KVM; 2.9. Oracle VM; 2.10. Deverá ser fornecido com base de dados embutida e proprietária ou com possibilidade de utilização de banco de dados externo SQL ou Oracle; 2.11. Para instalação da console em nuvem (cloud), a nuvem deve ser privada e do mesmo fabricante; 2.12. Permitir instalação remota via console WEB de gerenciamento para ambientes virtuais VMWare ou Citrix; 2.13. O mecanismo de varredura deverá estar disponível para download separadamente; 2.14. A solução deverá permitir a inclusão de um modulo de balanceamento para casos em que vários servidores tenham a mesma função (para alta disponibilidade, recuperação de desastres, performance, dentre outras necessidades); 2.15. Deve ser totalmente em português. 2.16. Funcionalidades Gerais 2.17. Licenciamento flexível; 2.18. A console de gerenciamento deve incluir informações detalhadas sobre as estações e servidores com no mínimo as seguintes informações: 2.18.1. Nome; 2.18.2. IP; 2.18.3. Sistema Operacional; 2.18.4. Política Aplicada; 2.19. A console de gerenciamento deverá incluir sessão de log com as seguintes informações: 2.19.1. Login; 2.19.2. Edição; 2.19.3. Criação; 2.19.4. Log-out; 2.20. Arquitetura simples de atualização, com um simples clique deve ser possível atualizar todas as funções e serviços da solução; 2.21. Permitir que o administrador escolha qual o pacote será atualizado; 2.22. As notificações devem ser destacadas como item não lido e notificar o administrador por e-mail; 2.23. No mínimo enviar notificações para as seguintes ocorrências: 2.24. Problemas com licenças; 2.25. Alertas de surto de vírus; 2.26. Máquinas desatualizadas; 2.27. Eventos de antimalware. 2.28. Deverá prover o acesso via HTTPS; 2.29. Deverá permitir a importação de certificados						

	digitais; 2.30. O gerenciamento e a comunicação com dispositivos móveis deve ser feito de forma segura utilizando certificados digitais. 3. MONITORAMENTO 3.1. Baseado em “portlets” configuráveis com no mínimo as seguintes especificações: 3.1.1. Nome; 3.1.2 Tipo de relatório; 3.1.3. Alvo do relatório; 3.2 Deverá disponibilizar “portlets” para gerência e monitoramento de qualquer tipo de endpoint, máquinas físicas, virtuais e dispositivos móveis. 3.3. Inventário da Rede 3.4. Possuir no mínimo as integrações abaixo: 3.4.1. Múltiplos domínios do Active Directory; 3.4.2. Múltiplos VMWare vCenters; 3.4.3. Múltiplos Citrix Xen Servers; 3.4.4. Possuir a possibilidade de definição de sincronização com o Active Directory em horas; 3.5. Descoberta de rede para máquinas em grupo de trabalho; 3.6. Possuir busca em tempo real pelo menos com os seguintes filtros: 3.7. Nome; 3.8. Sistema Operacional; 3.9. Endereço IP; 3.10. Possibilitar a instalação remota e desinstalação remota do antivírus; 3.11. Possibilitar a configuração de pacotes de instalação do produto de antivírus; 3.12. Possuir tarefas remotas e configuráveis de scan; 3.13. Possuir tarefa de reinicialização remota de estação ou servidor; 3.14. Assinar políticas para no mínimo os níveis: 3.14.1. Computador; 3.14.2 Máquina Virtual; 3.14.3 Grupo de Endpoints; 3.14.4. Usuário do AD; 3.14.5. Grupo do AD. 3.15. Possuir a propriedade detalhada de objetos gerenciados para: 3.15.1. Nome; 3.15.2. IP; 3.15.3. Sistema Operacional; 3.15.4. Grupo; 3.15.5. Política Assinada; 3.15.6. Ultimo status de malware. 3.15.7. Modelo único para todos os equipamentos, sejam físicos ou virtuais; 3.16. Cada serviço de segurança deve ter seu modelo configurável de política com opções específicas de ativar/desativar; 3.17. Através da console de gerenciamento o administrador poderá ser capaz de enviar uma política única para configurar o antivírus; 3.18. Deverá configurar as funcionalidades como escaneamento do antivírus, firewall de duas vias de detecção de intrusão, controle de acesso à rede, controle de aplicação, controle de acesso web, criptografia (Windows, Mac e Android), localização de dispositivo (Mobile), autenticação e ações para serem aplicadas em caso de vírus e dispositivos em não conformidade. 3.19. Relatórios - Deverá apresentar as seguintes funcionalidades: 3.20. Relatório para cada serviço de segurança; 3.21. Facilidade de usar e visualização simplificada; 3.22. Agendamento, com opção de envio por e-mail para qualquer destinatário conforme escolha do administrador;						

	3.23. Filtros de agendamento de relatórios; 3.24. Arquivo com todas as instâncias de relatório agendados; 3.25. Exportar o relatório nos formatos .pdf e/ou .csv; 3.26. Oferecer possibilidade de criar relatórios de maneira dinâmica no dashboard da console de gerenciamento. 3.27. Administração de Usuários 3.28. Deverá apresentas no mínimo as seguintes funcionalidades: 3.29. Administração baseada em regras; 3.30. Disponibilizar tipos de usuários pré-definidos como no mínimo: 3.31. Administrador – Gerente dos componentes da solução; 3.32. Administrador de rede - Gerente dos serviços de segurança; 3.33. Relatório – Monitora e cria relatórios; 3.34. Deverá ser possível customizar um tipo de usuário: 3.35. Deverá permitir a integração de usuários com o Active Directory para autenticação da console de gerenciamento; 3.36. Registrar as ações do usuário no console de gerenciamento; 3.37. Detalhar cada ação do usuário; 3.38. Permitir busca complexa baseada em ações do usuário, intervalos de tempo. 3.39. Segurança Para Estações e Servidores 3.40. Proteção para ambientes físicos 3.41. Deverá proteger em tempo real e agendado as máquinas físicas em qualquer plataforma de sistema operacional, seja Windows, Linux ou Mac, tanto no console local (on-premises) como na console em nuvem (cloud); 3.42. Deverá suportar no mínimo os seguintes sistemas operacionais para estação de trabalho: • Windows 10 64Bits; • Windows 8.1 64Bits; • Windows 8 64Bits; • Windows 7 64Bits; 3.43. Deverá suportar no mínimo os seguintes sistemas operacionais para servidores: • Windows Server 2012R2; • Windows Server 2012; • Windows Server 2008 R2; Windows Server 2008 apenas os módulos de antivírus e Active Virus Control; 3.44. Deverá suportar no mínimo os seguintes sistemas operacionais para distribuição Linux: • Ubuntu 14.04 LTS ou superior • Red Hat Enterprise Linux / CentOS 6 ou superior • SUSE Linux Enterprise Server 11 SP4 ou superior • OpenSUSE Leap 42.x • Fedora 25 ou superior • Debian 8.0 ou superior • Oracle Linux 6.3 ou superior • Amazon Linux AMI 2016.09 ou superior • Proteção para ambientes virtuais 3.45. Para plataforma de virtualização com VMWare, deverá: • Ter a disponibilidade de ser integrado e oferecer a escaneamento sem instalar o agente nas máquinas virtuais; • A console de gerenciamento central da						

	solução deverá ter a possibilidade de integrar com múltiplos vCenters da VMWare; • Deverá proteger em tempo real e agendado as máquinas virtuais em qualquer plataforma de sistema operacional, seja Windows, Linux ou Mac, tanto no console local (on-premises) como na console em nuvem (cloud); 3.46.O produto deverá oferecer agente para virtualização dos seguintes produtos: • Citrix Xen Server; • Microsoft Hyper-V; • VMware ESXi; • Red Hat Virtualization; • Oracle KVM; • KVM. • Instalação e Configuração remota 3.47. Deverá permitir ao administrador customizar a instalação; 3.48. Deverá permitir a instalação customizada do antivírus com no mínimo: 3.49. Instalar o antivírus sem o controle de acesso a internet; (Windows Desktop) 3.50. Instalar o antivírus sem o módulo de firewall; (Windows Desktop) 3.51. A instalação deverá ser executada no mínimo das seguintes maneiras: 3.52. Executar o pacote de antivírus diretamente na estação de trabalho; 13.53. Instalar remotamente, distribuído via console de gerencia web; 3.54. Deverá ser possível ter um relatório com as estações instaladas e as faltantes da instalação; 3.55. Ter a capacidade de criar um único pacote independente ser for para 32 bits ou 64 bits; 3.56. Deverá permitir ao administrador criar grupos e subgrupos para mover as estações de trabalho; 3.57. O agente utilizado na sincronização deve ser incluído no cliente do antivírus e não ser necessário à distribuição em um agente separado. 3.58. Funções Gerais 3.59. Deverá ter métodos de detecção de vírus, spyware, rootkits e outros mecanismos de segurança; 3.60. Deverá permitir a configuração do scan do antivírus do cliente como: 3.60.1. Scan local; 3.60.2. Scan hibrido (local\remoto); 3.60.3. Scan remoto; 3.61. Deverá reportar o estado atual das máquinas virtuais no mínimo, protegida/desprotegida; 3.62. Deverá fazer scan em tempo real e automático; 3.63. Deverá ser configurável para não escanear arquivos conforme necessidade do administrador, ou seja, por tamanho ou por tipo de extensão; 3.64. Deverá possuir escaneamento baseado em análise heurística; 3.65. Deverá permitir a escolha e configuração de pastas a serem scaneadas; 3.66. Para melhor proteção, o antivírus deverá ter no mínimo 3 tipos de detecção: 3.67. Baseada em assinaturas; 3.68. Baseada em heurística; 3.69. Baseada em monitoramento contínuo de processos; 3.70. Deverá ter a capacidade de escaneamento nos protocolos HTTP e SSL nas estações de trabalho; 3.71. O cliente do antivírus deverá ter o módulo de Antiphishing que deverá ter a opção de verificar links pesquisados com os sites de pesquisas Search Advisor nas estações de trabalho;						

	3.72. Deverá possuir módulo de firewall que de acordo com o administrador poderá ou não ser instalado/desinstalado nas estações de trabalho; 3.73. No módulo de firewall deverá ser possível configurar o modo invisível tanto em nível de rede local ou Internet nas estações de trabalho; 3.74. Deverá ter os seguintes requisitos mínimos de sistema: • Plataformas de Virtualização • VMware vSphere ESX 5.0 ou superior; • VMware vCenter Server 4.1 ou superior; • Citrix XenDesktop 5.0 ou superior; • Xen Server 5.5 ou superior; • Citrix VDI-in-a-Box 5; • Microsoft Hyper-V Server 2008 R2, 2012 • Oracle VM 3.0; • Red Hat Enterprise Virtualization 3.0. • Sistemas Operacionais para Desktops • Windows 10 64Bits; • Windows 8.1 64Bits; • Windows 8 64Bits; • Windows 7 64Bits; • Sistemas Operacionais para Servidores • Windows Server 2012R2; • Windows Server 2012; • Windows Server 2008 R2; • Windows Server 2008 apenas os módulos de antivírus e Active Virus Control; • Linux Red Hat Enterprise; • CentOS 5.6 ou superior; • Ubuntu 10.04 LTS ou superior; • SUSE Linux Enterprise Server 11 ou superior; • OpenSUSE 11 ou superior; • Fedora 15 ou superior; Debian 5.0 ou superior. • Quarentena • Deverá permitir restauração remota, com configuração de localidade e deleção; • Criação e exclusão para arquivos restaurados; • Deverá permitir o envio automático de arquivos da quarentena para o laboratório de vírus; • Deverá fazer a remoção automática de arquivos antigos, pré-definidos pelo administrador; • Deverá permitir a movimentação do arquivo da quarentena para seu local original ou outro destino que o administrador definir; • Deverá de forma automática criar exclusão para arquivos restaurados da quarentena; Deverá permitir escanear a quarentena após a atualização de assinaturas. • Controle de Usuário • Deverá ter módulo de controle de usuário integrando com as seguintes características: • Bloqueio de acesso à internet; Bloqueio de acesso a aplicações definidas pelo administrador. • Controle do Dispositivo • Deverá ser possível a instalação do módulo de controle de dispositivos através da console de gerenciamento;						

	3.75. Através do módulo de controle de dispositivo deverá ser possível controlar: • Bluetooth; • CDROM/DVDROM; • IEEE 1284.4; • IEEE 1394; • Windows Portable; • Adaptadores de Rede; • Adaptadores de rede Wireless; • Discos Externos; 3.76. Deverá escanear em tempo real qualquer informação localizada em mídias de armazenamento como: • CD/DVD; • Discos Externos; • Pen-Drivers; 3.77. Deverá permitir regras de definição de bloqueio/desbloqueio; 3.78. Deverá permitir regras de exclusão. 3.79. Criptografia 3.80. Deverá oferecer Possibilidade de criptografia de disco através da mesma console de gerenciamento do antivírus, seja em nuvem (cloud) ou local (on-premise); 3.81. Deverá utilizar, quando necessário, serviços de criptografia com agentes nativos da estação de trabalho seja baseada em Windows ou Mac; 3.82. Deverá solicitar autenticação quando iniciado o sistema operacional do equipamento; 3.83. Deverá ser compatível com Mac OS X Moutain, Mavericks, Yosemite, Sierra. 3.84. Atualização 3.85. Após a atualização o administrador deverá ter a capacidade de configurar uma reinicialização; 3.86. Possibilidade de utilizar um servidor local para efetuar as atualizações das estações de trabalho; 3.84. Permitir atualizações de assinatura de hora em hora; 3.85. Permitir motor de varredura local, no servidor de rede ou em nuvem afim de aumentar o desempenho da estação de trabalho quando a mesma estiver sendo escaneada. 3.86. Segurança Para Dispositivos Móveis 3.87. Requisitos mínimos do Sistema Operacional 3.88. Android 2.2 ou superior 3.89. Recursos 3.90. Permitir atribuir dispositivo com usuário do Active Directory; 3.91. A ativação do dispositivo da console de gerenciamento deverá ser através de um QR code; 3.92. Os pacotes de instalação devem estar disponíveis nas lojas dos Sistemas Operacionais; 3.93. Deverá permitir no mínimo as seguintes ações: 3.94. Impor bloqueio de tela e autenticação; 3.95. Desbloquear o dispositivo; 3.96. Restaurar as configurações de fábrica; 3.97. Localizar o Dispositivo; 3.98. Análise de dispositivos para o Sistema Operacional Android; 3.99. Criptografia de memória do dispositivo para o Sistema Operacional Android. 3.100. Configurações de Segurança 3.101. Caso o dispositivo não esteja em conformidade com as políticas estabelecidas deverá ser possível as ações abaixo: • Ignorar; • Bloquear acesso; • Bloquear o dispositivo; • Restaurar as configurações de fábrica;						

	• Remover o dispositivo da console de gerenciamento; 3.102. Deverá permitir o uso de senha. A senha pode ser configurada conforme necessidade do administrador com no mínimo os seguintes recursos: • Senha simples ou complexa; • Números e caracteres; • Comprimento mínimo; • Caracteres especiais mínimos; • Período de expiração da senha; • Definir restrição de reutilização de senha; • Definir o número de tentativas de entradas de senha incorretas; • Período de bloqueio do dispositivo. 3.103. Segurança De e-Mails • Fornecer proteção de antispam para ambiente com instalação local (on-premise) do MS Exchange; • Oferecer análise comportamental e proteção para zero-day; • Oferecer proteção contra vírus e tentativas de phishing. • Criptografia • Deverá oferecer: • Possibilidade de criptografia de disco através da console de gerenciamento seja em nuvem ou on-premise com módulo de Criptografia presente na mesma Console do Antivírus. • utilizar quando necessários serviços de criptografia através agentes nativos da estação de trabalho baseada em Windows (BitLocker) ou Mac (FileVault); • Deverá solicitar autenticação quando iniciado o sistema operacional do equipamento; • Deverá ser compatível com Mac OS X Moutain, Mavericks, Yosemite, Sierra.						
VALOR TOTAL DA PROPOSTA: R$							

***Observações Gerais*:**

- Deverá ser apresentado no envelope junto à proposta comercial, marca, modelo, catálogo, folder ou folheto, de todos os equipamentos e soluções propostas onde conste de maneira clara as características dos equipamentos cotados. NÃO SERÃO ACEITOS PROSPECTOS MONTADOS.
- Os proponentes deverão fornecer todos os dados relativos aos materiais e equipamentos ofertados, em especial os citados nesta especificação;
- Nos preços deverão estar contidos todos os encargos que incidam sobre os materiais e equipamentos até a efetiva entrega;
- Entregar os materiais e equipamentos de acordo com sua proposta, conforme especificações do Edital e seus anexos e que satisfaça o que foi descrito nos itens.
- Arcar com todas as despesas, diretas ou indiretas, decorrentes do cumprimento das obrigações assumidas.
- Emitir Nota Fiscal Eletrônica com o quantitativo e descritivo fornecido, de acordo com as especificações exigidas.

NOTA: As empresas que cotarem os software/equipamentos acima descritos deverão garantir a sua qualidade.

- **LOCAL DE ENTREGA DOS MATERIAIS E EQUIPAMENTOS:** Na sede do SAAE, situado à Rua Rio Branco, nº. 99, Bairro Centro, no município de Itabirito – MG, **no horário de 08:00 horas às 11:00 horas e das 13:00 horas às 15:30 horas, em dias úteis**, onde a Comissão do Serviço Autônomo de Saneamento Básico, designada para o recebimento, procederá a conferência e recebimento dos materiais.

- **PRAZO DE ENTREGA:** Em uma única parcela, com no máximo 45 (quarenta e cinco) dias corridos, após o recebimento da Nota de Empenho.

- **DO RECEBIMENTO:**

I. Os software/equipamentos da presente licitação serão recebidos pelo Serviço Autônomo de Saneamento Básico, através de sua Comissão de recebimento, em conformidade com o § 8º, do Art. 15, da lei nº 8.666/93 com suas posteriores alterações, bem como parceria com o setor de Informática da CONTRATANTE.

II. A Comissão rejeitará, no todo ou em parte, os itens em desacordo com os termos do Edital e seus anexos.

III. Todos os itens de que trata esta licitação deverão obedecer as especificações constantes do Edital e seus Anexos.

IV. O seguro, frete, impostos e tributos que recaiam sobre os materiais e equipamentos, até sua entrega à Rua Rio Branco, nº 99, Centro, no município de Itabirito – MG, nas condições estabelecidas para entrega, correrão por conta exclusiva da CONTRATADA.

- **DAS OBRIGAÇÕES DA CONTRATADA**

A CONTRATADA, no cumprimento desse contrato, obriga-se a:

a) Cumprir todas as determinações, as ordens verbais ou escritas dos responsáveis pela CONTRATANTE, quando o serviço e/ou materiais não atenderem às normas técnicas e legais estabelecidas;

b) Manter atualizados todos os documentos exigidos na fase de habilitação;

c) Credenciar prepostos para representá-la permanentemente junto a CONTRATANTE, com a incumbência de resolver todos os assuntos relativos à execução do Contrato;

d) Entregar todos os materiais conforme descritos no item 4 deste documento;

e) Garantir a troca dos materiais não conformes e ou danificados por fabricação ou transporte;

f) Entregar todos os materiais descritos no item 4 deste documento de uma só vez obedecendo os prazos especificados neste termo.

- **DAS OBRIGAÇÕES DA CONTRATANTE:**

A CONTRATANTE, no cumprimento deste contrato, obriga-se a:

a) Prestar todas as informações e dados relacionados ao objeto ora contratado sempre que se fizer necessário ao cumprimento deste Contrato;

b) Colocar à disposição funcionário(s) especializado(s) para orientações e fiscalização do Contrato;

c) Efetuar o pagamento devido no prazo determinado.

- **DA DOTAÇÃO ORÇAMENTÁRIA:**

A dotação necessária à realização da despesa decorrente do objeto desta licitação consta do Orçamento da Autarquia, a saber:

PROJ. CONSTR. AMPL. OBRAS INFRAEST. GESTÃO DA ADM GERAL SAAE.
17 512 1711 3.030 44.90.52.00

OP. MANUT. AÇÕES DE GESTÃO ADM GERAL SAAE.
17 512 1711 4.030 33.90.40.00

- **DA FISCALIZAÇÃO E ACOMPANHAMENTO:** A fiscalização e acompanhamento do objeto desta licitação se darão através do setor de Informática da CONTRATANTE, observados os artigos 73 a 76 da Lei Federal nº 8.666/93.

- **FORMA DE PAGAMENTO:** Em até **10 (dez) dias corridos**, após o aceite da Nota Fiscal Eletrônica. **Deverá a Nota fiscal Eletrônica estar em conformidade com a Nota de Empenho**, acompanhada de arquivos digitais contendo a cópia da ***CND*** acompanhada de cópia da CND (Certidão Negativa de Débitos Relativos aos Tributos Federais e a dívida ativa da União) e do CRF (Certificado de Regularidade do FGTS). Boleto bancário e/ou dados bancários da CONTRATADA (nº da Agência

bancária e nº da conta da CONTRATADA), e todas as incidências fiscais que sobre ela possam recair, condições estas indispensáveis para efetuar-se o pagamento.

- **VALIDADE DA PROPOSTA:** No mínimo 60 (sessenta) dias, contados da data-limite para a entrega dos envelopes.

  Declaro que no preço proposto encontram-se incluídos todos os tributos, encargos sociais, frete até o destino e quaisquer outros ônus que porventura possam recair sobre o fornecimento do objeto da presente licitação.

DATA: _____ **ASSINATURA:** _____

IDENTIFICAÇÃO DA EMPRESA E DO REPRESENTANTE LEGAL

ANEXO II – (MODELO)

(PAPEL TIMBRADO DA LICITANTE)

CARTA DE CREDENCIAMENTO

(Local e data)

Ao

Serviço Autônomo de Saneamento Básico

Ref.: Processo Licitatório nº. 083/2020, Pregão Presencial nº. 057/2020.

Por este presente instrumento, fica credenciado o Sr. (a) _____, inscrito no CPF/MF sob o nº. _____, identidade nº. _____, expedida por _____, junto ao Serviço Autônomo de Saneamento Básico de Itabirito - MG, para representar a empresa (**nome da empresa**) na licitação acima referida, a quem outorgam poderes para efetuar lances, rubricar propostas das demais licitantes, assinar atas e documentos, interpor recursos e impugnações, receber notificação, tomar ciência de decisões, desistir da interposição de recursos, acordar, transigir, enfim, praticar todo e qualquer ato necessário à perfeita representação ativa da outorgante no processo licitatório em referência.

Assinatura: _____

RECONHECER FIRMA

Obs.: Identificação, assinatura do representante legal e carimbo padronizado da empresa.

(Que deverá estar do lado de fora dos envelopes)

ANEXO III – (MODELO)

(PAPEL TIMBRADO DA LICITANTE)

DECLARAÇÃO DE HABILITAÇÃO

(Local e data)

Ao

Serviço Autônomo de Saneamento Básico

Ref.: Processo Licitatório nº. 083/2020, Pregão Presencial nº. 057/2020.

Pela presente, declaro (mos) que, nos termos do Art. 4°, VII da Lei nº. 10.520 / 2002, a empresa....., cumpre os requisitos de habilitação para o Pregão Presencial nº. **057/2020**, para contratação de empresa especializada em fornecimento de Hardware (Servidor de Dados, Switch e Storage) e Software, a serem utilizados na Sede Administrativa do Serviço Autônomo de Saneamento Básico de Itabirito – MG, conforme especificações do anexo I.

Por ser verdade, firmamos o presente.

_____

Representante legal

Assinatura: _____

Obs.: Identificação, assinatura do representante legal e carimbo padronizado da empresa.

(Que deverá estar do lado de fora dos envelopes)

ANEXO IV – (MODELO)

(PAPEL TIMBRADO DA LICITANTE)

DECLARAÇÃO DA EMPRESA

(Local e data)

Ao

Serviço Autônomo de Saneamento Básico

Ref.: Processo Licitatório nº. 083/2020, Pregão Presencial nº. 057/2020.

Pela presente, a (empresa.....), inscrito sob o CNPJ nº. ....., por intermédio de seu representante legal (o)s Sr(a) ....., portador(a) da carteira de identidade nº. ..... e do CPF nº. ....., DECLARA, para fins do disposto no inciso III e IV do art. 87 da Lei nº. 8.666, de 21 de junho de 1993, que não está suspensa e nem é impedida de licitar com órgão Público.

Por ser verdade, firmamos o presente.

_____

Representante legal

ANEXO V - (MODELO)

(PAPEL TIMBRADO DA LICITANTE)

DECLARAÇÃO DO EMPREGADOR

(Local e data)

Ao

Serviço Autônomo de Saneamento Básico

Ref.: Processo Licitatório nº. 083/2020, Pregão Presencial nº. 057/2020.

Pela presente, a (empresa.....), inscrito sob o CNPJ nº. ....., por intermédio de seu representante legal (o)s Sr(a) ....., portador(a) da carteira de identidade nº. ..... e do CPF nº. ....., DECLARA, para fins do disposto no inciso V do art. 27 da Lei nº. 8.666, de 21 de junho de 1993, acrescido pela Lei nº. 9.854, de 27 de outubro de 1.999, que não emprega menor de dezoito anos em trabalho noturno, perigoso ou insalubre e não emprega menor de dezesseis anos.

Ressalva: emprega menor, a partir de quatorze anos na condição de aprendiz ( ).

_____

Representante legal

(obs: em caso afirmativo assinar a ressalva acima)

ANEXO VI – (MODELO)

(PAPEL TIMBRADO DA LICITANTE)

DECLARAÇÃO PARA MICRO EMPRESAS E EMPRESAS DE PEQUENO PORTE

(Local e data)

À

Comissão Especial de Licitação

Ref.: Processo Licitatório nº. 083/2020, Pregão Presencial nº. 057/2020.

Pela presente, a (empresa_____), inscrito no CNPJ sob o n.° _____, por intermédio de seu representante legal (o)s Sr.(a)_____, portador(a) da carteira de identidade n°. _____ e do CPF n°. _____, DECLARA, sob as penas da Lei que é Micro Empresa ou Empresa de Pequeno Porte e que se encontra sob o regime da Lei complementar nº. 123/2006 fazendo jus aos benefícios contidos na referida Lei.

Por ser verdade, firmamos o presente.

_____

Representante legal

(Que deverá estar do lado de fora dos envelopes)

ANEXO VII – (MODELO)

(PAPEL TIMBRADO DA LICITANTE)

DECLARAÇÃO MICRO EMPRESA OU EMPRESA DE PEQUENO PORTE, QUANTO À RESTRIÇÃO EM DOCUMENTAÇÃO DE REGULARIDADE FISCAL.

(Local e data)

Ao

Pregoeiro(a) e sua Equipe de Apoio

Ref.: Processo Licitatório nº. 083/2020, Pregão Presencial nº. 057/2020.

Pela presente, a (empresa_____), inscrito no CNPJ sob o n.°_____, por intermédio de seu representante legal (o)s Sr.(a)_____, portador(a) da carteira de identidade n°. _____ e do CPF n°. _____, DECLARA, sob as penas da Lei, possuir restrição nos documentos de comprovação da regularidade fiscal, conforme faculdade prevista na Lei Complementar Federal nº. 123/2006 de 14 de dezembro de 2006 e se compromete a adotar todas as medidas necessárias, em razão do prazo concedido para este fim, para tentar promover sua regularização fiscal, caso venha a formular o lance vencedor, sob pena de aplicação do art. 6° do Decreto Municipal n°. 7191 de 28 de março de 2005, cumprindo plenamente os demais requisitos de habilitação para o **Pregão Presencial nº. 057/2020**.

Por ser verdade, firmamos o presente.

_____

Representante legal

ANEXO VIII – (MODELO)

DECLARAÇÃO DE ELABORAÇÃO INDEPENDENTE DE PROPOSTA

EDITAL DE PREGÃO PRESENCIAL Nº. 057/2020

PROCESSO LICITATÓRIO Nº. 083/2020

MODALIDADE: PREGÃO PRESENCIAL

TIPO DE LICITAÇÃO: MENOR PREÇO POR ITEM

DATA: 10/09/2020

HORÁRIO: 09:00 horas

LOCAL: Sala de reuniões do Serviço Autônomo de Saneamento Básico de Itabirito

[**IDENTIFICAÇÃO COMPLETA DO REPRESENTANTE DA LICITANTE**], como representante devidamente constituído de [**IDENTIFICAÇÃO COMPLETA DA LICITANTE**] (doravante denominado [Licitante/Consórcio]), para fins do disposto no item 9.1, XI do Edital do **Pregão Presencial nº. 057/2020**, declara, sob as penas da lei, em especial o art. 299 do Código Penal Brasileiro, que:

(a) a proposta anexa foi elaborada de maneira independente [**PELA LICITANTE**], e que o conteúdo da proposta anexa não foi, no todo ou em parte, direta ou indiretamente, informado a, discutido com ou recebido de qualquer outro participante potencial ou de fato do **Pregão Presencial nº. 057/2020, Processo Licitatório nº. 083/2020**, por qualquer meio ou por qualquer pessoa;

(b) a intenção de apresentar a proposta anexa não foi informada a, discutido com ou recebido de qualquer outro participante potencial ou de fato do **Pregão Presencial nº. 057/2020, Processo Licitatório nº. 083/2020**, por qualquer meio ou por qualquer pessoa;

(c) que não tentou, por qualquer meio ou por qualquer pessoa, influir na decisão de qualquer outro participante potencial ou de fato do **Pregão Presencial nº. 057/2020, Processo Licitatório nº. 083/2020**, quanto a participar ou não da referida licitação;

(d) que o conteúdo da proposta anexa não será, no todo ou em parte, direta ou indiretamente, comunicado a ou discutido com qualquer outro participante potencial ou de fato do **Pregão Presencial nº. 057/2020, Processo Licitatório nº. 083/2020**, antes da adjudicação do objeto da referida licitação;

(e) que o conteúdo da proposta anexa não foi, no todo ou em parte, direta ou indiretamente, informado a, discutido com ou recebido de qualquer integrante de outros licitantes antes da abertura oficial das propostas; e

(f) que está plenamente ciente do teor e da extensão desta declaração e que detém plenos poderes e informações para firmá-la.

_____, em __ de _____ de 2020.

_____

([REPRESENTANTE LEGAL DO LICITANTE NO ÂMBITO DA LICITAÇÃO, COM IDENTIFICAÇÃO COMPLETA]

ANEXO IX
TERMO DE REFERÊNCIA - TR

1. DO OBJETO

Contratação de empresa especializada em fornecimento de hardware (Servidor de Dados, Switch e Storage) e software, a serem utilizados na Sede Administrativa do SAAE de Itabirito-MG.

2. DA JUSTIFICATIVA

Justifica-se a aquisição dos equipamentos e sistemas devido ao fato do setor de Tecnologia da Informação do SAAE Itabirito entender que medidas de segurança devem ser tomadas para assegurar a integridade dos dados da Autarquia, além da atualização de hardware e software.

Neste ano de 2020 o SAAE Itabirito sofreu em seu sistema de dados três ataques por ocorrência de vírus que ocasionaram uma perda significativa da massa de dados dos setores: Contábil, Comercial, Comunicação, RH, Planejamento e Frota, inclusive perda de quatro das seis máquinas virtuais existentes, além de prejuízos financeiros. Estes incidentes acarretaram grande esforço e tempo (aproximadamente 120 (cento e vinte) horas) da equipe de TI para reconfigurar todas as máquinas virtuais e reestruturar parte da massa de dados corrompida, uma vez que o sistema de backup atual não comporta 100% da demanda e está ultrapassado, devido à falta de investimentos em exercícios anteriores.

Pontos a serem reparados:

- Servidores ultrapassados, com aproximadamente 9 anos de utilização, sem garantia de fabricante, se aproximando de 95% de sua capacidade física total de armazenamento;
- Storage apresentando problemas de reconhecimento em alguns slots prejudicando sua capacidade de armazenamento;
- Switch ultrapassado com várias portas danificadas (queimadas);
- Sistema Operacional Windows Server 2008 sem suporte e atualizações;
- Ausência de sistema de armazenamento secundário e recuperação de arquivos, backup físico e em nuvem;
- Sistema de virtualização de servidores ultrapassado, sem suporte e sem licença;
- Ausência de antivírus eficaz;
- Ausência de Firewall eficaz.

3. DA FUNDAMENTAÇÃO LEGAL

A contratação objeto desse termo de referência tem amparo legal, integralmente, na Lei Federal nº 8.666/93, suas posteriores alterações e demais legislações pertinentes à contratação com órgãos públicos.

4. DAS ESPECIFICAÇÕES

4.1 Especificações dos materiais:

PROJ. CONSTR. AMPL. OBRAS INFRAEST. GESTÃO DA ADM GERAL SAAE. 17 512 1711 3.030 44.90.52.00							
ITEM	**ESPECIFICAÇÕES – LOTE 01**	UNID	QTDE	PREÇO UNIT.	PREÇO TOTAL	MARCA/ FABRI-CANTE/ MODELO	SE IMPORTADO PAÍS DE ORIGEM
01	**SERVIDOR TORRE** Servidor torre, possuindo no mínimo 02 processadores instalados, com velocidade mínima de 2,00 ghz – cache mínimo de 18,75mb, com mínimo de 08 cores, e não pode estar descontinuado pelo fabricante. Memória Ram com no mínimo 128gb **tipo** ddr4 – mínimo 2400mhz homologada pelo fabricante. Suporte de no mínimo 600gb de Ram Placa mãe deve ser do mesmo fabricante do equipamento, não sendo aceitas soluções OEM. Energia: Deve possuir redundância de fontes, com no mínimo 02 unidades de 485w cada, 80 PLUS,	Unid.	01				

	CERTIFICAÇÃO PLATINUM. Gravador de DVD interno. Chassi: deve ser torre, com no mínimo 4u. Deve possuir chaves para trava de chassi (não sendo aceitas adaptações). O servidor deve vir com o kit original do fabricante para instalação do mesmo em rack. Discos: deve possuir no mínimo: 2 unidades de discos sas 300gb sff 10k e 03 unidades de discos sata 2tb 7.2k sdd. Os discos devem ser originais do fabricante, homologados, não sendo aceitas adaptações ou utilização de discos não originais. Deve ter suporte a raid 5 e 10. O servidor deve ter suporte para no mínimo 24 discos. Rede: deve possuir no mínimo 02 portas de rede gigabit e no mínimo 01 porta rede 10gb sfp plus pci-e homologada do mesmo fabricante do servidor ou processador. O servidor deve vir com no mínimo 02 portas usb 3.0 Garantia: servidor deve possuir no mínimo 36 meses de garantia. **Apresentar catálogo técnico do equipamento, sob pena de desclassificação.**						
02	**STORAGE** Storage para armazenamento e backup Fiber Channel / ISCSI Dual LFF –Deve possuir no mínimo 02 controladoras redundantes Gabinete tipo Rack 2U, suporte a RAID: 0, 1, 3, 5 ,6, 10, Gerenciamento: 1p por controladora 1GbE Memória cache mínimo de 16GB (8GB por controladora), deve suportar um mínimo de 12 baias e discos LFF (3,5) Interface de disco, suportando pelo menos discos NL-SAS/SSD. Deve ter capacidade máxima de armazenamento de, no mínimo, até 1PB em discos SSD (Storage + 4 Expansões). Conectividade: Suporta conexões FC e ISCSI Conectividade: Sem Gbics Inclusos Fonte com no mínimo: 900W (sendo fonte redundante) (100-240 V bivolt automático) garantia mínima do fabricante: 03 anos (suporte 9 x 5). Devem estar inclusos, no mínimo 10 discos com capacidade 4tb, originais, do fabricante do equipamento, não sendo aceitos discos de outro fabricante, evitando assim perda ou não cumprimento da garantia por parte do fabricante. O sistema operacional e software de gestão do mesmo devem ser do mesmo fabricante. **Apresentar catálogo técnico do equipamento e discos, sob pena de desclassificação.**	Unid.	01				
03	STORAGE Especificações mínima do equipamento Processador: Processador com no mínimo 1.5GHz (núcleos) Possuir criptografia embarcada Memória: estática sem possibilidade de expansão, mínimo 1,5GB Deve possuir no mínimo 04 baias internas Deverá suportar no mínimo 48 TB Portas: Deve possuir no mínimo 02 Portas USB 3.1 Deve possuir no mínimo 01 Porta de Rede Gigabit Ethernet Deve possuir no mínimo 01 Rede 10 Gigabit Ethernet Deve ter resfriamento próprio condizente com o equipamento Deve possuir no mínimo 01 Fonte de Alimentação externa: 75W Deve ser bivolt automático Deve possuir no mínimo as certificações: FCC, CE, VCCI, BSMI, C-TICK Deve possuir software próprio e homologado Estar incluso 05 Discos (04 internos + 01 spare) com capacidade mínima de 10 TB cada.	Unid.	01				

	Deve possuir garantia mínima de 12 meses Os discos devem ser próprios para Storage, não sendo aceito discos para Desktop ou Sistema de Segurança e devem ser homologados pelo fabricante, novos e sem uso, devem ter garantia diretamente no fabricante, no Brasil e garantia de 60 meses. **Apresentar catálogo técnico do equipamento e discos, sob pena de desclassificação**						
04	**SWITCH** Especificações mínimas do equipamento Possuir no mínimo 10 portas 10GB SFP+ Suporte IPV4 e IPV6 Layer 2 Possuir Porta console Possuir Porta Usb Capacidade de Switching: mínimo de 188 Mpps Rating: mínimo de 165 Gbps Endereços Mac: mínimo de 30K Buffer de memória: mínimo: 1MB Possuir WEB GUI Arquitetura para RacK (1U) 06 (seis) cabos SFP+ de pelo menos 3 metros homologados pelo fabricante do switch. Garantia: Lifetime (garantia deve ser prestada no Brasil pelo fabricante ou empresa autorizada pelo mesmo) **Apresentar catálogo técnico do equipamento, sob pena de desclassificação.**	Unid.	01				
OP. MANUT. AÇÕES DE GESTÃO ADM GERAL SAAE. **17 512 1711 4.030 33.90.40.00**							
ITEM	**ESPECIFICAÇÕES – LOTE 02**	UNID	QTDE	PREÇO UNIT.	PREÇO TOTAL	MARCA/ FABRI-CANTE	SE IMPORTADO PAÍS DE ORIGEM
01	**FERRAMENTA DE BACKUP** A solução ofertada deverá, obrigatoriamente, atender as especificações mínimas previstas neste termo quanto às funcionalidades, integrações e compatibilidades com o ambiente virtualizado da CONTRATANTE para criação de backups e recuperação desses ambientes com o mínimo de indisponibilidade e reestruturação da parte física necessária, de forma que recupere, total e/ou granular, qualquer item assegurado por sua funcionalidade de backup e restauração. Deverá ser fornecido licenciamento do software, em caráter de aluguel de licenças, de propriedade e registrado para o SAAE DE ITABIRITO, na modalidade de capacidade por quantidade de instâncias protegidas para o ambiente físico e virtualizado, com suporte para backup e restore de dados. Cada licença de software licenciará UM TOTAL DE 12 VMS, do ambiente virtualizado (provedor/host das máquinas virtuais). Não poderão ser limitadas pelo volume de dados movimentados pelos mesmos. **CARACTERÍSTICAS ESPECÍFICAS** Deverá incluir funcionalidades de proteção (backup) e replicação integradas em uma única solução. Não deverá necessitar de instalação de agentes para poder realizar suas tarefas de proteção, recuperação e replicação das máquinas virtuais. Deverá garantir, no mínimo, a proteção de máquinas virtuais e seus dados, gerenciadas através das soluções de virtualização VMware. Deverá ter a capacidade de replicação de dados armazenados entre storages ou máquinas de configuração e de fabricantes diferentes. Deverá proteger o ambiente, sem interromper a atividade das máquinas virtuais e sem prejudicar sua performance, facilitando as tarefas de proteção	Unid.	01				

	(backup) e migrações em conjunto. Deverá ter a capacidade de testar a consistência do backup e replicação (S.O., aplicação, VM), emitindo relatório de auditoria para garantir a capacidade de recuperação. Deverá prover a deduplicação e compressão durante a operação de qualquer backup sem a necessidade de hardware de terceiros (appliance deduplicadora). Deverá possibilitar a cópia de uma máquina virtual completa ou discos virtuais específicos. Deverá ser fornecida com ferramenta de gestão de arquivos para os administradores de máquinas virtuais no console do operador. Deverá ter a capacidade de integração através de API's dos fabricantes de infraestrutura virtualizada para a proteção de dados. Deverá ter a capacidade de realizar proteção (backup) incremental e replicação diferencial, aproveitando a tecnologia de "rastreio de blocos modificados" (CBT – changed block tracking), reduzindo ao mínimo necessário, o tempo de backup e possibilitando proteção (backup e replicação). Deverá oferecer múltiplas estratégias e opções de transporte de dados para as áreas de proteção (backup), a saber: Diretamente através de Storage Area Network (SAN); Diretamente do storage, através do hypervisor I/O (Virtual Appliance); Mediante uso da rede local (LAN); Deverá manter um backup sintético, eliminando assim a necessidade de realizar backups completos (full) periódicos, incremental permanente, o que permitirá economizar tempo e espaço. Deverá possibilitar a inicialização de uma máquina virtual diretamente do arquivo de backup, inclusive sem necessidade de "hidratação" dos dados "deduplicados" e "comprimidos". Deverá permitir a recuperação de mais de uma máquina virtual e/ou ponto de restauração simultâneo, permitindo assim, ter múltiplos pontos de tempo de uma ou mais máquinas virtuais. Todo serviço de migração das máquinas virtuais do repositório de backup até o armazenamento na produção restabelecida não deverá afetar a disponibilidade e acesso pelo usuário, sem paradas. Deverá prover acesso ao conteúdo das máquinas virtuais, para recuperação de arquivos, pastas ou anexos, diretamente do ambiente protegido (repositório de backup) ou replicados, sem a necessidade de recuperar completamente o backup e inicializar uma máquina virtual. Deverá permitir realizar buscas rápidas mediante os índices dos arquivos que sejam controlados por um sistema operacional Windows, quando este seja o sistema operacional executado dentro da máquina virtual da qual se tenha realizado o backup. Deverá assegurar a consistência de aplicações transacionais de forma automática por meio da integração com Microsoft VSS, dentro de sistemas operacionais Windows. Deverá permitir realizar a truncagem de logs transacionais (transaction logs) para máquinas virtuais com Microsoft Exchange, SQL Server e Oracle. Deverá permitir notificações por correio eletrônico, SNMP ou através dos atributos da máquina virtual do resultado da execução de seus trabalhos. Deverá permitir recuperar no nível de objetos e arquivos de qualquer aplicação virtualizada, em qualquer sistema operacional, utilizando as ferramentas de gestão das aplicações existentes. Deverá incluir ferramentas de recuperação sem a						

	necessidade de agentes, sem a necessidade de recuperar os arquivos da máquina virtual como um todo ou reiniciar a mesma (recuperação granular), para os servidores: Microsoft Exchange 2016, possibilitando recuperar objetos individuais, tais como contatos, mensagens, compromissos, anexos, entre outros; Microsoft Active Directory 2016, possibilitando recuperar objetos individuais, tais como usuários, recuperação de senhas de usuários e computadores, grupos, contas, Objetos de Política de Grupo (GPOs), registros do Microsoft DNS integrados ao Active Directory entre outros sem a necessidade de usar o agente tanto para backup e restauração; Microsoft SQL Server 2014 ou superior, possibilitando recuperar objetos individuais, tais como bases, tabelas, registros, entre outros; Microsoft Sharepoint 2016; Deverá oferecer testes automatizados de recuperação para todas as máquinas virtuais protegidas, garantindo a confiabilidade na execução correta das máquinas virtuais e de suas aplicações (DNS Server, Controlador de domínio, Servidor de e-mail, etc.), no momento da recuperação. Deverá ser possível executar uma ou várias máquinas virtuais a partir do arquivo de backup, em um ambiente isolado de forma automática através de schedule, sem a necessidade de espaço de armazenamento adicional e sem modificar os arquivos de backup (read-only), para criação de ambiente de homologação, teste, etc. Deverá oferecer arquivamento em fita, suportando VTL (Virtual Tape Libraries), biblioteca de fitas e drives LTO5 ou superior, possibilitando a gravação paralela em múltiplos drives, além da criação de pools de mídia globais e pools de mídia GFS, sem a necessidade de licenciamento individual por drive; Deverá oferecer trabalhos de cópia de backup com implementação de políticas de retenção. Deverá operar em ambientes virtualizados através das soluções da Vmware, incluindo: VMware vSphere 7. Deverá garantir a recuperação granular e consistente, sem necessidade de instalação de agentes adicionais para o ambiente virtualizado através das soluções acima, principalmente para os seguintes softwares: Microsoft Active Directory 2016; Microsoft Exchange Server 2016; Microsoft Sharepoint 2013 ou superior Oracle Database 12 ou superior. Deverá ser capaz de realizar réplicas em outros sites ou infraestruturas a partir dos backups realizados. Deverá regular de forma dinâmica e parametrizável, o uso de recursos computacionais, de forma que se possa diminuir o impacto na infraestrutura de produção, durante as atividades de backup. Deverá permitir um método de fácil de recuperação, desde ambientes de contingência, com as ações pré-configuradas para evitar ações manuais em caso de desastre, similar a um botão de emergência. Deverá oferecer a possibilidade de armazenar os arquivos de backup de forma criptografada, com algoritmo mínimo de 256 bits, ativando e desativando tal operação, assim como assegurar o trânsito da informação através desse cenário. Deverá permitir a criação de níveis de delegação de tarefas (perfis) de recuperação no nível de elementos da aplicação, inclusive para outros usuários, de forma a diminuir a carga de atividades executadas pelo administrador da plataforma. Deverá integrar uma solução unificada de monitoração de ambientes virtualizados, com fornecimento de relatórios capazes de apresentar informações do tipo:						

	Relatórios que permitam o planejamento de capacidade; Relatórios que permitam determinar a ineficiência dos recursos em uso; Relatórios que facilitem a visibilidade de tendências negativas e anomalias; Quadros de controle claros, apresentáveis e integráveis em sites web. A licença de software de Backup deverá, nativamente, ser capaz de emitir relatórios com informações completas, conforme subitens: Permitir acesso aos relatórios através de interface gráfica ou web; Suportar a geração de relatórios gráficos customizáveis de atividades de backups/restores, contendo: Horário de início e término dos jobs; Tempo de duração dos jobs; Todos os jobs em execução; Status (situação) de execução dos jobs; Relação e porcentagem de jobs executados por status, como por exemplo: com sucesso e com erros; Logs dos jobs; Volume de dados na origem e no destino, total e por job, por período de tempo, por localidade e por host (físico ou virtual); Tendência de crescimento; Dados históricos de, no mínimo, 24 (vinte e quatro) meses. Suportar a geração de relatórios gráficos customizáveis de atividades de backups, contendo: Identificação da ocupação nos destinos de backups: uso de disco e fita; Porcentagem de dados deduplicados; Taxa de deduplicação e compressão. Permitir a geração de relatórios baseados na utilização de recursos, identificando restrições associadas a aplicativos específicos. Permitir a geração de relatórios baseados em alertas pré-definidos, com o objetivo de reportar eventos ocorridos do ambiente operacional de backup e restore. Deverá correlacionar a execução de trabalhos de backup e réplica com os objetos do ambiente virtual. Deverá oferecer a capacidade de relatar o cumprimento das políticas de proteção de dados e disponibilidade de acordo com parâmetros definidos. Deve suportar múltiplas operações dos componentes/servidores participantes da estrutura de backup, permitindo atividades de backup e recuperação simultâneas; Deve suportar repositório de backup com aumento de escala ilimitado para o armazenamento de dados com suporte aos seguintes sistemas de armazenamento: Microsoft Windows; Linux; Pastas compartilhadas; Appliances de duplicadoras. Storages do tipo SAN e NAS Nuvem (Amazon AWS, Microsoft Azure) Deverá permitir a seleção de um destino de armazenamento do backup em um provedor de serviços em nuvem (BaaS – Backup as a Service); Deverá permitir a seleção de um destino para a réplica dos dados que poderá ser em um provedor de serviços em nuvem (DRaaS – DR as a Service); Possuir integração com armazenamento de objetos compatíveis com S3 como Amazon S3, Azure Blob Storage e qualquer outro dispositivo de armazenamento local compatível com S3; Realizar arquivamento dos dados de backup nos dispositivos e locais de armazenamento de objetos compatíveis com S3; Em caso de desastre, deverá ser possível realizar a recuperação dos dados diretamente do arquivamento em S3; A solução deverá possuir integração com soluções de antivírus de modo a realizar uma varredura de						

	segurança nos dados de backup antes de realizar sua recuperação; Deve possuir a funcionalidade de recuperar dados para servidores diferentes do equipamento de origem; Deve ser ofertada a versão mais atual do software de backup, liberada oficialmente pelo fabricante do software. Caso haja necessidade, por razões de compatibilidade com os demais componentes de hardware e software do ambiente de backup, O SAAE DE ITABIRITO se reserva o direito de utilizar a versão do software imediatamente anterior à versão mais atual, sem nenhum ônus adicional; Deve ser ofertada, junto com a solução, o armazenamento de 6 tb de dados em ambiente de cloud computing com suporte integrado à solução para backup dos dados, com proteção dentro da interface de gerenciamento da solução para evitar "inside atacks" (ataques que objetivam o backup e a deleção dos mesmos). O ambiente de nuvem deve ser integrado para permitir a partir de uma interface única desenvolver tanto o backup quanto o restore de todo o ambiente. **Apresentar catálogo técnico da solução, sob pena de desclassificação.** **Após aquisição será realizada prova de conceito da solução na Sede do SAAE de ITABIRITO antes do aceite da solução. Não sendo satisfatória, a troca será de total responsabilidade do fornecedor incluindo a mão de obra de instalação.**						
02	**FIREWALL** 1. Especificações Gerais 1.1. Distribuidor deve ter presença nacional de suporte. 1.2. Next-Generation Firewall (NGFW) para proteção de informação perimetral e de rede interna que inclui stateful firewall com capacidade para operar em alta disponibilidade (HA) em modo ativo-passivo para controle de tráfego de dados por identificação de usuários e por camada 7, com controle de aplicação, administração de largura de banda (QoS), VPN IPsec e SSL, IPS, prevenção contra ameaças de vírus, malwares, Filtro de URL, criptografia de email, inspeção de tráfego criptografado e proteção de firewall de aplicação Web. Deverá ser fornecida console de gerenciamento dos equipamentos e centralização de logs em hardware específico e virtualizado. 1.2.1. A solução deve consistir de appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), e console de gerência, monitoração e logs. 1.2.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões. 1.3. Para os itens que representem bens materiais, a CONTRATADA deverá fornecer produtos novos, sem uso anterior. 1.4. O backup e o reestabelecimento de configuração deverão ser feitos localmente, via FTP ou email com frequência diária, semanal ou mensal, podendo também ser realizado por demanda. 1.5. Suportar SNMP e Netflow. 1.6. A solução deverá permitir port-aggregation de interfaces de firewall suportando o protocolo 802.3ad, para escolhas entre aumento de throughput e alta disponibilidade de interfaces 1.7. A solução deverá permitir configurar os serviços de DNS, Dynamic DNS, DHCP e NTP. 1.8. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico. 1.9. Cada appliance deverá ser capaz de executar a	Unid.	01				

	totalidade das capacidades exigidas para cada função, não sendo aceitos somatórias para atingir os limites mínimos. 1.10. O hardware e o software fornecidos não podem constar, no momento da apresentação da proposta, em listas de end-of-sale, end-of-support, end-ofengineering-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante. 1.11. O contratante deve possuir a opção de abrir solicitações de suporte diretamente com o fabricante. 1.12. Suporte aos roteamentos estáticos, dinâmico (RIP, BGP e OSPF) e multicast (PIM-SM e IGMP) 1.13. O Appliance proposto deve fornecer logs e relatórios embarcados contendo no mínimo os itens abaixo: 1.13.1. Dashboard com informações do sistema: 1.13.1.1. Informações de CPU 1.13.1.2. Informações do uso da rede. 1.13.1.2. Informações de memória. 1.13.1.3. Informações de sessões ativas. 1.13.1.4. Permitir visualizar número políticas ativas. 1.13.1.5. Visualizar número de access point do fabricante conectados. 1.13.1.6. Visualizar número de usuários conectados remotamente. 1.13.1.7. Visualizar número de usuários conectados localmente. 1.13.2. Relatórios com informações sobre as conexões de origem e destino por países. 1.13.3. Relatórios informando as conexões dos hosts. 1.13.4. Visualizar relatórios por período de tempo, permitindo o agendamento e o envio destes relatórios por email. 1.13.5. Permitir exportar relatórios para as seguintes extensões/plataformas: 1.13.5.1. PDF 1.13.5.2. HTML 1.13.5.3. Excel 1.13.6. Permitir visualizar relatório de políticas ativas associado ao ID da política criada. 1.13.7. Relatório que informe o uso IPSEC por host e usuário. 1.13.8. Relatório que informe o uso L2TP por host e usuário. 1.13.9. Relatório que informe o uso PPTP por usuários. 1.13.10. Relatório abordando eventos de VPN. 1.13.11. Proporcionar sistema de logs em tempo real, com no mínimo as seguintes informações: 1.13.11.1. Logs do sistema. 1.13.11.2. Logs das políticas de segurança 1.13.11.3. Logs de autenticação 1.13.11.4. Logs de administração do appliance. 1.13.12. Permitir ocultar dos relatórios usuários e IPs cadastrados. 1.14. Ter relatórios customizados e em compliance com pelo menos estes órgãos: HIPAA, GLBA, SOX, FISMA, PCI, NERC CIP v3, CIPA. 1.15. Possuir no mínimo 6 interfaces 10/100/1000; 1.16. A solução proposta deve cumprir as normas da CE, FCC Class A, CB, VCCI, CTick, UL, CCC. 1.15. A solução proposta deve corresponder aos seguintes critérios de throughput máximo, considerando o tamanho do pacote UDP sendo 1518 byte: Suportar no mínimo 27.500 (vinte e sete mil e quinhentos) novas conexões por segundo; 1.16. Suportar no mínimo 6.000.000 (seis milhões) conexões simultâneas; 1.17. Possuir no mínimo 3.500 Mbps (três mil e quinhentos) de rendimento (throughput) do Firewall para pacotes UDP;						

	1.18. No mínimo 900 (novecentos) Mbps de rendimento (throughput) do IPS; 1.18. Possuir no mínimo 350 Mbps de throughput de VPN AES. 1.19. A solução proposta deve corresponder aos seguintes critérios de throughput em mundo real: 1.19.1. Entende-se como mundo real, testes realizados pelo fabricante que tenham sido feitos com o appliance utilizando até 50% da capacidade de processamento, utilizando um mix de protocolos usados no mundo corporativo. 1.19.2. Possuir no mínimo 103 Mbps de rendimento (throughput) de IPS mundo real. 1.19.3. Possuir no mínimo 30 Mbps de rendimento (throughput) de funcionalidades next generation em mundo real; 1.19.4. Possuir no mínimo 90 de rendimento (throughput) de VPN AES mundo real. 1.20. Entende-se como mundo real testes realizados utilizando ambientes e protocolos usados no mundo corporativo. 1.21. A solução proposta deve possuir licenças baseado nos recursos de hardware. 1.22. A solução proposta deve suportar a configuração de políticas baseadas em usuários para segurança e gerenciamento de internet. 1.23. A solução proposta deve fornecer os relatórios diretamente no Appliance, baseados em usuário, não só baseado em endereço IP. 1.24. A solução proposta deve possuir no mínimo 64 GB de espaço em disco SSD para o armazenamento de eventos e relatórios. 1.25. Possuir slot de FleXi Port 1.26. Possuir portas USB 2.0 e 3.0. 1.27. Possuir porta VGA. 1.28. Possuir ao menos uma porta COM (RJ45). 1.29. Número irrestrito de usuários/IP conectados. 1.30. Appliance com 1U para montagem em rack. 2. Especificações da Administração, Autenticação e Configurações em geral 2.1. A solução proposta deve suportar administração via comunicação segura (HTTPS, SSH) e Console. 2.2. A solução proposta deve ser capaz de importar e exportar cópias de segurança (backup) das configurações, incluindo os objetos de usuário. 2.3. O backup pode ser realizado localmente, enviado pela ferramenta para um ou mais emails pré-definidos e via FTP, deve-se também ser feito sob demanda, ou seja, agendar para que este backup seja realizado, por dia, semana, mês e ano. 2.4. A solução proposta deve suportar implementações em modo Router (camada 3) e transparente (camada 2) individualmente ou simultâneos. 2.5. A solução proposta deve suportar integrações com, Active Directory, LDAP, Radius, eDirectory, TACACS+ e Banco de Dados Local para autenticação do usuário. 2.6. A solução proposta deve suportar em modo automático e transparente "Single Sign On" na autenticação dos usuários do active directory e eDirectory. 2.7. Os tipos de autenticação devem ser, modo transparente, por autenticação Kerberus/NTLM e cliente de autenticação nas máquinas. 2.8. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços. 2.9. Deve permitir autenticação em modos: transparente, autenticação proxy (NTLM e Kerberos) e autenticação via clientes nas estações com						

	os sistemas operacionais Windows, MAC OS X e Linux 32/64. 2.10. Certificados de autenticação para iOS e Android. 2.11. A solução proposta deve suportar integração com Dynamic DNS de terceiros 2.12. A solução proposta deve ter gráficos de utilização de banda em modos diários, semanais, mensais ou anuais para os links de forma consolidada ou individual. 2.13. A solução proposta deve suportar Parent Proxy com suporte a IP / FQDN. 2.14. A solução proposta deve suportar NTP. 2.15. A solução proposta deverá suportar a funcionalidade de unir usuário/ip/mac para mapear nome de usuário com o endereço IP e endereço MAC por motivo de segurança. 2.16. A solução proposta deve ter suporte multilíngue para console de administração web. 2.17. A solução proposta deverá suportar fazer um roll back de versão. 2.18. A solução proposta deve suportar a criação de usuário baseada em ACL para fins de administração. 2.19. A solução proposta deve suportar instalação de LAN by-pass no caso do appliance estar configurado no modo transparente. 2.20. A solução proposta deve suportar cliente PPPOE e deve ser capaz de atualizar automaticamente todas as configurações necessárias, sempre que PPPOE trocar. 2.21. A solução proposta deve suportar SNMP v1, v2c e v3. 2.22. A solução proposta deve suportar SSL/TLS para integração com o Active Directory ou LDAP. 2.23. A solução proposta deve possuir serviço de "Host Dynamic DNS" sem custo e com segurança reforçada. 2.24. A solução proposta deve ser baseado em Firmware ao contrário de Software e deve ser capaz de armazenar duas versões de Firmware ao mesmo tempo para facilitar o retorno "rollback" da cópia de segurança. 2.25. A solução proposta deve fornecer uma interface gráfica de administração flexível e granular baseado em perfis de acesso. 2.26. A solução proposta deve fornecer suporte a múltiplos servidores de autenticação para diferentes funcionalidades (Exemplo: Firewall um tipo de autenticação, VPN outro tipo de autenticação) 2.27. A solução proposta deve ter suporte a ambientes de terminais (Microsoft e Citrix) suportando autenticação de usuário de diferentes sessões originando do mesmo endereço IP. 2.28. A solução proposta deve suportar: 2.28.1. Serviço de DHCP/DHCPv6; 2.28.2. Serviço de DHCP/DHCPv6 Relay Agent; 2.28.3. Suporte a DHCP sobre VPN IPSec; 2.29. A solução proposta deve trabalhar como DNS/DNSv6 Proxy. 2.30. Gráficos, relatórios e ferramentas avançadas de apoio para troubleshooting. 2.31. Permitir exportar informações de troubleshooting para arquivo PCAP. 2.32. Permitir o factory reset e troca do idioma via interface gráfica. 2.33. Atualização de firmware de forma automatizada 2.34. Reutilização de definições de objetos de rede, hosts, serviços, período de tempo, usuários, grupos, clientes e servers. 2.35. Portal de acesso exclusivo para usuários poderem realizar atividades administrativas que envolve apenas funcionalidades especificas a ele. 2.36. Controle de acesso e dispositivos por zoneamento. 2.37. Integrar com ferramenta de gerenciamento						

	centralizado disponibilizado pela própria fabricante. 2.38. Opção de habilitar acesso remoto do appliance para suporte diretamente com o fabricante através de um túnel seguro, esta funcionalidade deve estar embarcada dentro do próprio appliance ofertado. 2.39. Traps SNMP ou email para notificações do sistema. 2.40. Suportar envio de informações via Netflow e possuir informações via SNMP. 2.41. Suporte a TAP mode para POCs e trials. 2.42. Ter funcionalidade que permita que o administrador manualmente atribua e/ou desatribua cores do CPU para uma interface em particular, dessa forma, todo trafego que passar por esta interface, será tratado unicamente pelos núcleos definidos. 2.43. Possuir funcionalidade de Fast Path para realizar a otimização no tratamento dos pacotes. 3. Especificações de Balanceamento de Carga e Redundância para Múltiplos Provedores de Internet 3.1. A solução proposta deve suportar o balanceamento de carga e redundância para mais de 2 (dois) links de Internet. 3.2. A solução proposta deve suportar o roteamento explícito com base em origem, destino, nome de usuário e aplicação. 3.3. A solução proposta deve suportar algoritmo “Round Robin” para balanceamento de carga. 3.4. A solução proposta deve fornecer opções de condições em caso de falha "Failover" do link de Internet através dos protocolos ICMP, TCP e UDP. 3.5. A solução proposta deve enviar e-mail de alerta ao administrador sobre a mudança do status de gateway. 3.6. A solução proposta deve ter ativo/ativo utilizando algoritmo de "Round Robin" e ativo/passivo para o balanceamento de carga do gateway e suporte a falha (Failover). 3.7. A solução proposta deve fornecer o gerenciamento para múltiplos links de Internet bem como tráfego IPv4 e IPv6. 4. Especificações de Alta Disponibilidade 4.1. A solução proposta deve suportar Alta Disponibilidade (High Availability) ativo/ativo e ativo/passivo. 4.2. A solução proposta deve notificar os administradores sobre o estado (status) dos gateways mantendo a Alta Disponibilidade. 4.3. O tráfego entre os equipamentos em Alta Disponibilidade deverá ser criptografado. 4.4. A solução deverá detectar falha em caso de Link de Internet, Hardware e Sessão. 4.5. A solução proposta deve suportar sincronização automática e manual entre os appliances em "cluster". 4.6. A solução deve suportar Alta Disponibilidade (HA) em "Bridge Mode" e Mixed Mode" (Gateway + Bridge). 5. Proteção básica de firewall 5.1. Especificações do Firewall e roteamento 5.2. A solução deve ser Standalone Appliance e com Sistema Operacional fortalecido "Hardening" para aumentar a segurança. 5.3. Deve suportar controles por: porta e protocolos TCP/UDP, origem/destino e identificação de usuários. 5.4. Suporte a objetos e regras IPV6. 5.5. Suporte a objetos e regras multicast. 5.6. A solução proposta deve suportar “Stateful Inspection” baseado no usuário "one-toone", NAT Dinâmico e PAT. 5.7. A solução proposta deve usar a "Identidade do Usuário" como critério de Origem/Destino, IP/Subnet/Grupo e Porta de Destino na regra do Firewall. 5.8. A solução proposta deve unificar as políticas de						

	ameaças de forma granular como Antivírus/AntiSpam, IPS, Filtro de Conteúdo, Políticas de Largura de Banda e Política de Balanceamento de Carga baseado na mesma regra do Firewall para facilitar de uso. 5.9. A proteção Anti-Malware deverá realizar a proteção com emulação JavaScript. 5.10. Deve permitir o bloqueio de vulnerabilidades. 5.11. Deve permitir o bloqueio de exploits conhecidos. 5.12. A solução proposta deve suportar arquitetura de segurança baseado em Zonas 5.12.1. As zonas deverão ser divididas pelo menos em WAN, LAN e DMZ, sendo necessário que as zonas LAN e DMZ possam ser customizáveis. 5.13. A solução proposta deve ter predefinido aplicações baseadas na "porta/assinatura" e também suporte à criação de aplicativo personalizado baseado na "porta/número de protocolo". 5.14. A solução proposta deve suportar balanceamento de carga de entrada (Inbound NAT) com diferentes métodos de balanceamento como First Alive, Round Robin, Random, Sticky IP e Failover conforme a saúde (Health Check) do servidor por monitoramento (probe) TCP ou ICMP. 5.15. A solução proposta deve suportar 802.1q (suporte a marcação de VLAN). 5.16. A solução proposta deve suportar roteamento dinâmico como RIP1, RIP2, OSPF, BGP4. 5.17. A solução proposta deve possuir uma forma de criar roteamento Estático/Dinâmico via shell. 5.18. O sistema proposto deve prover mensagem de alertas no Dash Board (Painel de Bordo) quando eventos como: a senha padrão não foi alterada, acesso não seguro está permitindo ou a licença irá expirar em breve. 5.19. O sistema proposto deve prover Regras de Firewall através de endereço MAC (MAC Address) para prover segurança na camada de rede 2 até 7 do modelo OSI. 5.20. A solução proposta deve suportar IPv6. 5.20.1. IPv6 deve suportar os tunelamentos 6in4, 6to4, 4in6 e IPv6 Rapid Deployment (6rd) de acordo com a RFC 5969. 5.21. A solução proposta deve suportar implementações de IPv6 Dual Stack. 5.22. A solução proposta deve suportar tuneis 6in4,6to4,4in6,6rd. 5.23. A solução proposta deve suportar toda a configuração de IPv6 através da Interface Gráfica. 5.24. A solução proposta deve suportar DNSv6. 5.25. A solução proposta deve oferecer proteção DoS contra ataques IPv6. 5.26. A solução proposta deve oferecer prevenção contra Spoof em IPv6. 5.27. A solução proposta deve suportar 802.3ad para Link Aggregation. 5.28. A solução proposta deve suportar 3G UMTS e 4G modem via interface USB para VPN e Link Backup "Plano de Continuidade" - Balanceamento de Carga. 5.29. A solução proposta deve suportar gerenciamento de banda baseado em Aplicação que permite administradores criarem políticas de banda de utilização de link baseado por aplicação. 5.30. Flood protection, DoS, DDoS e Portscan. 5.31. Bloqueio de Países baseados em GeoIP. 5.32. Suporte a Upstream proxy. 5.33. Suporte a VLAN DHCP e tagging. 5.34. Suporte a Multiple bridge. 5.35. Funcionalidades do portal do usuário 5.35.1. Autenticação de dois fatores (OTP) para IPSEC						

	e SSL VPN, portal do usuário, e administração web (GUI). 5.35.2. Download dos clientes de autenticação disponibilizados pela ferramenta. 5.35.3. Download do cliente VPN SSL em plataformas Windows. 5.35.4. Download das configurações SSL em outras plataformas. 5.35.5. Informações de hotspot. 5.35.6. Autonomia de troca de senha do usuário. 5.35.7. Visualização do uso de internet do usuário conectado. 5.35.8. Acesso a mensagens quarentena. 5.36. Opções base de VPN 5.36.1. A VPN IPsec deve suportar: DES e 3DES, Autenticação MD5 e SHA-1;Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; Algoritmo Internet Key Exchange (IKE); AES 128, 192 e 256 (Advanced Encryption Standard); SHA 256, 384 e 512; Autenticação via certificado PKI (X.509) e Pre-shared key (PSK). 5.36.2. L2TP e PPTP. 5.36.3. VPN SSL, IPSEC. 5.36.4. Proporcionar através do portal do usuário uma forma de conexão via HTML5 de acesso remoto com suporte aos protocolos, RDP, HTTP, HTTPS, SSH, Telnet e VNC. 5.36.5. Suportar autenticação via AD/LDAP, Token e base de usuários local. 5.37. Funcionalidades base de QoS e Quotas 5.37.1. QoS aplicado a redes e usuários de download/Upload em tráfegos baseados em serviços. 5.37.2. Otimização em tempo real do protocolo Voip. 5.37.3. Suporte a marcação DSCP. 5.37.4. Regras associadas por usuário. 5.37.5. Criar regras que limitem e garantam upload e download. Permitir criar regra de QoS individualmente e compartilhada. 6. Proteção Web 7. Filtragem e Segurança Web 7.1. Proporcionar transparência total de autenticação no proxy, provendo segurança antimalware e filtragem web. 7.2. Possuir uma base de dados com mais de 1.000.000 (um milhão) de URLs reconhecidas e categorizadas agregadas a pelo menos 92 categorias oferecidas pela solução. 7.3. Realizar autenticação dos usuários nos modos transparente e padrão. 7.3.1. As autenticações devem ser feitas via NTLM. 7.4. Possuir sistema de quotas aplicado por usuários e grupos. 7.5. Permitir criar politicas por horário aplicado a usuários e grupos. 7.6. Possuir sistema de malware scanning que realize as seguintes ações: 7.6.1. Bloquear toda forma de vírus 7.6.2. Bloquear malwares web 7.6.3. Prevenir infecção de malwares, trojans e spyware em trafegos HTTPS, HTTP, FTP e emails baseados em acesso web (via navegador). 7.6.4. Proporcionar proteção de web malware avançado com emulação de Javascript. 7.7. Prover proteção em tempo real de todos os acessos web. 7.7.1.A proteção em tempo real deve consultar constantemente a base de dados na nuvem do fabricante que deverá manter-se atualizada prevenindo novas ameaças. 7.8. Prover pelo menos duas engines diferentes de antimalware para auxiliar na detecção de ataques e						

	ameaças realizadas durante os acessos web realizados pelos usuários. 7.9. Fornecer Pharming Protection. 7.10. Possuir pelo menos dois modos diferentes de escaneamento durante o acesso do usuário. 7.11. Permitir criação de regras customizadas baseadas em usuário e hosts. 7.12. Permitir criar exceções de URLs, usuários e hosts para que não sejam verificados pelo proxy. 7.13. Validação de certificado. 7.14. Prover cache de navegação, contribuindo na agilidade dos acessos a internet. 7.15. Realizar filtragem por tipo de arquivo, mime-type, extensão e tipo de conteúdo (exemplo: Activex, applets, cookies, etc.) 7.16. Integração com o youtube for schools. 7.17. Prover funcionalidade que força o uso das principais ferramentas de pesquisa segura (SafeSearch): Google, Bing e Yahoo. 7.18. Permitir alterar a mensagem de bloqueio apresentada pela solução para os usuários finais. 7.19. Permitir alterar a imagem de bloqueio que é apresentado para o usuário quando feito um acesso não permitido. 7.20. Permitir a customização da página HTML que apresenta as mensagens e alertas para os usuários finais. 7.21. Permitir visualizar as alterações feitas nos itens 7.17 e 7.18 antes de salvar as modificações. 7.22. Especificar um tamanho em Kbytes de arquivos que não devem ser escaneados pela proteção web. 7.22.1. Range aceitável de 1 a 25600KB. 7.23. Bloquear trafego que não segue os padrões do protocolo HTTP. 7.24. Permitir criar exceções de sites baseados em URL Regex, tanto para HTTP quanto para HTTPS. 7.25. Nas exceções, permitir definir operadores “AND” e “OR”. 7.26. Permitir definir nas exceções a opção de não realizar escaneamento HTTPS. 7.27. Permitir definir nas exceções a opção de não realizar escaneamento contra malware. 7.28. Permitir definir nas exceções a opção de não realizar escaneamento de critérios especificado por políticas. 7.29. Permitir criar regras de exceções por endereços IPs de origem. 7.30. Permitir criar regras de exceções por endereços IPs de destino 7.31. Permitir criar exceções por grupo de usuários. 7.32. Permitir criar exceções por categorias de sites. 7.33. Permitir a criação de agrupamento de categorias feitas pelo administrador do equipamento. 7.34. Ter grupos de categorias pré-configuradas na solução apresentando nomes sugestivos para tais agrupamentos, por exemplo: “Criminal Activities, Finance & Investing, Games and Gambling”, entre outras. 7.35. Permitir editar grupos de categorias pré-estabelecidos pela solução. 7.36. Deve ter sistema que permita a criação de novas categorias com as seguintes especificações: 7.36.1. Nome da regra; 7.36.2. Permitir criar uma descrição para identificação da regra. 7.36.3. Ter a possibilidade de classificação de pelo menos: 7.36.3.1. Produtivo; 7.36.3.2. Não produtivo; 7.36.3.3. Permitir aplicar Traffic shaping diretamente na categoria. 7.36.3.4. Na especificação das URLs e domínios que						

	farão parte da regra, deve-se permitir cadastrar por domínio e palavra-chave. 7.36.3.5. Deve permitir importar uma base com domínios e palavras chaves na hora da criação da categoria, a base com informações de domínios e palavras chaves deverá aceitar pelo menos as seguintes extensões: .tar, .gz, .bz, .bz2, e .txt. 7.36.3.6. Permitir importar a base citada no item anterior de forma externa, ou seja, especificar uma URL externa que contenha as informações com a lista domínios que poderá ser mantida pelo administrador ou um terceiro. 7.37. Ter função para criar grupos de URLs. 7.38. A base de sites e categorias devem ser atualizadas automaticamente pelo fabricante. 7.39. Permitir ao administrador poder especificar um certificado autoritário próprio para ser utilizado no escaneamento HTTPS. 7.40. Deve permitir que em uma mesma política seja aplicada ações diferentes de acordo com o usuário autenticado. 7.41. Nas configurações das políticas, deve-se existir pelo menos as opções de: Liberar categoria/URL, Bloquear e Alarmar o usuário quando feito acesso a uma categoria não desejada pelo administrador. 7.42. Forçar filtragem diretamente nas imagens apresentadas pelos buscadores, ajudando na redução dos riscos de exposição de conteúdo inapropriado nas imagens. 7.43. Permitir criar cotas de navegação com os seguintes requisitos: 7.43.1. Tipo do ciclo, especificando se o limite será por duração de acesso à internet ou se será especificado uma data limite para o acesso. 8. Controle e Segurança de Aplicações 8.1. Reconhecer pelo menos 2.700 aplicações diferentes, classificadas por nível de risco, características e tecnologia, incluindo, mas não limitado a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, serviços de rede, VoIP, streaming de mídia, proxy e tunelamento, mensageiros instantâneos, compartilhamento de arquivos, web e-mail e update de softwares. 8.2. Reconhecer pelo menos as seguintes aplicações: 4Shared File Transfer, Active Directory/SMB, Citrix ICA, DHCP Protocol, Dropbox Download, Easy Proxy, Facebook Graph API, Firefox Update, Freegate Proxy, FreeVPN Proxy, Gmail Video, Chat Streaming, Gmail WebChat, Gmail WebMail, Gmail-Way2SMS WebMail, Gtalk Messenger, Gtalk Messenger File Transfer, Gtalk-Way2SMS, HTTP Tunnel Proxy, HTTPort Proxy, LogMeIn Remote Access, NTP, Oracle database, RAR File Download, Redtube Streaming, RPC over HTTP Proxy, Skydrive, Skype, Skype Services, skyZIP, SNMP Trap, TeamViewer Conferencing e File Transfer, TOR Proxy, Torrent Clients P2P, Ultrasurf Proxy, UltraVPN, VNC Remote Access, VNC Web Remote Access, WhatsApp, WhatsApp File Transfer e WhatsApp Web. 8.3. Controlar aplicações baseadas em categorias, caracteristica(Ex: Banda e produtividade consumida), tecnologia(Ex:P2P) e risco. 8.4. Permitir criar regras de controle por usuário e hosts. 8.5. Permitir realizar traffic shaping por aplicação e grupo de aplicações. 8.6. Possibilitar que as regras criadas baseadas em aplicação permitam: 8.6.1. Bloquear o trafego para as aplicações 8.6.2. Liberar o trafego para as aplicações 8.6.3. Criar categorização das aplicações por risco: 8.6.3.1. Risco muito baixo						

	8.6.3.2. Risco baixo 8.6.3.3. Risco médio 8.6.3.4. Risco alto 8.6.3.5. Risco muito alto 8.6.4. Permitir visualizar as aplicações por suas características, por exemplo: aplicações que utilizam banda excessiva, consideradas vulneráveis, que geram perda de produtividade, entre outras. 8.6.5. Permitir selecionar pela tecnologia, por exemplo: p2p, client server, protocolos de redes, entre outros. 8.7. Permitir granularidade na hora da criação da regra baseada em aplicação, como por exemplo: Permitir bloquear anexo dentro de um post do Facebook, bloquear o like do Facebook, permitir acesso ao Youtube mas bloquear o upload de vídeos, e etc. 8.7.1. Deve realizar o escaneamento e controle de micro app incluindo, mas não limitado a: Facebook (Applications, Chat, Commenting, Events, Games, Like Plugin, Message, Pics Download e Upload, Plugin, Post Attachment, Posting, Questions, Status Update, Video Chat, Video Playback, Video Upload, Website), Freegate Proxy, Gmail (Android Application, Attachment), Google Drive (Base, File Download, File Upload), Google Earth Application, Google Plus, LinkedIN (Company Search, Compose Webmail, Job Search, Mail Inbox, Status Update), SkyDrive File Upload e Download, Twitter (Message, Status Update, Upload, Website), Yahoo (WebMail, WebMail File Attach) e Youtube (Video Search, Video Streaming, Upload, Website). 8.7.2.O escaneamento de micro app deverá ser habilitado via console gráfica (GUI) e via comando de linha (CLI). 8.8. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante. 8.9. Permitir agendar um horário e data especifico para a aplicação das regras de controle de aplicativos, podendo ser executadas apenas uma vez como também de forma recursiva. 8.10. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações por assinaturas e camada 7, utilizando portas padrões (80 e 443), portas não padrões, port hopping e túnel através de tráfego SSL encriptado. 8.11. Atualizar a base de assinaturas de aplicações automaticamente. 8.12. Reconhecer aplicações em IPv6. 8.13. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários. 8.14. Deve permitir o uso individual de diferentes aplicativos para usuários que pertencem ao mesmo grupo de usuários, sem que seja necessária a mudança de grupo ou a criação de um novo grupo. Os demais usuários deste mesmo grupo que não possuírem acesso a estes aplicativos devem ter a utilização bloqueada. 9. Suportar no mínimo 82.000 (oitenta e dois mil) novas conexões por segundo; 10. Suportar no mínimo 8.200.000 (oito milhões e duzentos mil) conexões simultâneas; 11. Possuir no mínimo 7.000 Mbps (sete mil) de rendimento (throughput) do Firewall para pacotes UDP; 1.12.4. No mínimo 1.700 (um mil e setecentos) Mbps de rendimento (throughput) do IPS; 12. Possuir no mínimo 950 Mbps de throughput de VPN AES.						

	13. A solução proposta deve corresponder aos seguintes critérios de throughput em mundo real: 13.1. Entende-se como mundo real, testes realizados pelo fabricante que tenham sido feitos com o appliance utilizando até 50% da capacidade de processamento, utilizando um mix de protocolos usados no mundo corporativo. 13.2. Possuir no mínimo 232 Mbps de rendimento (throughput) de IPS mundo real. 13.3. Possuir no mínimo 75 Mbps de rendimento (throughput) de funcionalidades next generation em mundo real; 13.4. Possuir no mínimo 240 de rendimento (throughput) de VPN AES mundo real. 14. Entende-se como mundo real testes realizados utilizando ambientes e protocolos usados no mundo corporativo. 15. A solução proposta deve possuir licenças baseado nos recursos de hardware. 16. A solução proposta deve suportar a configuração de políticas baseadas em usuários para segurança e gerenciamento de internet. 17. A solução proposta deve fornecer os relatórios diretamente no Appliance, baseados em usuário, não só baseado em endereço IP. 18. A solução proposta deve possuir no mínimo 64 GB de espaço em disco SSD para o armazenamento de eventos e relatórios. 19. Possuir portas USB 2.0 e 3.0. 20. Possuir porta VGA. 21. Possuir ao menos uma porta COM (RJ45). 22. Número irrestrito de usuários/IP conectados. Serviços e apoio na implementação Avançado 23. Através de serviços adicionais, a contratante mediante o contrato deste serviço adicional, poderá ter as seguintes opções durante a implementação: 23.1. Configuração de 1 appliance em modo standalone, HA ou cluster. 23.2. Ativação da licença. 23.3. Configuração inicial (hostname, horário, interface WAN e LAN). 23.4. Atualização da versão do firmware. 23.5. Repasse de conhecimentos para: 23.6. Configuração de interfaces adicionais e VLAN. 23.7. Roteamento estático e dinâmico. 23.8. Configuração de DNS e DHCP. 23.9. Configuração de NAT. 23.10. Integração de autenticação via Active Directory, RADIUS, LDAP ou TACACS+. 23.11. Configuração de regra de firewall, IPS, Application Control e QoS. 23.12. Configuração de Web Filter. 23.13. Configuração de Email Filter. 23.14. Configuração de Web Server Protection (WAF). 23.15. Configuração de Wireless Protection (com Access Point da Sophos). 23.16. Configuração do Sophos RED. 23.17. Configuração de VPN. 23.18. Configuração de backup. 23.19. Troubleshooting de erros **Apresentar catálogo técnico da solução, sob pena de desclassificação.**						
03	**ANTIVÍRUS** 1. Aquisição de Licenças e Atualização do Antivírus para o período de 36 meses, 50 (cinquenta) máquinas. 1.1. REQUISITOS MÍNIMOS PARA A SOLUÇÃO DE ANTIVÍRUS 1.2. Possuir uma única console de gerenciamento para gestão e configurações do antivírus, antispyware, firewall, detecção de intrusão, controle de dispositivos,	Unid.	01				

	controle de aplicações e criptografia de discos. 1.3. A solução deverá ter a capacidade de remoção do atual antivírus instalado e ser capaz de instalar de forma remota o agente do antivírus pela console de gerenciamento, e caso não tenha a capacidade de realização a remoção completa, a contratada deverá remover a atual solução utilizando scripts, softwares de terceiros, ou mesmo de forma manual; 1.4. O produto deverá possuir no mínimo os seguintes módulos e funcionalidades: 1.5. Console de gerenciamento fornecendo funcionalidades de gestão e configurações de políticas; 1.6. Módulos para estações físicas, notebooks e servidores; 1.7. Módulo para ambientes virtualizados, sendo criado especialmente para ambientes virtuais; 1.8. Módulo para dispositivos móveis no mínimo para tablets e smartphones com sistema operacional iOS e Android; 1.9. Utilizar o conceito de heurística para combate e ações contra possíveis malwares; 1.10. Oferecer tecnologia onde a solução explore vulnerabilidades de softwares instalados no intuito de reduzir o risco de infecções (anti-exploit); 1.11. Oferecer tecnologia nativa no intuito de eliminar ameaças que sequestram dados, do tipo ransomware; 1.12. Oferecer inventário de softwares; 1.13. Oferecer tecnologia onde a solução teste arquivos potencialmente perigosos em ambiente isolado antes da execução do mesmo no ambiente de produção; 1.14. Oferecer proteção por base de assinaturas (vacinas). 2. CONSOLE DE GERENCIAMENTO 2.1. Instalação e configuração 2.2. Permitir instalação de console local (on-premise) com banco de dados local ou instalação em nuvem (cloud) com banco de dados também em nuvem; 2.3. Para a opção de console local de ser fornecido como um appliance virtual ou executável para instalação em servidores Windows. Deverá suportar no mínimo as seguintes plataformas de virtualização: 2.4. VMWare vSphere; 2.5. Citrix XenServer; XenDesktop, VDI-in-a-Box; 2.6. Microsoft Hyper-V; 2.7. Red hat Enterprise Virtualization; 2.8. Kernel-based Virtual Machine ou KVM; 2.9. Oracle VM; 2.10. Deverá ser fornecido com base de dados embutida e proprietária ou com possibilidade de utilização de banco de dados externo SQL ou Oracle; 2.11. Para instalação da console em nuvem (cloud), a nuvem deve ser privada e do mesmo fabricante; 2.12. Permitir instalação remota via console WEB de gerenciamento para ambientes virtuais VMWare ou Citrix; 2.13. O mecanismo de varredura deverá estar disponível para download separadamente; 2.14. A solução deverá permitir a inclusão de um modulo de balanceamento para casos em que vários servidores tenham a mesma função (para alta disponibilidade, recuperação de desastres, performance, dentre outras necessidades); 2.15. Deve ser totalmente em português. 2.16. Funcionalidades Gerais 2.17. Licenciamento flexível; 2.18. A console de gerenciamento deve incluir informações detalhadas sobre as estações e servidores com no mínimo as seguintes informações: 2.18.1. Nome; 2.18.2. IP; 2.18.3. Sistema Operacional;						

	2.18.4. Política Aplicada; 2.19. A console de gerenciamento deverá incluir sessão de log com as seguintes informações: 2.19.1. Login; 2.19.2. Edição; 2.19.3. Criação; 2.19.4. Log-out; 2.20. Arquitetura simples de atualização, com um simples clique deve ser possível atualizar todas funções e serviços da solução; 2.21. Permitir que o administrador escolha qual o pacote será atualizado; 2.22. As notificações devem ser destacadas como item não lido e notificar o administrador por e-mail; 2.23. No mínimo enviar notificações para as seguintes ocorrências: 2.24. Problemas com licenças; 2.25. Alertas de surto de vírus; 2.26. Máquinas desatualizadas; 2.27. Eventos de antimalware. 2.28. Deverá prover o acesso via HTTPS; 2.29. Deverá permitir a importação de certificados digitais; 2.30. O gerenciamento e a comunicação com dispositivos móveis deve ser feito de forma segura utilizando certificados digitais. 3. MONITORAMENTO 3.1. Baseado em “portlets” configuráveis com no mínimo as seguintes especificações: 3.1.1. Nome; 3.1.2 Tipo de relatório; 3.1.3. Alvo do relatório; 3.2 Deverá disponibilizar “portlets” para gerência e monitoramento de qualquer tipo de endpoint, máquinas físicas, virtuais e dispositivos móveis. 3.3. Inventário da Rede 3.4. Possuir no mínimo as integrações abaixo: 3.4.1. Múltiplos domínios do Active Directory; 3.4.2. Múltiplos VMWare vCenters; 3.4.3. Múltiplos Citrix Xen Servers; 3.4.4. Possuir a possibilidade de definição de sincronização com o Active Directory em horas; 3.5. Descoberta de rede para máquinas em grupo de trabalho; 3.6. Possuir busca em tempo real pelo menos com os seguintes filtros: 3.7. Nome; 3.8. Sistema Operacional; 3.9. Endereço IP; 3.10. Possibilitar a instalação remota e desinstalação remota do antivírus; 3.11. Possibilitar a configuração de pacotes de instalação do produto de antivírus; 3.12. Possuir tarefas remotas e configuráveis de scan; 3.13. Possuir tarefa de reinicialização remota de estação ou servidor; 3.14. Assinar políticas para no mínimo os níveis: 3.14.1. Computador; 3.14.2 Máquina Virtual; 3.14.3 Grupo de Endpoints; 3.14.4. Usuário do AD; 3.14.5. Grupo do AD. 3.15. Possuir a propriedade detalhada de objetos gerenciados para: 3.15.1. Nome; 3.15.2. IP; 3.15.3. Sistema Operacional; 3.15.4. Grupo; 3.15.5. Política Assinada; 3.15.6. Ultimo status de malware. 3.15.7. Modelo único para todos os equipamentos,						

	sejam físicos ou virtuais; 3.16. Cada serviço de segurança deve ter seu modelo configurável de política com opções específicas de ativar/desativar; 3.17. Através da console de gerenciamento o administrador poderá ser capaz de enviar uma política única para configurar o antivírus; 3.18. Deverá configurar as funcionalidades como escaneamento do antivírus, firewall de duas vias de detecção de intrusão, controle de acesso à rede, controle de aplicação, controle de acesso web, criptografia (Windows, Mac e Android), localização de dispositivo (Mobile), autenticação e ações para serem aplicadas em caso de vírus e dispositivos em não conformidade. 3.19. Relatórios - Deverá apresentar as seguintes funcionalidades: 3.20. Relatório para cada serviço de segurança; 3.21. Facilidade de usar e visualização simplificada; 3.22. Agendamento, com opção de envio por e-mail para qualquer destinatário conforme escolha do administrador; 3.23. Filtros de agendamento de relatórios; 3.24. Arquivo com todas as instâncias de relatório agendados; 3.25. Exportar o relatório nos formatos .pdf e/ou .csv; 3.26. Oferecer possibilidade de criar relatórios de maneira dinâmica no dashboard da console de gerenciamento. 3.27. Administração de Usuários 3.28. Deverá apresentas no mínimo as seguintes funcionalidades: 3.29. Administração baseada em regras; 3.30. Disponibilizar tipos de usuários pré-definidos como no mínimo: 3.31. Administrador – Gerente dos componentes da solução; 3.32. Administrador de rede - Gerente dos serviços de segurança; 3.33. Relatório – Monitora e cria relatórios; 3.34. Deverá ser possível customizar um tipo de usuário: 3.35. Deverá permitir a integração de usuários com o Active Directory para autenticação da console de gerenciamento; 3.36. Registrar as ações do usuário no console de gerenciamento; 3.37. Detalhar cada ação do usuário; 3.38. Permitir busca complexa baseada em ações do usuário, intervalos de tempo. 3.39. Segurança Para Estações e Servidores 3.40. Proteção para ambientes físicos 3.41. Deverá proteger em tempo real e agendado as máquinas físicas em qualquer plataforma de sistema operacional, seja Windows, Linux ou Mac, tanto no console local (on-premises) como na console em nuvem (cloud); 3.42. Deverá suportar no mínimo os seguintes sistemas operacionais para estação de trabalho: • Windows 10 64Bits; • Windows 8.1 64Bits; • Windows 8 64Bits; • Windows 7 64Bits; 3.43. Deverá suportar no mínimo os seguintes sistemas operacionais para servidores: • Windows Server 2012R2; • Windows Server 2012; • Windows Server 2008 R2; Windows Server 2008 apenas os módulos de antivírus e Active Virus Control;						

	3.44. Deverá suportar no mínimo os seguintes sistemas operacionais para distribuição Linux: • Ubuntu 14.04 LTS ou superior • Red Hat Enterprise Linux / CentOS 6 ou superior • SUSE Linux Enterprise Server 11 SP4 ou superior • OpenSUSE Leap 42.x • Fedora 25 ou superior • Debian 8.0 ou superior • Oracle Linux 6.3 ou superior • Amazon Linux AMI 2016.09 ou superior • Proteção para ambientes virtuais 3.45. Para plataforma de virtualização com VMWare, deverá: • Ter a disponibilidade de ser integrado e oferecer a escaneamento sem instalar o agente nas máquinas virtuais; • A console de gerenciamento central da solução deverá ter a possibilidade de integrar com múltiplos vCenters da VMWare; • Deverá proteger em tempo real e agendado as máquinas virtuais em qualquer plataforma de sistema operacional, seja Windows, Linux ou Mac, tanto no console local (on-premises) como na console em nuvem (cloud); 3.46.O produto deverá oferecer agente para virtualização dos seguintes produtos: • Citrix Xen Server; • Microsoft Hyper-V; • VMware ESXi; • Red Hat Virtualization; • Oracle KVM; • KVM. • Instalação e Configuração remota 3.47. Deverá permitir ao administrador customizar a instalação; 3.48. Deverá permitir a instalação customizada do antivírus com no mínimo: 3.49. Instalar o antivírus sem o controle de acesso a internet; (Windows Desktop) 3.50. Instalar o antivírus sem o módulo de firewall; (Windows Desktop) 3.51. A instalação deverá ser executada no mínimo das seguintes maneiras: 3.52. Executar o pacote de antivírus diretamente na estação de trabalho; 13.53. Instalar remotamente, distribuído via console de gerencia web; 3.54. Deverá ser possível ter um relatório com as estações instaladas e as faltantes da instalação; 3.55. Ter a capacidade de criar um único pacote independente ser for para 32 bits ou 64 bits; 3.56. Deverá permitir ao administrador criar grupos e subgrupos para mover as estações de trabalho; 3.57. O agente utilizado na sincronização deve ser incluído no cliente do antivírus e não ser necessário à distribuição em um agente separado. 3.58. Funções Gerais 3.59. Deverá ter métodos de detecção de vírus, spyware, rootkits e outros mecanismos de segurança; 3.60. Deverá permitir a configuração do scan do antivírus do cliente como: 3.60.1. Scan local; 3.60.2. Scan hibrido (local\remoto); 3.60.3. Scan remoto;						

	3.61. Deverá reportar o estado atual das máquinas virtuais no mínimo, protegida/desprotegida; 3.62. Deverá fazer scan em tempo real e automático; 3.63. Deverá ser configurável para não escanear arquivos conforme necessidade do administrador, ou seja, por tamanho ou por tipo de extensão; 3.64. Deverá possuir escaneamento baseado em análise heurística; 3.65. Deverá permitir a escolha e configuração de pastas a serem scaneadas; 3.66. Para melhor proteção, o antivírus deverá ter no mínimo 3 tipos de detecção: 3.67. Baseada em assinaturas; 3.68. Baseada em heurística; 3.69. Baseada em monitoramento contínuo de processos; 3.70. Deverá ter a capacidade de escaneamento nos protocolos HTTP e SSL nas estações de trabalho; 3.71. O cliente do antivírus deverá ter o módulo de Antiphishing que deverá ter a opção de verificar links pesquisados com os sites de pesquisas Search Advisor nas estações de trabalho; 3.72. Deverá possuir módulo de firewall que de acordo com o administrador poderá ou não ser instalado/desinstalado nas estações de trabalho; 3.73. No módulo de firewall deverá ser possível configurar o modo invisível tanto a nível de rede local ou Internet nas estações de trabalho; 3.74. Deverá ter os seguintes requisitos mínimos de sistema: • Plataformas de Virtualização • VMware vSphere ESX 5.0 ou superior; • VMware vCenter Server 4.1 ou superior; • Citrix XenDesktop 5.0 ou superior; • Xen Server 5.5 ou superior; • Citrix VDI-in-a-Box 5; • Microsoft Hyper-V Server 2008 R2, 2012 • Oracle VM 3.0; • Red Hat Enterprise Virtualization 3.0. • Sistemas Operacionais para Desktops • Windows 10 64Bits; • Windows 8.1 64Bits; • Windows 8 64Bits; • Windows 7 64Bits; • Sistemas Operacionais para Servidores • Windows Server 2012R2; • Windows Server 2012; • Windows Server 2008 R2; • Windows Server 2008 apenas os módulos de antivírus e Active Virus Control; • Linux Red Hat Enterprise; • CentOS 5.6 ou superior; • Ubuntu 10.04 LTS ou superior; • SUSE Linux Enterprise Server 11 ou superior; • OpenSUSE 11 ou superior; • Fedora 15 ou superior; Debian 5.0 ou superior. • Quarentena • Deverá permitir restauração remota, com configuração de localidade e deleção; • Criação e exclusão para arquivos restaurados; • Deverá permitir o envio automático de arquivos da quarentena para o laboratório de vírus; • Deverá fazer a remoção automática de						

	arquivos antigos, pré-definidos pelo administrador; • Deverá permitir a movimentação do arquivo da quarentena para seu local original ou outro destino que o administrador definir; • Deverá de forma automática criar exclusão para arquivos restaurados da quarentena; Deverá permitir escanear a quarentena após a atualização de assinaturas. • Controle de Usuário • Deverá ter módulo de controle de usuário integrando com as seguintes características: • Bloqueio de acesso à internet; Bloqueio de acesso a aplicações definidas pelo administrador. • Controle do Dispositivo • Deverá ser possível a instalação do módulo de controle de dispositivos através da console de gerenciamento; 3.75. Através do módulo de controle de dispositivo deverá ser possível controlar: • Bluetooth; • CDROM/DVDROM; • IEEE 1284.4; • IEEE 1394; • Windows Portable; • Adaptadores de Rede; • Adaptadores de rede Wireless; • Discos Externos; 3.76. Deverá escanear em tempo real qualquer informação localizada em mídias de armazenamento como: • CD/DVD; • Discos Externos; • Pen-Drivers; 3.77. Deverá permitir regras de definição de bloqueio/desbloqueio; 3.78. Deverá permitir regras de exclusão. 3.79. Criptografia 3.80. Deverá oferecer Possibilidade de criptografia de disco através da mesma console de gerenciamento do antivírus, seja em nuvem (cloud) ou local (on-premise); 3.81. Deverá utilizar, quando necessário, serviços de criptografia com agentes nativos da estação de trabalho seja baseada em Windows ou Mac; 3.82. Deverá solicitar autenticação quando iniciado o sistema operacional do equipamento; 3.83. Deverá ser compatível com Mac OS X Moutain, Mavericks, Yosemite, Sierra. 3.84. Atualização 3.85. Após a atualização o administrador deverá ter a capacidade de configurar uma reinicialização; 3.86. Possibilidade de utilizar um servidor local para efetuar as atualizações das estações de trabalho; 3.84. Permitir atualizações de assinatura de hora em hora; 3.85. Permitir motor de varredura local, no servidor de rede ou em nuvem afim de aumentar o desempenho da estação de trabalho quando a mesma estiver sendo escaneada. 3.86. Segurança Para Dispositivos Móveis 3.87. Requisitos mínimos do Sistema Operacional 3.88. Android 2.2 ou superior 3.89. Recursos 3.90. Permitir atribuir dispositivo com usuário do Active Directory;						

	3.91. A ativação do dispositivo da console de gerenciamento deverá ser através de um QR code; 3.92. Os pacotes de instalação devem estar disponíveis nas lojas dos Sistemas Operacionais; 3.93. Deverá permitir no mínimo as seguintes ações: 3.94. Impor bloqueio de tela e autenticação; 3.95. Desbloquear o dispositivo; 3.96. Restaurar as configurações de fábrica; 3.97. Localizar o Dispositivo; 3.98. Análise de dispositivos para o Sistema Operacional Android; 3.99. Criptografia de memória do dispositivo para o Sistema Operacional Android. 3.100. Configurações de Segurança 3.101. Caso o dispositivo não esteja em conformidade com as políticas estabelecidas deverá ser possível as ações abaixo: • Ignorar; • Bloquear acesso; • Bloquear o dispositivo; • Restaurar as configurações de fábrica; • Remover o dispositivo da console de gerenciamento; 3.102. Deverá permitir o uso de senha. A senha pode ser configurada conforme necessidade do administrador com no mínimo os seguintes recursos: • Senha simples ou complexa; • Números e caracteres; • Comprimento mínimo; • Caracteres especiais mínimos; • Período de expiração da senha; • Definir restrição de reutilização de senha; • Definir o número de tentativas de entradas de senha incorretas; • Período de bloqueio do dispositivo. 3.103. Segurança De e-Mails • Fornecer proteção de antispam para ambiente com instalação local (on-premise) do MS Exchange; • Oferecer análise comportamental e proteção para zero-day; • Oferecer proteção contra vírus e tentativas de phishing. • Criptografia • Deverá oferecer: • Possibilidade de criptografia de disco através da console de gerenciamento seja em nuvem ou on-premise com módulo de Criptografia presente na mesma Console do Antivirus. • utilizar quando necessários serviços de criptografia através agentes nativos da estação de trabalho baseada em Windows (BitLocker) ou Mac (FileVault); • Deverá solicitar autenticação quando iniciado o sistema operacional do equipamento; • Deverá ser compatível com Mac OS X Moutain, Mavericks, Yosemite, Sierra.						
NOTA: A aquisição de todos os itens será realizada por menor preço global.							
JUSTIFICATIVA PARA AQUISIÇÃO EM MENOR PREÇO GLOBAL	Inicialmente, cabe reforçar que a pretensão deste processo licitatório não é apenas aquisição de uma solução ou hardware. O que se pretende é adquirir todo um ambiente de hiperdisponibilidade, por isso é necessária a expertise do licitante nesta área com a solução de recuperação de desastres e alta disponibilidade com a ferramenta ofertada. “A concepção da solução integrada relaciona-se com a proposta de identificar um fornecedor, que se obrigue a produzir um resultado eficiente, satisfatório e adequado para atender						

	determinada necessidade. Assim, o fornecedor assumirá o dever de produzir a conjugação de equipamentos e soluções, implementando os serviços correspondentes à necessidade do Contratante. Nesse caso, o dever do fornecedor não reside na mera tradição de equipamentos, nem no fornecimento de soluções. Cabe-lhe entregar um conjunto de bens e serviços em perfeita operação...” (Marçal Justen Filho, Comentários à lei de licitações e contratos administrativos. 11ª ed. São Paulo: Dialética, 2005. p.217). A compra de um pacote em fornecimento global garante a autarquia a aquisição de equipamentos e software com trabalho em perfeito sincronismo evitando problemas com compatibilidade e acionamento de assistência técnica ou suporte desnecessariamente. Assim, levando em consideração todos os eventos inesperados e que acarretaram grandes prejuízos citados neste edital, faz-se necessário otimizar o custo e o prazo de implantação prevendo para este projeto a entrega de uma solução global.
ATESTADO DE CAPACIDADE TÉCNICA NA HABILITAÇÃO	Apresentar na habilitação ATESTADO DE CAPACIDADE TÉCNICA emitido por pessoa jurídica de direito público ou privado, que comprove o fornecimento de materiais compatíveis com o objeto licitado. Será permitido a apresentação de mais de um atestado de capacidade técnica.
COMPROVAÇÃO DE QUALIFICAÇÃO TÉCNICA.	NECESSIDADE DE BASE EQUIVALENTE: Nos termos do artigo 37, inciso XXI, da CF, é plenamente cabível a exigência de comprovação de experiência da licitante, indispensável e pertinente à garantia do cumprimento das obrigações da Administração. Objetiva-se neste contexto, de requerer tais atestados e/ou certificados, não apenas garantir a capacidade técnica teórica, mas de obter a garantia mais adequada de que, na escala em que se está contratando os serviços e/ou equipamentos, este irá se comportar na prática conforme planejamento.
CATÁLOGOS E FOLDER	Deverá ser apresentado no envelope junto à proposta comercial, marca, modelo, catálogo, folder ou folheto, de todos os equipamentos e soluções propostas onde conste de maneira clara as características dos equipamentos cotados. NÃO SERÃO ACEITOS PROSPECTOS MONTADOS.

5. VISITA TÉCNICA

A visita técnica não é obrigatória para as empresas participantes, porém poderá ser realizada visita ao local com agendamento prévio para conhecer as instalações.

Contatos para agendamento:

(31) 9 8699-2756 - Sérgio Pereira dos Santos (Chefe de Setor)

(31) 3562-4113 - TI

6. DAS OBRIGAÇÕES DA CONTRATADA

A CONTRATADA, no cumprimento deste Contrato, obriga-se a:

a) Cumprir todas as determinações, as ordens verbais ou escritas dos responsáveis pela CONTRATANTE, quando o serviço e/ou materiais não atenderem às normas técnicas e legais estabelecidas;

b) Manter atualizados todos os documentos exigidos na fase de habilitação;

c) Credenciar prepostos para representá-la permanentemente junto a CONTRATANTE, com a incumbência de resolver todos os assuntos relativos à execução do Contrato;

d) Entregar todos os materiais conforme descritos no item 4 deste documento;

e) Garantir a troca dos materiais não conformes e ou danificados por fabricação ou transporte;

f) Entregar todos os materiais descritos no item 4 deste documento de uma só vez obedecendo aos prazos especificados neste termo.

7. DAS OBRIGAÇÕES DA CONTRATANTE

A CONTRATANTE, no cumprimento deste Contrato, obriga-se a:

a) Prestar todas as informações e dados relacionados ao objeto ora contratado sempre que se fizer necessário ao cumprimento deste Contrato;

b) Colocar à disposição funcionário(s) especializado(s) para orientações e fiscalização do Contrato;

c) Efetuar o pagamento devido no prazo determinado.

8. DA DOTAÇÃO ORÇAMENTÁRIA

A dotação orçamentária necessária à realização das despesas decorrentes do objeto desta licitação consta do Orçamento da Autarquia, a saber:

PROJ. CONSTR. AMPL. OBRAS INFRAEST. GESTÃO DA ADM GERAL SAAE.
17 512 1711 3.030 44.90.52.00

OP. MANUT. AÇÕES DE GESTÃO ADM GERAL SAAE.
17 512 1711 4.030 33.90.40.00

9. DO VALOR ESTIMADO

Conforme exigência legal foi realizada pesquisa de preços de mercado junto a empresas do ramo do objeto, sendo apurado para essa despesa o valor médio estimado de R$ 362.980,00 (Trezentos e sessenta e dois mil novecentos e oitenta reais) estando inclusos neste valor todos os impostos, taxas, tarifas e encargos.

10. DO ACOMPANHAMENTO E FISCALIZAÇÃO

Conforme o disposto no Artigo 67 da Lei nº 8666/93, a execução do Contrato deverá ser acompanhada e fiscalizada pelo Chefe do Setor Tecnologia da Informação, sendo representado pelo servidor - Sr. Sergio Pereira dos Santos.

11. DO LOCAL DA ENTREGA

Os materiais deveram ser entregues no escritório central do SAAE Itabirito, situado na Rua Rio Branco, número 99, Centro no Município de Itabirito-MG, **no horário de 08h00min as 12h00min**, onde a Comissão designada para recebimento dos materiais procederá à conferência e recebimento dos materiais e/ou produtos.

12. DO PRAZO PARA ENTREGA

A contratada deverá entregar os materiais no prazo máximo de **45 (quarenta e cinco)** dias corridos contados da emissão e recebimento da Nota de Empenho.

13. DO RECEBIMENTO

O recebimento dos materiais será realizado após aprovação e aceite da Fiscalização, sendo que a CONTRATADA será responsabilizada pela garantia dos materiais na forma da Lei e nos limites desta especificação técnica.

14. DAS CONDIÇÕES DE PAGAMENTO

O pagamento será realizado em **até 10 (dez) dias corridos** após a emissão e aceite da Nota Fiscal, através de **boleto bancário** ou **depósito bancário** em conta corrente, sendo que a **CONTRATADA** deverá fornecer o nº da agência e nº da Conta Bancária para a efetuação do depósito. As notas fiscais deverão estar em conformidade com a Nota de Empenho, devendo ser emitidas dentro dos parâmetros legais, acompanhada de cópia da **CND** (Certidão Negativa de Débitos relativa aos Tributos Federais e a Dívida Ativa da União) e do **CRF** (Certificado de Regularidade do FGTS) da **CONTRATADA** e todas as incidências fiscais que sobre ela possam recair, condições estas indispensáveis para a efetuação do pagamento.

Sérgio Pereira dos Santos
Chefe de setor

Nilson José França e Souza
Gerente Administrativo

saae
Itabirito-MG