PREGÃO ELETRÔNICO Nº 11/2020

(Processo nº. 2822/20)

“Contratação de empresas para fornecimento de licenças, suporte técnico em servidor e ambiente DATACENTER”.

O Prefeito Municipal de Vacaria, no uso de suas atribuições legais e de conformidade com a Lei nº 8.666 de 21/06/93, e suas alterações, Lei nº 10.520 de 17/07/02, Decreto Municipal nº 50 de 12/08/05 e Lei Complementar nº 123/06 de 14/12/06 e suas alterações, torna público, para conhecimento dos interessados que se encontra aberta, licitação, por meio da utilização de recursos de tecnologia da informação – internet, sob a modalidade de PREGÃO ELETRÔNICO, tipo MENOR PREÇO por lote, para contratação de empresa para fornecimento de licenças, suporte técnico em servidor e ambiente DATACENTER.

Data: 24/06/2020;

Início de recebimento das propostas no sistema eletrônico: 08hs do dia 08/06/2020;

Limite para recebimento de propostas no sistema: 09hs:00min dia 24/06/2020;

Abertura das propostas: 09hs:01min do dia 24/06/2020;

Início da sessão de disputa de preços: 24/06/2020, às 09hs e 02min;

Do tempo de disputa: Será de 30 (trinta) minutos, acrescido do tempo aleatório;

A critério do pregoeiro poderá ser aberta a disputa de vários lotes de forma simultânea.

O certame será realizado através do aplicativo “Pregão On Line” do Portal Eletrônico do Bannisul SA, conforme Acordo de Cooperação Técnica firmado, pelo seguinte endereço eletrônico www.pregaoonlinebanrisul.com.br. As empresas que desejarem participar do referido Pregão devem acessar o referido sítio, necessitando estar credenciadas junto a Seção de Cadastro da CELIC (Central de Licitações/RS), pelo sítio www.celic.rs.gov.br e fazer o CFE ou CRC para a habilitação.

Formalização de consultas:

E-mail: licita@vacaria.rs.gov.br

Fone/fax: 054-32316410.

Endereço Ramiro Barcelos, nº 915, Centro, CEP 95200-061, cidade de Vacaria/RS.

Nesta data e horário, será iniciada a sessão de abertura dos envelopes contendo as propostas, pelo pregoeiro nomeado na portaria nº 03/2020 e sua Comissão de Apoio, observado o horário oficial de Brasília/DF.

Este edital, devido a sua peculiaridade, é aberto a todas as empresas beneficiadas pela LC 123/06, no que tange a licitações, não se fazendo vantajoso a sua exclusividade.

COMO PARTICIPAR? Deverá ser criado um “**LOGIN** e **SENHA**” no site do portal de pregão Bannisul (www.pregaoonlinebanrisul.com.br) para acessar os editais dos órgãos.

ONDE PARTICIPAR? Com o login e senha criados, deverá ser acessado o site [pregaoonlinebanrisul](http://pregaoonlinebanrisul.com.br), procurar o edital do Município de Vacaria/RS e proceder o anexo da **proposta** e demais procedimentos do edital e site. A sessão será on line no mesmo site.

E A HABILITAÇÃO? Você deverá providenciar, **antes da abertura**, o CFE ou CRC ou, caso o edital possibilite, apresentar, no dia, toda a documentação do edital, caso sagre-se vencedor.

1 - OBJETO, JUSTIFICATIVA E SUAS ESPECIFICAÇÕES:

1.1. O presente procedimento licitatório destina-se à contratação de empresa especializada em suporte técnico em servidor e ambiente DATACENTER, bem como fornecimento de licenças, para atender as necessidades da Central de Processamento de Dados do Município de Vacaria/RS, tudo conforme descrição mínima do lote **no anexo II** (modelo de confecção da proposta) e **II.1 termo de referência** deste edital, **podendo ser cotado igual ou superior**. Em caso de discordância existente entre as especificações do objeto da licitação descritas no Pregão Online Barrisul e as especificações constantes neste edital, prevalecerão às últimas.

1.2 – A empresa deverá possuir, em seu quadro de funcionários, profissionais aptos na área de programação, manutenção e gestão de servidor, vide anexo II.1, para entender e atender as necessidades do Executivo Municipal.

1.3 – O descumprimento das cláusulas deste edital, memorial descritivo, sujeitarão a empresa a desclassificação/inabilitação/rescisão contratual, independentemente de multa e sanções previstas no item 10 deste edital.

2 - DA APRESENTAÇÃO DOS ENVELOPES:

Após declaradas vencedoras no sítio pela internet, as participantes/licitantes vencedoras, deverão encaminhar via e-mail (licita@vacaria.rs.gov.br), no prazo máximo de 01 (uma) hora da comunicação do pregoeiro, após encerrada a disputa, a documentação conforme consta na cláusula de HABILITAÇÃO, com posterior encaminhamento do original ou cópia autenticada no prazo de **03 (três) dias úteis**, a contar do encerramento da sessão que julgou vencedora, através de **SEDEX** (Setor de Licitações, Rua Ramiro Barcelos, 915, Centro, CEP 95.200-061), o conteúdo de HABILITAÇÃO e PROPOSTA, através de 02 (dois) envelopes com as seguintes indicações externas:

No primeiro envelope

Ao Município de Vacaria/RS
Setor de Licitações

Pregão Eletrônico n.º 11/2020

Abertura: (dia, mês, ano e horário)

Envelope n.º 01 - PROPOSTA DE PREÇOS (VALORES FINAIS – ASSINADA)

Licitante: (denominação social completa da empresa e n.º do CNPJ) Fone/E-mail:

No segundo envelope

Ao Município de Vacaria
Setor de Licitações

Pregão Eletrônico n.º 11/2020

Abertura: (dia, mês, ano e horário)

Envelope n.º 2 – DOCUMENTAÇÃO (EXIGIDA PELO EDITAL ITEM 4) Licitante:

(denominação social completa da empresa e n.º do CNPJ) Fone/E-mail:

2.1. CONDIÇÕES GERAIS DE PARTICIPAÇÃO:

2.1.2 Poderão participar da presente licitação os interessados que estejam cadastrados e habilitados junto à sessão de Cadastro da CELIC – Central de licitações do Estado, sito à Av. Farrapos, 151 – Porto Alegre ou www.celic.rs.gov.br, vide, também, www.compras.rs.gov.br e www.pregaoonlinebarrisul.com.br, e que atenderem a todas as exigências constantes deste

edital e seus anexos, sendo que o não atendimento de qualquer das condições implicará a inabilitação do licitante ou a desclassificação de sua proposta.

2.1.3 Não poderão participar deste Pregão: Empresas que se encontrarem em processo de falência, de dissolução ou liquidação, que estejam punidas com suspensão temporária de participar em licitações e impedidas de contratar com a Prefeitura Municipal de Vacaria; Licitantes tenham sido declaradas inidôneas para licitar ou contratar com a administração Pública, Direta ou Indireta, Federal, Estadual (vide Lei Estadual nº 11.389/99) ou Municipal; Licitantes cujos objetos sociais não sejam compatíveis com objeto deste Pregão; Não será admitida a participação de empresas em consórcio.

2.1.4 Como requisito para participação no pregão, em campo próprio do sistema eletrônico, o licitante deverá manifestar o pleno conhecimento e atendimento às exigências de habilitação previstas no Edital.

2.1.4.1 O não atendimento ao presente item ensejará a desclassificação da proposta no sistema, com automático impedimento da participação na disputa.

2.1.5 A participação dos interessados, no dia e hora fixados no preâmbulo deste Edital, dar-se-á por meio da digitação da senha privativa da licitante e subsequente encaminhamento da proposta de preços exclusivamente por meio eletrônico.

2.1.6 A informação de dados para acesso deve ser feita na página inicial do site www.pregaoonlinebanrisul.com.br.

2.1.7 A simples participação neste pregão implica aceitação de todos os seus termos, condições, normas, especificações e detalhes.

2.1.8 Recomenda-se a leitura integral e acurada deste Edital, pois a apresentação de proposta implica aceitação tácita dos seus termos, tendo em vista a decadência do direito de impugnação, não cabendo à licitante alegação de desconhecimento das normas que regem o presente certame e a contratação.

2.1.9 Por ser o Pregão uma modalidade de licitação com características similares à de leilão, em que o calor da competição pode levar a fortes emoções e, em consequência, a redução indiscriminada nos lances ofertados, é prudente que o ofertante tenha, previamente em mente, todos os custos e lucros que possam constituir o lance mínimo real a que se poderá alcançar, pois não serão aceitas desistências posteriores devido a imprudência, ficando os licitantes, nestas condições, sujeitos às penalidades legais e editalícia.

2.2 CREDENCIAMENTO

2.2.1 O credenciamento dos licitantes dar-se-á pelas atribuições de chave de identificação, e de senha pessoal e intransferível para acesso ao sistema obtidos junto à seção de Cadastro da Central de Licitações do Estado – CELIC (www.celic.rs.gov.br).

2.2.1.1 O credenciamento junto ao provedor do sistema implica a responsabilidade legal do licitante ou seu representante legal e a presunção de sua capacidade técnica para realização das transações inerentes ao pregão eletrônico.

2.2.2 O uso da senha de acesso ao sistema eletrônico é de inteira e exclusiva responsabilidade da licitante, incluindo qualquer transação efetuada diretamente ou por seu representante, não cabendo ao provedor do sistema ou ao Município de Vacaria, promotor da licitação, responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.

2.2.3 Todos os custos decorrentes da elaboração e apresentação de propostas serão de responsabilidade do licitante, bem assim, pelas transações que forem efetuadas em seu nome no sistema eletrônico ou de eventual desconexão sua.

2.2.4 A perda da senha ou quebra do sigilo deverão ser comunicadas imediatamente à seção de Cadastro da CELIC, para imediato bloqueio de acesso.

2.2.5 No caso de perda da senha, deverá ser solicitada nova senha na Seção de Cadastro da CELIC.

3 - DA PROPOSTA - Envelope n.º 01

3.1. A licitante é responsável por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras suas propostas e lances. A proposta deverá ser encaminhada eletronicamente e nos moldes do Anexo II.

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

3.3. Nos preços propostos e naqueles que, por ventura, vierem a serem ofertados através de lances, deverão estar inclusos todos os custos necessários ao fornecimento/execução do objeto licitado, bem como todos os impostos, encargos trabalhistas, previdenciários, fiscais, comerciais, taxas, tarifas, fretes, seguros e quaisquer outros que incidam ou venham incidir sobre o mesmo. Será desconsiderada qualquer reivindicação de pagamento adicional devido a erro ou má interpretação de parte da licitante.

3.4. Até a data e horário previstos no preâmbulo do edital, as licitantes poderão retirar ou substituir a proposta. Após o horário previsto, as ofertas serão de exclusiva responsabilidade da licitante, não lhe assistindo o direito de pleitear qualquer alteração dos mesmos, sob alegação de erro, omissão ou qualquer outro pretexto.

3.5. As propostas apresentadas nesta licitação terão prazo de validade mínima de 60 (sessenta) dias a contar da data da sessão pública do pregão.

3.6. A partir da publicação/divulgação deste edital no sítio informado, poderão ser encaminhadas as propostas dos licitantes interessados. A proposta de preços prevista no edital deverá ser encaminhada em formulário eletrônico específico, devendo constar preço unitário e total.

3.7. Os licitantes arcarão com todos os custos decorrentes da elaboração e apresentação de suas propostas.

3.8. A partir da data e horário previsto no preâmbulo deste edital, poderão ser encaminhadas às propostas de preços, exclusivamente por meio eletrônico, mediante o

credenciamento na CELIC e participação no sistema do site www.pregaoonlinebanrisul.com.br de acordo, também com o anexo II deste edital.

3.9. Deverão preencher campo próprio com a manifestação de que tem pleno conhecimento e atendimento às exigências de habilitação previstas no edital.

DEVERÁ SER ANEXADA JUNTO À PROPOSTA, SOB PENA DE DESCLASSIFICAÇÃO:

3.10. *Cópia de declaração de que cumpre com os requisitos de habilitação, sob as penas da lei (vide anexo V);*

3.11. A informação dos dados para acesso deve ser feita na página inicial do site www.pregaoonlinebanrisul.com.br

3.12. As propostas deverão atender os termos deste edital quanto à descrição do objeto, prazo de entrega e as condições de pagamento. Os Produtos devem estar com as especificações em conformidade com o que foi solicitado.

3.13. As propostas deverão conter preço unitário e total por item licitado, devendo conter de forma expressa na proposta a **marca** e o prazo de validade. **Será aceito apenas duas casas decimais após a vírgula, por exemplo: (R\$ 0,78).**

3.14. A apresentação da proposta pela licitante implica aceitação deste edital, bem como das normas legais que regem a matéria e, se por ventura a licitante for declarada vencedora, ao cumprimento de todas as disposições contidas nesta licitação.

3.15. As propostas que não atenderem os termos deste Edital serão **desclassificadas**.

3.16. O upload da proposta no site www.pregaoonlinebanrisul.com.br será de total responsabilidade do licitante, o qual deverá se certificar de que a proposta anexada seja visível e legível em sua integralidade, sem necessidade de qualquer ação do pregoeiro que não seja abrir e imprimir o arquivo, sob pena de desclassificação.

4- DA HABILITAÇÃO - Envelope n.º 2 (VER CFE ou CRC)

4.1. Primeiramente os interessados deverão efetuar credenciamento eletrônico prévio na CELIC. A habilitação no Pregão eletrônico dar-se-á por meio de uma, das três formas abaixo, constantes do item 4.2, encaminhados na forma deste edital.

4.1.1. As microempresas, empresas de pequeno porte e demais beneficiados pela Lei Complementar 123/06, no que tange a licitações, que quiserem usufruir dos benefícios da referida LC, deverão declarar no campo INFORMAÇÕES ADICIONAIS, a sua condição de beneficiada (o). Caso não o faça, será tratada (o) sem os privilégios da citada LC.

4.1.2. No caso de beneficiada, nos termos da LC 123/2006, que possua alguma restrição na documentação referente à regularidade fiscal, esta deverá ser mencionada, como ressalva, na supracitada declaração.

4.2. - Para fins de habilitação, o autor da melhor proposta deverá encaminhar via sistema a habilitação, no prazo máximo de 01 (uma) hora da comunicação do pregoeiro, após encerrada a disputa, com posterior

encaminhamento do original ou cópia autenticada no prazo de 03 (três) dias úteis a contar da sessão do pregão, nos moldes do item 02 deste edital, um dos seguintes documentos:

a) Certificado de Fornecedor do Estado do Rio Grande do Sul (CFE, www.celic.rs.gov.br), válido, com todos os documentos exigidos válidos e/ou regularizados, acompanhado da qualificação técnica 4.6; **OU:**

b) Certificado de Registro Cadastral do Município de Vacaria (CRC), válido, com todos os documentos exigidos válidos e/ou regularizados, acompanhado da qualificação técnica 4.6.

4.2.1. Se algum documento estiver vencido, a licitante poderá providenciar com antecedência junto ao Setor de Licitações (CRC), CELIC (CFE), no mesmo prazo de confecção, as atualizações que se fizerem necessárias no Certificado de Fornecedor/Cadastral ou anexar os documentos atualizados, junto do referido certificado. A preferência pela habilitação é com o CRC ou CFE, mas será aceito o envio de toda a documentação.

Os Certificados compõem-se dos seguintes documentos:

4.3. Habilitação Jurídica:

I - Ato Constitutivo, Estatuto ou Contrato Social e suas alterações, se houver, devidamente registrado na Junta Comercial, em se tratando de sociedades comerciais, acompanhado, no caso de sociedade por ações, de documento de eleição de seus atuais administradores; inscrição do ato constitutivo, no caso de sociedade civil, acompanhada de prova da diretoria em exercício; ou decreto de autorização, em se tratando de empresa ou sociedade estrangeira em funcionamento no País, em vigor;

a) A licitante poderá apresentar a versão consolidada, acompanhada das alterações posteriores, caso houver. Somente serão habilitadas as licitantes que apresentarem, além de toda a documentação exigida, o ramo pertinente ao objeto desta licitação no seu objeto social;

b) Cópia da cédula de identidade dos representantes legais;

II - **Declaração da licitante**, sob as penas da lei, de que cumpre com o artigo 7.º, inciso XXXIII, da Constituição Federal (conforme Anexo III), assinada por representante legal da empresa;

III - **Declaração da licitante**, sob as penas da lei, de que não foi declarada INIDÔNEA/IMPEDIDA de licitar ou contratar com a Administração Pública (conforme Anexo IV), assinada por representante legal da empresa;

4.4. Habilitação Fiscal e Trabalhista:

I - Prova de inscrição no Cadastro Nacional de pessoas Jurídicas – **CNPJ**.

II - Prova de Regularidade com a **Fazenda Federal**, em vigor;

III - Prova de Regularidade com a **Fazenda Estadual**, em vigor;

IV - Prova de Regularidade com a Fazenda Municipal, em vigor, conforme legislação tributária do Município expedidor da empresa que ora se habilita para este certame;

IV.a - A Certidão deverá expressar, de forma clara e objetiva, a situação da licitante em relação à totalidade dos tributos (Mobiliários e Imobiliários) a cargo da Fazenda Municipal. Mesmo no caso de a empresa não possuir imóvel em seu nome, ou seja, isenta de qualquer imposto municipal, deverá ser apresentada certidão emitida pela Fazenda Municipal;

V - Prova de Regularidade junto ao Fundo de Garantia por Tempo de Serviço, FGTS, em vigor, demonstrando a situação regular ao cumprimento dos encargos sociais instituídos por lei;

VI – Prova de Regularidade trabalhista, de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de Certidão Negativa de Débitos Trabalhistas – CNDT;

Obs.: as certidões mencionadas I a VI que não expressem o prazo de validade, deverão ter a data de expedição não superior a 30 (trinta) dias;

4.4.1. A licitante que se enquadrar no regime diferenciado e favorecido, previsto na Lei Complementar n.º 123/06, e que possuir restrição na comprovação da regularidade fiscal e ou trabalhista, dispostas nos subitens 4.4.I a 4.4.VI deste edital, terá sua habilitação condicionada à regularização da documentação, pagamento ou parcelamento do débito, em até 5 (cinco) dias úteis a contar da data da sessão pública que a declarar detentora da melhor oferta.

a - O prazo citado no subitem 4.4.1 deste edital, poderá ser prorrogado uma única vez, por igual período, a critério da Administração, desde que seja requerido pela licitante durante o transcurso do respectivo prazo.

b - O benefício de que trata o subitem 4.4.1 deste edital, não eximirá a licitante de apresentar na sessão pública todos os documentos exigidos para efeito da comprovação da regularidade fiscal e ou trabalhista, ainda que possua alguma restrição.

c - A não regularização da documentação, no prazo fixado, implicará decadência do direito à contratação, sem prejuízo das penalidades previstas no subitem 10.2.1III, deste edital.

4.5. HABILITAÇÃO ECONÔMICO-FINANCEIRA

4.5.1. Certidão Negativa de Falência ou Concordata, expedida pelo distribuidor da Sede da pessoa jurídica ou de filial, com data de emissão de no máximo 60 (sessenta) dias anteriores à data da abertura do edital;

4.5.2. Apresentação de Balanço patrimonial e Demonstrações Contábeis, do último exercício social, em conformidade com as normas contábeis, já exigível e apresentado na forma da Lei, para comprovação da boa situação da empresa, com **termo de abertura e encerramento**, devidamente registrados, no local e na forma que a lei exige para cada caso, exemplo (rol exemplificativo):

- a) Carimbo (junta comercial, etc.); ou
- b) Em se tratando de Sociedades por Ações (SA), publicação em órgão de imprensa oficial, de acordo com a lei; ou

c) prova de que a autenticação pela Junta Comercial foi realizada pelo Sistema Público de Autenticação digital (SPED) – Termo de Autenticação – Recibo de Entrega.

Observação: É vedada substituição do balanço por balancete ou balanço provisório, podendo aquele ser atualizado por índices oficiais quando encerrado há mais de 03 (três) meses da data de apresentação da proposta. As empresas deverão apresentar seus balanços na forma que prescreve a lei e normas contábeis.

Ila - A comprovação da boa situação financeira far-se-á com base nos indicadores a seguir relacionados:

$$LC = \frac{AC}{PC} \text{ igual ou superior a } \underline{0,8} \qquad LG = \frac{AC + ARLP}{PC + PELP} \text{ igual ou superior a } \underline{0,8}$$

$$SG = \frac{AR}{PC + PELP} \text{ igual ou superior a } \underline{1,2}$$

Legenda:

LC = Liquidez Corrente
AC = Ativo Circulante
PC = Passivo Circulante
LG = Liquidez Geral

ARLP = Ativo Realizável a Longo Prazo
PELP = Passivo Exigível a Longo Prazo
SG = Solvência Geral
AR = Ativo Real

Composição do Ativo Real - Ativo Total diminuído dos valores de duplicatas descontadas, despesas do exercício seguinte, empréstimo a coligadas/sócios/acionistas/diretores e Ativo Diferido.

Classificação final das empresas - As licitantes que apresentarem, **no mínimo, dois dos três indicadores**, iguais ou superiores aos estabelecidos neste item, obterão a classificação econômico-financeira, as demais serão inabilitadas.

Tendo em vista o que consta da Instrução Normativa da Receita Federal Brasileira nº 787/07, o SICAF (Sistema de Cadastramento Unificado de Fornecedores) foi alterado, no sentido de permitir que o Balanço Patrimonial do exercício 2008, referente ao ano-calendário de 2007, fosse considerado válido até maio de 2009. O **Balanço de 2020**, para este certame, ano-calendário de 2019, será considerado válido até maio de 2021, e assim sucessivamente, independente do tipo de constituição da pessoa jurídica, tudo como forma de garantir a isonomia entre os participantes de licitações e as contratações da Administração Pública. Esse procedimento, que foi adotado por alguns Estados da Federação, nos parece correto e será adotado também neste certame, decorrentes das modificações realizadas pela Instrução Normativa IN nº 1.420/13 e alterações supervenientes, da Receita Federal.

Justificativa dos índices adotados:

LC – Liquidez Corrente: Calculada a partir da razão entre os direitos a curto prazo da empresa (Caixas, bancos, estoques, clientes) e as dívidas a curto prazo (Empréstimos, financiamentos, impostos, fornecedores). No Balanço estas informações são evidenciadas respectivamente como Ativo Circulante e Passivo Circulante. A partir do resultado obtido podendo fazer a seguinte análise: Resultado da Liquidez Corrente: Maior que 0,8: Resultado que demonstra folga no disponível para uma possível liquidação das obrigações; Se igual a 0,8: Os valores dos direitos e obrigações a curto prazo são equivalentes; Se menor que 0,8: Não há disponibilidade suficiente para quitar as obrigações a curto prazo, caso fosse preciso.

LG - Liquidez Geral: Este índice leva em consideração a situação a longo prazo da empresa, incluindo no cálculo os direitos e obrigações a longo prazo. Estes valores também são obtidos no balanço patrimonial.

SG – Solvência Geral: Este índice mostra a capacidade de pagamento da empresa tomando como base o seu ativo total, “quanto maior melhor”.

4.6 – Habilitação Técnica:

I - Comprovação de aptidão do licitante, (em nome da empresa), através da apresentação de atestado de prestação de serviço, emitido pelo adquirente (pessoa jurídica de direito público ou privado), de complexidade equivalente ou superior ao objeto da presente licitação. **Define-se como complexidade equivalente, para fins deste certame, a execução de serviços de manutenção de servidor e ambiente DATACENTER.**

Justificativa: Justifica-se o atestado tendo em vista que os equipamentos que compõe o ambiente DATACENTER são de custo elevado e, além disso, a interrupção por imprudência e/ou imperícia podem causar prejuízos incalculáveis ao Município.

II - Declaração, sob as penas da lei, de que possui/possuirá, no momento da contratação, as condições estabelecidas no edital para execução do objeto, principalmente no que tange ao

pessoal técnico especializado que executará o objeto, item 07 (sete) do memorial descritivo, anexo II.1, devendo ser os mesmos da execução.

Obs. Em caso de troca de pessoal, a licitante deverá apresentar substitutos de igual ou superior qualificação.

4.6. Os interessados deverão efetuar credenciamento eletrônico e estar previamente cadastrados na CELIC através do Certificado de Fornecedor do Estado – CFE, www.celic.rs.gov.br ou CRC.

4.7. Os documentos exigidos nos subitens 4.3 ao 4.5 poderão ser substituídos por um dos seguintes certificados:

a) Certificado de Fornecedor do Estado do Rio Grande do Sul (CFE, www.celic.rs.gov.br), válido, com todos os documentos exigidos válidos e/ou regularizados, acompanhado da qualificação técnica 4.6; **OU:**

b) Certificado de Registro Cadastral do Município de Vacaria (CRC), válido, com todos os documentos exigidos válidos e/ou regularizados, acompanhado da qualificação técnica 4.6.

4.8. A substituição prevista no item anterior somente será aceita se o Certificado de Fornecedor/Cadastral estiver dentro de seu período de vigência, com todos os documentos exigidos atualizados. Se algum documento estiver vencido, a licitante deverá providenciar com antecedência junto ao Setor de Licitações para o (CRC), e CELIC para o (CFE), no mesmo prazo de confecção, as atualizações que se fizerem necessárias no Certificado de Fornecedor/Cadastral ou anexar os documentos atualizados, junto do referido certificado.

4.9. Os documentos deverão ser apresentados em original, ou por qualquer processo de cópia autenticada por cartório oficial competente, ou por servidor da Prefeitura de Vacaria/RS (no caso de CRC). Os documentos expedidos pela *Internet* deverão ser apresentados com o respectivo endereço eletrônico (link) e/ou código verificador de autenticidade para consulta e confirmação de sua veracidade.

4.10. Todos os documentos apresentados deverão ser correspondentes unicamente à matriz ou à filial da empresa que ora se habilita para este certame licitatório. Os documentos devem ser em nome de uma única empresa (razão social e CNPJ), salvo os documentos que valem para ambas.

4.11. Todos os documentos deverão conter data de expedição de até 30 (trinta) dias da abertura do certame, salvo disposição em contrário neste edital.

4.12. As empresas que emitirem declarações, ou utilizarem declarações de outras empresas, como requisitos necessários para as fases de classificação, habilitação e pagamento, ou qualquer outro procedimento do processo licitatório, se responsabilizarão pela autenticidade contida nas mesmas, sob as penas descritas em lei e edital.

5 - DA PARTICIPAÇÃO DAS BENEFICIADAS PELA LC 123/06 E ALTERAÇÕES:

5.1. Nos termos dos artigos 42 e 43 da Lei Complementar nº 123, de 14/12/2006 e alterações, as microempresas, empresas de pequeno porte e demais beneficiadas deverão apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal e trabalhista, conforme item 5.1.2 deste Edital, mesmo que esta apresente alguma restrição.

5.1.1. Havendo alguma restrição na comprovação da regularidade fiscal e trabalhista, será assegurado o prazo de 05 (cinco) dias úteis, contados a partir da data da sessão pública que a declarar detentora da melhor oferta, prorrogáveis por igual período, uma única vez, a critério da Administração Pública, para a regularização da documentação, pagamento ou parcelamento do débito, e emissão de eventuais certidões negativas ou positivas com efeito de certidão negativa.

5.1.2. O benefício de que trata o subitem 5.1.1 deste edital, não eximirá a licitante de apresentar na sessão pública todos os documentos exigidos para efeito da comprovação da regularidade fiscal e trabalhista, ainda que possua alguma restrição.

5.2. A não regularização da documentação no prazo previsto no subitem 5.1.1, implicará decadência do direito à contratação, sem prejuízo das sanções previstas no edital, subitem 14.2.1, III, sendo facultado à Administração convocar para nova sessão pública os licitantes remanescentes, na ordem de classificação, para contratação, ou revogar a licitação.

5.3. Encerrada a sessão de lances, será verificada a ocorrência do empate ficto, previsto no art. 44, § 2.º, da Lei Complementar n.º 123/06, sendo assegurada, como critério do desempate, a preferência de contratação para as microempresas e empresas de pequeno porte e demais beneficiadas. Entende-se como empate ficto, aquelas situações em que as propostas apresentadas pelas licitantes sejam iguais ou superiores em até 05% (cinco por cento) à proposta de menor valor e desde que a melhor oferta inicial não seja de uma beneficiada.

5.4. Ocorrendo o empate, proceder-se-á da seguinte forma:

5.4.1. A licitante beneficiada pela Lei Complementar nº 123/06, detentora da proposta de menor valor, será convocada para apresentar no prazo de até 05 (cinco) minutos, após o encerramento dos lances, nova proposta, inferior àquela considerada de menor preço, situação em que será adjudicado em seu favor o objeto licitado;

5.4.2. Não ocorrendo a contratação da beneficiada, na forma do subitem 5.4.1, serão convocadas as remanescentes que porventura se enquadrem na hipótese do subitem 5.3, na ordem classificatória, para o exercício do mesmo direito;

5.4.3. No caso de equivalência dos valores apresentados pelas licitantes beneficiadas que se encontre no intervalo estabelecido no subitem 5.3, será realizado sorteio entre elas para que se identifique àquela que primeiro poderá apresentar melhor oferta.

5.4.4. Na hipótese da não contratação nos termos previstos no item 5.3 e 5.4, se existir mais de um licitante com propostas idênticas, será dada preferência aos bens/serviços, pela ordem:

- Produzidos no País;
- Produzidos ou prestados por empresas brasileiras; e
- Produzidos ou prestados por empresas que invistam em pesquisa e no desenvolvimento de tecnologia no país;

5.5. Na hipótese da não contratação nos termos anteriores, o objeto licitado será adjudicado em favor da proposta originalmente vencedora do certame. Em caso de permanecer o empate será escolhido o vencedor através de sorteio, realizado em ato público, no setor de licitações da Prefeitura Municipal de Vacaria em dia e horário a ser fixado em ata dando ciência a todos os licitantes.

5.6. O disposto nos subitens 5.3 e 5.4, não se aplicam às hipóteses em que a proposta de menor valor tiver sido apresentada por licitante enquadrada no regime da Lei Complementar n.º 123/06.

5.7. A licitante beneficiada pela LC nº 123/06, mais bem classificada, será convocada para apresentar nova proposta no prazo máximo de 5 (cinco) minutos após o encerramento dos lances, sob pena de preclusão.

5.8. A licitante que usufruir dos benefícios de que trata a LC 123/2006 deverá apresentar, na forma da lei, declaração de que se enquadra como beneficiada da referida LC 123/06 e que não se encontra em nenhuma das situações do § 4º do art. 3º da LC 123/2006, nos moldes do anexo I, enviando conforme item 02 deste edital. A declaração não será necessária caso conste em campo específico dos certificados CFE ou CRC.

6 DA SESSÃO DO PREGÃO

6.1 A partir do horário previsto no edital, terá início a sessão pública do pregão eletrônico, onde o Pregoeiro verificará as propostas apresentadas, classificando aquelas que atendam ao Edital e desclassificando aquelas que não estejam em conformidade com os requisitos estabelecidos.

6.1.1 O sistema ordenará, automaticamente, as propostas classificadas.

6.2 Somente poderá participar da rodada de lances, a licitante que anteriormente tenha encaminhado proposta eletrônica de preços.

6.2.1 Os representantes das empresas beneficiadas pela LC nº 123/06, no que tange a licitações, deverão declarar em campo próprio do sistema, quando do envio da proposta inicial, que se enquadram nessa categoria. A ausência da declaração naquele momento, quando for um edital exclusivo as beneficiadas, impossibilitará a participação no Pregão.

6.3 Aberta à etapa competitiva, os representantes dos licitantes deverão estar conectados ao sistema para participar da sessão de lances. A cada lance ofertado o participante será imediatamente informado de seu recebimento e respectivo horário de seu registro e valor.

6.4 O licitante poderá oferecer lances sucessivos, observado o horário fixado e somente serão aceitos lances cujos valores forem inferiores ao último lance que tenha sido anteriormente registrado no sistema.

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

6.6 Durante o transcurso da sessão pública, os participantes serão informados, em tempo real, do valor do menor lance registrado. O sistema não identificará o autor dos lances aos demais participantes.

6.7 No caso de desconexão com o pregoeiro, no decorrer da etapa de lances, se o sistema eletrônico permanecer acessível as licitantes, os lances continuarão sendo recebidos, retomando o pregoeiro quando possível, sua atuação no Pregão, sem prejuízo dos atos realizados.

6.8 Quando a desconexão persistir por tempo superior a 10 (dez) minutos, a sessão do Pregão será suspensa e terá reinício após comunicação expressa aos participantes.

6.9 A etapa de lances da sessão pública será encerrada mediante aviso de fechamento iminente dos lances, emitido pelo sistema eletrônico, após o que transcorrerá o período de tempo de até 30 (trinta) minutos, aleatoriamente, determinado também pelo sistema eletrônico, findo o qual será automaticamente encerrada a recepção de lances.

6.10 Facultativamente, o pregoeiro poderá encerrar a sessão pública mediante encaminhamento de aviso de fechamento iminente dos lances e subsequente transcurso do prazo de até 30 minutos, findo o qual será encerrada a recepção de lances. Neste caso, antes de anunciar o vencedor, o pregoeiro poderá encaminhar, pelo sistema eletrônico, contraproposta diretamente ao proponente que tenha apresentado o lance de menor preço, para que seja obtido preço melhor, bem como decidir pela sua aceitação.

6.11 O sistema informará a proposta de menor preço imediatamente após o encerramento da etapa de lances, quando for o caso, após negociação e decisão pelo pregoeiro acerca da aceitação do lance de menor valor.

6.12 A classificação das propostas se dará em ordem crescente dos preços apresentados, sendo considerada vencedora a proposta que cotar o MENOR PREÇO.

6.13 Encerrada a etapa de lances da sessão pública, o licitante detentor da melhor oferta deverá remeter via sistema, caso o Pregoeiro não solicite o anexo por email, em até 01 (uma) hora, cópia do Certificado de Fornecedor do Estado – **CFE** ou Certificado de Registro Cadastral - **CRC** e demais documentos exigidos no instrumento convocatório habilitação técnica, com posterior encaminhamento do original ou cópia autenticada no prazo máximo de 03 (três) dias úteis (via SEDEX, conforme item 02), contados da data da sessão pública. Os documentos originais deverão ser entregues na Rua Ramiro Barcelos, 915, Centro, Setor de Licitações, Vacaria – RS, CEP 95200-061.

6.14 Se a proposta ou lance de menor valor não for aceitável, ou se o fornecedor desatender às exigências habilitatórias, o pregoeiro examinará a proposta ou o lance subsequente, verificando a sua compatibilidade e a habilitação do participante, na ordem de classificação e assim sucessivamente, até a apuração de uma proposta ou lance que atenda o edital. Também nesta etapa o pregoeiro poderá negociar com o participante para que seja obtido melhor preço.

6.15 Concluída a etapa de lances, ou negociação quando houver, será aberto prazo, a critério do pregoeiro, para a empresa vencedora realizar o *upload* da sua proposta final no sistema. A pedido da empresa e por decisão do pregoeiro, tal prazo poderá ser prorrogado.

6.15.1 A proposta deverá atender a todos os requisitos do item 03 do edital.

6.15.2 No caso da proposta não ser aceita, o Pregoeiro convocará a próxima empresa conforme a ordem de classificação da etapa de lances.

6.16 Aceita a proposta, abrir-se-á o prazo para manifestação de intenção de recurso contra a classificação da empresa.

6.17 Não havendo recurso ou não sendo aceita a intenção do mesmo, dar-se-á prosseguimento à fase de habilitação, com a apresentação dos documentos e da proposta final original.

6.18 Satisfeito o atendimento das exigências fixadas neste Instrumento e inexistindo manifestação recursal, o Pregoeiro adjudicará o objeto da licitação ao licitante vencedor, com a posterior homologação do resultado pela autoridade superior competente.

7 IMPUGNAÇÃO AO EDITAL E RECURSOS

7.1. Até 03 (três) dias úteis antes da data fixada para recebimento das propostas, qualquer pessoa poderá impugnar o ato convocatório do Pregão. E, antes da abertura, solicitar esclarecimentos.

7.1.1. A impugnação não possui efeito suspensivo e caberá ao pregoeiro, auxiliado pelos responsáveis pela elaboração do edital e dos anexos, decidir sobre a impugnação no prazo de dois dias úteis, contado da data de recebimento da impugnação. A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo pregoeiro, nos autos do processo de licitação.

7.1.2. Acolhida a impugnação contra o edital, será definida e publicada nova data para realização do certame.

7.2. Dos atos do pregão caberá recurso que dependerá de manifestação do licitante ao final da sessão pública, em formulário específico, manifestando sua intenção com registro da síntese das suas razões, devendo juntar memoriais relacionados à intenção manifestada no prazo de 03 (três) dias, ficando os demais licitantes desde logo intimados para apresentar contra razões em igual número de dias, que começarão a contar do término do prazo do recorrente.

7.3. O recurso contra decisão do Pregoeiro não terá efeito suspensivo e o seu acolhimento importará a invalidação apenas dos atos insuscetíveis de aproveitamento;

7.4. A falta de manifestação imediata e motivada do licitante, de intenção de recurso, importará na decadência do direito de recurso, estando o pregoeiro autorizado a adjudicar o objeto ao licitante vencedor.

7.5. Não serão aceitos como recursos as alegações e memoriais que não se relacionem às razões indicadas pelo licitante na sessão pública.

7.6. Decididos os recursos e constatada a regularidade dos atos procedimentais, a Autoridade competente homologará o resultado da licitação.

7.7. O acolhimento de recurso importará a invalidação apenas dos atos insuscetíveis de aproveitamento.

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

8 DA ADJUDICAÇÃO E HOMOLOGAÇÃO

8.1 Inexistindo manifestação recursal, o pregoeiro adjudicará o objeto da licitação ao licitante vencedor, com a posterior homologação do resultado pela autoridade superior.

8.2 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.

9 DA CONTRATAÇÃO

9.1 Esgotados todos os prazos recursais, o Município, no prazo de até 60 (sessenta) dias contados da data de entrega dos envelopes, convocará a vencedora para assinar o contrato, **caso o Município não opte pela entrega única**, que deverá firmar a contratação no prazo instituído no subitem 9.1.1 deste edital, sob pena de decair do direito à contratação, sem prejuízo das sanções previstas no subitem 10.2.2.II deste edital.

9.1.1 A licitante vencedora terá o prazo de até 03 (três) dias úteis para assinatura do contrato, contados da data de convocação feita, por escrito, pelo Município.

9.2 O contrato advindo desta licitação entrará em vigor na data da assinatura e vigorará até, quando for o caso, o final (garantia, assistência técnica, validade, entrega, serviço, exercício financeiro), podendo ser prorrogado a critério da administração, ou rescindido por inexecução contratual. Caso o contrato ultrapasse doze meses, o mesmo poderá ser reajustado monetariamente pelo IGP-M/FGV do período, ou outro índice oficial que vier a substituí-lo.

9.3 Caso a licitante vencedora se recuse a assinar o contrato (não se eximindo das sanções do edital), será convocada a segunda classificada, sendo examinada a última oferta válida e verificada a aceitabilidade da proposta, sem prejuízo das sanções cabíveis, e assim, sucessivamente, até a apuração de uma proposta que atenda ao edital. O Pregoeiro poderá negociar para que seja obtido preço melhor, e, após, procederá à habilitação da licitante detentora da melhor oferta.

9.4 A licitante vencedora, antes da assinatura do contrato, deverá, somente se solicitado pelo Município, prestar a garantia nas modalidades previstas, **no valor de 5% (cinco por cento) do valor global do contrato**, consoante artigo 56, *caput*, § 1.º, 2.º e 4.º da lei regradora.

9.4.1 Caso a licitante opte pela **carta de fiança bancária ou seguro garantia**, esta **deverá ser apresentada no seu original** e terá validade por todo o período de execução do contrato.

9.4.2 Caso a licitante optar pelo depósito em moeda corrente, este deverá avisar o Município por escrito, para que possa fornecer a conta.

9.4.3 A garantia prestada será liberada ou restituída, ao término da vigência do contrato, se não utilizada nas formas do artigo 86, parágrafo 3.º da Lei n.º 8.666/93. Contudo, reverterá a garantia a favor do Município, no caso de rescisão do contrato por culpa exclusiva da licitante vencedora, sem prejuízo da indenização por perdas e danos porventura cabíveis.

9.4.4 Se a garantia for prestada em moeda corrente nacional, quando devolvida, deverá sofrer atualização monetária. A garantia será liberada após o recebimento definitivo do serviço.

9.5 O contratado fica obrigado a aceitar nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessárias neste certame em até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

9.6 O Município de Vacaria poderá se utilizar dos benefícios do art. 57 da lei nº 8.666/93, caso tenha interesse.

9.7 O Município designa como responsável pela fiscalização do contrato/recebimento dos itens o Diretor do CPD **Sr. Adimir Gotardo Scudiero, ou outro expressamente designado por este.**

9.8 O contrato a ser assinado terá como base a minuta integrante deste edital (Anexo VI, quando a entrega/execução não for única) e/ou prever garantia.

9.9. Para fins de futuro reajustes e reequilíbrios, a empresa vencedora deverá na contratação apresentar planilha completa de valores unitários adjudicados, desmembrados do valor global, como serviços, mão de obra, licenças, para fins comparativos, ex. de planilha:

Suporte na área de infraestrutura de TI	R\$
Serviço de suporte e Administração do ambiente de segurança firewall e equipamentos de rede	R\$
Extensão de garantia (s)	R\$
Renovação/Ampliação de firewal	R\$
Renovação de licença (s)	
VMware	R\$
Veeam	R\$
(...)	
Atualização e Expansão (ões)	
Switche de Rede	R\$
Switche de Borda	R\$
Access Point	R\$
(...)	

10 – DO RECEBIMENTO / ACEITE DO OBJETO

10.1 O recebimento do objeto licitado será feito provisoriamente e, após as formalidades legais, o **Sr. Adimir Gotardo Scudiero, ou outro expressamente designado por este,** receberão definitivamente, obedecidas às condições especificadas neste edital e seus anexos.

10.2 O período para recebimento definitivo do (s) objeto (s) licitado (s), coincidirá com o prazo estabelecido para pagamento.

10.3 Considerar-se-á adimplido o contrato quando do recebimento definitivo pelo Município de Vacaria do (s) objeto (s) da licitação, na forma do item 10.1 supra.

10.4 Será (ão) rejeitado (s) no todo ou em parte o (s) objeto (s) da licitação, se entregue (s) em desacordo com este edital e contrato cabendo ao contratado todos os ônus decorrentes da rejeição.

10.5 Dentro de 05 (cinco) dias úteis, contados do Recebimento Provisório a área técnica do Município, comprovará o atendimento aos requisitos técnicos e funcionais do produto/serviço e os atributos informados pela Contratada na proposta por ela apresentada na licitação de que decorre este contrato. Na hipótese de o bem se apresentar-se em desacordo com as especificações técnicas e funcionais ofertados pela CONTRATADA, ficará facultado ao CONTRATANTE, rejeitá-lo, rescindindo este Contrato e aplicando à contratada as sanções previstas no presente instrumento para o caso de inadimplemento, ou conferido novo prazo para efetivação da entrega nos termos acordados, sob pena de rescisão e aplicação das penalidades aqui pactuadas.

10.5.1 Uma vez constatado pelo contratante que o bem/serviço entregue, quer no prazo inicial, quer nos prazos por ele conferidos, está em conformidade com as especificações definidas no ato convocatório e/ou na proposta da CONTRATADA, será emitido o Termo de Recebimento Definitivo, configurando-se a efetiva entrega do bem ao CONTRATANTE, para todos os fins e efeitos de direito.

10.5.2 O recebimento provisório ou definitivo não exclui a responsabilidade da CONTRATADA, pela reparação, correção, remoção ou substituição, às suas expensas e no prazo assinalado, do bem/serviço objeto da presente contratação, se esse apresentar vícios, defeitos ou incorreções.

11. DO PAGAMENTO

11.1. Os pagamentos serão efetuados mensalmente, em até 30 dias, após autorização da Secretaria competente (SMGF - CPD), de que os serviços foram efetuados conforme solicitado, com preço fixo.

11.2. Ao emitir a nota fiscal, a empresa deverá fazer constar nos dados, sob pena de retificação: 1 - Município de Vacaria; 2 – Número do edital (**Pregão Eletrônico nº 11/2020**); 3 - Número do (s) item (s) constantes na ordem sequencial do objeto no anexo II; 4 - A especificação do (s) item (s); 5 - Número do (s) empenho (s) correspondente (s), sob pena de ter de refazê-la. Atendem para a confecção da Nota fiscal eletrônica, conforme protocolo ICMS 42/09 e alterações. Dúvidas nfe@sefaz.rs.gov.br. A mesma deverá fazer menção, na Nota Fiscal, de Instituição Bancária, Agência e Conta para os créditos oriundos do fornecimento do material. Qualquer dúvida, entrar em contato com o Setor de Pagamentos pelo fone nº (054) 3231 6415 ou, transmitir via e-mail para o endereço eletrônico – pagamentos@vacaria.rs.gov.br.

11.3. Para fins de adjudicação, homologação e empenho, o preço do lote poderá sofrer, automaticamente, uma pequena variação para menos, resultante da necessidade de ser obtido valor unitário com duas casas decimais, sendo que serão desconsideradas todas as casas posteriores à segunda.

12. DO PRAZO DE EXECUÇÃO:

12.1. O prazo de execução dos serviços será de 12 (doze) meses, podendo ser prorrogado, a critério da Administração, até o limite legal.

13. DA FORMA E DO LOCAL DE EXECUÇÃO:

13.1. Os locais de execução dos serviços estão descritos no anexo II.1.

14. DAS SANÇÕES ADMINISTRATIVAS

14.1 – ADVERTÊNCIA

A penalidade de **ADVERTÊNCIA** poderá ser aplicada nas seguintes hipóteses:

14.1.1. Descumprimento das obrigações assumidas contratualmente ou na licitação, desde que não acarrete prejuízos para a entidade, independentemente da aplicação de multa moratória.

14.1.2. Outras ocorrências que possam acarretar pequenos transtornos ao desenvolvimento dos serviços da entidade, independentemente da aplicação de multa moratória.

14.2. MULTA

A entidade poderá aplicar à licitante ou contratada, multa moratória e multa por inexecução contratual:

14.2.1. MULTA MORATÓRIA

A multa moratória poderá ser cobrada pelo atraso injustificado, entrega/execução em desacordo com o solicitado no objeto ou de prazos estipulados no Edital para os compromissos assumidos.

I - A multa moratória será de 0,50% (cinquenta centésimos por cento) por dia corrido de atraso, sobre o valor da NOTA DE EMPENHO, até o máximo de 05 (cinco) dias de atraso. Após esse prazo, poderá, também, ser rescindido o contrato e/ou imputada à licitante vencedora a pena prevista no item 14.3.1, pelo prazo de até 60 (sessenta meses).

II – A multa moratória será de 0,50% (cinquenta centésimos por cento) pela entrega em desacordo com as exigências do edital, sobre o valor total da NOTA DE EMPENHO, por infração, com prazo de até 05 (cinco) dias consecutivos para a efetiva adequação. Após (duas) infrações e/ou após o prazo para adequação, poderá, também, ser rescindido o contrato e/ou imputada à licitante vencedora a pena prevista no item 14.3.1, pelo prazo de até 60 (sessenta meses).

III – A multa moratória será de 10% (dez por cento), pela não regularização da documentação referente à regularidade fiscal, no prazo previsto neste edital, por parte da licitante detentora da melhor proposta, e poderá, também, ser imputada à licitante vencedora a pena prevista no item 14.3.1, pelo prazo de até 60 (sessenta meses).

14.2.2. MULTA POR INEXECUÇÃO CONTRATUAL

I - A multa por inexecução contratual poderá ser aplicada no percentual de 10% (dez por cento) sobre a respectiva fatura/contratação, acrescida de correção monetária e juros de 12 (doze por cento) ao ano.

II – Em caso de inexecução parcial do contrato/fatura a multa será aplicada sobre o valor do respectivo inadimplemento.

III – Além da multa, poderá ser aplicada a cobrança por prejuízos efetivamente sofridos, desde que restarem comprovados através de processo administrativo especial a relação de causalidade.

IV – O atraso injustificado na assinatura do contrato ou a rescisão do mesmo por culpa da contratada implicará em multa de 10% (dez por cento) sobre o valor total da proposta, até o máximo de 05 (cinco) dias de atraso. Após esse prazo, poderá, também, ser rescindido o contrato e/ou imputada à licitante vencedora a pena prevista no item 14.3.1.

14.3. IMPEDIMENTO DE LICITAR

14.3.1. Nos termos do Art. 7º da Lei nº. 10.520/02, a licitante, sem prejuízo das demais cominações legais e contratuais, poderá ficar, pelo prazo de até 60 (sessenta) meses, impedida de licitar e contratar com a Administração Pública e ter cancelado o Registro Cadastral de Fornecedores do Município de Vacaria, nos casos de:

- a) deixar de entregar ou apresentar documentação falsa exigida para o certame;
- b) retardamento na execução do objeto;
- c) não manutenção da proposta ou lance verbal;
- d) fraude ou falha na execução do contrato.
- e) comportamento inidôneo ou cometer fraude fiscal;

14.4. As penalidades previstas neste Edital poderão ser aplicadas, isoladas ou cumulativamente, sem prejuízos de outras sanções cabíveis, sendo facultado a licitante o prazo de 5 (cinco) dias úteis para a apresentação de defesa prévia, na ocorrência de quaisquer das situações previstas nesta cláusula 14.

15. DA DOTAÇÃO ORÇAMENTÁRIA

04 – (04.01) Secretaria Municipal de Gestão e Finanças

2.015 – Manutenção Secretaria Municipal de Gestão e Finanças

33904000 – Serviços de Tecnologia da Informação e Comunicação - 5672/5686

16. DAS DISPOSIÇÕES GERAIS

16.1. Caso o licitante vencedor não apresente situação regular no ato da assinatura do contrato, ou venha recusar-se a celebrá-lo, injustamente, dentro do prazo estabelecido e na vigência de sua proposta, sujeitar-se-á às sanções cabíveis, reservando-se a Administração, o direito de independente de qualquer aviso ou notificação, renovar a licitação ou convocar os remanescentes.

16.2. Na convocação dos remanescentes, será observada a classificação final da sessão originária do pregão e o disposto nos itens 6.12, 6.13 e 6.15.1, devendo o (s) convocado (s) apresentar (em) os documentos de habilitação cuja validade tenha-se expirado no prazo transcorrido da data da primeira sessão.

16.3. Somente será considerado habilitado o licitante que houver preenchido os requisitos de habilitação na data da primeira sessão e que apresentar, na segunda sessão, os documentos que porventura estiverem vencidos.

16.4. Os concorrentes remanescentes convocados na forma do subitem 16.2 se obrigam a atender a convocação e a assinar o contrato respectivo, no prazo fixado pelo Município, ressalvados os casos de vencimento das respectivas propostas, sujeitando-se às penalidades cabíveis, no caso de recusa ou de não atendimento das condições de habilitação.

16.5. Os proponentes são responsáveis pela fidelidade e legitimidade das informações e dos documentos apresentados em qualquer fase da licitação, inclusive a preparação e apresentação das propostas.

16.6. O Município de Vacaria, na pessoa de sua Pregoeira ou da Autoridade Superior, reserva-se o direito de proceder ao exame das informações e comprovantes, por visitas “in loco” ou por outras medidas adequadas.

16.8. Caso seja necessária à diligência do Pregoeiro para verificação da proposta ou habilitação do licitante, a sessão poderá ser interrompida ou suspensa por ordem do Pregoeiro, que determinará o reinício dos trabalhos em momento oportuno, após a realização das diligências necessárias.

16.9. É facultado ao Pregoeiro relevar erros formais ou simples omissões em quaisquer documentos, para fins de habilitação e classificação dos proponentes, desde que sejam irrelevantes, não firam o entendimento da proposta e o ato não acarrete violação aos princípios básicos da licitação.

16.10. É facultado ainda ao pregoeiro convocar os licitantes para quaisquer esclarecimentos porventura necessários ao entendimento de suas propostas; que uma vez intimados, deverão fazê-lo no prazo determinado pelo Pregoeiro, sob pena de desclassificação/inabilitação.

16.11. A administração do Município de Vacaria poderá anular ou revogar, parcialmente ou na sua totalidade este Pregão, observadas as disposições legais pertinentes.

16.12. Os casos omissos serão resolvidos pelo Pregoeiro, que a eles aplicará as disposições da Lei 10.520/02 e da Lei 8666/93, e disposições subjetivas, se couber, desde que não venha conflitar com a referida legislação.

16.13. Fica desde logo esclarecido, que todos os participantes deste Pregão, pelo simples fato de nele licitarem, sujeitam-se a todos os seus termos, condições, normas, especificações e detalhes, comprometendo-se a cumpri-lo fielmente, independentemente de qualquer manifestação escrita ou expressa.

16.14. O desatendimento de exigências formais não essenciais não importará no afastamento da licitante, desde que sejam possíveis as aferições das suas qualificações e as exatas compreensões da sua proposta, durante a realização da sessão pública de Pregão, e desde que não comprometa o interesse do município, bem como a finalidade e a segurança da futura contratação.

16.15. As normas que disciplinam este Pregão serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse do município e a segurança da contratação.

16.16. A proponente que vier a ser contratada ficará obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, dentro do limite legalmente admitido na Lei 8666/93, sobre o valor inicial do contrato.

16.17. Após a apresentação da proposta, não caberá desistência, salvo por motivo justo decorrente de fato superveniente e aceito pelo Pregoeiro.

16.18. Fica eleito o Foro da comarca de Vacaria para dirimir quaisquer dúvidas oriundas deste Pregão.

16.19. Fazem parte deste edital:

- Anexo I - Declaração de Enquadramento para ME e EPP (beneficiada)
- Anexo II - Proposta (Paradigma da proposta eletrônica) e II.1 Memorial Técnico
- Anexo III - Declaração de Cumprimento ao Artigo 7.º, Inciso XXXIII, da CF.
- Anexo IV - Declaração de Idoneidade.
- Anexo V - Declaração de que cumpre com os requisitos de habilitação
- Anexo VI - Minuta de Contrato (Quando não for entrega única).

16.20. Para maiores informações:

a) Setor de licitações, Edital: (54) 3231-6410, Ronerson Bueno, Lisiane de Oliveira;

- b) **Informações de Cadastro - CRC:** (54) 3231-6410, João Alfredo Leite;
- c) **Fac-símile Setor de Licitações:** (54) 3232-2426
- d) **Email Setor:** licita@vacaria.rs.gov.br
- e) **Email Cadastro:** licitacadastro@vacaria.rs.gov.br
- f) **Endereço:** Ramiro Barcelos, 915, centro, CEP 95.200-000.

Obs.: Informações por telefone, somente no horário de externo, das 10h às 16h, de segunda a sexta-feira, em dias úteis.

Vacaria, 03 de junho de 2020.

Amadeu de Almeida Boeira
Prefeito Municipal

ANEXO I

(MODELO)

AO (À) PREGOEIRO (A)
REF. PREGÃO ELETRÔNICO/201.....

DECLARAÇÃO DE ENQUADRAMENTO PARA ME E EPP (BENEFICIADOS PELA LC 123/06 E ALTERAÇÕES)

(Razão Social)....., por meio de seu Responsável Legal e Contador ou Técnico Contábil, declara, sob as penas da lei, que:

- a) enquadra-se na situação de microempresa ou empresa de pequeno porte (beneficiado);
- b) o valor da receita bruta anual da sociedade, no último exercício, não excedeu o limite fixado nos incisos I e II, art. 3.º, da Lei Complementar n.º 123/06;
- c) não se enquadra em quaisquer das hipóteses de exclusão relacionadas no art. 3.º, § 4.º, incisos I a X, da mesma Lei.

Por ser expressão da verdade, firmamos a presente.

....., em de de 2020.

(Assinatura) _____

RAZÃO SOCIAL:

CNPJ:

NOME DO REPRESENTANTE LEGAL:

(PROCURADOR JUNTAR PROCURAÇÃO OU CREDENCIAMENTO)

CPF:

(Assinatura) _____

NOME (completo, contador ou técnico contábil):

CPF:

Nº DE INSCRIÇÃO CRC:

Ressalva (se houver).....

ANEXO II

PREGÃO ELETRÔNICO N.º 11/2020

PROPOSTA (Paradigma da Eletrônica – www.pregaoonlinebanrisul.com.br)

RAZÃO SOCIAL: CNPJ-MF:
FONE/FAX: (.....)..... EMAIL:

LOTE	QUANT	DESCRIÇÃO (solicitações mínimas)	VALOR MENSAL ESTIMADO
1	01	O presente certame licitatório tem como objeto a contratação de empresa especializada em prestação de serviços técnicos e suporte na área de infraestrutura de Tecnologia da Informação e atualização tecnológica, conforme especificações do Termo de Referência, anexo II.1. Além disso, visa também a prestação de serviços corretivos, preventivos, evolutivos e de manutenção do ambiente, a prestação de serviços de consultoria e a elaboração de projetos de melhorias e modernização tecnológicas, visando garantir a disponibilidade, segurança e alto desempenho na infraestrutura do ambiente de tecnologia de informação do Município de Vacaria/RS.	R\$ 22.310,00
Valor Estimado Anual GLOBAL do Lote R\$ 267.720,00 , podendo ser prorrogado, a critério da Administração, até o limite legal.			

Decremento mínimo do lance R\$ 1.000,00

Declaro que cumpro com as condições de habilitação;
Validade da Proposta 60 dias.

Local, Data _____

Nome completo e assinatura do representante legal da empresa
VIDE ITEM 3.10, 4.6 E 9.9

ANEXO II.1

TERMO DE REFERÊNCIA

MEMORIAL TÉCNICO DESCRITIVO

1. DO Objeto

1. O presente tem como objeto a contratação de empresa especializada em prestação de serviços técnicos e suporte na área de infraestrutura de Tecnologia da Informação, conforme a especificação e seus Anexos.

1.1. Detalhamento do Objeto:

1.1.1. A prestação de serviços corretivos, preventivos, evolutivos e de manutenção do ambiente, a prestação de serviços de consultoria e a elaboração de projetos de melhorias e modernização tecnológica visando garantir disponibilidade, segurança e alto desempenho na infraestrutura do ambiente de Tecnologia da Informação do MUNICÍPIO DO VACARIA demandados por intermédio da emissão de “Ordem de Serviço” (OS).

1.1.2. A cada período mínimo de 04 (quatro) meses enviar responsável técnico do projeto para alinhar novas demandas e ajustes necessários para a boa execução dos serviços.

1.2. A prestação de serviços técnicos e suporte na área de infraestrutura de Tecnologia da Informação contempla a execução das seguintes atividades:

1.2.1.1. Proposição de estratégias, alternativas e exemplos de implementação considerando o investimento e seu retorno;

1.2.1.2. Proposição de requisitos para projetos visando à otimização, segurança e alto desempenho do ambiente;

1.2.1.3. Proposição de novas tecnologias para o ambiente considerando o investimento e seu retorno visando à otimização, segurança e alto desempenho;

1.2.1.4. Análise de vulnerabilidades do ambiente; elaboração de proposta de política de segurança e plano de continuidade de negócio (PCN) conforme boas práticas da ITIL V3;

1.2.1.5. Realização e manutenção da documentação do mapeamento dos processos de trabalho e proposição de otimizações, conforme boas práticas da ITIL V3;

1.2.1.6. Criação e acompanhamento de indicadores para promover controle sobre as atividades de suporte e infraestrutura;

1.2.1.7. Prestação de suporte técnico com atendimento presencial e remoto **conforme Anexo II.2 - Descrição do Ambiente;**

1.2.1.8. Instalação, configuração e manutenção de servidores, Storage e ativos de rede conforme **Anexo II.2 - Descrição do Ambiente;**

1.2.1.9. Instalação, configuração, operação e manutenção de sistema automatizado de monitoração dos equipamentos do ambiente de TI, especialmente: disponibilidade, registro de ocorrências, estatísticas de atendimentos, controle de configuração dos equipamentos corporativos;

1.2.1.10. Realização de atividades de testes de servidores, acompanhamento da manutenção e atualização dos recursos dos equipamentos corporativos;

1.2.1.11. Implementação e manutenção de redes TCP/IP e redes sem fio no ambiente;

1.2.1.12. Administração e gerência de rede local (plano de endereçamento, gerenciamento de VLANs);

1.2.1.13. Planejamento, instalação, configuração, reconfiguração, ajustes do sistema de backup, seus recursos e administração da solução de backup dos servidores virtualizados e físicos conforme **Anexo II.2 - Descrição do Ambiente;**

1.2.1.14. Gerenciamento, atualização e aplicação de patches de segurança;

1.2.1.15. Criação, instalação, configuração, manutenção e administração de serviço de virtualização de servidores conforme **Anexo II.2 - Descrição do Ambiente;**

1.2.1.16. Instalação, configuração, manutenção e administração do serviço de armazenamento de dados em ambiente SAN (Storage Area Network);

1.2.1.17. Prover serviços de monitoramento de alertas para o MUNICÍPIO DO VACARIA;

1.2.1.18. Fornecer sistema automatizado, aplicações, softwares ou ferramentas a serem utilizados para este monitoramento e gerenciamento, conforme as boas práticas da ITIL V3;

1.2.1.19. Efetuar análise de desempenho do ambiente, com periodicidade trimestral, mensal ou conforme demanda de necessidade, visando identificar possíveis “gargalos” ou pontos de saturação que prejudiquem o alto desempenho do ambiente;

1.2.1.20. Emitir relatórios com diagnósticos, indicações e medidas preventivas para solução de problemas que impeçam a otimização e alto desempenho do ambiente - *CAPACITY PLANNING* - conforme as boas práticas da ITIL V3;

1.2.1.21. Disponibilizar sistema automatizado ou ferramentas para a monitoração e gerenciamento dos equipamentos, aplicações e serviços críticos do ambiente de TI, especialmente: disponibilidade, incidentes, alerta de limites, alerta para chamados, consumo de utilização, estatísticas, relatórios, gráficos de disponibilidade e utilização visando à otimização e alto desempenho do ambiente;

2. Da execução dos serviços

2.1. A prestação de serviços consiste em serviços técnicos especializados para o suporte nível 2 e nível 1 e aos administradores de TI do MUNICÍPIO DO VACARIA, com atendimento presencial e/ou remoto;

2.2. Os serviços serão demandados por intermédio da emissão de “Ordem de Serviço” (OS), numeradas sequencialmente, com prazos, produtos bem caracterizados e locais de execução dos serviços definidos.

2.3. Os serviços serão solicitados gradativamente, de acordo com as necessidades do MUNICÍPIO DO VACARIA, não ficando a mesma obrigada a utilizar o total de unidades de serviço técnico estimadas.

2.4. Os prazos para início das atividades serão definidos pelo MUNICÍPIO DO VACARIA, a partir da data de assinatura do contrato, em reunião técnica para o planejamento das atividades e emissão das Ordens de Serviços.

2.5. O MUNICÍPIO DO VACARIA emitirá quantas Ordens de Serviços forem necessárias durante a vigência do contrato, de acordo com seu planejamento executivo.

2.6. Os processos definidos para prestação de serviço de infraestrutura e suporte técnico devem ser rigorosamente cumpridos, atendendo aos critérios para abertura e fechamento de incidentes, escalonamento para Gestão de Problemas e respectivo fechamento, bem como as interfaces com os processos de Gestão de Mudanças, Configuração e Entrega em sistema automatizado de gestão a ser implantado pela CONTRATADA no MUNICÍPIO DO VACARIA;

2.7. Caberá integralmente à CONTRATADA estruturar e dimensionar sua equipe de trabalho para atender satisfatoriamente o NSR (Nível de Serviço Requerido), resguardando-se ao MUNICÍPIO DO VACARIA revisar e definir os perfis e qualificações necessários para o desempenho das atividades objeto da contratação;

2.8. Os colaboradores da CONTRATADA envolvidos na prestação de serviço de infraestrutura e suporte técnico aos funcionários do CPD do MUNICÍPIO DO VACARIA deverão estar cientes, claramente comunicados dos comportamentos, responsabilidades, atividades, ações e autoridades concedidas à pessoa ou grupo designado.

2.9. Não deverão ser realizados atendimentos presenciais que não estejam formalmente designados, escalonados e documentados, salvo nos casos previstos de priorização, onde o registro do incidente deverá, mesmo que a posteriori, ser realizado no sistema automatizado de gestão a ser implantado pela CONTRATADA no MUNICÍPIO DO VACARIA;

2.10. As acomodações e a infraestrutura física (mesas, computadores, telefones, etc.), e lógica para o Suporte nas dependências do CONTRATANTE serão de responsabilidade do MUNICÍPIO DO VACARIA.

3. Prazos de Execução dos Serviços

3.1. Os prazos e definição do tamanho dos serviços técnicos e suporte na área de Infraestrutura de Tecnologia da Informação contratados utilizarão a Hora Homem (HH).

3.2. O prazo é o tempo decorrido desde a emissão da Ordem de Serviço até o final do processo de homologação técnica do serviço, com a emissão do Termo de Aceite Técnico.

4. Da Garantia dos Serviços Entregues

4.1. Fica estabelecido como garantia o prazo de 60 dias da execução dos serviços pela CONTRATADA, apresentado no Termo de Recebimento de Serviço, para correção de defeitos gerados por este serviço, mesmo após o encerramento do contrato.

4.2. Durante o prazo de garantia estabelecido a CONTRATADA deverá manter canal de comunicação por telefone, e-mail ou sistema disponibilizado, atendendo aos seguintes critérios:

4.2.1. As correções deverão ser documentadas e encaminhadas ao MUNICIPIO DO VACARIA conforme as boas práticas da ITIL V3 para os processos de gerenciamento de incidentes, requisições, configurações e mudanças.

4.2.2. A documentação deverá ser atualizada segundo as alterações corretivas realizadas e gerada nova versão da documentação no prazo de 3 (três) dias úteis após o atendimento.

4.2.3. As correções oriundas da solicitação deverão ser testadas conforme procedimentos estabelecidos e homologadas antes da atualização no Ambiente de Produção.

4.2.4. Os horários para atualização do Ambiente de Produção deverão ocorrer de forma a minimizar impactos aos usuários estabelecidos em comum acordo.

4.3. Terminado o prazo de garantia estabelecido, a manutenção do sistema será realizada através de Ordem de Serviço específica para manutenção e correção.

4.4. Caso seja constatada a impossibilidade de cumprimento do prazo estabelecido em decorrência da abrangência do problema, a CONTRATADA deverá apresentar e o novo prazo proposto, submetendo-o ao MUNICIPIO DO VACARIA para aprovação.

5. do NÍVEL DE SERVIÇO REQUERIDO

5.1. O Nível de Serviço Requerido - NSR - tem por objetivo estabelecer as diretrizes para a entrega de serviços de alta qualidade para os serviços técnicos e suporte na área de infraestrutura de Tecnologia da Informação, de acordo com as necessidades do MUNICIPIO DO VACARIA.

5.2. A CONTRATADA reconhece que o não atendimento do Nível de Serviço Requerido - NSR - contratado e os prazos para a execução dos serviços técnicos e suporte na área de infraestrutura de Tecnologia da Informação podem resultar em impacto adverso e relevante nos negócios e nas operações do MUNICIPIO DO VACARIA.

5.3. O NSR a ser executado pela CONTRATADA a contar do instante do registro de chamado realizado pelo MUNICIPIO DO VACARIA deve obedecer aos prazos especificados nesta tabela:

Problemas Reportados	Horas para:			Período Abrangido	Severidade
	Atendimento	Solução	Máximo		
Parada total de serviços de rede ou serviços críticos	8	12	20	24X7	4-Muito Crítica
Parada parcial de serviços	8	16	24	24X7	3-Crítica

Anomalias ou problemas nos servidores	3	TS	PDU	8X5	2-Severa
Solicitação de tuning, configurações, melhorias de performance e similares	PDU	PDU+1	PDU+2	8X5	1-Normal

Convenção:

- a. 24X7: é o atendimento a ser prestado das 00h00min às 23h59min, de segunda-feira a domingo.
- b. 8X5: é o atendimento a ser prestado das 09h00min às 18h00min, de segunda-feira a sexta-feira, excetuando-se os feriados.
- c. PDU - Próximo Dia Útil: é o atendimento a ser prestado no próximo dia útil após o chamado.
- d. TS - Turno Seguinte: é o atendimento a ser prestado no "turno seguinte" ao do chamado, em dias e horários comerciais.

5.4. Em se tratando de serviço severidade 3 (crítico) ou 4 (muito crítico) o atendimento por parte da CONTRATADA, quando da necessidade de atendimento no MUNICIPIO DO VACARIA, será compreendido das 00h00min às 23h59min, de segunda-feira a domingo, caracterizando-se atendimento 24x7. Estes serviços críticos serão estabelecidos em reunião técnica após assinatura do contrato para o planejamento das atividades, deverão ser realizados durante as 24 (vinte e quatro) horas nos sete dias da semana (segunda a domingo - 24X7), colocados ata técnica a ser elaborada em comum acordo entre o MUNICIPIO DE VACARIA e a CONTRATADA.

OBS: O histórico de atendimentos exigidos neste horário diferenciado, no ambiente do MUNICIPIO DE VACARIA desde 2015, não ultrapassa uma ocorrência a cada dois meses ou seis eventos por ano.

5.5. No caso de serviço de severidade 1 ou 2 o atendimento por parte da CONTRATADA, quando da necessidade de atendimento no MUNICIPIO DE VACARIA, será compreendido das 09h00min às 18h00min, de segunda-feira a sexta-feira, caracterizando-se atendimento 8X5;

5.6. Em caso de parada parcial da rede ou serviços críticos (severidade 3) a CONTRATADA se obriga a atender os chamados num prazo máximo de 12 (doze) horas a partir do chamado, tendo 12 (doze) horas para resolução do problema a partir da chegada do técnico no MUNICIPIO DO VACARIA. Caso o técnico não chegue dentro do prazo estipulado, começará a contar o tempo para a resolução do problema. Portanto, o tempo total para a chegada do técnico e a resolução do problema não pode ultrapassar o prazo máximo de 24 (vinte e quatro) horas;

5.7. Em caso de parada total ou de serviços críticos (severidade 4) a CONTRATADA se obriga a atender os chamados num prazo máximo de 8 (oito) hora a partir do chamado, tendo 12 (doze) horas para resolução do problema a partir da chegada do técnico no MUNICIPIO DE VACARIA.

5.8. A CONTRATADA deverá ter a opção de abrir chamado Técnico diretamente ao Fabricante, caso em que os prazos de atendimento ao chamado serão os mesmos que regulam este "NSR".

5.9. Além de cumprir o Nível de Serviço Requerido - NSR - para fins de aceitação dos serviços prestados, deverão ser atendidos os demais critérios e condições estabelecidas neste Termo de Referência, tal como obrigações contratuais.

6. DA Propriedade Intelectual e Direito Autoral

6.1. Todos os produtos gerados na vigência do contrato serão de propriedade do CONTRATANTE. Isso inclui todos os dados, documentos e elementos de informação pertinentes à tecnologia de concepção, desenvolvimento, fixação em suporte físico de qualquer natureza e aplicação, tais como produtos de software, programas-fonte, classes e componentes, relatórios, diagramas, fluxogramas, modelos e arquivos. A regra está em conformidade com o artigo 111 da Lei nº 8.666/93, com a Lei nº 9.609/98, que dispõe sobre propriedade intelectual de programa de computador e com a Lei nº 9.610/98, que dispõe sobre direito autoral, sendo vedada a comercialização, a qualquer título, destes por parte da CONTRATADA.

6.2. A utilização de soluções ou componentes proprietários da CONTRATADA ou de terceiros na construção dos programas ou quaisquer artefatos relacionados ao presente contrato, que possam afetar a propriedade do produto, deve ser formal e previamente autorizada pelo MUNICIPIO DO VACARIA.

7. EQUIPE TÉCNICA NECESSÁRIA PARA PRESTAÇÃO DOS SERVIÇOS e qualificação:

7.1. A CONTRATADA se compromete a alocar, em todos os serviços, profissionais com perfis e qualificações adequados, mantendo ao longo da vigência do contrato todas as condições apresentadas em sua habilitação e qualificação no processo licitatório, a comprovação de sua equipe técnica deve ser através de vínculo empregatício, comprovado através da carteira de trabalho ou ficha de registro de empregado,

7.2. A qualificação dos profissionais técnicos para execução dos serviços deverá ser comprovada por meio da apresentação da certificação abaixo.

7.2.1. Técnico para Suporte Ambiente de Servidores - presencial ou remoto – certificação Microsoft;

7.2.2. Técnico para Suporte Ambiente de Virtualização - presencial ou remoto – certificação VCP VMware Certified Professional.

7.2.3. Certificação Oficial do Fabricante Extreme Networks de Rede LAN, WLAN e Gerenciamento – presencial ou remoto.

7.2.4. Certificação Oficial do Fabricante Palo Alto de administrador “PCNSA -Palo Alto Networks Certified Network Security Administrator”.

7.3. A CONTRATADA deverá selecionar, designar e manter profissionais cuja qualificação esteja em conformidade com os tipos de serviços descritos no objeto do edital.

7.4. A CONTRATADA se compromete a garantir a alocação de profissionais devidamente capacitados para solucionar problemas relacionados à prestação de serviços e ocorrências nos sistemas, incluindo os que exijam a presença física nas dependências do MUNICIPIO DO VACARIA.

8. serviços de suporte técnico do firewall e equipamentos de rede (switches)

8.1. A Contratada deverá prestar serviços de garantia, assistência técnica e suporte técnico, em todos os produtos listados, pelo período de 48 (quarenta e oito) meses, a contar da data de assinatura do contrato:

8.2. Manutenção corretiva de hardware dos produtos fornecidos, incluindo a reparação de eventuais falhas, mediante a substituição de peças e componentes por outros de mesma especificação, e originais, de acordo com os manuais e normas técnicas específicas para os mesmos;

8.3. Atualizações corretivas e evolutivas de software e firmware, incluindo pequenas atualizações de release, reparos de pequenos defeitos (bug fixing patches);

8.4. Ajustes e configurações conforme manuais e normas técnicas do fabricante;

8.5. Demais procedimentos destinados a recolocar os equipamentos em perfeito estado de funcionamento;

8.6. Assistência técnica especializada para investigar, diagnosticar e resolver incidentes e problemas relativos à solução;

8.7. Fornecimento de informações e esclarecimentos de dúvidas sobre instalação, administração, configuração, otimização ou utilização dos produtos listados no contrato.

8.8. A suporte de 48 (Quarenta Oito) meses;

- 8.9.** Os serviços de assistência técnica e suporte técnico deverão ser prestados 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano, remotamente ou se necessário no local onde os equipamentos se encontrarem instalados (on-site), por técnicos devidamente habilitados e credenciados pelo fabricante, com nível de certificação compatível com as atividades a serem executadas, e sem qualquer ônus adicional.
- 8.10.** A Contratada e ou o fabricante da solução deverão disponibilizar canal de atendimento para abertura de chamados técnicos, mediante número 0800. Adicionalmente, poderá ser disponibilizado serviço de abertura de chamado via site ou e-mail.
- 8.11.** Para cada chamado técnico, a Contratada deverá informar um número de controle (protocolo) para registro, bem como manter histórico de ações e atividades realizadas.
- 8.12.** Os chamados técnicos serão classificados por criticidade, de acordo com o impacto no ambiente computacional, conforme abaixo:
- 8.12.1.** Prioridade Alta: Sistema indisponível ou com severa degradação de desempenho;
- 8.12.2.** Prioridade Média: Sistema disponível, com mau funcionamento, que importe baixa degradação de desempenho ou comprometimento em um de seus elementos que importe em risco para a disponibilidade do sistema.
- 8.12.3.** Prioridade Baixa: Sistema disponível, sem impacto em seu desempenho ou disponibilidade; consultas gerais sobre instalação, administração, configuração, otimização, troubleshooting ou utilização.
- 8.13.** O nível de severidade será informado pelo CONTRATANTE no momento da abertura do chamado.
- 8.14.** O CONTRATANTE poderá escalar os chamados para níveis mais altos ou baixos, de acordo com a criticidade do problema. Nesse caso, os prazos de atendimento e de solução, bem como os prazos e percentuais de multa, serão automaticamente ajustados para o novo nível de prioridade.
- 8.15.** Os serviços de suporte e assistência técnica deverão atender, respectivamente, os seguintes prazos de atendimento inicial e solução do incidente:
- 8.15.1.** Os chamados de Prioridade Alta deverão ser atendidos em até 02 horas (duas) horas e solucionados em até 8 (oito) horas;
- 8.15.2.** Os chamados de Prioridade Média deverão ser atendidos em até 4 (quatro) hora e solucionados em até 24 (vinte e quatro) horas;
- 8.15.3.** Os chamados de Prioridade Baixa deverão ser atendidos em até 8 () horas e solucionados em até 48 (quarenta e oito) horas.
- 8.16.** O prazo de atendimento começará a ser contado a partir da hora do acionamento do suporte a partir da Central de Atendimento da CONTRATADA.
- 8.17.** Entende-se por início de atendimento a hora de chegada do técnico de suporte ao local onde está o produto ou a intervenção remota.
- 8.18.** Caso não seja possível a intervenção remota, seja por impossibilidade de comunicação, seja por impossibilidade de análise do problema, um técnico da CONTRATADA deverá realizar o atendimento on-site, obrigatoriamente.
- 8.19.** Entende-se por término do atendimento a ocorrência de um dos eventos abaixo relacionados:
- 8.19.1.** Solução definitiva; Solução de contorno e escalonamento do chamado para um nível de menor severidade, mediante prévia aprovação do CONTRATANTE;
- 8.19.2.** Solução de contorno e escalonamento do chamado para o fabricante, em caso de correção de falhas (bugs) ou da liberação de novas versões e patches de correção, desde que comprovados pelo fabricante da solução. Para esses problemas, a CONTRATADA deverá restabelecer o ambiente, através de uma solução paliativa, informando o CONTRATANTE em um prazo máximo de 48 (quarenta e oito) horas quando a solução definitiva será disponibilizada.
- 8.20.** A solução definitiva deverá ser disponibilizada no prazo máximo de 60 (sessenta) dias úteis, no caso da necessidade de criação de um patch/fix.
- 8.21.** O encerramento do chamado será dado por servidor da Contratante na conclusão dos serviços, após a disponibilização da solução para uso em perfeitas condições de funcionamento no local onde está instalada.
- 8.22.** Caberá aos técnicos do fabricante ou da empresa autorizada pelo fabricante identificar os componentes, peças e materiais responsáveis pelo mau funcionamento dos produtos/equipamentos.

- 8.23.** Em caso de falhas irrecuperáveis de hardware ou impossibilidade de solução pela assistência técnica, a CONTRATADA deverá providenciar a troca por equipamento idêntico.
- 8.24.** Casos em que se tornará obrigatória a substituição de equipamentos pela CONTRATADA:
- 8.24.1.** Falha de hardware e/ou software que interrompa o funcionamento do equipamento por mais de 12 (doze) horas consecutivas;
- 8.24.2.** Inoperância do equipamento, por tempo superior a 2 (duas) horas, em 2 (duas) ocasiões separadas por, no máximo, um período de 60 (sessenta) dias corridos.
- 8.24.3.** Por questão de segurança, os equipamentos e softwares nunca deverão ser removidos das dependências da CONTRATANTE sem a remoção de dados ou regras sigilosas.
- 8.24.4.** No caso de troca do produto por defeito, não haverá qualquer ônus adicional para o CONTRATANTE.
- 8.25.** Relativamente à manutenção corretiva de hardware e software:
- 8.25.1.** Os componentes danificados deverão ser substituídos, entregues, instalados e configurados, de modo a deixar o equipamento em perfeitas condições de uso e com todas as funcionalidades operacionais, nas dependências do CONTRATANTE, nos prazos de solução estabelecidos acima, sem a cobrança de quaisquer custos adicionais (frete, seguro, etc.);
- 8.25.2.** Concluída a manutenção, a CONTRATADA fornecerá ao CONTRATANTE, documento em que conste a identificação do chamado técnico, data e hora de início e término da assistência técnica, descrição dos serviços executados, indicação da peça e/ou componente eventualmente substituído, assim como relato referente às condições inadequadas ao funcionamento do equipamento ou sua má utilização, fazendo constar a causa e as medidas para a sua correção.
- 8.25.3.** Durante todo o período de contrato, a CONTRATADA atualizará ou disponibilizará para download, sem ônus adicionais para o CONTRATANTE, os softwares necessários ao funcionamento dos produtos fornecidos, fornecendo as novas versões ou releases lançados. Os softwares tratados neste item incluem vacinas de antivírus/anti-malware, assinaturas do filtro de conteúdo web, software de gerenciamento, firmwares de bios e drivers.
- 8.26.** A atualização ou disponibilização para download deverá ocorrer em um prazo máximo de 15 (quinze) dias úteis, contados da data de lançamento da nova versão ou release. Caso a nova versão ou release seja disponibilizada para download, deverá a CONTRATADA prestar o suporte necessário para a instalação e configuração da mesma.
- 8.27.** Qualquer manutenção e/ou intervenção por solicitação da CONTRATADA ou do fabricante, mesmo não implicando em inoperância da solução ou alteração de suas características, deverá ser agendada e acordada previamente com o CONTRATANTE.
- 8.28.** Nos casos em que os produtos operem em alta disponibilidade a CONTRATADA e/ou fabricante deverão realizar o reparo ou troca do equipamento que apresente falha ou defeito ainda que o serviço não seja interrompido, sendo contados normalmente os prazos de atendimento.
- 8.29.** Os serviços deverão ser prestados por equipe técnica qualificada pelo fabricante da solução.
- 8.30.** A CONTRATADA não poderá impor qualquer limitação de quantitativo de chamados, seja diário, mensal, anual, ou de tempo de duração dos chamados, durante o período de prestação dos serviços.
- 8.31.** O CONTRATANTE poderá acompanhar os chamados técnicos abertos pela CONTRATADA junto ao fabricante.
- 8.32.** Será admitida a subcontratação dos serviços de garantia, assistência técnica e suporte técnico, desde que previamente autorizada por escrito pelo CONTRATANTE, por empresa comprovadamente autorizada pelo fabricante dos equipamentos, observadas as mesmas condições de habilitação e qualificação no ato convocatório.

9. LISTA DE EQUIPAMENTOS – FIREWALL E ATIVOS DE REDE

QTE	PN	DESCRIÇÃO
1	WS-V2110-8-ROW	V2110 Virtual Controller for Rest-of-World (verify country availability before ordering). Base of 8 APs, expandable to 248 APs in 1 or 16 AP increments
1	WS-CTLREG8P-ROW	V8 Regulatory Domain Key for Rest of World. Enables WLAN controller and access points with appropriate wireless settings for region.
8	WS-MB3705-01	AP3705i Wall Mounting Bracket
8	WS-AP3705I	Dual radio 11abgn 2X2:2 MIMO indoor access point w/ integrated ceiling clips (wall and protruded drop ceiling brackets sold separate)
1	NMS-BASE-10	Base NMS for up to 10 devices and up to 100 thin APs (includes Console with 3
5	08G20G4-24	800 Series switch w (24) 10/100/1000 RJ45 ports , (4) SFP ports and external RPS connector

QTE	PN	DESCRIÇÃO
1	PAN-PA-3020	Palo Alto Networks PA-3020
1	PAN-PA-3020-TP*	Threat prevention subscription year 1, PA-3020
1	PAN-PA-3020-URL4*	PANDB URL filtering subscription year 1, PA-3020
1	PAN-SVC-PREM-3020*	Premium support year 1, PA-3020

Descrição recursos para atualização necessária.

1. Storage

1.1. Controladoras

1.1.1. Possuir controladora redundante, sendo que a falha de uma das controladoras não acarrete interrupção ou degradação dos serviços, sendo capaz de suportar a capacidade máxima dos discos suportada pelo equipamento;

1.1.2. Suportar no mínimo os padrões RAID 0, 1, 5, 6 e 10;

1.1.3. Permitir reconstrução transparente do RAID sem necessidade de reiniciar o equipamento;

1.1.4. Suportar reconfigurações dinâmicas, inclusão de LUN, assinalamento de HOST, sem necessidade de parada dos demais serviços;

1.1.5. Permitir a adição de gavetas e serviços sem parada do equipamento;

1.2. Cache

1.2.1. Possuir memória cache líquida, ou seja, disponível para aplicativos de, no mínimo, 8GB por controladora, espelhado entre as controladoras, que garanta integridade dos dados presentes na memória e ainda não gravados em disco, em caso de falha de uma das controladoras ou falta súbita de energia;

1.2.2. As soluções protegidas por bateria deverão ter autonomia mínima de 24 (vinte e quatro) horas, exceção feita às tecnologias que tenham autonomia interna suficiente para efetuar a gravação dos dados presentes na memória em disco ou Flash Drive e posterior desligamento do equipamento, mesmo em caso de falta súbita de energia;

1.2.3. Recurso que garanta que os dados residentes no cache sejam salvos para uma unidade Flash Drive ou em discos rígidos, em caso de falta de alimentação elétrica;

1.2.4. Expansível a, no mínimo, 2 (duas) interfaces, sem que seja necessária a aquisição de novas controladoras ou clusterização;

1.2.5. Possuir nativamente pelo menos 2 (duas) interfaces (front-end) para conexão à SAN, padrão Fibre Channel de 16Gbps ou superior;

1.2.6. Possuir no mínimo 2 (duas) interfaces externas (front-end) para conexão à SAN, padrão iSCSI de 1Gbps ou superior;

1.3. Capacidade de armazenamento e unidades de disco

1.3.1. Suportar recurso de hot-spare para as unidades de disco rígido, ou seja, havendo falha de qualquer disco em determinado array/gaveta, o sistema deverá substituir, automaticamente, o disco defeituoso pelo disco spare;

1.3.2. Os discos deverão ser hot-plug/hot-swap;

1.3.3. Permitir a instalação de discos com capacidades diferentes, dentro da mesma gaveta de discos (enclosure);

1.3.4. Possuir capacidade instalada inicial de:

1.3.4.1. 22 (doze) unidades de disco padrão SAS de 12 Gbps com capacidade bruta mínima individual de 1.8 TB e velocidade rotacional de 10k RPM;

1.3.4.2. 2 (duas) unidades de disco padrão SSD de 12 Gbps com capacidade bruta mínima individual de 800 GB;

1.3.4.3. Capacidade de expansão da quantidade de discos instalada a um total de, pelo menos, 96 (noventa e seis) discos, através da simples adição de gavetas de expansão de capacidade;

1.4. Alimentação e Ventilação

1.4.1. Possuir fontes de alimentação e sistema de ventilação redundante tipo “hot-swap”, que mantenham o equipamento em operação integral, sem prejuízo do desempenho, em caso de falha de uma das fontes ou ventiladores, quaisquer que sejam a temperatura e a tensão de alimentação, respeitados os limites máximos e mínimos de operação;

1.4.2. As fontes de alimentação deverão operar na faixa de 100 a 240 Volts, 60 Hz, com seleção automática;

1.5. Funcionalidades e Gerenciamento

1.5.1. Possuir software(s) para monitoração, controle, gerenciamento e configuração do storage através de interface única, com as seguintes funções:

1.5.1.1. Permitir o envio de mensagens de e-mail ao administrador em caso de falhas;

1.5.1.2. Permitir o envio de mensagens de e-mail ao suporte técnico do fabricante do equipamento em caso de falhas – sendo que o atendimento de suporte técnico deve ser oferecido em idioma português;

1.5.1.3. Permitir a criação e configuração, através do software de gerenciamento, de RAID groups e volumes lógicos (LUNs);

1.5.1.4. Permitir a adição de capacidade de armazenamento e expansão de volumes de forma dinâmica;

1.5.1.5. Permitir a configuração de LUN Masking, LUN Partitioning ou similar, ou seja, restringir o acesso a determinado volume lógico (LUN) para um servidor ou conjunto de servidores, físicos ou virtuais (VMware);

1.5.1.6. Permitir o envio de alertas SNMP para uma console de gerenciamento centralizada;

1.5.1.7. Deve permitir gerar registros para todos os eventos relacionados ao storage, sejam eles de falhas ou configurações;

1.5.2. Além do software gerenciamento, devem ser inclusos os seguintes software/facilidades abaixo, licenciados para a capacidade total instalada, e com o mesmo prazo manutenção/garantia do hardware ofertado:

1.5.2.1. Permitir a realização de cópias instantâneas (snapshots/flashcopy) de volumes online em tempo real e cópias completas do volume (full copy), sendo que estas funcionalidades deverão estar licenciadas para a capacidade total de armazenamento suportada pelo equipamento;

1.5.2.2. Permitir o provisionamento nativo da capacidade realmente utilizada pelos aplicativos e usuários através de funcionalidade de thin provisioning, sendo que esta funcionalidade deverá ser licenciada para a capacidade total de armazenamento suportada pelo equipamento. Não será aceita a implementação da funcionalidade através de equipamentos externos.

1.5.2.3. Deverá possuir a capacidade de realizar a migração de dados de sistemas de armazenamento (storages), do mesmo fabricante do equipamento ofertado e de outros fabricantes do mercado, para a área interna do sistema de armazenamento ofertado, de forma transparente. Caso o equipamento ofertado não possua a funcionalidade solicitada de forma nativa, deverão ser fornecidos juntamente com a solução os equipamentos e softwares necessários a essa finalidade;

1.5.2.4. Deverá permitir a implementação futura de tecnologia que possibilite a movimentação automática e nativa dos dados mais ativos no storage para discos de estado sólido (SSD), com o objetivo de aumento de desempenho. Não será aceita a implementação da funcionalidade através de equipamentos externos;

1.5.2.5. Permitir o espelhamento de volumes em diferentes gavetas de armazenamento de dados com o objetivo do aumento da disponibilidade em caso de falha da gaveta, sendo que essa funcionalidade deverá ser licenciada para a capacidade total suportada pelo equipamento;

1.5.2.6. Permitir o monitoramento de desempenho em tempo real do sistema das seguintes métricas: % de utilização de portas; % de utilização de processadores; taxas de I/O; taxas de transferência (MB/seg), e Latência;

1.5.2.7. Incluir drives de multipathing do próprio fabricante para a quantidade de hosts/servidores suportada pelo equipamento.

1.5.2.8. Suportar integração com VMware vStorage API for Array Integration (VAAI), suportar gerenciamento via VMWare vCenter, e suportar Recuperação de Desastres com VMWare SRM,

sendo que esta funcionalidade deverá ser licenciada para a capacidade total de armazenamento suportada pelo equipamento;

1.5.2.9. O software de gerenciamento deverá estar licenciado para a capacidade total de armazenamento suportado pelo equipamento;

1.5.2.10. Todos os softwares envolvidos deverão ser fornecidos na modalidade de licenciamento perpétuo;

1.6. Características Gerais

1.6.1. O equipamento deverá ser fornecido com todos os elementos necessários para sua correta fixação em rack padrão 19" (trilhos, parafusos, etc.) bem como cabos de alimentação.

1.7. Compatibilidade

1.7.1. O storage deverá suportar, no mínimo os Sistemas Operacionais Microsoft Windows 2012, Linux Red Hat 3, 4 e 5 e VMWare ESX 6;

1.7.2. A Solução de storage deverá comprovar compatibilidade com a API do Vmware VAAI (vSphere APIs for Array Integration).

1.7.3. Comprovação de que o fabricante do equipamento ofertado deverá ser participante do SNIA (Storage Networking Industry Association), na qualidade de "Large Voting Member", com comprovação através do site: http://www.snia.org/member_com/member_directory/ e aderente ao GSI (Green Storage Initiative), com comprovação no site <http://www.snia.org/forums/green/>. Cópia do documento comprovando tal informação deverá estar contida na proposta.

1.7.4. Deverá ser compatível com as normas estabelecidas pela SNIA (Storage Networking Industry Association) e prover interface de gerenciamento de acordo com o padrão SMI-S (Storage Management Initiative Specification) versão 1.2 ou superior, para gerenciamento do ambiente através de ferramentas de gerência de infraestrutura de armazenamento que utilizem esse padrão. A conformidade poderá verificada através de consulta ao site oficial do SNIA Interoperability Conformance Test Program (SNIA-CTP) <http://www.snia.org/ctp/conformingproviders/index.html>

1.8. Rede SAN (Storage Area Network)

1.8.1. Deverá ser entregue o total de 2 (dois) switches iSCSI para interligação dos equipamentos (storage e servidores) na rede de armazenamento de dados, contendo as características mínimas:

1.8.2. Deve possuir no mínimo 24 (vinte e quatro) portas gigabit habilitadas;

1.8.3. Deve possuir no mínimo 4 (quatro) portas SFP;

1.8.4. Suportar os padrões IEEE 802.1w, 802.3ad, 802.1q e 802.3x

1.8.5. Possibilitar utilização de jumbo-frames

1.8.6. Ter suporte a camadas 2 e 3;

2. Fornecimento de nobreaks

2.1.1. Deverá ser fornecido no mínimo 02 (dois) nobreaks, sendo cada nobreak deve possuir outros 02 (dois) módulos de expansão de baterias de capacidade igual ou superior.

2.1.2. Possuir montagem padrão de rack 19" (compatível com o rack fornecido na solução);

2.1.3. Possuir tensão de entrada 220V e tensão de saída 110V;

2.1.4. Suportar tecnologia de dupla conversão de forma on-line;

2.1.5. Possibilitar expansões futuras de outros bancos de baterias do mesmo fabricante;

2.1.6. Baterias livres de manutenção;

2.1.7. Deverá ser capaz de suportar toda solução disponibilizada, em seu pleno funcionamento, por período não inferior a 60 (sessenta) minutos;

2.1.8. Capacidade inicial não inferior a 3kVA;

2.1.9. Fator de eficiência mínimo de 95%;

2.1.10. Possuir interface para gerenciamento e monitoração;

3. Especificação dos servidores:

3.1. Servidores

3.1.1. Deverá ser entregue o total de 3 (três) servidores de produção para o ambiente virtualizado, com as seguintes características:

3.1.1.1. Microcomputador do tipo servidor rack, com tecnologia octa-core ou superior, compatível com padrão x86 e desenvolvido para servidores, com, no mínimo, 2 (dois) discos rígidos SAS;

3.1.1.2. Fonte redundante com, no mínimo, 2 (dois) cabos de alimentação ou sistema que garanta conexão em duas fases de energia elétrica distintas, com comprimento mínimo de 1,8m;

3.1.1.3. Interface SVGA, ou superior, que garanta resolução mínima de 1280x1024;

- 3.1.1.4. Registro no Windows Server Catalog – WSC na categoria Hardware para Windows Server 2012 ou superior;
- 3.1.1.5. Plena compatibilidade com sistema operacional Linux RedHat ou Suse com kernel 2.6. ou superior;
- 3.1.1.6. Ventilação redundante tipo “Hot Swap”;
- 3.1.1.7. O servidor e seus componentes eletroeletrônicos deverão possuir conformidade comprovada com a diretiva RoHS (Restriction of Hazardous Substances);
- 3.2. Gabinete
 - 3.2.1. Gabinete Rack com botão Liga/Desliga, LED’s indicativos de equipamento ativo, acionamento de disco rígido no painel frontal e indicadores de falha no equipamento, padrão 19” com no máximo 1U de altura;
 - 3.2.2. Sistema de fontes de alimentação redundantes hot-plug ou hot-swap, com dispositivo de alerta no caso de falha e com capacidade suficiente para suportar todos os dispositivos internos na configuração máxima admitida pelo equipamento (processadores, placa-mãe, interfaces, discos rígidos, memória RAM e todos os fans);
 - 3.2.3. Possuir sistema de ventilação redundante hot-plug ou hot-swap adequado para o perfeito funcionamento do equipamento, conforme recomendações do fabricante do processador, o sistema deverá ter a capacidade de alterar a rotação dos ventiladores conforme a necessidade, visando economia de energia;
 - 3.2.4. Baía instalada internamente ao servidor, mas com acesso externo, que permita a utilização de, no mínimo, 8 (oito) discos rígidos hot-plug ou hot-swap;
 - 3.2.5. Não possuir cantos-vivos, arestas ou bordas, internas ou externas, que sejam cortantes;
 - 3.2.6. O servidor deverá permitir a abertura sem necessidade de utilização de ferramentas.
- 3.3. Processador
 - 3.3.1. Possuir, no mínimo, 2 (dois) processadores padrão x86 com tecnologia octa-core ou superior, desenvolvido para servidor, com tecnologia QPI – Quick Patch Interconnect ou similar;
 - 3.3.2. Frequência de clock igual ou superior a 1,5GHz;
 - 3.3.3. Possuir FAN Intelligent System ou tecnologia similar, que possibilite alta dispersão térmica e seja auxiliado por ventilação forçada do gabinete para garantir a vida útil do processador bem como dissipador de alta dispersão calórica, implementados de acordo com as recomendações do fabricante do processador;
 - 3.3.4. Suporte a SMP (multiprocessamento simétrico);
 - 3.3.5. Suporte às tecnologias SSE 4.2 (Streaming SIMD Extensions 4) e AES (Advanced Encryption Standard).
- 3.4. Placa principal
 - 3.4.1. Memória RAM instalada, no mínimo, 256 (duzentos e cinquenta e seis) Gigabytes em pentes de 32 (trinta e dois) Gigabytes, ou maiores;
 - 3.4.2. Permitir a expansão da memória RAM a, no mínimo, 512 (quinhentos e doze) Gigabytes sem a necessidade de troca de componentes;
 - 3.4.3. Possuir sistemas de proteção a memória com suporte a: Error Correcting Code –ECC, memory Spare, memory mirroring, Advanced ECC ou chipkill;
 - 3.4.4. Possuir, no mínimo, 12 (doze) slots compatíveis com a memória ofertada;
 - 3.4.5. Disponibilidade de, no mínimo, 1 (um) slot de expansão padrão PCI-e (PCI Express) Gen 2 com barramento x16 ou superior, livre após a instalação de todos os dispositivos;
 - 3.4.6. Possuir 1 (uma) interface para conexão de teclado com conector padrão USB;
 - 3.4.7. Possuir 1 (uma) interface para conexão de mouse padrão USB;
 - 3.4.8. Possuir, no mínimo, uma saída com conector tipo DB15 para monitor;
 - 3.4.9. Interface de vídeo compatível com padrão SVGA, ou superior, embutida, com pelo menos 16 (dezesesseis) Megabytes de memória de vídeo e interface de interconexão com a placa no padrão PCI Express ou tecnologicamente superior;
 - 3.4.10. Possuir, no mínimo, 1 (uma) interface serial com conector tipo DB-9;
 - 3.4.11. Possuir, no mínimo, 4 (quatro) interfaces USB (Universal Serial BUS) padrão 2.0 ou superior;
 - 3.4.12. Não serão aceitas interfaces USB instaladas por meio de placas de expansão de portas ou qualquer outro tipo de interface que não seja nativa do equipamento;
 - 3.4.13. Possuir recurso tecnológico integrado que garanta que o servidor seja automaticamente reinicializado em caso de instabilidade grave do sistema (como por exemplo travamento devido a memory leak, overclocking, instabilidade elétrica, falha de processador, etc.).

- 3.5. BIOS ou uEFI
 - 3.5.1. BIOS ou Uefi do fabricante;
 - 3.5.2. Tipo flash EPROM (atualizável por software);
 - 3.5.3. Senha de acesso ativada e desativada via setup;
 - 3.5.4. Relógio não-volátil.
- 3.6. Unidade de disco rígido
 - 3.6.1. Possuir, no mínimo, 2 (dois) discos com tecnologia Serial Attached SCSI - SAS (todos idênticos) de, no mínimo, 300 (trezentos) GB cada e dimensões máximas de 2,5", compatíveis com a controladora SAS cotada com o equipamento;
 - 3.6.2. Cada unidade de disco utilizada deve possuir:
 - 3.6.2.1. Rotação de, no mínimo, 10.000 RPM;
 - 3.6.2.2. Interface SAS 12 (doze) Gb/s;
 - 3.6.3. Taxa de transferência externa mínima de 600 (seiscentos) MB/s;
 - 3.6.4. Montagem interna ao gabinete do servidor, em baia específica de 2,5" cada;
 - 3.6.5. Cabo de comunicação entre o disco rígido e a controladora SAS cotada com o equipamento;
 - 3.6.6. Possuir facilidade hot-swap.
- 3.7. Controladora SAS
 - 3.7.1. Possuir, no mínimo, 1 (um) controlador SAS com processador embarcado;
 - 3.7.2. Compatível com os padrões RAID 0, RAID 1, RAID 0+1, RAID 5, RAID 6 e RAID 60 por hardware;
 - 3.7.3. Oferecer detecção e recuperação automática de falhas e reconstrução transparente do RAID;
 - 3.7.4. Memória cache de, no mínimo, 512 (quinhentos e doze) MB, com sistema de proteção ECC e servida por bateria;
 - 3.7.5. Operar com taxa de transferência de, no mínimo, 6 (seis) Gbit/s;
 - 3.7.6. Operar comunicação no modo Full Duplex;
 - 3.7.7. Possuir suporte a hot-swap e "hot-spare";
 - 3.7.8. Ser totalmente compatível com os discos ofertados;
 - 3.7.9. Suportar, no mínimo, 8 (oito) unidades de disco.
- 3.8. Interfaces
 - 3.8.1. Possuir, no mínimo, 4 (quatro) portas padrão Gigabit Ethernet, com as seguintes características:
 - 3.8.2. Operar comunicação no modo full-duplex;
 - 3.8.3. Possuir conector RJ-45 fêmea
 - 3.8.4. Possuir barramento PCI, ou superior, de 64 bits e 100 MHz
 - 3.8.5. Compatível com o padrão IEEE 802.3
 - 3.8.6. LED's indicadores de link ativo e de tráfego;
 - 3.8.7. Permitir a configuração via software (jumperless);
 - 3.8.8. Oferecer opção de configuração automática da interface (auto-sense);
 - 3.8.9. Compatível com Plug & Play;
 - 3.8.10. Suporte ao gerenciamento SNMP;
 - 3.8.11. Possuir software de diagnóstico, capaz de identificar o funcionamento correto dos componentes;
 - 3.8.12. Suporte a Wake Up on LAN;
 - 3.8.13. Suporte a PXE;
 - 3.8.14. Permitir balanceamento de carga;
 - 3.8.15. Permitir Link Aggregation;
 - 3.8.16. Possuir fail-over automático;
 - 3.8.17. Suporte aos protocolos: 802.1q (VLAN tagging), 802.3x (flow control), 802.3ad (LACP);
- 3.9. Interface de vídeo
 - 3.9.1. Possuir, no mínimo, 16 MB de memória de vídeo com interface PCI Express compatível com o padrão SVGA ou tecnologicamente superior;
 - 3.9.2. Capacidade para trabalhar com resolução de 1280x1024;
- 3.10. Fonte de alimentação
 - 3.10.1. O servidor deveria possuir, no mínimo, 2 (duas) fontes redundantes que suportem o servidor em sua capacidade máxima.
 - 3.10.2. Devem ser de, no máximo, 800W.
 - 3.10.3. As fontes devem alternar entre 110 e 220V automaticamente

3.11. Software de gerenciamento

3.11.1. Todos os servidores devem ser fornecidos com uma solução completa de hardware e software para gerenciamento remoto de sistemas, com todas as funcionalidades habilitadas para pleno gerenciamento remoto dos equipamentos, com no mínimo as seguintes características:

3.11.1.1. Possui microprocessador e memória próprios;

3.11.1.2. Possuir conexão que permita o acesso à console do equipamento através da rede. Esta conexão deve possuir 1 (uma) interface 10/100Mbps/s, ou superior, exclusiva;

3.11.1.3. Possuir acesso a console através de HTTPS ou software proprietário, possuindo usuário e senha de conexão, com criptografia de dados trafegados;

3.11.1.4. Permitir gerenciar e monitorar remotamente o sistema, mesmo quando ele estiver fora do ar;

3.11.1.5. Gerenciar servidores remotamente de qualquer lugar por meio de uma conexão IP;

3.11.1.6. Permitir instalação de software de qualquer lugar, por meio de uma conexão IP, de forma criptografada;

3.11.1.7. Possuir console de vídeo contínuo independente de SO que capture a última tela e acompanhe a reinicialização do servidor;

3.11.1.8. Permitir monitorar o status do servidor remoto durante uma reinicialização;

3.11.1.9. Permitir autenticação e autorização do Active Directory para melhor segurança;

3.11.1.10. Possuir a capacidade de reiniciar um servidor desligado e desligar um servidor remotamente;

3.11.1.11. Permitir autoridade baseada em funções através da atribuição de permissões para diferentes tarefas de gerenciamento de sistemas;

3.11.1.12. Possui a funcionalidade de emitir alertas para problemas potenciais de nós gerenciados por meio de mensagens de e-mail ou SNMP;

3.11.1.13. Possui análise de pré-falha por hardware para, pelo menos, processador, memórias e discos rígidos;

3.11.1.14. O software deve ter a capacidade de monitorar e controlar o consumo de energia do servidor, com possibilidade de se estabelecer limites para o servidor;

3.11.1.15. Permitir o deployment de sistema operacional para um grupo de servidores;

3.11.1.16. Permitir trabalhar com ambientes e ferramentas virtualizados, incluindo Microsoft Virtual Server, VMware e virtualização Xen executando funcionalidades como descoberta de máquinas virtuais, inventário, topologia, monitoração da saúde dos servidores virtuais, operações de ligar e desligar, realocação e thresholds;

3.11.1.17. Permitir a visualização dos sistemas de acordo com a VLAN; Coleta e visualização dos componentes de network virtuais ou físicos; Suporte as soluções dos principais fabricantes de mercado Qlogic, Lenovo, Brocade, Cisco e Juniper;

3.11.2. Caso seja necessário software proprietário, este deve ser entregue em quantidade suficiente para administrar todos os servidores fornecidos e com todas as funcionalidades habilitadas;

4. Especificação do licenciamento de virtualização e backup e servidor do backup

4.1. Deverá ser fornecido atualização do licenciamento de VMware vCenter para gerenciamento dos servidores disponibilizados com VMware vSphere 6.7 ou superior;

4.1.1. Deve possuir suporte 9x5 e direito a atualizações direto pelo fabricante da solução, não sendo aceito licenciamento em regime de OEM.

4.2. Software de backup e replicação

4.2.1. Deverá ser fornecido licenciamento de software de backup Veeam Backup & Replication para todo ambiente, contendo, no mínimo, as seguintes características ativas:

4.2.1.1. Recuperação granular de e-mail;

4.2.1.2. Permitir configuração de replicação das máquinas virtuais;

4.2.1.3. Ser licenciado de forma perpétua para toda solução disponibilizada;

4.2.1.4. Permitir a recuperação granular de servidor de arquivos;

4.2.1.5. Possibilitar a recuperação de máquinas virtuais em menos de 5 (cinco) minutos;

4.2.1.6. Deve possuir suporte 9x5 e direito a atualizações direto pelo fabricante da solução, não sendo aceito licenciamento em regime de OEM;

4.3. Deverá ser entregue servidor no padrão rack para instalação da solução de backup, possuindo os requisitos mínimos de:

4.3.1. Possuir, no mínimo, 1 processador padrão x86 com tecnologia Six-Core ou superior com frequência de clock igual ou superior a 2,0Ghz;

- 4.3.2. Memória RAM instalada, no mínimo, 32 (trinta e dois) Gigabytes em pentes de 16 (dezesesseis) Gigabytes
- 4.3.3. Permitir a expansão da memória RAM a, no mínimo, 256 (duzentos e cinquenta e seis) Gigabytes sem a necessidade de troca de componentes
- 4.3.4. Possuir, no mínimo, 2 (dois) discos com tecnologia Serial Attached SCSI - SAS (todos idênticos) de, no mínimo, 300 (trezentos) Gbytes cada e dimensões máximas de 2,5", compatíveis com a controladora SAS cotada com o equipamento, mais 6 (seis) discos com tecnologia NLSAS ou SAS de, no mínimo, 2 TB cada e dimensões máximas de 2,5"
- 4.3.5. Possuir suporte a hot-swap e/ou hot-spare para discos;
- 4.3.6. Possuir sistema de fontes de alimentação e fans redundantes hot-plug ou hot-swap, com dispositivo de alerta no caso de falha e com capacidade suficiente para suportar todos os dispositivos internos na configuração máxima admitida pelo equipamento (processadores, placa-mãe, interfaces, discos rígidos, memória RAM e todos os fans);
- 4.3.7. Possuir, no mínimo, 1 (um) controlador SAS com processador embarcado;
- 4.3.8. Compatível com os padrões RAID 0, RAID 1, RAID 0+1, RAID 5, RAID 6 e RAID 60 por hardware
- 4.3.9. Deverá ser fornecido licenciamento Windows Server Standard 2012 ou superior para a capacidade total do servidor
- 4.3.10. Possuir controladora Fibre Channel (HBA) para conexão com a biblioteca de fitas contemplada na solução, no mínimo 2 (dois) canais padrão FC, com velocidade de conexão de 8 (oito) Gbps por canal.
- 4.3.11. Possuir controladora ethernet para conexão à rede SAN da contemplada na solução, com no mínimo 4 (quatro) portas, com velocidade de conexão gigabit.
- 4.3.12. As controladoras devem ser compatíveis com sistemas operacionais Windows 2012 Server, vmware vSphere 6 e com os switches SAN ofertados na solução.
5. Biblioteca de fitas
 - 5.1.1. Deverá ser entregue biblioteca de fitas interligada no servidor de backup. Esta deve ser no padrão rack para operação da solução de backup, possuindo os requisitos mínimos de:
 - 5.1.2. Suportar, no mínimo, 2 (dois) drives half-height com a tecnologia LTO7;
 - 5.1.3. Possuir, no mínimo, 12 (doze) slots de fitas de dados;
 - 5.1.4. Padrão para instalação em rack de 19" de largura;
 - 5.1.5. Possuir fontes de alimentação com tensão de entrada de 110/220 V e frequência de 60 Hz;
 - 5.1.6. Possuir leitor de código de barras com o objetivo de identificar os cartuchos através das etiquetas;
 - 5.1.7. Possuir drives com padrão de conexão FC;
 - 5.1.8. Deverão ser entregues 22 (vinte dois) cartuchos padrão ultrium LTO7 e 2(dois) cartuchos de limpeza;
 - 5.1.9. Suportar gerenciamento via SNMP;
 - 5.1.10. Suportar gerenciamento da unidade de backup remotamente através de um web-browser, incluindo as principais funções de operação e monitoração local da Biblioteca;
 - 5.1.11. Possuir gerenciamento de erros e status de logs;
 - 5.1.12. Suportar os protocolos de rede IPv6 e IPv4;
 - 5.1.13. A unidade de backup deve ser capaz de:
 - 5.1.14. Monitorar a utilização dos drives e cartuchos;
 - 5.1.15. Reportar informações através de notificação do status do hardware como saúde e vida útil;
 - 5.1.16. Garantia total mínima de 3 (três) anos, a partir da data de entrega, no local de instalação do equipamento;
6. Descrição dos serviços
 - 6.1. Instalação e configuração dos equipamentos
 - 6.1.1. Instalação do rack, incluindo regulagem e nivelamento do mesmo;
 - 6.1.2. Instalação física de todos os equipamentos da solução (storage, gavetas, discos, servidores, switches), incluindo desembalar, montagem, afixação e cabeamentos nos racks fornecidos, englobando ligações elétricas, lógicas (LAN e SAN) e ativação da solução;
 - 6.1.3. Energização dos equipamentos e análise do funcionamento do ambiente;
 - 6.1.4. Identificação de todas as conexões efetuadas para futuras manutenções e alterações na configuração;

- 6.1.5. Atualização do firmware dos componentes de hardware da solução (módulos de gerenciamento, módulos Lan e SAN, controladoras, gavetas, discos BIOS de servidores) para a última versão disponível conforme matriz de compatibilidade do fabricante;
- 6.1.6. Configuração dos parâmetros de BIOS dos servidores e interfaces para atender as recomendações dos fabricantes para o software de virtualização;
- 6.1.7. Criação do RAID na controladora de discos locais;
- 6.1.8. Execução do zoning e ISL's dos switches SAN;
- 6.1.9. Criação de VLAN's nos módulos LAN dos para o ambiente da rede Prefeitura Municipal de Vacaria;
- 6.1.10. Sessão de orientação onde será abordada a utilização do software de gerenciamento e do software de monitoramento, incluindo criação de novos usuários, configuração de autorizações na plataforma. A Prefeitura Municipal de Vacaria deve ter a capacidade de adição de novos equipamentos e/ou recursos, implementar configurações, consultar as configurações existentes, efetuar o monitoramento da solução, enfim, a completa utilização da ferramenta;
- 6.2. Configuração da solução de armazenamento
 - 6.2.1. Instalação do software de gerenciamento, replicação e movimentação de dados no storage, incluindo patches e atualizações necessárias;
 - 6.2.2. Habilitação das funcionalidades e recursos previstas na solução disponibilizada;
 - 6.2.3. Sessão de orientação onde será abordada a utilização do software e do hardware de armazenamento do presente edital, incluindo criação de snapshots, clones, mirror, utilização de Thin Provisioning e Tierização, criação de disk groups, monitoramento de utilização e carga, enfim, a completa utilização da ferramenta e do hardware adquirido;
- 6.3. Instalação do software de virtualização
 - 6.3.1. Instalação do software de virtualização (hypervisor) VMware vSphere 6 em sua última release nos servidores, conforme matriz de compatibilidade dos equipamentos;
 - 6.3.2. Instalação de patches e atualizações necessários;
 - 6.3.3. Instalação e configuração da ferramenta de gerenciamento do ambiente virtualizado VMware vCenter Server 6;
 - 6.3.4. Configuração da integração do software de virtualização com o software de replicação da storage e reconhecimento das áreas de discos replicadas;
 - 6.3.5. Configuração da replicação das máquinas virtuais no software de backup e replicação;
 - 6.3.6. Instalação e configuração da ferramenta de alta disponibilidade de entre servidores (módulo HA). Os servidores de virtualização deverão operar em um ambiente de alta disponibilidade onde, em caso de falha de qualquer um dos servidores, as máquinas virtuais deste servidor poderão ser reiniciadas automaticamente em qualquer outro servidor de virtualização;
 - 6.3.7. Configuração da funcionalidade de migração online de máquinas virtuais entre servidores físicos sem interrupção do processamento;
 - 6.3.8. Criação de clusters de alta-disponibilidade entre os hypervisors;
 - 6.3.9. Instalação e configuração da ferramenta de recuperação de desastres disponibilizada na solução e todos os seus componentes;
 - 6.3.10. Criação de até 2 (duas) políticas de replicação e recuperação de desastres para até 8 (oito) máquinas virtuais.
 - 6.3.11. Demonstração da verificação do perfeito funcionamento do plano de recuperação, em ambiente isolado, sem afetar as máquinas virtuais em produção;
 - 6.3.12. A configuração dos softwares VMware vCenter Server 6.7, ou superior, deve ser efetuada em máquina virtual hospedada nos clusters de alta disponibilidade e não em servidores externos ao ambiente caso houver;
 - 6.3.13. Criação de até 8 (oito) templates de máquinas virtuais a ser utilizado no ambiente Prefeitura Municipal de Vacaria;
 - 6.3.14. Criação de novas máquinas virtuais através de modelos pré-definidos ou de forma manual e individual;
 - 6.3.15. Deverá permitir o gerenciamento dos recursos físicos e virtuais do ambiente de virtualização, com estatísticas online do uso destes recursos, como I/O, Memória, Processamento, Latência;
- 6.4. Conversão de máquinas físicas
 - 6.4.1. Conversão de até 6 (seis) máquinas físicas existentes na infraestrutura de TI Prefeitura Municipal de Vacaria para máquinas virtuais no novo ambiente de virtualização;

- 6.4.2. Instalação de ferramentas de otimização nas máquinas virtuais convertidas de forma a funcionar com perfeita integração e máximo desempenho no novo ambiente de virtualização;
- 6.4.3. A contratada deverá garantir que os servidores inicializem corretamente o sistema operacional após a conversão;
- 6.4.4. A conversão não será executada em lote, sendo que a cada conversão será feita a validação dos serviços e do funcionamento da máquina virtual antes de iniciar a migração da próxima máquina virtual;

7. Atualização Tecnológica com Expansão de 02 Firewall Palo Alto

- 7.1.1. Atualização da solução de proteção de rede com características de Next Generation Firewall (NGFW) para segurança de informação perimetral que inclui filtro de pacote, controle de aplicação, administração de largura de banda (QoS), VPN IPSec e SSL, IPS, prevenção contra ameaças de vírus, spywares e malwares “Zero Day”, Filtro de URL, bem como controle de transmissão de dados e acesso à internet compondo uma plataforma de segurança integrada e robusta;
- 7.1.2. Por plataforma de segurança entende-se hardware e software integrados do tipo appliance, com operação em Alta Disponibilidade com configuração Ativo-Passivo;
- 7.1.3. A plataforma de segurança deve possuir a capacidade e as características abaixo, por equipamento:
 - 7.1.4. Throughput de 500 Mbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir;
 - 7.1.5. Throughput de 250 Mbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito;
 - 7.1.6. Não será aceito aceleração de pacotes na placa de rede limitando a análise somente até camada 4.
 - 7.1.7. Suporte a, no mínimo, 60.000 conexões simultâneas;
 - 7.1.8. Suporte a, no mínimo, 3.000 novas conexões por segundo;
 - 7.1.9. Deve possuir fonte redundantes 120/240 AC;
 - 7.1.10. Disco de, no mínimo, 30 GB.
 - 7.1.11. No mínimo, 08 (oito) interfaces de rede 10/100/1000 base-TX;
 - 7.1.12. 1 (uma) interface de rede 1 Gbps dedicada para gerenciamento;
 - 7.1.13. 1 (uma) interface do tipo console ou similar;
 - 7.1.14. Suporte a, no mínimo, 10 (dez) zonas de segurança;
 - 7.1.15. Estar licenciada para ou suportar sem o uso de licença, 200 (duzentos) clientes de VPN SSL simultâneos;
 - 7.1.16. Estar licenciada para ou suportar sem o uso de licença, 200 (duzentos) túneis de VPN IPSEC simultâneos;
 - 7.1.17.
 - 7.1.18. Por cada equipamento que compõe a plataforma de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento;
 - 7.1.19. Por console de gerência e monitoração, entende-se as licenças de software necessárias para as duas funcionalidades, bem como hardware dedicado para o funcionamento das mesmas;
 - 7.1.20. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale.
 - 7.1.21. A solução deve consistir de appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração;
 - 7.1.22. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
 - 7.1.23. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;
 - 7.1.24. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
 - 7.1.25. O hardware e software que executem as funcionalidades de proteção de rede, bem como a console de gerência e monitoração, devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;
 - 7.1.26. O software deverá ser fornecido em sua versão mais atualizada;

- 7.1.27. Suportar sub-interfaces ethernet logicas.
- 7.1.28. Suporte a, no mínimo, 3 (três) roteadores virtuais na mesma instancia de firewall;
- 7.1.29. O firewall deve ter a capacidade de testar o funcionamento de rotas estáticas e rota default com a definição de um endereço IP de destino que deve estar comunicável através de uma rota. Caso haja falha na comunicação o firewall deve ter a capacidade de usar rota alternativa para estabelecer a comunicação;
- 7.1.30. Proteção contra anti-spoofing;
- 7.1.31. Deve permitir bloquear sessoes TCP que usem variações do 3-way hand-shake, como 4 way e 5 way split hand-shake, prevenindo desta forma possíveis tráfegos maliciosos;
- 7.1.32. Dever permitir bloquear conexões que contenham dados no payload de pacotes TCP-SYN e SYN-ACK durante o three-way handshake;
- 7.1.33. Deve exibir nos logs de tráfego o motivo para o término da sessão no firewall, incluindo sessões finalizadas onde houver de-criptografia de SSL e SSH;
- 7.1.34. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
- 7.1.35. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
- 7.1.36. Suportar a OSPF graceful restart;
- 7.1.37. Deve suportar o protocolo MP-BGP (Multiprotocol BGP) permitindo que o firewall possa anunciar rotas multicast para IPv4 e rotas unicast para IPv6;
- 7.1.38. Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);
- 7.1.39. Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- 7.1.40. Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
- 7.1.41. Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;
- 7.1.42. Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
- 7.1.43. Controle de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações.
- 7.1.44. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
- 7.1.45. Deve suportar a consulta a fontes externas de endereços IP, domínios e URLs podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego;
- 7.1.46. Deve permitir autenticação segura através de certificado nas fontes externas de endereços IP, domínios e URLs;
- 7.1.47. Deve permitir consultar e criar exceção para objetos das listas externas a partir da interface de gerência do próprio firewall;
- 7.1.48. Controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS).
- 7.1.49. Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound).
- 7.1.50. Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif, e reg
- 7.1.51. Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo)
- 7.1.52. QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações.
- 7.1.53. Suporte a objetos e regras IPV6.
- 7.1.54. Suporte a objetos e regras multicast.
- 7.1.55. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:
- 7.1.56.
- 7.1.57. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos.
- 7.1.58. Reconhecer pelo menos 3400 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
- 7.1.59. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active

directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs, etc;

7.1.60. Deve inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo. A checagem de assinaturas também deve determinar se uma aplicação está utilizando a porta default ou não, incluindo, mas não limitado a RDP na porta 80 ao invés de 389;

7.1.61. 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;

7.1.62. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas;

7.1.63. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Gtalk, Facebook Chat, etc.) possuindo granularidade de controle/políticas para os mesmos;

7.1.64. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Gtalk chat e bloquear a transferência de arquivos;

7.1.65. Deve possibilitar a diferenciação de aplicações Proxies (ghostsurf, freegate, etc.) possuindo granularidade de controle/políticas para os mesmos;

7.1.66. Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:

7.1.67. Tecnologia utilizada na aplicações (Client-Server, Browse Based, Network Protocol, etc).

7.1.68. Nível de risco da aplicação.

7.1.69. Categoria e sub-categoria de aplicações.

7.1.70. Aplicações que usem técnicas evasivas, utilizadas por malwares, como transferência de arquivos e/ou uso excessivo de banda, etc.

7.1.71. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de Firewall ou entregue através de composição com outro equipamento ou fabricante.

7.1.72. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

7.1.73. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.

7.1.74. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;

7.1.75. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS, Antipyyware e Antivirus: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset;

7.1.76. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

7.1.77. Exceções por IP de origem ou de destino devem ser possíveis nas regras, de forma geral e assinatura a assinatura;

7.1.78. Deve suportar granularidade nas políticas de IPS Antivírus e Anti-Spyware , possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.

7.1.79. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPflood, etc;

7.1.80. Detectar e bloquear a origem de portscans com possibilidade de criar exceções para endereços IPs de ferramentas de monitoramento da organização;

7.1.81. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;

7.1.82. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

7.1.83. Possuir assinaturas para bloqueio de ataques de buffer overflow;

7.1.84. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

7.1.85. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS e anti-spyware, permitindo a criação de exceções com granularidade nas configurações;

- 7.1.86. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- 7.1.87. É permitido uso de appliance externo (antivírus de rede), para o bloqueio de vírus e spywares em protocolo SMB de forma a conter malwares se espalhando horizontalmente pela rede;
- 7.1.88. Suportar bloqueio de arquivos por tipo;
- 7.1.89. Identificar e bloquear comunicação com botnets;
- 7.1.90. Deve suportar várias técnicas de prevenção, incluindo Drop e tcp-rst (Cliente, Servidor e ambos);
- 7.1.91. Deve suportar referência cruzada com CVE;
- 7.1.92. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:
- 7.1.93. O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 7.1.94. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS e antispymware;
- 7.1.95. Deve permitir que na captura de pacotes por assinaturas de IPS e antispymware seja definido o número de pacotes a serem capturados. Esta captura deve permitir selecionar, no mínimo, 50 pacotes;
- 7.1.96. Deve possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos sejam resolvidas pelo Firewall com endereços (IPv4 e IPv6), previamente definidos;
- 7.1.97. Permitir o bloqueio de vírus, pelo menos, nos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- 7.1.98. Os eventos devem identificar o país de onde partiu a ameaça;
- 7.1.99. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms.
- 7.1.100. Proteção contra downloads involuntários usando HTTP de arquivos executáveis. maliciosos.
- 7.1.101. Rastreamento de vírus em pdf.
- 7.1.102. Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.)
- 7.1.103. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.
- 7.1.104. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:
- 7.1.105. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
- 7.1.106. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, Ips, Redes e Zonas de segurança.
- 7.1.107. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local.
- 7.1.108. Permite popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;
- 7.1.109. Suporta a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;
- 7.1.110. Deve bloquear o acesso a sites de busca (Google, Bing e Yahoo), caso a opção Safe Search esteja desabilitada. Deve ainda exibir página de bloqueio fornecendo instruções ao usuário de como habilitar a função;
- 7.1.111. Suporta base ou cache de URLs local no appliance, evitando delay de comunicação/validação das URLs;
- 7.1.112. Possui pelo menos 60 categorias de URLs;
- 7.1.113. A categorização de URL deve analisar toda a URL e não somente até o nível de diretório;
- 7.1.114. Suporta a criação categorias de URLs customizadas;
- 7.1.115. Suporta a exclusão de URLs do bloqueio, por categoria;

- 7.1.116. Permite a customização de página de bloqueio;
- 7.1.117. Suporta a inclusão nos logs do produto de informações das atividades dos usuários;
- 7.1.118. Deve salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent, Referer, e X-Forwarded For;
- 7.1.119. Centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento;
- 7.1.120. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
- 7.1.121. Deve permitir substituir o certificado de fábrica no acesso HTTPS a gerência do firewall como possibilidade de uso de certificado criado localmente na própria solução ou importado de fonte externa;
- 7.1.122. Caso haja a necessidade de instalação de cliente para administração da solução o mesmo deve ser compatível com sistemas operacionais Windows e Linux;
- 7.1.123. Acesso concorrente de administradores;
- 7.1.124. Deve permitir que administradores concorrentes façam modificações, valide configurações e reverta configurações do firewall simultaneamente e que cada administrador consiga aplicar apenas as suas alterações de forma independente das realizadas por outro administrador;
- 7.1.125. Deve mostrar ao administrador do firewall a hora e data do último login e tentativas de login com falha para acessos a partir da interface gráfica e CLI.
- 7.1.126. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;
- 7.1.127. Deve permitir usar palavras chaves e cores para facilitar identificação de regras;
- 7.1.128. Deve suportar também o monitoramento dos seguintes recursos via SNMP: IP fragmentation, TCP state e dropped packets;
- 7.1.129. Bloqueio de alterações, no caso acesso simultâneo de dois ou mais administradores;
- 7.1.130. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
- 7.1.131. Autenticação integrada ao Microsoft Active Directory e servidor Radius;
- 7.1.132. Localização de em quais regras um endereço IP, IP Range, subnet ou objetos estão sendo utilizados;
- 7.1.133. Deve atribuir sequencialmente um número a cada regra de firewall, NAT, QOS e regras de DOS;
- 7.1.134. Criação de regras que fiquem ativas em horário definido;
- 7.1.135. Criação de regras com data de expiração;
- 7.1.136. Backup das configurações e rollback de configuração para a última configuração salva;
- 7.1.137. Suportar Rollback de Sistema Operacional para a última versão local;
- 7.1.138. Habilidade de upgrade via SCP, TFTP e interface de gerenciamento;
- 7.1.139. Deve possuir mecanismo de análise de impacto na política de segurança antes de atualizar a base com novas aplicações disponibilizadas pelo fabricante;
- 7.1.140. Validação de regras antes da aplicação;
- 7.1.141. Deve implementar mecanismo de validação de configurações antes da aplicação das mesmas permitindo identificar erros, tais como: rota de destino inválida, regras em shadowing etc.
- 7.1.142. É permitido o uso de appliance externo para permitir a validação de regras antes da aplicação.
- 7.1.143. Validação da políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
- 7.1.144. É permitido o uso de appliance externo para permitir a validação de políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
- 7.1.145. Deve possibilitar a visualização e comparação de configurações Atuais, configuração anterior e configurações antigas.
- 7.1.146. Deve possibilitar a integração com outras soluções de SIEM de mercado (third-party SIEM vendors)
- 7.1.147. Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;
- 7.1.148. Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-Spware), etc;

- 7.1.149. Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus e Anti-Spware), e URLs que passaram pela solução;
- 7.1.150. Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em RealTime;
- 7.1.151. Nas opções de "Drill-Down", ser possível identificar o usuário que fez determinado acesso;
- 7.1.152. Em cada critério de pesquisa do log deve ser possível incluir múltiplas entradas (ex. 10 redes e IP's distintos; serviços HTTP, HTTPS e SMTP), exceto no campo horário, onde deve ser possível definir um faixa de tempo como critério de pesquisa;
- 7.1.153. Gerar alertas automáticos via:
 - 7.1.154. Email;
 - 7.1.155. SNMP;
 - 7.1.156. Syslog;
- 7.1.157. A plataforma de segurança deve permitir através de API-XML (Application Program Interface) a integração com sistemas existentes no ambiente da contratante de forma a possibilitar que aplicações desenvolvidas na contratante possam interagir em RealTime com a solução possibilitando assim que regras e políticas de segurança de possam ser modificadas por estas aplicações com a utilização de scripts em linguagens de programação como Perl ou PHP.

8. Atualização Tecnológica com Expansão de 02 Switches Core de Rede Extreme Networks:

- 8.1. Possuir fonte de alimentação interna que trabalhe em 100V-240V, 50/60 Hz, com detecção automática de tensão e frequência.
- 8.2. Possuir bandeja de ventiladores substituível em campo (field replaceable e hot swappable).
- 8.3. Deve possuir 48 portas com detecção automática MDI/MDIX de 10/100/1000BASE-T RJ-45.
- 8.4. Possuir porta de console com conector RJ-45 ou DB9 macho.
- 8.5. Possuir leds indicativos de funcionamento da fonte de alimentação, ventiladores e status das portas.
- 8.6. O equipamento deve possuir além das portas acima citadas uma porta adicional 10/100 ou 10/100/1000 com conector RJ-45 para gerência out-of-band do equipamento.
- 8.7. Implementar empilhamento de no mínimo oito equipamentos e gerência através de um único endereço IP.
- 8.8. O equipamento deve possuir portas específicas para empilhamento com velocidade de pelo menos 42Gbps cada (ou 21Gbps Full Duplex), totalizando 84 Gbps (ou 42 Gbps full-duplex). Não será aceito empilhamento que se utilize de portas RJ45 ou SFP ou SFP+ ou X2 ou XENPAK ou XFP.
- 8.9. A Memória Flash instalada deve ser suficiente para comportar no mínimo duas imagens do Sistema Operacional simultaneamente, permitindo que seja feito um upgrade de Software e a imagem anterior seja mantida.
- 8.10. Todas as interfaces ofertadas devem ser non-blocking.
- 8.11. Possuir altura máxima de 1U (1,75").
- 8.12. Deve armazenar, no mínimo, 64.000 (sessenta e quatro mil) endereços MAC.
- 8.13. Implementar agregação de links conforme padrão IEEE 802.3ad com, no mínimo, 128 grupos, sendo 32 links agregados por grupo.
- 8.14. Implementar, no mínimo, 4.000 (quatro mil) regras de ACL de entrada (ingress ACLs).
- 8.15. Implementar, no mínimo, 1.000 (um mil) regras de ACL de saída (egress ACLs).
- 8.16. Deve suportar o armazenamento de, no mínimo, 16.000 (dezesesseis mil) rotas IPv4 em hardware.
- 8.17. Deve suportar o armazenamento de, no mínimo, 8.000 (oito mil) rotas IPv6 em hardware.
- 8.18. Possuir homologação da ANATEL, de acordo com a Resolução número 242.
- 8.19. Implementar agregação de links conforme padrão IEEE 802.3ad com suporte a LACP.
- 8.20. deve eliminar convergência do Spanning Tree, possibilitando o tráfego simultâneo por mais de uma conexão.
- 8.21. Implementar jumbo frames em todas as portas ofertadas, com suporte a pacotes de até 9216 Bytes.
- 8.22. Implementar Proxy-ARP (RFC 1027).
- 8.23. Implementar IGMP v1, v2 e v3 Snooping.
- 8.24. Implementar IGMPv1 (RFC 1112), IGMP v2 (RFC 2236) e IGMPv3 (RFC 3376).
- 8.25. Implementar MVR (Multicast VLAN Registration).
- 8.26. Implementar DHCP/Bootp relay configurável por VLAN para IPv4 e IPv6.

- 8.27. Implementar servidor DHCP interno que permita a configuração de um intervalo de endereços IP a serem atribuídos os clientes DHCP e possibilite ainda a atribuição de, no mínimo, default-gateway, servidor DNS e servidor WINS.
- 8.28. Implementar DHCP Option 82, de acordo com a RFC 3046, com identificação de porta e VLAN, configurável por VLAN.
- 8.29. Implementar DHCP Client para IPv4 e IPv6.
- 8.30. Implementar RFC 3021 - Using 31-Bit Prefixes on IPv4 Point-to-Point Links
- 8.31. Implementar Spanning-Tree (IEEE 802.1d), Rapid Spanning Tree (IEEE 802.1w), Multiple Instance STP (802.1s) e PVST+.
- 8.32. Implementar a configuração de Multiple Spanning Tree Protocol, com suporte a, pelo menos, 64 domínios.
- 8.33. Implementar funcionalidade vinculada ao Spanning-tree onde é possível designar portas de acesso (por exemplo onde estações estão conectadas) que não sofram o processo de Listening-Learning, passando direto para o estado de Forwarding. No entanto, as portas configuradas com esta funcionalidade devem detectar loops na rede normalmente.
- 8.34. Implementar funcionalidade vinculada ao Spanning-tree que evite a eleição de outros switches da rede como Root.
- 8.35. Implementar funcionalidade vinculada ao Spanning-tree que permita desabilitar uma porta de acesso assim que a mesma receba uma BPDU.
- 8.36. Implementar 4000 VLANs por porta, ativas simultaneamente, através do protocolo 802.1Q.
- 8.37. Deverá permitir a criação, remoção, gerenciamento e distribuição de VLANs de forma dinâmica através de portas configuradas como tronco IEEE 802.1Q utilizando o protocolo MVRP segundo o padrão IEEE802.1ak.
- 8.38. Possibilitar a coleta de estatísticas de tráfego baseada em VLANs IEEE 802.1Q e double-tagged VLANs IEEE 802.1ad.
- 8.39. Implementar MAC Based VLAN.
- 8.40. Implementar VLAN Translation.
- 8.41. Suportar VLAN Aggregation ou funcionalidade que permita o compartilhamento de uma mesma subnet e de um mesmo endereço IPv4 utilizado como default-gateway por hosts de diferentes VLANs.
- 8.42. Implementar Private VLANs.
- 8.43. Implementar Port Isolation ou funcionalidade que permita isolamento de portas específicas do switch. As portas isoladas não devem se comunicar entre si, porém podem se comunicar com qualquer outra porta no equipamento que não esteja isolada.
- 8.44. Implementar IEEE 802.1ad com a possibilidade de associar CVIDs específicos para diferentes SVIDs (selective Q-in-Q ou 802.1ad CEP). A implementação deverá permitir a tradução do CVID.
- 8.45. Implementar IEEE 802.1ag (Connectivity Fault Management).
- 8.46. Implementar IEEE 802.3ah Ethernet OAM – Unidirectional Link Fault Management.
- 8.47. Implementar funcionalidade baseada na recomendação do ITU-T Y.1731 com medição de, no mínimo, Frame Delay.
- 8.48. Implementar o protocolo ITU-T G.8032 ERPS.
- 8.49. Implementar protocolo de resiliência em camada 2, específico para topologias em anel, que permita tempo de convergência inferior a 200 ms.
- 8.50. Implementar IEEE 802.1ab Link Layer Discovery Protocol (LLDP).
- 8.51. Implementar LLDP-MED (Media Endpoint Discovery).
- 8.52. Implementar roteamento estático com suporte a, no mínimo, 1000 rotas.
- 8.53. Implementar, no mínimo, 2000 interfaces IP (IPv4 ou IPv6).
- 8.54. Implementar os protocolos de roteamento IP: RFC 1058 – RIP v1 e RFC 2453 – RIP v2.
- 8.55. Suportar o protocolo de roteamento OSPFv2, incluindo autenticação MD5.
- 8.56. "A implementação de OSPF deve estar de acordo com as seguintes RFCs:
- 8.57. RFC 1587 The OSPF NSSA Option
- 8.58. RFC 1765 OSPF Database Overflow
- 8.59. RFC 2370 The OSPF Opaque LSA Option
- 8.60. RFC 3623 Graceful OSPF Restart"
- 8.61. A implementação de OSPF e rotas estáticas deve incluir ECMP (Equal Cost Multi Path).
- 8.62. Implementar PIM Snooping.

- 8.63. Suportar protocolo de multicast PIM-SM para IPv4 e IPv6.
- 8.64. Suportar PIM-DM para IPv4 e IPv6.
- 8.65. Suportar PIM-SSM segundo a RFC 3569.
- 8.66. Suportar MSDP (Multicast Source Discovery Protocol), de acordo com a RFC 3618.
- 8.67. Suportar VRRPv3 (RFC 5798).
- 8.68. Deve suportar BGPv4 de acordo com as seguintes RFCs:
- 8.69. "RFC 4271, Border Gateway Protocol 4
- 8.70. RFC 5065, Autonomous System Confederations for BGP
- 8.71. RFC 4456, BGP Route Reflection
- 8.72. RFC 1997, BGP Communities Attribute
- 8.73. RFC 1745, BGP4/IDRP for IP-OSPF Interaction
- 8.74. RFC 2439, BGP Route Flap Damping
- 8.75. RFC 5492, Capabilities Advertisement with BGP-4
- 8.76. RFC 2918, Route Refresh Capability for BGP-4
- 8.77. RFC 4360, BGP Extended Communities Attribute
- 8.78. RFC 4760, Multiprotocol Extensions for BGP4
- 8.79. RFC 4724, Graceful Restart Mechanism for BGP
- 8.80. RFC 6793, BGP Support for four-octet AS number space"
- 8.81. A implementação de BGP deve incluir ECMP (Equal Cost Multi Path).
- 8.82. "Deve implementar Dual Stack, ou seja, IPv6 e IPv4, com suporte as seguintes funcionalidades/RFCs:
- 8.83. RFC 1981, Path MTU Discovery for IPv6, August 1996 - Host Requirements
- 8.84. RFC 5095, Internet Protocol, Version 6 (IPv6) Specification
- 8.85. RFC 4861, Neighbor Discovery for IP Version 6, (IPv6)
- 8.86. RFC 2462, IPv6 Stateless Address Auto configuration - Host Requirements
- 8.87. RFC 2463, Internet Control Message Protocol (ICMPv6) for the IPv6 Specification
- 8.88. RFC 2464, Transmission of IPv6 Packets over Ethernet Networks
- 8.89. RFC 2465, IPv6 MIB, General Group and Textual Conventions
- 8.90. RFC 2466, MIB for ICMPv6
- 8.91. RFC 3513, Internet Protocol Version 6 (IPv6) Addressing Architecture
- 8.92. RFC 3587, Global Unicast Address Format"
- 8.93. Implementar os seguintes protocolos em IPv6: Ping, Traceroute, Telnet, SSHv2, SNMP, Syslog, Sntp e DNS.
- 8.94. "Deve suportar IPv6 de acordo com as seguintes RFCs:
- 8.95. RFC 1981, Path MTU Discovery for IPv6, August 1996 - Router Requirements
- 8.96. RFC 2462, IPv6 Stateless Address Auto configuration - Router Requirements
- 8.97. RFC 2080, RIPng
- 8.98. RFC 2893, Configured Tunnels
- 8.99. RFC 3056, 6-to-4
- 8.100. RFC 2462, IPv6 Stateless Address Auto configuration - Router Requirements
- 8.101. RFC 2710, IPv6 Multicast Listener Discovery v1 (MLDv1) Protocol
- 8.102. RFC 3810, IPv6 Multicast Listener Discovery v2 (MLDv2) Protocol
- 8.103. RFC 6106, IPv6 Router Advertisement Options for DNS Configuration

- 8.104. Suportar OSPFv3 conforme a RFC 5340.
- 8.105. Suportar OSPFv3 Graceful Restart conforme RFC 5187.
- 8.106. A implementação de OSPFv3 e rotas estáticas para IPv6 deve incluir ECMP (Equal Cost Multi Path).
- 8.107. Implementar BFD (Bidirectional Forwarding Detection).
- 8.108. Suportar IS-IS, de acordo com as seguintes RFCs:
- 8.109. "RFC 1195, Use of OSI IS-IS for Routing in TCP/IP and Dual Environments (TCP/IP transport only)
- 8.110. RFC 2763, Dynamic Hostname Exchange Mechanism for IS-IS
- 8.111. RFC 2966, Domain-wide Prefix Distribution with Two-Level IS-IS
- 8.112. RFC 2973, IS-IS Mesh Groups
- 8.113. Draft-ietf-isis-restart-02, Restart Signaling for IS-IS
- 8.114. Draft-ietf-isis-ipv6-06, Routing IPv6 with IS-IS

- 8.115. Draft-ietf-isis-wg-multi-topology-11, Multi Topology (MT) Routing in IS-IS"
- 8.116. Implementar Policy Based Routing.
- 8.117. Implementar upload e download de configuração em formato ASCII ou XML, permitindo a edição do arquivo de configuração e, posteriormente, o download do arquivo editado para o equipamento.
- 8.118. Implementar TACACS+ segundo a RFC 1492.
- 8.119. "Implementar autenticação RADIUS com suporte a:
- 8.120. RFC 2865 RADIUS Authentication
- 8.121. RFC 2866 RADIUS Accounting
- 8.122. RFC 3579 RADIUS EAP support for 802.1X"
- 8.123. A implementação de RADIUS deve suportar alteração dinâmica de parâmetros de autorização de uma sessão que já esteja ativa.
- 8.124. A implementação de RADIUS e TACACS+ deve estar disponível para autenticação de usuários via Telnet e Console serial.
- 8.125. Implementar per-command authorization para RADIUS e TACACS+.
- 8.126. Possuir DNS Client para IPv4 segundo a RFC 1591 e DNS Client para IPv6.
- 8.127. Possuir Telnet client and server segundo a RFC 854.
- 8.128. Implementar os seguintes grupos de RMON através da RFC 1757: History, Statistics, Alarms e Events.
- 8.129. Deve implementar RMON2-probe configuration segundo a RFC 2021, podendo ser implementada internamente no switch ou externamente, por meio de probe em hardware utilizando uma porta 1000BaseTX.
- 8.130. Implementar sFlow ou Netflow, em hardware.
- 8.131. Implementar a atualização de imagens de software e configuração através de um servidor TFTP.
- 8.132. Suportar múltiplos servidores Syslog.
- 8.133. Implementar ajuste de clock do equipamento utilizando NTP com autenticação MD5 e SNTP.
- 8.134. Implementar Port Mirroring, permitindo espelhar até 128 portas físicas ou 16 VLANs para até 16 portas de destino (portas de análise). Deve ser possível configurar mais de uma sessão de espelhamento simultânea.
- 8.135. Implementar RSPAN (Remote Mirroring), permitindo espelhar o tráfego de uma porta ou VLAN de um switch remoto para uma porta de um switch local (porta de análise).
- 8.136. Implementar gerenciamento através de SNMPv1 (RFC 1157), v2c (RFCs 1901 a 1908), v3 (RFCs 3410 a 3415) e SNMP para IPv6.
- 8.137. Implementar SMON de acordo com a RFC 2613.
- 8.138. Implementar cliente e servidor SSHv2.
- 8.139. Implementar cliente e servidor SCP e servidor SFTP.
- 8.140. Implementar gerenciamento via web com suporte a HTTP e HTTPS/SSL, permitindo visualização gráfica da utilização (em percentual, bytes e pacotes) das portas.
- 8.141. A interface gráfica deve permitir visualização de informações do sistema (VLAN, Portas, Fonte e Fans), monitoramento de Log, utilização de portas, QoS e configuração de portas, VLANs e ACLs.
- 8.142. O equipamento ofertado deve possuir um sistema operacional modular.
- 8.143. O sistema operacional deve possuir função grep/pipe para filtrar a saída de determinado comando.
- 8.144. O sistema operacional deve possuir comandos para visualização e monitoração de cada processo, sendo possível verificar por processo qual o consumo de cpu, process-id e qual o consumo de memória por processo.
- 8.145. O sistema operacional deve possuir comandos para que processos sejam terminados ou reiniciados sem que seja necessário a reinicialização do equipamento. Esta funcionalidade deve estar disponível pelo menos para Telnet, TFTP, HTTP e LLDP na versão atual.
- 8.146. O sistema operacional deve possuir comandos para que processos sejam terminados ou reiniciados sem que seja necessário a reinicialização do equipamento. Esta funcionalidade deve estar disponível pelo menos para Telnet, TFTP, HTTP, LLDP, OSPF e BGP na versão atual.
- 8.147. Implementar linguagem de scripting baseada em Python, permitindo a automatização de tarefas. A linguagem deve implementar estruturas de controle como loops e execução condicional e permitir a definição de variáveis.

- 8.148. Implementar protocolo de monitoramento de status de comunicação entre dois switches, que possibilite que uma porta seja desabilitada caso seja detectada uma falha de comunicação entre os dois peers.
- 8.149. Implementar funcionalidade que permita sua auto-configuração através dos protocolos DHCP e TFTP, permitindo o provisionamento em massa com o mínimo de intervenção humana.
- 8.150. Deve disponibilizar API (Application Programming Interface) aberta para integração com aplicações.
- 8.151. Implementar Rate limiting de entrada em todas as portas. A granularidade deve ser configurável em intervalos de 64Kbps para portas de até 1Gbps. Caso o equipamento ofertado possua suporte a portas 10Gbps, a granularidade para este tipo de interface deve ser configurável em intervalos de 1Mbps. A implementação de Rate Limiting deve permitir a classificação do tráfego utilizando-se ACLs e parâmetros, MAC origem e destino (simultaneamente) IP origem e destino (simultaneamente), portas TCP, portas UDP e campo 802.1p.
- 8.152. Implementar Rate Shaping de saída em todas as portas. A granularidade deve ser configurável em intervalos de 64Kbps para portas de até 1Gbps. Caso o equipamento ofertado possua suporte a portas 10Gbps, a granularidade para este tipo de interface deve ser configurável em intervalos de 1Mbps.
- 8.153. A funcionalidade de Rate Shaping deve permitir a configuração de CIR (Committed Rate), banda máxima, banda mínima e peak rate.
- 8.154. Implementar a leitura, classificação e remarcação de QoS (802.1p e DSCP).
- 8.155. Implementar remarcação de prioridade de pacotes Layer 3, remarcando o campo DiffServ para grupos de tráfego classificados segundo portas TCP e UDP, endereço/subrede IP, VLAN e MAC origem e destino.
- 8.156. Implementar 8 filas de prioridade em hardware por porta.
- 8.157. Implementar os algoritmos de gerenciamento de filas WRR (Weighted Round Robin), WDRR (Weighted Deficit Round Robin) e SP (Strict Priority).
- 8.158. Deve implementar, ao menos dois dos algoritmos acima, simultaneamente em uma mesma porta.
- 8.159. "Implementar as seguintes RFCs:
- 8.160. RFC 2474 DiffServ Precedence
- 8.161. RFC 2598 DiffServ Expedited Forwarding (EF)
- 8.162. RFC 2597 DiffServ Assured Forwarding (AF)
- 8.163. RFC 2475 DiffServ Core and Edge Router Functions"
- 8.164. Implementar classificação de tráfego para QoS em Layer1-4 (Policy-Based Mapping) baseado em MAC origem e destino, IP origem e destino, TCP/UDP port, Diffserv e 802.1p.
- 8.165. Implementar detecção de oscilação (flap) de links, permitindo desabilitar uma porta caso a porta oscile acima de um limiar configurado.
- 8.166. Implementar funcionalidade que permita que somente endereços designados por um servidor DHCP tenham acesso à rede.
- 8.167. Implementar funcionalidade que permita que somente servidores DHCP autorizados atribuam configuração IP aos clientes DHCP (Trusted DHCP Server).
- 8.168. Implementar Gratuitous ARP Protection.
- 8.169. Implementar detecção e proteção contra ataques Denial of Service (DoS) direcionados a CPU do equipamento por meio da criação dinâmica e automática de regras para o bloqueio do tráfego suspeito.
- 8.170. Implementar limitação de número de endereços MAC aprendidos por uma porta, para uma determinada VLAN.
- 8.171. Implementar travamento de endereços MAC, permitindo a adição estática de endereços para uma determinada porta ou utilizando os endereços existentes na tabela MAC. O acesso de qualquer outro endereço que não esteja previamente autorizado deve ser negado.
- 8.172. Implementar login de rede baseado no protocolo IEEE 802.1x, permitindo que a porta do switch seja associada a VLAN definida para o usuário no servidor RADIUS.
- 8.173. A implementação do IEEE 802.1x deve incluir suporte a Guest VLAN, encaminhando o usuário para esta VLAN caso este não possua suplicante 802.1x ativo, em caso de falha de autenticação e no caso de indisponibilidade do servidor AAA.

- 8.174. Implementar múltiplos suplicantes por porta, onde cada dispositivo deve ser autenticado de forma independente, podendo ser encaminhados a VLANs distintas. As múltiplas autenticações devem ser realizadas através de IEEE 802.1x.
- 8.175. Implementar autenticação baseada em web, com suporte a SSL, através de RADIUS ou através da base local do switch.
- 8.176. Implementar autenticação baseada em endereço MAC, através de RADIUS ou através da base local do switch.
- 8.177. Implementar ACLs de entrada (ingress ACLs) em hardware, baseadas em critérios da camada 2 (MAC origem e destino e campo 802.1p), camada 3 (IP origem e destino) e camada 4 (portas TCP e UDP), em todas as interfaces e VLANs, com suporte a endereços IPv6.
- 8.178. As ACLs devem ser configuradas para permitir, negar, aplicar QoS, espelhar o tráfego para uma porta de análise, criar entrada de log e incrementar contador.
- 8.179. Implementar funcionalidade que permita a execução de ACLs em um determinado horário do dia (time-based ACLs).
- 8.180. Implementar políticas por usuário, permitindo que as configurações de ACL, QoS sejam aplicadas na porta utilizada para a conexão à rede, após a autenticação.
- 8.181. Implementar a configuração de telefones IP de forma automática, permitindo a detecção do aparelho através do protocolo LLDP e a configuração de VLAN e QoS para a porta.
- 8.182. Implementar a configuração de telefones IP de forma automática, permitindo a detecção do aparelho através do protocolo LLDP e repasse de configuração de VLAN e QoS para o telefone através do protocolo LLDP-MED.
- 8.183. Implementar Policy Based Switching, ou seja, possibilitar que o tráfego classificado por uma ACL seja redirecionado para uma porta física específica.
- 8.184. Implementar funcionalidade que permita o mapeamento de usuários identificados via Kerberos (com a credencial de usuário no domínio), IEEE 802.1x e LLDP, provendo informações como endereço MAC, VLAN e porta física. Estas informações devem estar disponíveis na linha de comando (CLI) do equipamento.
- 8.185. Suportar protocolo OpenFlow versão 1.0.
- 9. Atualização Tecnológica com Expansão de 5 Swiches de Borda Extreme Networks:**
- 9.1. Switch de acesso com 24 portas 10/100/1000 Mbps UTP e 2 interfaces SFP+ 10Gbps.
- 9.2. Montável em rack 19" incluindo todos os acessórios necessários.
- 9.3. Deve possuir fonte de alimentação AC bivolt, com seleção automática de tensão (na faixa de 100 a 240 V) e de frequência (de 50/60 Hz).
- 9.4. Deve possuir cabo de alimentação para fonte com, no mínimo, 1,00m (um metro) de comprimento com plugue no padrão (NBR 14136:2002).
- 9.5. Deve possuir capacidade para, pelo menos, 16.000 endereços MAC na tabela de comutação.
- 9.6. Deve implementar no mínimo 1024 vlans simultaneamente.
- 9.7. Deve possuir switching bandwidth full-duplex de, no mínimo, 88 Gbps e taxa de encaminhamento de, no mínimo, 65 Mpps, considerando transmissões de 84 bytes (frame de dados com 64 bytes mais overhead de 20 bytes).
- 9.8. Deve suportar Jumbo Frames de, no mínimo, 9 KBytes.
- 9.9. Deve possuir, no mínimo, 26 portas ativas sendo 24 portas Ethernet 10/100/1000 autosensing com conectores RJ-45 e 2 slots 10 Gbps do tipo SFP+ (módulos/transceiver), full-duplex, para fibras ópticas.
- 9.10. As interfaces 10/100/1000 devem obedecer às normas técnicas IEEE802.3i (10BaseT), IEEE802.3u (100BaseT), IEEE 802.3ab (1000BaseT) e IEEE802.3x (Flow Control).
- 9.11. Todas as portas Ethernet 10/100/1000 devem suportar configuração Half Duplex e Full Duplex, com a opção de negociação automática.
- 9.12. Todas as portas Ethernet 10/100/1000 devem suportar autoconfiguração de crossover (Auto MDIX).
- 9.13. Deve possuir LEDs para a indicação do status das portas e atividade.
- 9.14. Deve possuir capacidade de associação das portas 10/100/1000 e das portas 10 Gbps SFP+ formando uma única interface lógica com as mesmas facilidades das interfaces originais, compatível com a norma IEEE 802.3ad.
- 9.15. Deve possuir porta de console para ligação direta para acesso à interface de linha de comando. Poderá ser fornecida porta de console com interface USB.

- 10.** Atualização Tecnológica com Expansão de 30 Access Point Extreme Networks
- 10.1. Deve ser do mesmo fabricante do controlador WLAN;
- 10.2. Access Point (AP) atendendo simultaneamente aos padrões:
 - 10.2.1. IEEE 802.11a;
 - 10.2.2. IEEE 802.11b;
 - 10.2.3. IEEE 802.11g;
 - 10.2.4. IEEE 802.11n;
 - 10.2.5. IEEE 802.11ac;
- 10.3. Implementar a conexão simultânea de dispositivos configurados nos padrões:
 - 10.3.1. IEEE 802.11b/g/n;
 - 10.3.2. IEEE 802.11a/n;
 - 10.3.3. IEEE 802.11ac;
- 10.4. Implementar funcionamento simultâneo dos rádios 2.4GHz e 5.0 GHz;
- 10.5. Implementar todas as seguintes taxas de transmissão e fallback automático:
 - 10.5.1. IEEE 802.11a: 54, 48, 36, 24, 18, 12, 9 e 6 Mbps;
 - 10.5.2. IEEE 802.11b: 11, 5.5, 2 e 1 Mbps;
 - 10.5.3. IEEE 802.11g: 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2 e 1 Mbps;
 - 10.5.4. IEEE 802.11n: 450, 300, 270, 180, 120, 60, 45, 30 e 15 Mbps;
 - 10.5.5. IEEE 802.11ac: 1300, 866.7, 780, 390, 260, 130, 97.5, 65 e 32.5 Mbps;
- 10.6. Deve vir acompanhado dos componentes que permitam sua fixação especificamente em parede;
- 10.7. O Access Point ofertado deve consumir de no máximo 13W com todas as suas funcionalidades habilitadas;
- 10.8. Possuir desempenho em conexão cabeada de, no mínimo, 50000pps;
- 10.9. Deve implementar instalação plug and play;
- 10.10. Transmissão máxima de potência de cada rádio deve ser de, no mínimo, 26dBm em 2.4 GHz e 5 GHz;
- 10.11. Deve implementar associação de policieis para clientes, sem precisar de segmentação via SSIDs dedicados;
- 10.12. PORTAS DE REDE
- 10.13. Possuir pelo menos 1 (uma) porta Gigabit Ethernet 10/100/1000 Mbps, auto-sensing, com conector RJ-45 Fêmea para dados, não sendo aceito portas de gerência;
- 10.14. Implementar sua energização por pelo menos uma das interfaces de rede descrita no item anterior, através de um único injetor padrão IEEE 802.3af PoE;
- 10.15. O Access Point deve permitir sua operação em capacidade máxima mesmo quando energizado através do injetor PoE;
- 10.16. Suportar sua energização através de fonte externa ou interna que opere com tensão de entrada para a fonte em 110/220VAC;
- 10.17. LEDS E SINALIZAÇÃO
- 10.18. Possuir LEDs indicativos do estado de operação;
- 10.19. Possuir LEDs indicativos da estado dos rádios;
- 10.20. Possuir LEDs indicativos da estado da interface Gigabit Ethernet;
- 10.21. ANTENAS
- 10.22. Possuir antenas:
- 10.23. Internas ao AP;
- 10.24. Com ganho de, no mínimo, 3dBi para 2.4GHz;
- 10.25. Com ganho de, no mínimo, 4dBi para 5.0GHz;
- 10.26. Que implemente padrão de irradiação omnidirecional;
- 10.27. Que implemente operação simultânea em 2x2:2 MIMO;
- 10.28. MODO DE OPERAÇÃO
- 10.29. Implementar modo de operação onde o AP possa estar remotamente conectado ao controlador wireless tanto de forma direta em uma rede de camada 2 ou em qualquer ponto de uma rede segmentada em subredes de camada 3;
- 10.30. O AP deve permitir sua operação através da conexão a um controlador principal e a um controlador secundário;
- 10.31. Selecionar automaticamente o canal de transmissão;

- 10.32. Ajustar dinamicamente o nível de potência e canal de rádio;
- 10.33. Possuir suporte a pelo menos 8 SSIDs para 2.4GHz e 8 SSIDs para 5.0GHz;
- 10.34. Permitir habilitar e desabilitar a divulgação do SSID;
- 10.35. Deve implementar Fast Roaming ou funcionalidade similar de forma a garantir o Roaming sem perda de conexão;
- 10.36. Não deve haver licença restringindo o número de usuários por AP;
- 10.37. Implementar VLANs conforme padrão IEEE 802.1Q;
- 10.38. Implementar cliente DHCP, para configuração automática de rede;
- 10.39. Configurar-se automaticamente ao ser conectado na rede;
- 10.40. Implementar Packet aggregation A-MPDU, A-MSDU para 802.11ac e 802.11n;
- 10.41. GERENCIAMENTO
- 10.42. Possuir porta de console para configuração;
- 10.43. Permitir via controlador wireless, a atualização remota do sistema operacional;
- 10.44. Permitir via controlador wireless, a atualização remota dos arquivos de configuração utilizados no equipamento;
- 10.45. Implementar funcionamento em modo gerenciado pelo controlador wireless;
- 10.46. SEGURANÇA e QoS
- 10.47. Possuir entrada para dispositivo antifurto do tipo Kensington lock ou similar;
- 10.48. Suportar varredura de Rádio Frequência nas tecnologias 802.11a, 802.11b/g, 802.11n e 802.11ac para identificação de APs não autorizados (rogues);
- 10.49. Suportar varredura de Rádio Frequência nas tecnologias 802.11a, 802.11b/g, 802.11n, 802.11ac para identificação de interferências nos canais na rede WLAN;
- 10.50. Implementar IEEE 802.1x de acesso do próprio AP a rede cabeada;
- 10.51. Implementar autenticação com geração dinâmica de chaves criptográficas por sessão e por usuário;
- 10.52. Implementar, em conjunto com o Controlador WLAN, WEP, chaves estáticas e dinâmicas;
- 10.53. Implementar, em conjunto com o Controlador WLAN, WPA com algoritmo de criptografia TKIP e MIC;
- 10.54. Implementar, em conjunto com o Controlador WLAN, WPA2 com algoritmo de criptografia AES;
- 10.55. Implementar padrão IEEE 802.11e WMM da Wi-Fi Alliance para priorização de tráfego, suportando aplicações em tempo real, tais como VoIP e vídeo;
- 10.56. Suportar modo de operação WIPS dedicado onde o AP possa estar
- 10.57. Possuir certificação/homologação da ANATEL;

ANEXO II.2

AMBIENTE DE INFORMÁTICA - DATACENTER

Objeto: infraestrutura, composta por: Processamento de dados com virtualização, armazenamento de dados, Rede Lan e wireless com gerenciamento centralizado, sistema de segurança e demais componentes que compõem a solução - DATACENTER.

As descrições abaixo podem estar na primeira pessoa, devido ao mesmo ser cópia do antigo edital que destinava-se a contratação de empresa para fornecimento e ambientação de DATACENTER, mas que servem de parâmetro para este edital, como orientação e base, para que as licitantes saibam em que instrumentos deverão operacionalizar.

A solução deverá ser fornecida por um único licitante afim de garantir a perfeita integração a empresa vencedora deverá prover o serviço de manutenção suporte e gestão da solução proposta. Todos os equipamentos integrantes da solução deverão ser novos sem uso anterior, os equipamentos rede, wireless e software de gerenciamento deverão ser do mesmo fabricante, para garantir a integração e o gerenciamento centralizado.

Descrição dos equipamentos e serviços que compõem a solução:

1. Serviços de implementação da solução de infraestrutura:

- 1.1. Instalação do rack fornecido no presente edital, incluindo regular e nivelamento do mesmo;
- 1.2. Instalação física de todos os equipamentos do presente edital (storage, gavetas, discos, servidores e switches) incluindo desembalagem, montagem, afiação e cabeamento nos racks fornecidos, englobando ligações elétricas, lógicas (LAN e SAN) e ativação da solução;
- 1.3. Energização dos equipamentos e análise do funcionamento do ambiente;
- 1.4. Identificação de todas as conexões efetuadas para futuras manutenções e alterações na configuração;
- 1.5. Atualização do firmware dos componentes de hardware da solução (módulos de gerenciamento, módulos LAN e SAN, controladoras, gavetas, discos, BIOS de servidores) para a última versão disponível conforme matriz de compatibilidade do fabricante;
- 1.6. Configuração dos parâmetros de BIOS dos servidores e interfaces para atender as recomendações dos fabricantes para o software de virtualização;
- 1.7. Criação do RAID na controladora de discos locais;
- 1.8. Execução do zoning e ISLs dos switches SAN
- 1.9. Criação de VLANs nos módulos LAN dos para o ambiente de rede da PM de Vacaria;
- 1.10. Instalação, atualização e configuração do software de gerenciamento da solução, incluindo configuração das contas de administrador para acesso à solução, e-mails de alerta, filtragem de eventos e envio de SNMP para software de monitoramento;
- 1.11. Adição dos equipamentos no ambiente do software de gerenciamento;
- 1.12. Sessão de orientação onde será abordada a utilização do software de gerenciamento e do software de monitoramento, incluindo criação de novos usuários, configuração de autorizações na plataforma. A PM Vacaria deve ter a capacidade de adição de novos equipamentos e/ou recursos, implementar configurações, consultar as configurações existentes, efetuar o monitoramento da solução, enfim, a completa utilização da ferramenta;
2. Configuração da solução de armazenamento
 - 2.1. Instalação do software de gerenciamento, replicação e movimentação de dados no storage, incluindo patches e atualizações necessárias;
 - 2.2. Habilitação das funcionalidades e recursos previstas na solução disponibilizada;
 - 2.3. Sessão de orientação onde será abordada a utilização do software e do hardware de armazenamento do presente edital, incluindo criação de snapshots, clones, mirror, utilização de Thin Provisioning e Tierização, criação de disk groups, monitoramento de utilização e carga, enfim, a completa utilização da ferramenta e do hardware adquirido;
3. Instalação do software de virtualização
 - 3.1. Instalação do software de virtualização (hypervisor) VMware vSphere 5.1 em sua última release nos servidores, conforme matriz de compatibilidade dos equipamentos;
 - 3.2. Instalação de patches e atualizações necessários;
 - 3.3. Instalação e configuração da ferramenta de gerenciamento do ambiente virtualizado VMware vCenter Server 5.1;
 - 3.4. Configuração da integração do software de virtualização com o software de replicação da storage e reconhecimento das áreas de discos replicadas;
 - 3.5. Configuração da replicação das máquinas virtuais no software de backup e replicação;
 - 3.6. Instalação e configuração da ferramenta de alta disponibilidade de entre servidores (módulo HA). Os servidores de virtualização deverão operar em um ambiente de alta disponibilidade onde, em caso de falha de qualquer um dos servidores, as máquinas virtuais deste servidor poderão ser reiniciadas automaticamente em qualquer outro servidor de virtualização;

- 3.7. Configuração da funcionalidade de migração online de máquinas virtuais entre servidores físicos sem interrupção do processamento;
- 3.8. Criação de clusters de alta-disponibilidade entre os hypervisors;
- 3.9. Instalação e configuração da ferramenta de recuperação de desastres disponibilizada na solução e todos os seus componentes;
- 3.10. Criação de até 2 (duas) políticas de replicação e recuperação de desastres para até 5 (cinco) máquinas virtuais.
- 3.11. Demonstração da verificação do perfeito funcionamento do plano de recuperação, em ambiente isolado, sem afetar as máquinas virtuais em produção;
- 3.12. A configuração dos softwares VMware vCenter Server 5.1 deve ser efetuada em máquina virtual hospedada nos clusters de alta disponibilidade e não em servidores externos ao ambiente caso houver;
- 3.13. Criação de até 2 (dois) templates de máquinas virtuais a ser utilizado no ambiente da PM de Vacaria,
- 3.14. Criação de novas máquinas virtuais através de modelos pré-definidos ou de forma manual e individual;
- 3.15. Deverá permitir o gerenciamento dos recursos físicos e virtuais do ambiente de virtualização, com estatísticas online do uso destes recursos, como I/O, Memória, Processamento, Latência;
4. Conversão de máquinas físicas
 - 4.1. Conversão de 2 (duas) máquinas físicas existentes na infraestrutura de TI da PM de Vacaria para máquinas virtuais no novo ambiente de virtualização;
 - 4.2. Instalação de ferramentas de otimização nas máquinas virtuais convertidas de forma a funcionar com perfeita integração e máximo desenho no novo ambiente de virtualização;
 - 4.3. A contratada deverá garantir que os servidores inicializem corretamente o sistema operacional após a conversão;
 - 4.4. A conversão não será executada em lote, sendo que a cada conversão será feita a validação dos serviços e do funcionamento da máquina virtual antes de iniciar a migração da próxima máquina virtual;
5. Instalação e Configuração da solução de segurança, Firewall;
 - 5.1. A instalação dos equipamentos deverá ser feita por profissionais devidamente qualificados e certificados pelo fabricante contemplando os itens abaixo:
 - 5.1.1. Análise da topologia e arquitetura da rede da contratante, considerando os roteadores e switches de backbone instalados, acesso à Internet, sites remotos, serviços de rede oferecidos aos funcionários da contratante, serviços externos, regras de firewall existentes, bem como qualquer outro equipamento ou sistema relevante na segurança do perímetro, sendo então feitas as configurações gerais do sistema de firewall de acordo com a configuração atual.
 - 5.1.2. Para as regras específicas de usuários e aplicações deverá ser repassado o modo de criação do modelo destas regras, ficando a cargo deste órgão o desenvolvimento conforme suas políticas.
 - 5.1.3. Durante toda a implantação do projeto, o técnico da contratada deverá demonstrar aos técnicos da contratante como instalar e configurar o firewall (instalação assistida). Esta demonstração deverá ser no formato treinamento hands-on com no mínimo 08(oito) horas de duração, contemplando os conceitos das tecnologias utilizadas pelo equipamento e a operação dos principais recursos dos produtos ofertados.
 - 5.1.4. Todo o processo de instalação e configuração do sistema deverá ser documentado pela contratada sob a forma de relatório ou roteiro, de forma que os técnicos da contratante possam reproduzir a instalação do firewall quando necessário consultando a documentação.
6. Instalação e Configuração da solução de Rede Wireless;
 - 6.1. A instalação dos equipamentos deverá ser feita por profissionais devidamente qualificados e certificados pelo fabricante contemplando os itens abaixo:
 - 6.1.1. Deve contemplar todos os acessórios de fixação e a controladora e os access points com os respectivos injetores deverão ser instalados e fixados em local apropriado de forma que cubram toda a área determinada no site survey.
 - 6.1.2. A fixação deverá ser precedida de análise técnica para determinação da melhor altura e posicionamento dos access points e as configurações devem ser realizadas de tal forma que seja obtido o melhor desempenho para transmissão de dados.
 - 6.1.3. As atividades instalação e configuração solução deverão abranger aspectos acerca da disposição dos equipamentos, cronograma de implantação definido após contratação, parâmetros, topologia de rede, conectorização e plano de testes. Tais informações serão confeccionadas e validadas junto à equipe técnica da CONTRATANTE e deverão ser otimizadas para garantir total operabilidade e desempenho no ambiente computacional, considerando:
 - 6.1.3.1. Preparação do atual ambiente para integração com os novos equipamentos;
 - 6.1.3.2. Configuração de interfaces, endereçamento e serviços de rede;
 - 6.1.3.3. Definição e configuração de VLANs para rede WLAN, gerenciamento, roteamento, entre outros;
 - 6.1.3.4. Definição e configuração de métricas de priorização de tráfego de dados, gerência, entre outros;
 - 6.1.3.5. Definição e configuração de parâmetros de roteamento dinâmico, trunking e de agregação de links entre os equipamentos wireless e equipamentos atuais;
 - 6.1.3.6. Definição e configuração de parâmetros de gerenciamento SNMP;
 - 6.1.3.7. Definição e configuração de parâmetros de segurança, incluindo autenticação de usuários e regras de acesso;
 - 6.1.3.8. Plano de testes de conformidade da solução, com acompanhamento de técnico certificado na tecnologia.
 - 6.1.3.9. Todos custos referentes à configuração e instalação dos access points, fornecimento de material, mão de obra e realização dos serviços acima mencionados deverão estar incluídos na proposta.
 - 6.1.4. A empresa deverá configurar a rede sem fio de acordo com as necessidades do CONTRATANTE;
 - 6.1.5. A empresa deverá fornecer a documentação do projeto especificada neste item impressa, encadernada e em arquivo digital.
 - 6.1.5.1. Documentação de site survey
 - 6.1.5.2. Cronograma do projeto;
 - 6.1.5.3. Memorial dos serviços executados contendo marca e modelo dos equipamentos utilizados;

- 6.1.5.4. Relatório de testes contemplando os aspectos: Testes de Performance; Testes de PER (Packet Error Rate) – erros nos pacotes detectados pelo CRC devido, sobretudo, a efeitos de multi-percurso ou colisões na rede.
- 6.1.5.5. Testes de Interferências:
- 6.1.5.6. Análise de Cobertura da rede;
- 6.1.5.7. Verificação do cumprimento dos requisitos;
- 6.1.5.8. Verificação do projeto da rede e documentação disponível.
- 7. Instalação e Configuração Switch Core de Rede e Distribuição;
- 7.1. Entende-se como Equipamento de Core todos os dispositivos modulares ofertados. Os serviços a serem fornecidos para este atendimento são:
 - 7.1.1. Instalação física de chassi em rack;
 - 7.1.2. Instalação de fontes de alimentação, principais e redundantes, com respectivos cabos de energia; 7.1.3. Configuração básica de endereçamento IP, sistema e dados SNMP.;
 - 7.1.4. Configuração do equipamento, com todas as funcionalidades solicitadas e necessárias para seu correto funcionamento: VLAN, Rotas estáticas ou dinâmicas, configuração SNMP, configuração de segurança, ACL, 802.1x.
- 7.2. Deve ser fornecida documentação com configurações dos equipamentos e diagrama da rede instalada;
- 7.3. O cabeamento lógico e elétrico necessário para implantação de toda a solução será de responsabilidade da contratada, assim não sendo necessário a contemplar no projeto.

Ferramenta de Gerenciamento Centralizado

Quantidade: 01 unidade

- 1. Descobrimto, Mapeamento e Configuração Básica
 - 1.1. Deve permitir o gerenciamento de configurações, desempenho e falhas na rede;
 - 1.2. Deve permitir sua instalação nas seguintes plataformas:
 - Windows Server 2003
 - Windows XP
 - Windows Server 2008 Enterprise
 - Windows 7
 - Windows 8
 - Red Hat Enterprise Linux
 - SuSE Linux versions 10 and 11
 - Ubuntu 11.10 Desktop version
 - VMware ESXi 4.0, 4.1, 5.0 or 5.1 server
 - 1.3. O software de gerenciamento deve suportar o protocolo SNMP de gerenciamento de versão 1, 2 e 3;
 - 1.4. Deve permitir o gerenciamento de todos os agentes SNMP dos dispositivos que compõe a infraestrutura de TI; isto é; deve permitir a coleta e alteração das informações contidas nos objetos da Management Information Base (MIB) dos mesmos;
 - 1.5. Deve permitir o descobrimento de equipamentos presentes em uma ou mais sub-redes, a fim de garantir uma auditoria constante na infra-estrutura de TI;
 - 1.6. Deve permitir a criação de topologias / mapas automáticos da rede através de protocolos Layer 2 e Layers 3 (OSFP)
 - 1.6.1. O mapa deve permitir a identificação de problemas com os dispositivos visualmente;
 - 1.6.2. Permitir a visão agrupada da topologia conforme configuração do usuário;
 - 1.7. O software deve permitir a criação, edição, remoção de VLANs nos dispositivo e associação das portas as mesmas;
 - 1.8. Deve possuir um servidor de TFTP e BOOTP integrado a ferramenta, possibilitando o upgrade e downgrade de softwares dos dispositivos;
 - 1.9. Deve permitir a identificação do status das portas dos dispositivos up ou down, enable ou disable, tecnologia e velocidade das portas;
 - 1.10. Deve permitir a configuração do Dynamic Egress dos switches da rede;
 - 1.11. Deve permitir a configuração de alertas da estação de gerenciamento, baseado nos eventos, severidade, tipo e categoria;
 - 1.12. A ferramenta deve permitir a configuração gráfica de múltiplos domínios spanning tree (MSTP);
 - 1.13. A ferramenta deve permitir a configuração gráfica de um servidor SMTP externo para o envio de informações de gerenciamento da ferramenta.
 - 1.14. Deve permitir a alteração dos valores de um conjunto de objetos da MIB, em vários dispositivos;
 - 1.15. Deve permitir exportar a tabela de dados coletados e alarmes, para os formatos "csv e html";
 - 1.16. Deve permitir envio de e-mail ou execução de um script ou programa integrado com a ferramenta para alertas;
 - 1.17. A ferramenta deve permitir o gerenciamento dos dispositivos através de uma página WEB customizável;
 - 1.18. Permitir a localização de um dispositivo da rede baseado nos argumentos endereço IP, endereço MAC, user name, nome da máquina e sub-rede;
 - 1.19. Permitir integração com a base de dados do framework HP Open View;
 - 1.20. Deve permitir a otimização do processo de busca na tabela Node/Alias dos dispositivos da rede;
 - 1.21. A solução deverá prover recursos de "troubleshooting" capaz de mostrar por meio do RMON dados presentes nos switches performance ou estatísticas de utilização;
- 2. Configurações de Segurança e QoS:
 - 2.1. Deve permitir o gerenciamento das configurações de filas e priorização de tráfego dos dispositivos da rede;
 - 2.2. Deve permitir a criação de perfis de classificação do tráfego nos dispositivos, baseado em usuários;
 - 2.3. Deve permitir a criação e o gerenciamento de políticas de acesso a rede nos dispositivos;
 - 2.4. Deve suportar e gerenciar graficamente as características do padrão IEEE 802.1X;

- 2.5. Deve permitir a configuração para atribuição de perfil de usuário com regras e QoS específico conforme autenticação do usuário;
- 2.6. A ferramenta deve permitir a configuração gráfica das taxas de inbound rate limit – IRL;
- 2.7. A ferramenta deve permitir a configuração estática e dinâmica da funcionalidade MAC Locking ou Port Security, para executar o LOCK de MAC Address na rede;
- 2.8. A ferramenta deve permitir a configuração gráfica de vários métodos de autenticação, atendendo no mínimo a configuração da autenticação WEB, autenticação MAC e autenticação IEEE 802.1x;
- 2.9. A ferramenta deve permitir a configuração de classes de serviços, utilizando no mínimo os parâmetros de Class of Service – COS, 802.1p priority e IP Type of Service – TOS;
- 2.10. A ferramenta deve permitir a configuração gráfica dos parâmetros da RFC 3580 (VLAN dinâmica conforme autenticação) nos dispositivos de rede;
- 2.11. Deve permitir o agrupamento de portas automático e/ou manual para atribuição de regras de segurança. (ex. Uplinks em fibra)
- 2.12. A ferramenta deve permitir a configuração gráfica dos parâmetros de re-autenticação dos usuários nas portas dos switches;
- 2.13. A ferramenta deve permitir a configuração da autenticação CEP – Convergence End Point, para atribuição automática de VLAN ou perfil de equipamentos com suporte a CEP – ex. telefones IP, câmeras IP, etc.
3. Controle de Inventário e Backup
- 3.1. A ferramenta deve permitir o inventário detalhado de atributos dos dispositivos da rede, atendendo no mínimo números seriais, versão de firmware, tipo de CPU e memória;
- 3.2. A ferramenta deve permitir o armazenamento histórico das configurações dos dispositivos;
- 3.3. A ferramenta deve permitir a comparação da configuração atual do dispositivo com a configuração armazenada na ferramenta;
- 3.4. A ferramenta deve possuir a capacidade de gerar relatórios de para planejamento de capacidade, atendendo no mínimo a geração de relatórios da utilização mínima de chassis e portas, informações sobre FRU – Field Replaceable Upgradeable nos dispositivos;
- 3.5. Deve permitir o upgrade da PROM de BOOT dos dispositivos, unitariamente e para um grupo de dispositivos;
- 3.6. A ferramenta deve permitir a execução do reset dos dispositivos através do protocolo SNMP;
4. Resposta Automática para Eventos de Segurança
- 4.1. Permitir a criação de um grupo de VLANs com características pré-definidas, permitindo uma implementação ou auditoria instantânea dos domínios de colisão criados nos dispositivos da rede
- 4.2. Capacidade de localizar o usuário originador de um ataque ou exploração de vulnerabilidade, proveniente da identificação do IDS, através das tabelas Node Alias dos switches;
- 4.3. Capacidade de localização de um usuário em qualquer porta de um switch, através do protocolo SNMP, quando detectado a ação worms e vírus na rede;
- 4.4. A ferramenta deve possuir um trigger test que permita o teste de comunicação entre os mecanismos de segurança e localização dos usuários na rede;

Quantidade: 05 unidades

Características Físicas

1. Deve possuir estrutura do tipo desktop, para instalação em rack padrão EIA (19”) e possuir kits completos para instalação;
 - 1.1. Deve possuir altura máxima de 1 RU;
 - 1.2. Deve possuir fonte de alimentação interna ao equipamento, que opere com tensões de entrada entre 100 e 240 VAC e suporte frequência entre 50/60 Hz;
 - 1.3. Deve suportar fonte redundante externa.

Quantidade de Portas

- 1.4. Deve possuir porta console RS-232 com conectores DB9 ou RJ-45;
- 1.5. Deve estar configurado com pelo menos:
 - 1.5.1. 24 (vinte e quatro) portas fixas em Gigabit Ethernet, 10/100/1000Base-T em conectores RJ45;
 - 1.5.2. 04 (quatro) portas do tipo SFP;
- 1.6. O equipamento deve permitir o uso simultâneo de todas as interfaces solicitadas.

Capacidade e Performance

- 1.7. Deve possuir capacidade de throughput de, no mínimo 40 Mpps;
- 1.8. Deve possuir capacidade de switching de, no mínimo 55 Gbps;
- 1.9. Deve implementar tabela de endereçamento para, no mínimo, 16.000 endereços MAC;
- 1.10. Deve implementar, no mínimo, 250 VLANs (IEEE 802.1Q);
- 1.11. Deve permitir, no mínimo, 4.090 identificadores de VLAN (VID).

Funcionalidades

- 1.12. Deve permitir agregação de links conforme o padrão IEEE802.3ad suportando no mínimo 05 grupos LAG com no mínimo 08 portas por grupo LAG;
- 1.13. Deve implementar espelhamento de tráfego para análise de rede;
- 1.14. Deve implementar gerenciamento via protocolo SNMP v1, v2c e v3. Sendo que para a versão 3 deve implementar autenticação via MD5 e criptografia DES;
- 1.15. Deve suportar o gerenciamento via interface gráfica;

- 1.16. Deve implementar autenticação IEEE802.1x;
- 1.17. Deve implementar autenticação MAC.

Protocolos

- 1.18. Deve implementar IEEE 802.1Q (VLAN Tagging);
- 1.19. Deve implementar IEEE 802.1s (Multiple Spanning Tree);
- 1.20. Deve implementar IEEE 802.3x (Flow Control);
- 1.21. Deve implementar IEEE 802.1D (MAC Bridges);
- 1.22. Deve implementar IEEE 802.1w (Rapid Spanning Tree);
- 1.23. Deve implementar IGMP snooping v1, v2 e v3;
- 1.24. Deve implementar Jumbo Frame;
- 1.25. Deve implementar o padrão IEEE 802.1AB e LLDP-MED.

Roteamento

- 1.26. Deve implementar roteamento IP através de rotas estáticas.

Qualidade de serviço

- 1.27. Deve implementar IEEE 802.1p (Classificação de tráfego);
- 1.28. Deve implementar Rate Limiting;
- 1.29. Deve possuir, no mínimo, 06 filas de prioridade por porta;
- 1.30. Deve possuir algoritmo de enfileiramento Strict Priority e Weighted Round Robin.

Segurança

- 1.31. Deve permitir o controle de acesso a rede baseado no endereço MAC;
- 1.32. Deve implementar ACL ou outra funcionalidade de filtragem de tráfego por endereço MAC de origem/destino e por endereço IP de origem/destino;
- 1.33. Deve possuir facilidade que permita desabilitar automaticamente uma interface de acesso que esteja recebendo pacotes BPDU (Bridge Protocol Data Unit), através de funcionalidade BPDU Guard ou similar;
- 1.34. Deve implementar funcionalidade que bloqueie a operação de servidores DHCP inválidos (DHCP Spoof Protection);
- 1.35. Deve implementar funcionalidade de ARP Spoof Protection;
- 1.36. Deve permitir o isolamento de portas pertencente à uma mesma VLAN, através da funcionalidade Private VLAN ou similar.

Gerenciamento

- 1.37. Deve implementar SSHv2;
- 1.38. Deve implementar SNMP v1, v2c e v3;
- 1.39. Deve implementar NTP ou SNTP;
- 1.40. Deve implementar Syslog;
- 1.41. Deve possibilitar autenticação em base remota por meio do protocolo RADIUS;
- 1.42. Deve implementar RADIUS ou TACACS+ para controle de gerenciamento do switch;
- 1.43. Deve implementar Telnet;
- 1.44. Deve implementar TFTP;
- 1.45. Deve implementar CLI;
- 1.46. Deve implementar, no mínimo, 04 grupos de RMON – Statistics, History, Alarms e Events. Deve possuir as seguintes RFC and MIB
 - GVRP – Generic VLAN Registration Protocol
 - IEEE 802.1X MIB – Port Access
 - ANSI/TIA-1057 – LLDP-MED MIB
 - IEEE 802.1AB – LLDP MIB
 - RFC 768 – UDP
 - RFC 783 – TFTP • RFC 791 – IP
 - RFC 792 – ICMP
 - RFC 793 – TCP
 - RFC 826 – Ethernet ARP
 - RFC 854 – Telnet
 - RFC 1157 – SNMP
 - RFC 1213 – MIB/MIB II
 - RFC 1493 – BRIDGE-MIB
 - RFC 1643 – Ethernet-like MIB
 - RFC 2618 – RADIUS Authentication Client MIB
 - RFC 2620 – RADIUS Accounting Client MIB
 - RFC 2737 – Entity MIB (physical branch only)
 - RFC 2819 – RMON-MIB
 - RFC 2933 – IGMP MIB
 - RFC 3413 – SNMP v3 Applications MIB
 - RFC 3584 – SNMP Community MIB

Solução Wireless – Controlador

Quantidade: 01 unidades

1) Características Básicas

- 1.1) Deve ser fornecido em hardware do tipo appliance, ou máquina virtual para ambiente VMWare ESXi, dedicado à funcionalidade de gerenciamento e controle de Access Points, possuindo firmware ou sistema operacional próprio;
- 1.2) Deve suportar a adição de funcionalidade de IDS/IPS, seja por adição de software ou appliance de mesmo fabricante;
- 1.3) A solução deve permitir, através de adição de licenças, o gerenciamento de pelo menos 240 APs e estar licenciada para gerenciar pelo menos 80 APs.
- 1.4) Em caso de fornecimento em Appliance, deve ser montável em rack padrão EIA 19" (dezenove polegadas) e possuir kits completos para instalação.
- 1.5) Equipamento do tipo WLAN Controller, para controle de access points distribuídos pela infraestrutura de rede.
- 1.6) Deve permitir gerenciar simultaneamente access points nos padrões IEEE802.11a, IEEE802.11b, IEEE802.11g e IEEE802.11n.
 - 1.7) Deve suportar configuração automática para os access points.
- 1.8) Deve implementar controles automatizados de rádio frequência tais como ajustes de canal e potência.
 - 1.9) Deve ser capaz de detectar falhas na cobertura wireless e automaticamente corrigi-las.
- 1.10) O WLAN Controller poderá estar diretamente e/ou remotamente conectado aos access points por ele gerenciados, inclusive via roteamento nível 3 da camada OSI.
- 1.11) Implementar varredura de RF contínua, programada ou sob demanda, com identificação de access points ou clientes irregulares.
- 1.12) Permitir o armazenamento de sua configuração em memória não volátil podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação.
- 1.13) Cada unidade da solução deve possuir tamanho máximo de 1 RU e ser appliance único somente para a função de WLAN Controller. Não serão aceitas soluções onde o WLAN Controller seja módulo ou sub módulo de algum switch.
- 1.14) Deve ser acompanhado de todos os acessórios necessários para operacionalização do equipamento, tais como: softwares, cabos de console, cabos de energia, kits para montagem no rack, documentação técnica e manuais que contenham informações suficientes que possibilitem a instalação, configuração e operacionalização dos equipamentos.

2) Interfaces e Fontes (em caso de Appliance)

- 2.2) Deve possuir, no mínimo, 2 portas 10/100/1000BaseT ou 1000BaseT, em conector RJ45 fêmea, diretamente instalado no equipamento.
- 2.3) Deve possuir, no mínimo, 1 interface dedicada ao gerenciamento do tipo Gigabit Ethernet 10/100/1000.
- 2.4) Deve possuir fonte de alimentação interna ao equipamento, que opere com tensões de entrada entre 110-240VAC e frequência 50/60hz.

3) Funcionalidades

- 3.1) Deve implementar sincronismo de relógio interno via NTP ou SNTP.
- 3.2) O WLAN controller deve suportar modo de operação em alta disponibilidade operando em conjunto com um ou mais WLAN Controllers.
 - 3.3) Deve implementar o padrão 802.1q.
 - 3.4) Deve possuir servidor DHCP interno.
 - 3.5) Implementar DHCP relay e DHCP Server.
 - 3.6) Deve suportar armazenamento de imagens para os access points.
 - 3.7) Deve implementar RADIUS Client.
 - 3.8) Deve implementar TFTP Client ou FTP Client.
 - 3.9) Deve implementar Syslog.
- 3.10) Deve possuir localmente no WLAN Controller um portal web para autenticação dos usuários visitantes, sendo possível a customização com informações e características visuais (mensagem, logo, banner, etc).
- 3.11) O portal web de autenticação, bem como a ferramenta de administração e gerência, devem ser acessadas via web nativo, sem a necessidade de instalação de nenhum software ou plug-in adicional.
- 3.12) A base de usuários visitantes deve ser interno ao WLAN Controller, não sendo necessário alterações (inclusão/exclusão/alteração) na base de dados dos usuários corporativos (Active Directory/LDAP).
- 3.13) A criação das contas de visitantes deve possibilitar a criação de no mínimo os seguintes parâmetros:
 - o Nome do usuário o
 - o Senha
 - o Descrição da conta o
 - o Data de início e
 - o término de validade o
 - o Horário permitido o
 - o Tempo de sessão

- 3.14) A ferramenta de criação dos usuários visitantes deverá ter uma página onde constem as informações de conta e políticas de uso da instituição, sendo possível a impressão destas informações para entrega ao visitante no momento do registro.
- 3.15) Implementar sistema de balanceamento de carga para associação de clientes entre access points próximos, para otimizar a performance.
- 3.16) Permitir configuração em Cluster, suportando em conjunto pelo menos 480 APS, Se um WLAN Controller falhar, os access points relacionados deverão se associar a um WLAN Controller alternativo (isso deve ocorrer somente se houver 2 WLAN Controller instalados em paridade).

4) Capacidades

- 4.1) Deve ser capaz de gerenciar, através de um ponto central, os access points que estejam conectados em ativos da infra-estrutura de rede existente, em diversas vlans e sub-redes IP.
- 4.2) Cada WLAN Controller deve gerenciar, no mínimo, 80 access points ativos simultaneamente e permitir o upgrade através de licenças para até 240 access points ativos simultaneamente.

5) Voz

- 5.1) Deve implementar 802.11e.
- 5.2) Deve implementar WMM (Wi-Fi Multimedia).
- 5.3) Deve implementar CAC (Call Admission Control) para as chamadas de voz dos clientes.
- 5.4) Deve implementar U-APSD para economia de bateria dos clientes.
- 5.5) Deve implementar Roaming entre diferentes subredes.
- 5.6) Deve implementar Roaming entre WLAN Controllers.

6) Segurança

- 6.1) Deve implementar mecanismo de AAA para para usuários da rede wireless.
- 6.2) Deve implementar o protocolo de autenticação IEEE802.1x com atribuição dinâmica de VLAN.
- 6.3) Deve implementar autenticação de usuário conforme o padrão IEEE 802.1x com suporte a atribuição automática de filtros de acesso no access point de acordo com os parâmetros do usuário.
- 6.4) Deve implementar o protocolo de autenticação IEEE802.1x com suporte aos seguintes métodos: EAP-TLS, PEAP, EAP-FAST, EAP-MD5.
- 6.5) Deve implementar autenticação através de endereço MAC.
- 6.6) Deve implementar os seguintes algoritmos de criptografia: AES (CCMP), RC4 – 40, 128bit (TKIP, WEP).
- 6.7) Deve implementar Wi-Fi Protected Access (WPA) e WPA2.
- 6.8) Deve implementar 802.11i.
- 6.9) Deve implementar autenticação remota via RADIUS Server.
- 6.10) Implementar mecanismo de minimização do tempo de roaming (deslocamento) de clientes autenticados via 802.1x (Fast Secure Roaming) entre dois access points no mesmo segmento de rede ou em segmentos de rede distintos.

7) Gerenciamento

- 7.1) Deve ser gerenciado através de web browser comum via protocolo HTTPS.
- 7.2) Deve implementar gerenciamento via linha de comando através de Telnet e SSH.
- 7.3) Deve possuir uma porta console para configuração local via linha de comando CLI (Command Line Interface).
- 7.4) Deve suportar SNMP versão 3.

Wireless - Access Point 802.11 a/b/g/n

Quantidade: 8 unidades

Access Point 802.11a/b/g/n

1. Características Básicas

- 1.1. Equipamento do tipo access point, que opere em conjunto com WLAN Controller.
- 1.2. Deve ser do mesmo fabricante do WLAN Controller.
- 1.3. O equipamento deve suportar os padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g e IEEE 802.11n.
- 1.4. Possuir certificação da Wi-Fi Alliance para 802.11a/b/g/n.
- 1.5. Deve operar simultaneamente com usuários configurados nos padrões 802.11a/b/g e n.
- 1.6. Deve possuir obrigatoriamente antenas internas, de forma a impedir sua remoção e possíveis furtos.
- 1.7. Deve possuir antenas internas com ganho de no mínimo 3 dBi para 2,4GHz e no mínimo 6 dBi para 5 GHz.
- 1.8. Deve implementar as técnicas de modulação 802.11a OFDM; 802.11g DSSS e OFDM; 802.11b DSSS; MIMO 2x2 para 802.11n.
- 1.9. Deve possuir 1 interface Gigabit Ethernet 10/100/1000 Base-T, com conector RJ-45.

- access point e de conectividade.
- 1.10. Deve possuir leds de indicação de status do
- 1.11. Deve implementar funcionalidade de descoberta automática do WLAN Controller.
- 1.12. Deve implementar até 16 SSIDs.
- 1.13. Permitir criptografia, Qos e gerenciamento de RF.
- 1.14. Permitir a continuidade da sessão do usuário no caso de queda do WLAN Controller principal (isso deve ocorrer somente se houver 2 WLAN Controller instalados em paridade).
- 1.15. Permitir, no mínimo, 120 usuários simultâneos por rádio.
- 1.16. Deve suportar a função de alimentação de energia elétrica do equipamento através de cabo UTP categoria 5 ou superior.
- 1.17. Deve suportar a alimentação elétrica do access point gerenciado via interface de rede 10/100/1000 Mbps, de acordo com o padrão PoE (power over ethernet), mantendo todas as suas funcionalidades em plena capacidade, sem perda do desempenho máximo do access point e consumindo apenas 1 porta do access point e do switch.
- 1.18. O equipamento deve suportar fonte de alimentação com as tensões de alimentação 100/240 VAC.
- 1.19. Deverá ser fornecido junto com Access Point módulo PoE, compatível.

- 1.20. Deve possuir, no mínimo, as seguintes taxas de dados:
- 1.21. 802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps
- 1.22. 802.11b: 1, 2, 5.5, 11 Mbps
- 1.23. 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
- 1.24. 802.11n: 6,5 Mbps a 300 Mbps
- 1.25. Deve possuir, no mínimo, a sensibilidade de

recepção dos rádios conforme abaixo:

- 1.26. -90 dBm operando em 802.11b com velocidade de 11 Mbps
- 1.27. -81 dBm operando em 802.11g com velocidade de 54 Mbps
- 1.28. -80 dBm operando em 802.11a com velocidade de 54 Mbps
- 1.29. -68 dBm operando em 802.11n 5Ghz HT40 MCS15
- 1.30. -69 dBm operando em 802.11n 2.4 Ghz HT40 MCS15

300 Mbps

300 Mbps

- 1.31. Deve estar em conformidade com os seguintes padrões de segurança: UL / IEC / EN 60950.
- 1.32. Deve estar em conformidade com os seguintes padrões: EN 301 893; EN 300 328; EN 301 489 -1 & 17; EN 60601-1-2.

1.33. O p

Controller, inclusive via roteamento nível 3 da camada OSI.

- 1.34. Permitir habilitar e desabilitar a divulgação do SSID.
- 1.35. Possuir porta de console para gerenciamento e configuração via linha de comando (CLI – comand line interface).
- 1.36. Implementar cliente DHCP, para configuração

automática de rede.

- 1.37. Implementar 802.1X do access point à rede, isto é, autenticação através de 802.1x do próprio access point.
- 1.38. Deve ser acompanhado de todos os acessórios necessários para operacionalização do equipamento, tais como: softwares, cabos de energia elétrica, estrutura para fixação em paredes e teto, documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento.
2. Voz
- 2.1. Deve implementar Call Admission Control (CAC).
- 2.2. Deve implementar U-APSD para economia de bateria dos clientes.
- 2.3. Implementar qualidade de serviço WMM, 802.11e.
- 2.4. Permitir até 12 chamadas de voz simultâneas (802.11b, G.711).

3. Segurança

- 3.1. Permitir suporte a passagem de tráfego VPN IPSec, PPTP, L2TP.
- 3.2. Implementar segurança via WEP, WPA (TKIP), WPA2 (AES), 802.11i, 802.1x para acesso dos clientes wireless.
- 3.3. Implementar Fast Secure Roaming e handover com Pre-authentication e Opportunistic Key Caching.
- 3.4. Deve possuir funcionalidade de rogue detection.
- 3.5. Deve poder trabalhar como sensor WIPS.

Solução Segurança - Firewall

Quantidade: 01 unidades

1. Requisitos Gerais:
- 1.1. Deve ser fornecida Solução de Segurança;
- 1.2. Solução de segurança de informação perimetral que inclui dois firewall, administração de largura de banda de serviço de internet (QoS), suporte para conexões VPN IPSec e SSL, proteção contra ameaças de vírus e malware, bem como controle de transmissão de dados e acesso a internet.
- 1.3. Deverá incluir um módulo de proteção contra ameaças de rede, bloqueio de vírus, spyware, controle de transferência de arquivos, controle da navegação de internet e bloqueio de arquivos por tipo.
- 1.4. O firewall devem ter a capacidade de operar de forma simultânea mediante o uso das suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (I2) e camada 3 (I3).

- 1.4.1. Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede.
 - 1.4.2. Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação.
 - 1.4.3. Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação. Gerar roteamento virtual para pelo menos 10 roteadores virtuais e administração do tráfego entre diferentes áreas de segurança e sub-redes, suportando pelo menos 30 áreas de segurança e um mínimo de 5 sistemas virtuais.
 - 1.4.4. Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas.
 - 1.5. Suporte para múltiplos sistemas virtuais lógicos (Contextos) no firewall Físico.
 - 1.6. Os contextos virtuais devem suportar todas as funcionalidades base desde edital, como por exemplo, Firewall, VPN, Controle de Aplicações, IPS, Anti-virus, Anti-Spyware, NAT, Filtro de URL, decriptografia de SSL e Identificação de usuários.
- Deverá contar com suporte para os serviços a seguir:
- 1.7. Redes Virtuais, vlans 802.1q, 802.3ad link aggregation;
 - 1.8. Tradução de endereços da rede (NAT) por origem e destino, por endereços ip dinâmicos e pool de portas.
 - 1.9. PPPOE, bgp, ospf e rip2, dhcp server e dhcp relay.
- 1.10. Protocolos de encriptação IKE, 3Des (com criptografia de 128, 192 e 256 bits), AES, SHA1 e MD5.
 - 1.11. Deverá suportar pelos menos os seguintes protocolos de VOIP: H.323, SIP, SCCP e MGCP.
 - 1.12. Identificação, Controle e visibilidade sendo:
 - 1.12.1. Identificação, Controle (Uso de aplicações por usuário mediante interação com Ldap, Active Directory ou Radius e endereço ip).
 - 1.12.2. Identificação deve ser de modo independente à porta lógica e/ou aplicações que utilizam as portas 80 e 443 (Implica a descrição bidirecional de SSL e Identificação de aplicações que encapsuladas em túnel SSL).
 - 1.12.3. Visibilidade de pelo menos 1400 aplicações incluindo peer-to-peer, facebook, twitter e web 2.0.
 - 1.12.4. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Ultrasurf, Skype e ataques mediante a porta 443.
 - 1.13. Em caso de protocolos desconhecidos, poderão designar-se assinaturas próprias.
 - 1.14. Descrição e controle de tráfego SSHv2.
 - 1.15. Detecção de aplicações dinâmicas dentro de sessões de proxy HTTP.
 - 1.16. Controle de tráfego IPv4 e IPv6, este último inclui visibilidade e inspeção de ameaças em aplicações e controle de conteúdo. O IPV6 deve ser suportado em interfaces trabalhando em L2 e L3.
 - 1.17. A solução deve ser ofertada em Appliance/hardware específico para o propósito solicitado, não sendo aceito soluções baseadas em servidores abertos.
 - 1.18. A Solução deve utilizar sistema operacional próprio "hardenizado", não sendo aceitos sistemas operacionais Linux ou baseados em distribuições abertas.
 - 1.19. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7.
2. Controles por Políticas de Firewall
 - 2.1. Deverá suportar controles por zona de segurança.
 - 2.2. Suportar as seguintes características:
 - 2.2.1. Controles de políticas por porta e protocolo.
 - 2.2.2. Controle de políticas por Aplicações e categorias de aplicações.
 - 2.2.3. Controle de políticas por Usuários, Grupos de Usuários, Ips, Redes e Zonas de segurança.
 - 2.2.4. Controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS).
 - 2.2.5. Controle de inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saida (Outbound).
 - 2.2.6. Controle de inspeção e de-criptografia de SSH por política.
 - 2.3. Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif, e reg.
 - 2.4. Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo)
 - 2.5. QoS baseado em políticas para marcação de pacotes (diffserv marking).
 - 2.6. Suporte a objetos e regras IPV6.
 - 2.7. Suporte a objetos e regras multicast.
 - 2.8. Suporta a atribuição de agendamento as políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.
 3. Controle de Aplicações
 - 3.1. Deverá contar com ferramentas de visibilidade que permitam administrar o tráfego de aplicações, permitindo a execução de aplicações autorizadas e bloqueio de aplicações não autorizadas.
 - 3.2. O controle de aplicações deve identificar as mesmas independente das portas e protocolos assim como técnicas de evasão utilizadas.
 - 3.3. Descrever técnicas utilizadas pela solução para a detecção das aplicações (Assinaturas, Heurística, etc).
 - 3.4. Deverá suportar múltiplos métodos de identificação e classificação das aplicações.
 - 3.5. O controle de aplicações é baseado em Inspeção IPS ou inspeção profunda de pacotes (Deep Packet Inspection).
 - 3.6. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas.
 - 3.7. Deverá suportar a criação de aplicações customizadas pela interface gráfica do produto.
 - 3.8. Deverá incluir a capacidade de atualização para identificar novas aplicações.
 - 3.9. Deverá atualizar a base de assinaturas de aplicações automaticamente.
 - 3.10. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas do fabricante.
 - 3.11. Deverá alertar o usuário quando uma aplicação foi bloqueada.

- 3.12. Deverá possibilitar que o controle de portas seja aplicado para todas as aplicações.
 - 3.13. Deverá possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, neonet, etc.) possuindo granularidade de controle/políticas para os mesmos.
 - 3.14. Deverá possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, YIM, Facebook Chat, etc.) possuindo granularidade de controle/políticas para os mesmos.
 - 3.15. Deverá possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o YIM chat e bloquear a transferência de arquivos.
 - 3.16. Deverá possibilitar a diferenciação de aplicações Proxies (ultrasurf, ghostsurf, freegate, etc.) possuindo granularidade de controle/políticas para os mesmos.
 - 3.17. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-diretório e base de dados local.
 - 3.18. Deverá possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários.
 - 3.19. Deverá possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários.
 - 3.20. Deverá possuir integração com ldap para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários.
 - 3.21. Deverá incluir a capacidade de criação de políticas baseadas no controle por aplicação, categoria de aplicação, subcategoria, tecnologia e fator de risco.
 - 3.22. Deverá incluir a capacidade de criação de políticas baseadas no controle por usuário, grupos de usuários ou endereço ip.
 - 3.23. Deverá incluir a capacidade de criação de políticas baseadas em "traffic shaping" por aplicação, usuário, origem, destino, túnel vpn-ipsec-ssl.
 - 3.24. Deverá permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal).
 - 3.25. Suporte a autenticação Kerberos.
 - 3.26. Deverá possuir suporte a identificação de usuários em ambiente Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços.
4. Prevenção de ameaças.
- 4.1. IPS
 - 4.1.1. Para proteção do ambiente contra ataques, deve ser incluído modulo de IPS integrado na própria ferramenta de Firewall ou entregue com composição com outro fabricante.
 - 4.1.2. O módulo de IPS oferecido deve ter passado nos testes da NSS Labs para produtos de IPS com pelo menos 90% de efetividade, ter 100% de efetividade nos testes de evasão e estar entre os recomendados do relatório.
 - 4.1.3. Deverá suportar granularidade nas políticas de IPS, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.
 - 4.1.4. Deverá possibilitar a criação de diferentes perfis de IPS a serem aplicados por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.
 - 4.1.5. Deverá permitir o bloqueio de vulnerabilidades.
 - 4.1.6. Deverá permitir o bloqueio de exploits conhecidos.
 - 4.1.7. Deverá incluir proteção contra ataques de negação de serviços.
 - 4.1.8. Deverá possuir os seguintes mecanismos de inspeção de IPS:
 - 4.1.8.1. Análise de padrões de estado de conexões
 - 4.1.8.2. Análise de decodificação de protocolo
 - 4.1.8.3. Análise para detecção de anomalias de protocolo
 - 4.1.8.4. Análise heurística
 - 4.1.8.5. IP Defragmentation
 - 4.1.8.6. Remontagem de pacotes de tcp
 - 4.1.8.7. Bloqueio de pacotes malformados
 - 4.1.9. Deverá possuir assinaturas para bloqueio de ataques "buffer overflow".
 - 4.1.10. Deverá possuir assinaturas para auxílio no bloqueio de ataques DoS/DDoS.
 - 4.1.11. Deverá suportar o reconhecimento de ataques em tráfego IPV6.
 - 4.1.12. Deverá possuir assinaturas e mecanismos de detecção de anomalias prontas.
 - 4.1.13. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto.
 - 4.1.14. Deverá ser possível a criação de exceções/exclusões por hosts para determinadas assinaturas.
 - 4.1.15. Deverá suportar referencia cruzada com CVE.
 - 4.1.16. Deverá possuir granularidade de ajustes com opções para sobrescrever assinaturas individualmente.
 - 4.1.17. Deverá suportar atualização automática das assinaturas através de conexão segura.
 - 4.1.18. Todos os modelos de equipamentos devem utilizar as mesmas assinaturas.
 - 4.1.19. Deverá suportar varias técnicas de prevenção, incluindo Drop e tcp-rst (Cliente, Servidor e ambos).
 - 4.1.20. Deverá suportar ações por assinaturas.
 - 4.1.21. Suportar notificações e alertas via e-mail, SNMP traps e log de pacotes.
 - 4.2. Antivírus / Anti-Spyware
 - 4.2.1. Para proteção do ambiente contra Malware conhecido, deve ser incluído modulo de Anti-virus e Ant-Spyware de gateway integrado na própria ferramenta de Firewall ou entregue com composição com outro fabricante.
 - 4.2.2. Deverá permitir o bloqueio de Malwares e Spywares.

- 4.2.3. Deverá ser possível a inspeção de Antivírus para pelo menos nos seguintes tipos de tráfegos: HTTP, SMTP, POP3, IMAP e SMB.
- 4.2.4. Deverá incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms.
- 4.2.5. Proteção contra downloads involuntários usando HTTP de arquivos executáveis. maliciosos.
- 4.2.6. Rastreamento de vírus em pdf.
- 4.2.7. Deverá permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.)
- 4.2.8. Deverá suportar bloqueio de arquivos por tipo (pelo menos 50 tipos).
- 4.2.9. A atualização de assinaturas deverá ser diária, semanal e de emergência.
- 4.2.10. Deve suportar atualização automática das assinaturas através de conexão segura.
- 4.2.11. As atualizações de ameaças, Antivírus e Anti-spyware não devem depender de reboot do equipamento para efetivação.
- 4.2.12. Todos os modelos de equipamentos devem utilizar as mesmas assinaturas.
- 4.2.13. Suportar notificações e alertas via e-mail, SNMP traps e log de pacotes.
- 4.3. Deve suportar, e estar licenciada, análise de Malware "In Cloud"
- 4.3.1. Devido aos Malwares hoje em dia serem muito dinâmicos e um antivírus comum reativo não ser capaz de detectar os mesmos com a mesma velocidade que suas variações são criadas, a solução ofertada deve possuir funcionalidades para análise de Malwares não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante.
- 4.3.2. Para ameaças/Malwares não conhecidos, o produto deve ser capaz de enviar o arquivo para análise automática "In Cloud". Onde o arquivo será executado e simulado em ambiente controlado.
- 4.3.3. Essa análise deve suportar a monitoração do arquivo para mais de 60 comportamentos maliciosos.
- 4.3.4. Esse sistema automático de análise "In Cloud" deve prover:
 - 4.3.4.1. Informações Sobre as ações do Malware na máquina infectada.
 - 4.3.4.2. Informações sobre quais aplicações são utilizadas para causar/propagar a infecção.
 - 4.3.4.3. Detectar aplicações não confiáveis utilizadas pelo Malware.
 - 4.3.4.4. Gerar assinaturas de Antivírus e Anti-Spyware automaticamente.
 - 4.3.4.5. Definir URLs não confiáveis utilizadas pelo novo Malware.
 - 4.3.4.6. Entre outros provendo uma maior segurança para a rede do cliente.
- 5. Filtro de URL
- 5.1. Para maior controle e visibilidades dos acessos dos usuários do ambiente, deve ser incluído modulo de filtro de URL integrado na própria ferramenta de Firewall ou entregue com composição com outro fabricante.
- 5.2. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, Ips, Redes e Zonas de segurança.
- 5.3. Deve ser possível definir horários para o funcionamento da política.
- 5.4. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-diretório e base de dados local.
- 5.5. Deverá possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários.
- 5.6. Deverá possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários.
- 5.7. Deverá possuir integração com ldap para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários.
- 5.8. Deverá incluir a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL.
- 5.9. Deverá permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal).
- 5.10. Deverá possuir suporta a identificação de usuários em ambiente Citrix e Microsoft Terminal Server, permitindo visibilidade e controle sobre o uso das URLs que estão sendo acessadas através destes serviços.
- 5.11. Deve possibilitar base de URLs local no Appliance, evitando delay de comunicação/validação da URLs.
- 5.12. Deverá possuir pelo menos 50 categorias de URLs.
- 5.13. Deverá possibilitar a criação Categorias de URLs customizadas.
- 5.14. Deverá possibilitar a exclusão de URLs do bloqueio por categoria.
- 5.15. Deve possibilitar a customização de pagina de bloqueio.
- 5.16. Deve possibilitar o bloqueio e continuação (Possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para possibilitar o usuário continuar acessando o site por um tempo).
- 5.17. Os logs do produto devem incluir informações das atividades dos usuários.
- 5.18. A atualização da base de dados deve ser automática com a opção de ser feita manualmente via tftp.
- 6. Filtro de Dados
- 6.1. Deve ser possível a criação de filtros para arquivos e dados pré-definidos.
- 6.2. Os arquivos devem ser identificados por extensão e assinaturas.
- 6.3. O firewall deve ser capaz de identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (ex. MS Office, PDF,etc) identificados sobre aplicações (Ex. P2P, IM, SMB, etc).
- 6.4. Deve ser possível a identificação de arquivos compactados e a aplicações de políticas sobre o conteúdo desses tipos de arquivos.
- 6.5. O firewall deve ser capaz de identificar e opcionalmente prevenir a transferência de informações sensíveis (Ex. Numero de cartão de credito, etc) possibilitando a criação de novos tipos de dados via expressão regular.
- 6.6. Listar o número de aplicações suportadas para controle de dados.

- 6.7. Listar o numero de tipos de arquivos suportados para controle de dados.
- 7. QoS
- 7.1. Deverá permitir o controle de políticas de uso com base nas aplicações: permitir, negar, agendar, inspecionar e controlar o uso da largura de banda que utilizam cada aplicação ou usuário.
- 7.2. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, ustream, etc.) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deva ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming.
- 7.3. Suportar a criação de políticas de QoS por:
 - 7.3.1. Endereço de origem
 - 7.3.2. Endereço de destino
 - 7.3.3. Por usuário ou Grupo do AD.
 - 7.3.4. Por aplicações (como por exemplo Skype, Bittorrent, YouTube, Azureus)
 - 7.3.5. Por aplicações estaticamente ou grupos dinamicamente (como por exemplo Instant Messaging ou grupo de aplicações P2P)
- 7.3.6. Por porta
- 7.4. O QoS deve possibilitar a definição de classes por:
 - 7.4.1. Banda Garantida
 - 7.4.2. Banda Máxima
 - 7.4.3. Fila de Prioridade.
- 7.5. Suportar priorização RealTime de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype.
- 7.6. Suportar marcação de pacotes Diffserv
- 7.7. Disponibilizar estatísticas RealTime para classes de QoS.
- 7.8. Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.
- 8. GeoLocation
- 8.1. Suportar a criação de políticas por Geo Localização, permitindo o tráfego de determinado Pais/Países sejam bloqueados.
- 8.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.
- 8.3. Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar politicas utilizando as mesmas.
- 9. De-criptografia SSL/SSH
- 9.1. Deve identificar, de-criptografar e analisar o tráfego SSL em conexões de saída (Outbound)
- 9.2. Deve identificar, de-criptografar e analisar o tráfego SSL em conexões de entrada (Inbound)
- 9.3. Deve identificar, de-criptografar e analisar o tráfego SSH em conexões de saída (Outbound)
- 9.4. Deve identificar, de-criptografar e analisar o tráfego SSH em conexões de entrada (Inbound)
- 9.5. A inspeção de SSL deve permitir a diferenciação de conexões pessoais (Bancos, Shopping, etc) e tráfegos não Pessoais.
- 9.6. Deve de-criptografar o tráfego em todos os tipos de implementação, como:
 - 9.6.1. Tap mode
 - 9.6.2. Modo Transparente/Bridge
 - 9.6.3. Layer 2
 - 9.6.4. Layer 3
- 10. Identificação de Usuários.
- 10.1. Deve suportar pelo menos os seguintes serviços de autenticação para identificação de usuários:
 - 10.1.1. Active Directory
 - 10.1.2. LDAP
 - 10.1.3. eDirectory
 - 10.1.4. RADIUS
 - 10.1.5. Kerberos
 - 10.1.6. Client Certificate
- 10.2. Deve suportar a criação de políticas baseado em Grupos e Usuários do Active Directory adicionalmente a IP Origem / Destino.
- 10.3. Deve possibilitar a identificação de usuários sem a necessidade de instalação de agente individualmente em cada equipamento da rede.
- 10.4. Deve suportar a identificação de usuários em ambientes Citrix e Terminal server, assim como a utilização dos mesmos nas políticas de acesso.
- 10.5. Deve popular todos os logs de tráfego, IPS, URL, Data, Aplicações entre outros com as informações dos usuários.
- 10.6. Os logs de identificação de usuários deve ser feito RealTime e não correlacionado após a ocorrência do Tráfego em questão.
- 11. Funcionalidades de Rede
- 11.1. Suportar funcionamento em Tap Mode (Via porta espelhada, Tap ou SPAN port).
- 11.2. Suportar funcionamento em mode transparente (Bridge ou similar).
- 11.3. Suportar funcionamento em Layer 2
- 11.4. Suportar funcionamento em Layer 3
- 11.5. Suportar a implementação simultânea em todos os modos descritos acima (Tap, Transparente, Layer2 e Layer3) no mesmo equipamento.
- 11.6. Deve suportar Vlan Tagging (802.1Q) em todas os cenários de implementação acima (Tap, Transparente, Layer2 e Layer3) .

- 11.7. Deve suportar controle de aplicações em IPV6 em todas os cenários de implementação acima (Tap, Transparente, Layer2 e Layer3).
- 11.8. Suportar sub-interfaces ethernet logicas.

- 12. NAT
 - 12.1. Deverá suportar:
 - 12.1.1. Porta/IP Nat dinâmico (Many-to-1 e Many-to-Many).
 - 12.1.2. IP Nat dinâmico (Many-to-Many).
 - 12.1.3. IP Nat estático (1-to-1, Many-to-Many, Ips).
 - 12.1.4. Nat estático bidirecional 1-to-1.
 - 12.2. IP Virtual (VIP)
 - 12.3. Tradução de porta (PAT).
 - 12.4. NAT de Origem
 - 12.5. NAT de Destino
 - 12.6. Suportar NAT de Origem e NAT de Destino simultaneamente.
 - 12.7. Prover capacidade de NAT Traversal, suportando aplicações e Serviços VoIP.

- 13. VPN
 - 13.1. Suportar VPN Site-to-Site e Cliente-To-Site.
 - 13.2. Suportar IPSec VPN
 - 13.3. Suportar SSL VPN
 - 13.4. Suportar atribuição de Ips nos clientes remotos de VPN.
 - 13.5. Suportar atribuição de DNS nos clientes remotos de VPN.
 - 13.6. Estar licenciada para 2000 clientes de VPN simultâneos.
 - 13.7. IPSec VPN deve suportar:
 - 13.7.1. DES, 3DES, AES
 - 13.7.2. Autenticação MD5 e SHA- 1
 - 13.7.3. Diffie- Hellman Group 1 , Group 2 e Group 5
 - 13.7.4. Algoritmo Internet Key Exchange (IKE)
 - 13.7.5. AES 128, 192 & 256 (Advanced Encryption Standard).
 - 13.8. Deve possuir interoperabilidade com os seguintes fabricantes:
 - 13.8.1. Cisco
 - 13.8.2. Checkpoint
 - 13.8.3. Juniper
 - 13.8.4. Palo Alto Networks
 - 13.8.5. Fortinet
 - 13.8.6. Sonic Wall
 - 13.9. O módulo de VPN IPSec deve suportar pelo menos 2.000 túneis e ter performance de pelo menos 500 Mbps de throughput.
 - 13.10. Deverá permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL.
 - 13.11. Deverá contar com um software cliente de VPN-SSL para os sistemas operacionais Windows SP, Vista (32 e 64 bits) e Windows 7 (32 e 64 bits).
 - 13.12. Deverá permitir criar políticas para tráfego VPN-SSL.
 - 13.13. SSL VPN com suporte a proxy arp e uso de interfaces PPPOE.
 - 13.14. Deverá suportar pelo menos 2.000 usuários simultâneos via SSL VPN.
 - 13.15. Suporte para autenticação de VPNs SSL, Ldap, Secure id e base de dados própria.
- 14. Roteamento
 - 14.1. Deve suportar as seguintes funcionalidades de roteamento:
 - 14.1.1. Estático e Dinâmico.
 - 14.1.2. RIP v2
 - 14.1.3. OSPF
 - 14.1.4. BGP v4
 - 14.1.5. EIGRP
 - 14.2. Suporte a roteamento IPv6.
 - 14.3. Suporte a roteadores Virtuais (Virtual Routers).
 - 14.4. Suporte a "Policy Based Forwarding" por:
 - 14.4.1. Zona de segurança
 - 14.4.2. Endereço de Origem e Destino
 - 14.4.3. Porta de Origem e Destino
 - 14.4.4. Aplicação
 - 14.4.5. Usuários e/ou Grupos da base AD/LDAP
 - 14.4.6. Combinação de todos acima.
- 15. Alta Disponibilidade
 - 15.1. Configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo:
 - 15.1.1. Em modo Transparente.
 - 15.1.2. Em layer 2
 - 15.1.3. Em layer 3
 - 15.2. O H.A. deve sincronizar:
 - 15.2.1. Todas as sessões.
 - 15.2.2. Certificados de-criptografados
 - 15.2.3. Todas Associações de Segurança das VPNs

- 15.2.4. Todas as assinaturas de Antivírus, Anti-spyware e Aplicações.
- 15.2.5. Todas as configurações
- 15.2.6. Tabelas FIB.
- 15.3. O H.A. deve possibilitar tracking de IP
- 15.4. Monitoração de falha de link.
- 16. Suporte à Segurança nos equipamentos host da instituição
- 16.1. Deverá suportar um agente que quando instalado nos equipamentos desktop ou laptop da instituição, transportem as políticas e todas as características de segurança do Firewall a tal equipamento.
- 16.2. O Agente de software a ser instalado nos equipamentos desktop e laptops, deverá ser capaz de ser distribuído de maneira automática via SMS, Active Directory e ser descarregado diretamente desde o seu próprio portal, o qual residirá no Firewall.
- 16.3. O agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário,
- 16.4. Deverá Manter uma conexão segura com o portal durante a sessão.
- 16.5. Determinar o perfil de host com base em: Sistema Operacional e seus níveis de instalação de patches, versão de anti-malware no host, versão de Firewall no host, criptografia do disco, chaves de registros e processos ativos.
- 16.6. Deverá ser possível a criação de perfis customizados com base em Sistema Operacional e seus níveis de instalação de patches, versão de anti-malware no host, versão de Firewall no host, criptografia do disco, chaves de registros e processos ativos.
- 16.7. O portal deverá enviar ao agente a lista de portais trabalhando como gateways ativos, os quais serão administrados centralmente e deverá trabalhar com os certificados de autenticação correspondentes a cada usuário. O cliente poderá encontrar a melhor rota com base nos gateways disponíveis e a localização do host, determinando a rota com o tempo de resposta mais rápido.
- 16.8. Em conformidade com o perfil de segurança detectado, se o end-point não for suficientemente seguro, serão determinadas políticas de segurança novas com base no seu perfil. Estas políticas estarão baseadas em: Sistema Operacional e seus níveis de instalação de patches, versão de anti-malware no host, versão de Firewall no host, criptografia do disco, chaves de registros e processos ativos.
- 16.9. Deverá estabelecer um túnel VPN-SSL do cliente ao Gateway, fornecendo uma solução de singesign-on aos usuários, integrando-se com as ferramentas de Windows-login.
- 16.10. Deverá ter suporte para os sistemas operacionais Windows SP, Vista (32 e 64 bits) e Windows 7 (32 e 64 bits).
- 17. Requerimentos de Hardware e Performance, cada unidade da solução.
 - 17.1. O equipamento deve possuir:
 - 17.1.1. 12 interfaces 10/100/1000 Copper Ethernet
 - 17.1.2. 8 Interfaces 1GB SFP
 - 17.2. O equipamento deve possuir interface "Out-Of-Band" dedicada para gerenciamento.
 - 17.3. Suportar pelo menos 4 Gbps de throughput para Firewall.
 - 17.4. Suportar pelo menos 2 Gbps de throughput para controle de aplicações.
 - 17.5. Suportar pelo menos 2 Gbps de throughput para controle de Anti-vírus e Antispyware.
 - 17.6. Suportar pelo menos 2 Gbps de throughput de IPS.
 - 17.7. Suportar pelo menos 500 Mbps de throughput para VPN IPSec.
- 17.8. Suportar pelo menos 2 Gbps de throughput para as funcionalidades de Firewall, Controle de Aplicações, IPS, Anti-vírus e Anti-Spyware habilitados simultaneamente.
- 17.9. Deve suportar pelo menos 500.000 sessões concorrentes.
- 17.10. Deve suportar pelo menos 50.000 novas sessões por segundo.
- 17.11. Deve suportar pelo menos 2.000 Interfaces Tunel de VPN IPSec
- 17.12. Suportar pelo menos 2.000 Usuários concorrentes de SSL VPN.
- 17.13. Deve suportar pelo menos 5 Sistemas Virtuais (Contextos). 18. Gerenciamento
 - 18.1. Deve ser suportado o gerenciamento por:
 - 18.1.1. CLI via SSH
 - 18.1.2. WebUI via HTTPS
 - 18.1.3. Console
 - 18.1.4. API Aberta
 - 18.2. O gerenciamento local do equipamento deve permitir/Possuir:
 - 18.2.1. Criação e administração de políticas
 - 18.2.2. Administração de políticas de IPS, Anti-virus e Anti-Spyware
 - 18.2.3. Política de Filtro de Dados e Filtro de URLs.
 - 18.2.4. Monitoração de logs.
 - 18.2.5. Ferramentas de investigação de logs
 - 18.2.6. Debugging
 - 18.2.7. Captura de pacotes.
- 18.3. Deverá suportar solução de gerenciamento centralizado, possibilitando o gerenciamento de diversos equipamentos.
- 18.4. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos gateways de segurança.
- 18.5. Deverá possuir relatórios de utilização dos recursos por aplicações, URL, Ameaças, etc.
- 18.6. Prover uma visualização sumarizada de todas as aplicações, ameaças e URLs que passaram pela solução.
- 18.7. Deverá possuir mecanismo "Drill-Down" para navegação nos relatórios RealTime.
- 18.8. Nas opções de "Drill-Down", ser possível identificar o usuário que fez determinado acesso.
- 18.9. Deverá ser possível exportar os logs CSV.

- 18.10. Deverá ser possível acessar o equipamento a aplicar configurações durante momentos onde o trafego é muito alto e a CPU e memória do equipamento estiver totalmente utilizada.
- 18.11. Deverá ser possível capturar as URLs acessadas para todas as sessões HTTP.
- 18.12. Deverá possibilitar a criação de diferentes perfis de administração separando pelo menos: Leitura, Alterações, Relatórios e Monitoração.
- 18.13. Deverá ser possível de forma granular, assinar permissões para os administradores criarem outros usuários, alterarem configurações, Ler configurações, etc.
- 18.14. Deverá ser possível administrar o firewall localmente ou remotamente sem causar problemas de sincronismo de configurações.
- 18.15. Deverá possuir interface ethernet "Out-of-Band" para gerenciamento:
 - 18.15.1. SSH
 - 18.15.2. HTTPS
- 18.16. Gerar alertas automáticos via:
 - 1
 - 8.16.1. mail
 - 1
 - 8.16.2. NMP
 - 1
 - 8.16.3. syslog
- 18.17. Habilidade de upgrade via SCP, TFTP e Web-UI.
- 18.18. Suportar Rollback de configuração para a ultima configuração salva.
- 18.19. Suportar Rollback de Sistema Operacional para a ultima versão local.
- 18.20. Validação de regras antes da aplicação.
- 18.21. Possibilitar o bloqueio da interface para alterações, evitando o conflito de configurações entre administradores quando tiver mais de um administrador executando alterações simultaneamente.
- 18.22. Deve possibilitar a visualização e comparação de configurações Atuais, configuração anterior e configurações antigas.

- 18.23. Deve possibilitar a integração com outras soluções de SIEM de mercado (third-party SIEM vendors)
- 18.24. Controle sobre todos os Firewalls em uma única console, com administração de privilégios ou funções.
- 18.25. O gerenciamento centralizado deve possibilitar a instalação como virtual appliance sobre VMware, fornecendo a flexibilidade para instalar-se em diferentes combinações de Hardware e sistemas operacionais.
- 18.26. Administração baseada em Web e Linha de comandos.
- 18.27. Deverá suportar autenticação de administradores usando base de dados local e Radius.
- 18.28. Linha de comandos mediante SSHv2, telnet
- 18.29. Geração de relatórios de atividades do usuário.
- 18.30. Controle Global de Políticas
- 18.31. Deve suportar organização em grupos de Firewalls: Os sistemas virtuais serão administrados como dispositivos individuais, os grupos podem ser geográficos, por Funcionalidade (por exemplo, como IPS), e distribuição.
- 18.32. Objetos e políticas compartilhadas.
- 18.33. Relatórios predefinidos e relatórios projetados pelo usuário (custom), todos os relatórios deverão poder ser exportados a formatos CSV e PDF.
- 19. Autenticação
 - 19.1. Para autenticação dos administradores da solução deve ser suportado:
 - 19.1.1. LDAP
 - 19.1.2. Radius
 - 19.1.3. Soluções Baseadas em Token (i.e. Secure-ID)
 - 19.2. Kerberos
 - 19.3. Para autenticação de VPN SSL deve ser suportado:
 - 19.3.1. LDAP
 - 19.3.2. Radius
 - 19.3.3. Soluções Baseadas em Token (i.e. Secure-ID)
 - 19.3.4. Kerberos
- 20. Captura de pacotes.
 - 20.1. Deverá ser possível a captura de pacotes por:
 - 20.1.1. Endereço de Origem
 - 20.1.2. Endereço de destino
 - 20.1.3. Aplicações
 - 20.1.4. Aplicações desconhecidas
 - 20.1.5. Portas
 - 20.1.6. IPS
 - 20.1.7. Antivírus
 - 20.1.8. Anti-Spyware
 - 20.1.9. Filtro de dados.
 - 20.1.10. Qualquer combinação acima.
- 21. Relatórios
 - 21.1. Deverá incluir a capacidade de proporcionar um resumo gráfico de aplicações utilizadas e ameaças encontradas diariamente.

- 21.2. Deverá permitir o controle de transferência de dados não autorizados com ferramenta para realizar padrões definidos por usuário.
- 21.3. Deverá contar com a funcionalidade para exportação de logs, captura de tráfego URL e ameaças.
- 21.4. Deverá permitir a criação de relatórios personalizáveis.
- 21.5. Deverá contar com ferramenta para criar filtros de monitoramento das sessões históricas no firewall seja por aplicação, ip origem e ip destino.
- 21.6. Deverá ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado.
- 21.7. Geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição.
- 21.8. O equipamento deverá proporcionar os seguintes conjuntos de relatórios:
 - 21.8.1. Utilização de largura de banda de entrada e saída por aplicação (TOP 10)
 - 21.8.2. Numero de Sessões por aplicação (TOP 10)
 - 21.8.3. Comparativo semanal de aplicações utilizadas na rede que possam induzir Latência. (TOP 10)
 - 21.8.4. Taxa de transferência (em bytes) por aplicação (TOP 10).
 - 21.8.5. Origem e destino do tráfego por aplicação – Usuário (TOP 10)
 - 21.8.6. Sessões e E-mail público
 - 21.8.7. Utilização de navegação
 - 21.8.8. Eventos / Ataques por: Origem, Categoria, Ameaça, Protocolo. (TOP 10)
 - 21.8.9. Nível de risco da rede
 - 21.8.10. Principais protocolos e aplicações que circulam pelo Firewall (TOP 25).
 - 21.8.11. Principais endereços de IP destino por protocolo (TOP 25).
 - 21.8.12. Os principais endereços IP para cada um dos protocolos e aplicações principais (TOP 50);

ESPECIFICAÇÃO DOS SERVIDORES

1 SERVIDORES

Quantidade: 02 unidades

- 1.1 Deverá ser entregue o total de 2 (dois) servidores de produção para o ambiente virtualizado, contendo as características mínimas:
 - 1.1.1 Microcomputador do tipo servidor rack, com tecnologia Octa-Core ou superior, compatível com o padrão x86 e desenvolvido para servidores, com, no mínimo, 2 (dois) discos rígidos SAS, unidade gravadora de DVD.
 - 1.1.2 O servidor deverá possuir fonte redundante com, no mínimo, dois cabos de alimentação ou sistema que garanta a conexão em duas fases de energia elétrica distintas, com comprimento mínimo de 1,80m;
 - 1.1.3 O servidor deverá possuir interface SVGA, ou superior que garanta resolução mínima de 1280x1024;
 - 1.1.4 O servidor deverá possuir registro no Windows Server Catalog – WSC na categoria Hardware para Windows Server 2008 ou superior.
 - 1.1.5 O servidor deverá possuir plena compatibilidade com sistema operacional Linux Debian com o kernel 2.6.24.6 ou superior.
 - 1.1.6 O servidor deverá possuir ventilação redundante tipo “Hot Swap”
 - 1.1.7 O servidor e seus componentes eletro-eletrônicos deverão possuir conformidade comprovada com a diretiva RoHS (Restriction of Hazardous Substances).
 - 1.1.8 Performance
 - 1.1.8.1 O servidor deverá ter índice de, no mínimo, 260 pontos de SPECint2006rate_base, medidos pelo SPEC.org.
 - 1.1.8.2 Não serão aceito servidores com processadores diferentes dos processadores auditados.
- 1.2 GABINETE
 - 1.2.1 Gabinete rack com botão Liga/Desliga, LEDs indicativos de equipamento ativo, acionamento de disco rígido no painel frontal e indicadores de falha no equipamento, padrão 19” com no máximo 1U de altura.
 - 1.2.2 Possuir sistema de fontes de alimentação redundantes hot-plug ou hot-swap, com dispositivo de alerta no caso de falha e com capacidade suficiente para suportar todos os dispositivos internos na configuração máxima admitida pelo equipamento (processadores, placa-mãe, interfaces, discos rígidos, memória RAM e todos os fans);
 - 1.2.3 Possuir sistema de ventilação redundante e hot-plug ou hot-swap adequado para o perfeito funcionamento do equipamento, conforme recomendações do fabricante do processador, o sistema deventer ter a capacidade de alterar a rotação dos ventiladores conforme a necessidade, visando a economia energia;
 - 1.2.4 Possuir baia instalada internamente ao servidor, mas com acesso externo, que permita a utilização de, no mínimo, 8 (oito) discos rígidos Hot-Swap ou hot plug;
 - 1.2.5 Não possuir “cantos vivos”, arestas ou bordas, internas ou externas, que sejam cortantes;
 - 1.2.6 O servidor deverá permitir a abertura sem a necessidade da utilização ferramentas.
- 1.3 PROCESSADOR
 - 1.3.1 Possuir, no mínimo, 2 processadores padrão x86 com tecnologia Octa-Core ou superior e desenvolvido para servidor, com tecnologia QPI – Quick Patch Interconnect ou similar;
 - 1.3.2 Confeccionado com tecnologia de 32nm;
 - 1.3.3 Possuir frequência de clock igual ou superior a 2,0Ghz;
 - 1.3.4 Possuir potência de dissipação máxima de 60W(rms) por socket;
 - 1.3.5 Possuir FAN Intelligent System ou tecnologia similar, que possibilite alta dispersão térmica e seja auxiliado por ventilação forçada do gabinete para garantir a vida útil do processador bem como dissipador de alta dispersão calórica, implementados de acordo com as recomendações do fabricante do processador;
 - 1.3.6 Suporte a SMP (multiprocessamento simétrico); 1.3.7 Possuir barramento interno de, no mínimo, 5.86 GT/s.
 - 1.3.8 Possuir recursos para virtualização de I/O e de CPU.

1.3.9 Suporta as tecnologias: SSE 4.2 (Streaming SIMD Extensions 4), AES (Advanced Encryption Standard).

1.3.10 Suporta memórias com até 1333MHz de frequência.

1.4 PLACA PRINCIPAL

1.4.1 Memória RAM instalada, no mínimo, 64 (sessenta e quatro) Gigabytes em pentes de 8 (oito) Gigabytes, ou maiores, com arquitetura DDR3, frequência de operação mínima de 1333Mhz e consumir no máximo 1.35 V cada.

1.4.2 Permitir a expansão da memória RAM a, no mínimo, 256 (duzentos e cinquenta e seis) Gigabytes sem a necessidade de troca de componentes;

1.4.2 Possuir sistemas de proteção a memória com suporte a: Error Correcting Code –ECC, memory Spare, memory mirroring, Advanced ECC ou chipkill;

1.4.3 Possuir, no mínimo, 12(doze) slots compatíveis com a memória ofertada;

1.4.4 Disponibilidade de, no mínimo, 1 (um) slot de expansão padrão PCI-e (PCI Express) Gen 2 com barramento x16 ou superior, livre após a instalação de todos os dispositivos;

1.4.5 Possuir 1 (uma) interface para conexão de teclado com conector padrão PS/2 fêmea ou USB;

1.4.6 Possuir 1 (uma) interface para conexão de mouse padrão PS/2 fêmea ou USB;

1.4.7 Possuir, no mínimo, 2 (duas) saídas com conector tipo DB15 para monitor;

1.4.8 Interface de vídeo compatível com padrão SVGA, ou superior, embutida, com pelo menos 16(dezesseis) Megabytes de memória de vídeo e interface de interconexão com a placa no padrão PCI Express ou tecnologicamente superior;

1.4.9 Possuir, no mínimo, 1 (uma) interface serial com conector tipo DB-9;

1.4.10 Possuir, no mínimo, 4 (quatro) interfaces USB (Universal Serial BUS) padrão 2.0 ou superior;

1.4.11 Não serão aceitas interfaces USB instaladas por meio de Placas de expansão de portas ou qualquer outro tipo de interface que não seja nativa do equipamento;

1.4.12 Possuir recurso tecnológico integrado que garanta que o servidor seja automaticamente reinicializado em caso de instabilidade grave do sistema (como por exemplo travamento devido a memory leak, overclocking, instabilidade elétrica, falha de processador etc).

1.5 BIOS

1.5.1 Bios do fabricante;

1.5.2 Tipo flash EPROM (atualizável por software); 1.5.3

Senha de acesso ativada e desativada via setup;

1.5.4 Relógio não-volátil.

1.6 UNIDADE DE DISCO RÍGIDO

1.6.1 Possuir, no mínimo, 2 (dois) discos com tecnologia Serial Attached SCSI - SAS (todos idênticos) de, no mínimo, 300 (trezentos) Gbytes cada e dimensões máximas de 2,5", compatíveis com a controladora SAS cotada com o equipamento;

1.6.2 Cada unidade de disco utilizada deve possuir:

1.6.2.1 Rotação de, no mínimo, 10.000 RPM

1.6.2.2 Interface SAS 6(seis) Gb/s;

1.6.2.3 Taxa de transferência externa mínima de 600 (seissentos) MB/s;

1.6.2.4 Montagem interna ao gabinete do servidor, em baia específica de 2,5" cada;

1.6.2.5 Cabo de comunicação entre o disco rígido e a controladora SAS cotada com o equipamento.

1.6.2.6 Possuir facilidade hot swap.

1.7 CONTROLADOR SAS

1.7.1 Possuir, no mínimo, 1 (um) controlador SAS com processador embarcado;

1.7.2 Compatível com os padrões RAID 0, RAID 1, RAID 0+1, RAID 5, RAID 6 e RAID 60 por hardware; 1.7.3 Oferecer detecção e recuperação automática de falhas e reconstrução transparente do RAID;

1.7.4 Memória cache de, no mínimo, 512 (quinhentos e doze) MB, com sistema de proteção ECC e servida por bateria;

1.7.5 Operar com taxa de transferência de, no mínimo, 6(seis)Gbit/s;

1.7.6 Operar comunicação no modo Full Duplex;

1.7.7 Possuir suporte a "hot-swap"e"hot-spare";

1.7.8 Ser totalmente compatível com os discos ofertados;

1.7.9 Suportar, no mínimo, 8 (oito) unidades de disco;

1.8 UNIDADE GRAVADORA DE DVD/CD

1.8.1 Capacidade de gravação de DVD-R e DVD-RW de camada dupla;

1.8.2 Velocidade de gravação de DVD-R de no mínimo 8x para DVD-R de camada dupla;

1.8.3 Velocidade de gravação de DVD+RW de no mínimo 8x;

1.8.4 Interface SATA ou superior.

1.9 INTERFACES

1.9.1 Possuir, no mínimo, 4 (quatro) portas padrão Gigabit Ethernet (100-1000BASE-TX), com as seguintes características:

1.9.1.1 Operar comunicação no modo full-duplex

1.9.1.2 Possuir conector RJ-45 fêmea

1.9.1.3 Possuir barramento PCI, ou superior, de 64 bits e 100 MHz

1.9.1.4 Compatível com o padrão IEEE 802.3

1.9.1.5 Leds indicadores de link ativo e de tráfego;

1.9.1.6 Permitir a configuração via software (jumperless);

1.9.1.7 Oferecer opção de configuração automática da interface (auto-sense);

1.9.1.8 Compatível com Plug & Play;

1.9.1.9 Suporte ao gerenciamento SNMP;

1.9.1.10 Possuir software de diagnóstico, capaz de identificar o funcionamento correto dos componentes;

1.9.1.11 Suporte a Wake UP on LAN;

1.9.1.12 Suporte a PXE;

1.9.1.13 Permitir balanceamento de carga;

1.9.1.14 Permitir Link Aggregation;

- 1.9.1.15 Possuir fail-over automático;
- 1.9.1.16 Suporte a TOE;
- 1.9.1.17 Suporte aos protocolos: 802.1q (VLAN tagging), 802.3x (flow control), 802.3ad (LACP);

1.10 INTERFACE DE VÍDEO

1.10.1 Possuir, no mínimo, 16 MB de memória de vídeo com interface PCI Express compatível com o padrão SVGA ou tecnologicamente superior;

1.10.2 Capacidade para trabalhar com resolução de 1280x1024;

1.11 FONTE DE ALIMENTAÇÃO

1.11.1 O servidor devera possuir, no mínimo, duas fontes redundantes que suporte o servidor em sua capacidade máxima.

1.11.2 Devem ser de, no máximo, 800w.

1.11.3 As fontes devem alternar entre 110 e 220W automaticamente.

1.12 SOFTWARE DE GERENCIAMENTO

1.12.1 Todos os servidores devem ser fornecidos com uma solução completa de hardware e software para gerenciamento remoto de sistemas, com todas as funcionalidades habilitadas para pleno gerenciamento remoto dos equipamentos, com no mínimo as seguintes características:

1.12.1.2 Possui microprocessador e memória próprios;

1.12.1.3 Possuir conexão que permita o acesso à console do equipamento através da rede. Esta conexão deve possuir 1 (uma) interface 10/100Mbps/s, ou superior, exclusiva;

1.12.1.4 Possuir acesso a console através de HTTPS ou software proprietário, possuindo usuário e senha de conexão, com criptografia de dados trafegados;

1.12.1.5 Permitir gerenciar e monitorar remotamente o sistema, mesmo quando ele estiver fora do ar;

1.12.1.6 Gerenciar servidores remotamente de qualquer lugar por meio de uma conexão IP;

1.12.1.7 Permitir instalação de software de qualquer lugar, por meio de uma conexão IP, de forma criptografada;

1.12.1.8 Possuir console de vídeo contínuo independente de SO que capture a última tela e acompanhe a reinicialização do servidor;

1.12.1.9 Permitir monitorar o status do servidor remoto durante uma reinicialização;

1.12.1.10 Permitir autenticação e autorização do Active Directory para melhor segurança;

1.12.1.11 Possuir a capacidade de reiniciar um servidor desligado e desligar um servidor remotamente;

1.12.1.12 Permitir autoridade baseada em funções através da atribuição de permissões para diferentes tarefas de gerenciamento de sistemas;

1.12.1.13 Possui a funcionalidade de emitir alertas para problemas potenciais de nós gerenciados por meio de mensagens de e-mail ou SNMP;

1.12.1.14 Possuir análise de pré-falha por hardware para, pelo menos, processador, memórias e discos;

1.12.1.15 O software deve ter a capacidade de monitora e controla o consumo de energia do servidor, com possibilidade de se estabelecer limites para o servidor;

1.12.1.16 Permitir o deployment de sistema operacional para um grupo de servidores;

1.12.1.17 Permitir trabalhar com ambientes e ferramentas virtualizados, incluindo Microsoft Virtual Server, VMware e virtualização Xen executando funcionalidades como descoberta de máquinas virtuais, inventário, topologia, monitoração da saúde dos servidores virtuais, operações de ligar e desligar, realocação e thresholds;

1.12.1.18 Permitir a visualização dos sistemas de acordo com a VLAN; Coleta e visualização dos componentes de network virtuais ou físicos; Suporte as soluções dos principais fabricantes de mercado Qlogic, Brocade, Cisco e Juniper;

1.12.2 Caso seja necessário software proprietário, este deve ser entregue em quantidade suficiente para administrar todos os servidores fornecidos e com todas as funcionalidades habilitadas;

1.13 SOFTWARE DE VIRTUALIZAÇÃO

1.13.1 Deverá ser fornecido licenciamento VMware vSphere 5.1 Essentials Plus para a capacidade total do servidor.

1.13.2 Deve possuir suporte 9x5 e direito a atualizações por 3 (três) anos direto pelo fabricante da solução, não sendo aceito licenciamento em regime de OEM.

ESPECIFICAÇÃO DO STORAGE

Quantidade: 01 unidades

1. Controladoras
- 1.1. Possuir controladora redundante, sendo que a falha de uma das controladoras não acarrete interrupção ou degradação dos serviços, sendo capaz de suportar a capacidade máxima de discos suportada pelo equipamento;
- 1.2. Suportar no mínimo os padrões RAID 0, 1, 5, 6 e 10;
- 1.3. Permitir reconstrução transparente do RAID sem necessidade de reiniciar o equipamento;
- 1.4. Suportar reconfigurações dinâmicas, inclusão de LUN, assinalamento de HOST, sem necessidades de parada dos demais serviços
- 1.5. O equipamento deverá permitir a adição de gavetas e serviços sem parada do equipamento
2. Cache
- 2.1. Possuir memória cache líquido, isto é, disponível para aplicativos de, no mínimo, 4 GB por controladora, espelhado entre as controladoras, que garanta integridade dos dados presentes na memória e ainda não gravados em disco, em caso de falha de uma das controladoras ou falta súbita de energia;
- 2.2. As soluções protegidas por bateria deverão ter autonomia mínima de 24 (vinte e quatro) horas, exceção feita às tecnologias que tenham autonomia interna suficiente para efetuar a gravação dos dados presentes na memória em disco ou Flash Drive e posterior desligamento do equipamento, mesmo em caso de falta súbita de energia;
- 2.3. Recurso que garanta que os dados residentes no cache sejam salvos para uma unidade "Flash Drive" ou em discos rígidos, em caso de falta de alimentação elétrica;

- 2.4. Expansível a, no mínimo, 8GB por controladora, sem que seja necessária a aquisição de novas controladoras ou clusterização;
- 2.5. Possuir nativamente pelo menos 8 (oito) interfaces externas (front-end) para conexão à SAN, padrão Fibre Channel de 8 Gbps;
- 2.6. Possuir no mínimo 4 (quatro) interfaces externas (front-end) para conexão à SAN, padrão iSCSI de 1 Gbps;
3. Capacidade de armazenamento e unidades de disco
 - 3.1. Suportar recurso de hot-spare para as unidades de disco rígido, ou seja, havendo falha de qualquer disco em determinado array/gaveta, o sistema deverá substituir, automaticamente, o disco defeituoso pelo disco spare;
 - 3.2. Os discos deverão ser hot-plug/hot-swap;
 - 3.3. Permitir a instalação de discos com capacidades diferentes, dentro da mesma gaveta de discos (enclosure);
 - 3.4. Possuir capacidade instalada inicial de:
 - 3.4.1. 12 (doze) unidades de disco padrão SAS de 6 Gbps com capacidade bruta mínima individual de 900 GB e velocidade rotacional de 10k RPM;
 - 3.4.2. Capacidade de expansão da quantidade de discos instalada a um total de, pelo menos, 120 (cento e vinte) discos, através da simples adição de gavetas de expansão de capacidade;
4. Alimentação e Ventilação
 - 4.1. Possuir fontes de alimentação e sistema de ventilação redundante e tipo "hot-swap", que mantenham o equipamento em operação integral, sem prejuízo do desempenho, em caso de falha de uma das fontes ou ventiladores, quaisquer que sejam a temperatura e a tensão de alimentação, respeitados os limites máximos e mínimos de operação;
 - 4.2. As fontes de alimentação deverão operar na faixa de 100 a 240 Volts, 60 Hz, com seleção automática;
 5. Funcionalidades e Gerenciamento
 - 5.1. Possuir software(s) para monitoração, controle, gerenciamento e configuração do storage através de interface única, com as seguintes funções:
 - 5.1.1. Permitir o envio de mensagens de e-mail ao administrador em caso de falhas;
 - 5.1.2. Permitir o envio de mensagens de e-mail ao suporte técnico do fabricante do equipamento em caso de falhas – sendo que o atendimento de suporte técnico deve ser oferecido em idioma português;
 - 5.1.3. Permitir a criação e configuração, através do software de gerenciamento, de RAID groups e volumes lógicos (LUNs);
 - 5.1.4. Permitir a adição de capacidade de armazenamento e expansão de volumes de forma dinâmica;
 - 5.1.5. Permitir a configuração de LUN Masking, LUN Partitioning ou similar, ou seja, restringir o acesso a determinado volume lógico (LUN) para um servidor ou conjunto de servidores, físicos ou virtuais (VMware);
 - 5.1.6. Permitir o envio de alertas SNMP para uma console de gerenciamento centralizada;
 - 5.1.7. Deve permitir gerar registros para todos os eventos relacionados ao storage, sejam eles de falhas ou configurações;
 - 5.2. Além do software gerenciamento, devem ser incluso os seguintes software / facilidades abaixo, licenciados para a capacidade total instalada, e com o mesmo prazo manutenção/garantia do hardware ofertado;
 - 5.2.1. Permitir a realização de cópias instantâneas (snapshots / flashcopy) de volumes online em tempo real e cópias completas do volume (full copy), sendo que estas funcionalidades deverão estar licenciadas para a capacidade total de armazenamento suportada pelo equipamento;
 - 5.2.2. Permitir o provisionamento nativo da capacidade realmente utilizada pelos aplicativos e usuários através de funcionalidade de thin provisioning, sendo que esta funcionalidade deverá ser licenciada para a capacidade total de armazenamento suportada pelo equipamento. Não será aceita a implementação da funcionalidade através de equipamentos externos.
 - 5.2.3. Deverá possuir a capacidade de realizar a migração de dados de sistemas de armazenamento (storages), do mesmo fabricante do equipamento ofertado e de outros fabricantes do mercado, para a área interna do sistema de armazenamento ofertado, de forma transparente. Caso o equipamento ofertado não possua a funcionalidade solicitada de forma nativa, deverão ser fornecidos juntamente com a solução os equipamentos e softwares necessários a essa finalidade;
 - 5.2.4. Deverá permitir a implementação futura de tecnologia que possibilite a movimentação automática e nativa dos dados mais ativos no Storage para discos de estado sólido (SSD), com o objetivo de aumento de desempenho. Não será aceita a implementação da funcionalidade através de equipamentos externos;
 - 5.2.5. Permitir o espelhamento de volumes em diferentes gavetas de armazenamento de dados com o objetivo do aumento da disponibilidade em caso de falha da gaveta, sendo que essa funcionalidade deverá ser licenciada para a capacidade total suportada pelo equipamento;
 - 5.2.6. Permitir o monitoramento de desempenho em tempo real do sistema das seguintes métricas: % de utilização de portas; % de utilização de processadores; taxas de I/O; taxas de transferência (MB/seg), e Latência;
 - 5.2.7. Incluir drives de multipathing do próprio fabricante para a quantidade de hosts/servidores suportada pelo equipamento.
 - 5.2.8. Suportar integração com VMware vStorage API for Array Integration (VAAI), suportar gerenciamento via VMWare vCenter, e suportar Recuperação de Desastres com VMWare SRM, sendo que esta funcionalidade deverá ser licenciada para a capacidade total de armazenamento suportada pelo equipamento;
 - 5.2.9. O software de gerenciamento deverá estar licenciado para a capacidade total de armazenamento suportado pelo equipamento;
 - 5.2.10. Todos os softwares envolvidos deverão ser fornecidos na modalidade de licenciamento perpétuo;
6. Características Gerais
 - 6.1. O equipamento deverá ser fornecido com todos os elementos necessários para sua correta fixação em rack padrão 19" (trilhos, parafusos...) bem como cabos de alimentação;
 - 6.2. 04 (quatro) cordões óticos de 05 (cinco) metros de comprimento ou superior, com conectores do tipo LC-LC;
7. Compatibilidade

8.1 O Storage deverá suportar, no mínimo os Sistemas Operacionais Microsoft Windows 2008, Linux Red Hat 3, 4 e 5 e VMWare ESX 5.1;

8.2 A Solução de Storage deverá comprovar compatibilidade com a API do Vmware VAAI (vSphere APIs for Array Integration).

8.3 Comprovação de que o fabricante do equipamento ofertado deverá ser participante do SNIA (Storage Networking Industry Association), na qualidade de "Large Voting Member", com comprovação através do site: http://www.snia.org/member_com/member_directory/ e aderente ao GSI (Green Storage Initiative), com comprovação no site <http://www.snia.org/forums/green/>. Cópia do documento comprovando tal informação deverá estar contida na proposta.

8.4 Deverá ser compatível com as normas estabelecidas pela SNIA (Storage Networking Industry Association) e prover interface de gerenciamento de acordo com o padrão SMI-S (Storage Management Initiative Specification) versão 1.2 ou superior, para gerenciamento do ambiente através de ferramentas de gerência de infra-estrutura de armazenamento que utilizem esse padrão. A conformidade poderá verificada através de consulta ao site oficial do SNIA Interoperability Conformance Test Program (SNIACTP) <http://www.snia.org/ctp/conformingproviders/index.html>

9. Rede SAN (Storage Area Network)

9.1. Deverá ser entregue o total de 2 (dois) switches iscsi para interligação dos equipamentos (storage e servidores) na rede de armazenamento de dados, contendo as características mínimas do Switch de Acesso - Tipo O2 especificado em item anterior:

ESPECIFICAÇÃO DO RACK E NOBREAKS

1. Para acomodação física dos equipamentos propostos na solução deverá ser disponibilizado 1 (um) rack com as seguintes características mínimas:

1.1. Possuir capacidade mínima de 42U de altura.

1.2. Estar de acordo o padrão de 19" polegadas;

1.3. Possuir no mínimo 2 (duas) PDU's com as seguintes características:

1.3.1. Possuir 8 (oito) conexões AC 110/220v;

1.3.2. Possuir interruptor de carga;

1.3.3. Ser com padrão compatível com os equipamentos e no-breaks que compõe a solução;

1.4. Possuir portas frontal e traseira que permitam o devido fluxo de ar;

1.5. As portas devem possuir opção de bloqueio/fechadura;

1.6. As laterais devem possibilitar remoção no caso de manuseio dos equipamentos;

2. Deverá ser fornecido juntamente com a solução no mínimo 2 (dois) módulos de nobreak com as seguintes características mínimas:

2.1. Possuir montagem padrão de rack 19" e compatível com o rack disponibilizado na solução;

2.2. Possuir tensão de entrada para 220v

2.3. Possuir tensão de saída para 220v;

2.4. Suportar tecnologia de dupla conversão de forma on-line;

2.5. Possibilitar expansões futuras de outros bancos de baterias do mesmo fabricante;

2.6. As baterias devem ser livres de manutenção;

2.7. Deverá ser capaz de suportar toda solução disponibilizada em seu pleno funcionamento pelo período mínimo de 30 (trinta) minutos;

2.8. Capacidade inicial não deverá ser inferior a 3.000 VA

2.9. O fator de eficiência deve ser no mínimo de 95%;

2.10. Possuir interface para gerenciamento e monitoração;

ESPECIFICAÇÃO DO LICENCIAMENTO DE VIRTUALIZAÇÃO E BACKUP

1. Deverá ser fornecido licenciamento de VMware vCenter para gerenciamento dos servidores disponibilizados com VMware vSphere 5.1

1.1. Deve possuir suporte 9x5 e direito a atualizações por 3 (três) anos direto pelo fabricante da solução, não sendo aceito licenciamento em regime de OEM.

2. Software de Backup e replicação

2.1. Deverá ser fornecido licenciamento de software de backup para todo ambiente, contendo as seguintes características mínimas:

2.2. Ser homologado para hypervisor VMware

2.3. Possibilitar a recuperação granular de e-mail em plataforma Microsoft Exchange;

2.4. Permitir configuração de replicação das máquinas virtuais;

2.5. Ser licenciamento de forma perpétua para toda solução disponibilizada;

2.6. Caso o licenciamento seja por capacidade, deve ser considerada a capacidade máxima da biblioteca de fitas disponibilizada na solução;

2.7. Permitir a recuperação granular de servidor de arquivos;

2.8. Possibilitar a recuperação de máquinas virtuais em menos de 5 (cinco) minutos;

2.9. Deve possuir suporte 9x5 e direito a atualizações por 3 (três) anos direto pelo fabricante da solução, não sendo aceito licenciamento em regime de OEM.

2.10. Deverá ser entregue servidor no padrão rack para instalação da solução de backup, possuindo os requisitos mínimos de:

2.10.1. Possuir, no mínimo, 1 processador padrão x86 com tecnologia Six-Core ou superior;

2.10.1.1 Possuir frequência de clock igual ou superior a 2,0Ghz;

2.10.2. Memória RAM instalada, no mínimo, 16 (dezesesseis) Gigabytes em pentes de 8 (oito) Gigabytes, ou maiores, com arquitetura DDR3, frequência de operação mínima de 1333Mhz e consumir no máximo 1.35 V cada.

- 2.10.3. Permitir a expansão da memória RAM a, no mínimo, 128 (duzentos e cinquenta e seis) Gigabytes sem a necessidade de troca de componentes
- 2.10.4. Possuir, no mínimo, 6 (seis) discos com tecnologia Serial Attached SCSI - SAS (todos idênticos) de, no mínimo, 300 (trezentos) Gbytes cada e dimensões máximas de 2,5", compatíveis com a controladora SAS cotada com o equipamento;
- 2.10.5. Possuir suporte a "hot-swap" e/ou "hot-spare" para discos;
- 2.10.6. Possuir sistema de fontes de alimentação e fans redundantes hot-plug ou hot-swap, com dispositivo de alerta no caso de falha e com capacidade suficiente para suportar todos os dispositivos internos na configuração máxima admitida pelo equipamento (processadores, placa-mãe, interfaces, discos rígidos, memória RAM e todos os fans);
- 2.10.7. Possuir, no mínimo, 1 (um) controlador SAS com processador embarcado;
- 2.10.8. Compatível com os padrões RAID 0, RAID 1, RAID 0+1, RAID 5, RAID 6 e RAID 60 por hardware
- 2.10.9. Deverá ser fornecido licenciamento Windows Server Standard 2008 ou superior para a capacidade total do servidor
- 2.10.10. Possuir controladora Fibre Channel (HBA) para conexão com a biblioteca de fitas contemplada na solução, no mínimo 2 (dois) canais padrão FC, com velocidade de conexão de 8 (oito) Gbps por canal.
- 2.10.11. Possuir controladora ethernet para conexão a rede SAN da contemplada na solução, com no mínimo 4 (quatro) portas, com velocidade de conexão gigabit.
- 2.10.12. As controladoras devem ser compatíveis com sistemas operacionais Windows 2008 Server, VMware vSphere 5.1 e com os switches SAN ofertados na solução.
- 2.11. Deverá ser entregue biblioteca de fitas interligada no servidor de backup. Esta deve ser no padrão rack para operação da solução de backup, possuindo os requisitos mínimos de:
 - 2.11.1. Suportar, no mínimo, 2 (dois) drive half-height com a tecnologia LTO-5;
 - 2.11.2. Possuir, no mínimo, 24 (vinte e quatro) slots de fitas de dados;
 - 2.11.3. Padrão para instalação em rack de 19" de largura;
 - 2.11.4. Possuir fontes de alimentação com tensão de entrada de 110/220 V e frequência de 60 Hz;
 - 2.11.5. Possuir leitor de código de barras com o objetivo de identificar os cartuchos através das etiquetas; 2.11.6. Possuir drives com padrão de conexão FC;
 - 2.11.7. A unidade de backup deve possuir capacidade de ler, no mínimo, duas gerações anteriores e gravar em uma geração anterior, ou seja, ler LTO-4 e LTO-3 e gravar em LTO-4;
 - 2.11.8. Deverá ser entregue 22 (vinte dois) cartuchos padrão ultrium LTO5 e 2 (dois) de cartuchos de limpeza;
 - 2.11.9. Suportar gerenciamento via SNMP;
 - 2.11.10 Suportar gerenciamento da unidade de backup remotamente através de um web-browser, incluindo as principais funções de operação e monitoração local da Biblioteca;
 - 2.11.11. Possuir gerenciamento de erros e status de logs;
 - 2.11.12. Suportar os protocolos de rede IPv6 e IPv4;
 - 2.11.13. A unidade de backup deve ser capaz de:
 - 2.11.14. Monitorar a utilização dos drives e cartuchos;
 - 2.11.15. Reportar informações através de notificação do status do hardware como saúde e vida útil;

Serviço de Manutenção e Suporte

1. Deve possuir atendimento telefônico 0800 em língua portuguesa realizado pela equipe técnica especializada dos fabricante ou prestadora de serviço certificada pelo fabricante em horário comercial na modalidade 8X5, a licitante devere informar o ou os 0800 na proposta.
2. Defeitos em qualquer parte física da unidade incluindo fonte de alimentação e ventiladores;
3. Sistema operacional "IOS ou firmware" onde deve ser disponibilizado acesso direto ao site do fabricante para download de novas versões que contenham correções e/ou atualizações;
4. Suporte e Manutenção dos fabricantes ou empresa licitante, pelo período do contrato com atendimento On-Site, com tempo de atendimento de até 24 horas e solução de problemas pelo período máximo de 48 horas, contadas à partir da abertura do chamado.
5. Caso a solução do problema implique na substituição do equipamento defeituoso, o mesmo será entregue à contratada no momento da instalação do equipamento substituído.
6. A contratada deverá garantir o mais rigoroso sigilo sobre quaisquer dados, informações, documentos e especificações que a ela venham a ser confiados ou que venha a ter acesso em razão dos serviços prestados, não podendo, sob qualquer pretexto, revela-los, divulga-los, reproduzi-los ou dar conhecimento a quaisquer terceiro.
7. Possuir em seu quadro funcional, no mínimo, 01 técnico Certificado na Tecnologia de Rede para design, instalação e administração para switches empilháveis;
8. Autorização para comercialização dos equipamentos e técnico(s) certificados pelo fabricante para realizar a instalação, configuração e suporte técnico da solução ofertada;
9. Banco de horas em horário comercial para atendimento remoto ou caso necessário local/ on-site; 10. Limitado ao período do contrato;
11. Solicitações de complexidade nível 2 e 3;
12. Será disponibilizado acesso remoto sempre que necessário;
13. Contemplar coleta mensal do ambiente para análise e acompanhamento preventivo;

ANEXO III

(MODELO)

AO (À) PREGOEIRO (A)
REF. PREGÃO ELETRÔNICO/20.....

DECLARAÇÃO

Declaramos para os fins de direito, na qualidade de licitante do presente processo licitatório, que, em cumprimento ao inciso XXXIII do artigo 7.º da Constituição Federal combinado ao inciso V do artigo 27 da Lei n.º 8.666/93, não possuímos em nosso quadro funcional pessoas menores de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e, de menores de 16 (dezesesseis) anos em qualquer trabalho, salvo na condição de aprendiz, a contar dos 14 (quatorze) anos.

Por ser expressão da verdade, firmamos a presente.

....., em de de 2020.

(Assinatura) _____

RAZÃO SOCIAL:

CNPJ:

NOME DO REPRESENTANTE LEGAL:

(PROCURADOR JUNTAR PROCURAÇÃO OU CREDENCIAMENTO)

CPF:

ANEXO IV

(MODELO)

AO (À) PREGOEIRO (A)
REF. PREGÃO ELETRÔNICO/201.....

DECLARAÇÃO DE IDONEIDADE

(Razão Social da licitante), por meio de seu responsável legal, declara, sob as penas da lei, que não foi considerada INIDÔNEA/IMPEDIDA para licitar ou contratar com a Administração Pública, nos termos do art. 87, IV, da Lei de Licitações e art. 7º da Lei 10.520/02.

Por ser expressão da verdade, firmamos a presente.

....., em de de 2020.

(Assinatura) _____

RAZÃO SOCIAL:

CNPJ:

NOME DO REPRESENTANTE LEGAL:

(PROCURADOR JUNTAR PROCURAÇÃO OU CREDENCIAMENTO)

CPF:

ANEXO V

(MODELO)

AO (À) PREGOEIRO (A)
REF. PREGÃO ELETRÔNICO/20.....

DECLARAÇÃO

(Razão Social da licitante), por meio de seu Diretor ou Responsável Legal, declara, sob as penas da lei, que cumpre plenamente com os requisitos de habilitação.

Por ser expressão da verdade, firmamos a presente.

....., em de de 2020.

(Assinatura) _____

RAZÃO SOCIAL:

CNPJ:

NOME DO REPRESENTANTE LEGAL:

(PROCURADOR JUNTAR PROCURAÇÃO OU CREDENCIAMENTO)

CPF: