TERMO DE CONTRATO

CONTRATO Nº 150/2025
PROCESSO Nº 8679/2024
Dispensa de Licitação, conforme Artigo 75, VIII da Lei nº 14.133/2021 c/c do Decreto Federal nº 12.343/2024.

CONTRATO de **"Prestação de Serviços de Tecnologia da Informação-TI"** QUE ENTRE SI CELEBRAM O **MUNICÍPIO DE CONCEIÇÃO DA BARRA E A EMPRESA SISINFRA TECNOLOGIA LTDA**, NA FORMA ABAIXO.

O Município de Conceição da Barra, pessoa jurídica de direito público interno, inscrita no **CNPJ/MF nº. 27.174.077/0001-34** com Sede na Praça Prefeito José Luiz da Costa, s/n, Centro, Conceição da Barra/ES, neste ato representado pelo Prefeito Municipal, **Srº JOSÉ ERIVAN TAVARES DE MORAES**, portador do CPF-MF nº 776.942.524-72 e RG 1106121 SSP-AL, residente na Rua: 22 de Novembro, S/Nº, Nova Barra, Conceição da Barra-ES, CEP: 29.960-000, adiante denominado Contratante, e a empresa **SISINFRA TECNOLOGIA LTDA** pessoa jurídica de direito privado, inscrita no **CNPJ-MF sob o nº 30.634.546/0001-74**, com sede Rua: Presidente Café Filho, nº 396, Bairro: Novo Horizonte, Linhares-ES, CEP: 29.902-400, por seu representante legal, Sr. André Luiz Monjardim da Silva Filho, inscrito no CPF nº 123.243.687-90 e na Carteira de Identidade nº 3002738-ES, E-mail: andre.monjardim@sisinfra.com.br, TEL: 27-99962-0949, doravante denominada como Contratada, tendo em vista o que consta no **Processo nº 8679/2024** e em observância às disposições da Lei nº 14.133, de 2021, resolvem celebrar o presente Termo de Contrato, decorrente da Dispensa de Licitação, mediante as cláusulas e condições a seguir enunciadas.

CLÁUSULA PRIMEIRA - DO OBJETO

1.1. O objeto do presente instrumento é a prestação de serviços especializados na área de Tecnologia da Informação – TI, visando o atendimento das necessidades da Secretaria Municipal de Administração para manutenção, ampliação e recuperação da Infraestrutura atual do Data Center e implementação aplicação de e-mails e Suíte de gerenciamento, conforme o Termo de Referência, nas condições estabelecidas no **Processo nº 8679/2024**.

1.2. Objeto da contratação:
1.3. São anexos a este instrumento e vinculam esta contratação, independentemente de transcrição:
1.3.1. O Termo de Referência que embasou a contratação;
1.3.2. Aviso de Dispensa Eletrônica, caso existentes;
1.3.3. A Proposta do Contratado; e
1.3.4. Eventuais anexos dos documentos supracitados.

2. CLAUSULA SEGUNDA – VIGÊNCIA E PRORROGAÇÃO

2.1. O prazo de vigência da contratação até **06 (Seis) Meses,** contados da assinatura deste, na forma do artigo 105 da Lei nº 14.133/2021.

2.1.1. O prazo de vigência será automaticamente prorrogado, independentemente de termo aditivo, quando o objeto não for concluído no período firmado acima, ressalvadas as providências cabíveis no caso de culpa do contratado, previstas neste instrumento.

3. CLÁUSULA TERCEIRA – EXECUÇÃO E GESTÃO CONTRATUAIS

3.1. O regime de execução contratual, o modelo de gestão, assim como os prazos e condições de conclusão, entrega, observação e recebimento definitivo constam no Termo de Referência, anexo ao **Processo nº 8679/2024**.

4. CLÁUSULA QUARTA – SUBCONTRATAÇÃO

4.1. Não será admitida a subcontratação do objeto contratual.

5. CLÁUSULA QUINTA – PAGAMENTO

5.1. PREÇO

5.1.1. O valor total da contratação é de **R$ 33.300,00 (Trinta e Três Mil Trezentos Reais)** sendo o valor mensal de **R$ 5.550,00 (Cinco Mil Quinhentos e Cinquenta Reais).**

5.1.2. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

5.2. FORMA DE PAGAMENTO

5.2.1. O pagamento será realizado através de ordem bancária, para crédito em banco, agência e conta corrente indicado pelo contratado.
5.2.2. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

5.3. PRAZO DE PAGAMENTO

5.3.1. O pagamento será efetuado no prazo máximo de até 30 (Trinta) dias, contados do recebimento da Nota Fiscal/Fatura.
5.3.2. Considera-se ocorrido o recebimento da nota fiscal ou fatura quando o órgão contratante atestar a execução do objeto do contrato.
5.3.3. No caso de atraso pelo Contratante, os valores devidos ao contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação de correção monetária.

5.4. CONDIÇÕES DE PAGAMENTO

5.4.1. A emissão da Nota Fiscal/Fatura será precedida do recebimento definitivo do objeto da contratação, conforme disposto neste instrumento e/ou no Termo de Referência.
5.4.2. Quando houver glosa parcial do objeto, o contratante deverá comunicar a empresa para que emita a nota fiscal ou fatura com o valor exato dimensionado.
5.4.3. O setor competente para proceder ao pagamento deve verificar se a Nota Fiscal ou Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como:
a. o prazo de validade;
b. a data da emissão;

c. os dados do contrato e do órgão contratante;
d. o período respectivo de execução do contrato;
e. o valor a pagar; e
f. eventual destaque do valor de retenções tributárias cabíveis.

5.4.4. Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, o pagamento ficará sobrestado até que o contratado providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para o contratante;

5.4.5. A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133/2021.

5.4.6. Previamente à emissão de nota de empenho e a cada pagamento, a Administração deverá realizar consulta ao SICAF para:

a) verificar a manutenção das condições de habilitação exigidas no edital;

b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas.

5.4.7. Constatando-se, junto ao SICAF, a situação de irregularidade do contratado, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do contratante.

5.4.8. Não havendo regularização ou sendo a defesa considerada improcedente, o contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do contratado, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

5.4.9. Persistindo a irregularidade, o contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao contratado a ampla defesa.

5.4.10. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso o contratado não regularize sua situação junto ao SICAF.

5.4.11. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

5.4.11.1. Independentemente do percentual de tributo inserido na planilha, no pagamento serão retidos na fonte os percentuais estabelecidos na legislação vigente.

5.4.12. O contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

6. CLÁUSULA SEXTA – REAJUSTE

6.1. Não haverá previsão de reajuste contratual.

7. CLÁUSULA SÉTIMA – OBRIGAÇÕES DO CONTRATANTE

7.1. São obrigações do Contratante:

7.1.1. Exigir o cumprimento de todas as obrigações assumidas pelo Contratado, de acordo com o contrato e seus anexos;

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

7.1.3. Notificar o Contratado, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto fornecido, para que seja por ele substituído, reparado ou corrigido, no total ou em parte, às suas expensas;

7.1.4. Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pelo Contratado;

7.1.5. Efetuar o pagamento ao Contratado do valor correspondente ao fornecimento do objeto, no prazo, forma e condições estabelecidos no presente Contrato;

7.1.6. Aplicar ao Contratado sanções motivadas pela inexecução total ou parcial do Contrato;

7.1.7. Cientificar o órgão de representação judicial da Advocacia-Geral da União para adoção das medidas cabíveis quando do descumprimento de obrigações pelo Contratado.

7.1.8. Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente Contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste.

7.1.8.1. Concluída a instrução do requerimento, a Administração terá o prazo de 90 (noventa) dias para decidir, admitida a prorrogação motivada por igual período.

7.1.9. A Administração não responderá por quaisquer compromissos assumidos pelo Contratado com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato do Contratado, de seus empregados, prepostos ou subordinados.

8. CLÁUSULA OITAVA – OBRIGAÇÕES DO CONTRATADO

8.1. O Contratado deve cumprir todas as obrigações constantes deste Contrato, em seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas:

8.1.1. Manter preposto aceito pela Administração no local da obra ou do serviço para representá-lo na execução do contrato.

8.1.1.1. A indicação ou a manutenção do preposto da empresa poderá ser recusada pelo órgão ou entidade, desde que devidamente justificada, devendo a empresa designar outro para o exercício da atividade.

8.1.2. Atender às determinações regulares emitidas pelo fiscal do contrato ou autoridade superior (art. 137, II);

8.1.3. Alocar os empregados necessários, com habilitação e conhecimento adequados, ao perfeito cumprimento das cláusulas deste contrato, fornecendo os materiais, equipamentos, ferramentas e utensílios demandados, cuja quantidade, qualidade e tecnologia deverão atender às recomendações de boa técnica e a legislação de regência;

8.1.4. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

8.1.5. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa

responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo Contratante, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida no edital, o valor correspondente aos danos sofridos;

8.1.6. Não contratar, durante a vigência do contrato, cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente do contratante ou do Fiscal ou Gestor do contrato, nos termos do artigo 48, parágrafo único, da Lei nº 14.133, de 2021;

8.1.7. Quando não for possível a verificação da regularidade no Sistema de Cadastro de Fornecedores – SICAF, a empresa contratada deverá entregar ao setor responsável pela fiscalização do contrato, até o dia trinta do mês seguinte ao da prestação dos serviços, os seguintes documentos:

1) prova de regularidade relativa à Seguridade Social;

2) certidão conjunta relativa aos tributos federais e à Dívida Ativa da União;

3) certidões que comprovem a regularidade perante a Fazenda Municipal ou Distrital do domicílio ou sede do contratado;

4) Certidão de Regularidade do FGTS – CRF; e

5) Certidão Negativa de Débitos Trabalhistas – CNDT;

8.1.8. Responsabilizar-se pelo cumprimento das obrigações previstas em Acordo, Convenção, Dissídio Coletivo de Trabalho ou equivalentes das categorias abrangidas pelo contrato, por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao Contratante;

8.1.9. Comunicar ao Fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local dos serviços.

8.1.10. Prestar todo esclarecimento ou informação solicitada pelo Contratante ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do empreendimento.

8.1.11. Paralisar, por determinação do Contratante, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros.

8.1.12. Promover a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à execução do objeto, durante a vigência do contrato.

8.1.13. Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local dos serviços e nas melhores condições de segurança, higiene e disciplina.

8.1.14. Submeter previamente, por escrito, ao Contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo ou instrumento congênere.

8.1.15. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos, nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre;

8.1.16. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação na licitação, ou para qualificação, na contratação direta;

8.1.17. Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas na legislação (art. 116);

8.1.18. Comprovar a reserva de cargos a que se refere a cláusula acima, no prazo fixado pelo fiscal do contrato, com a indicação dos empregados que preencheram as referidas vagas (art. 116, parágrafo único);
8.1.19. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;
8.1.20. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da contratação, exceto quando ocorrer algum dos eventos arrolados no art. 124, II, d, da Lei nº 14.133, de 2021.
8.1.21. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança do Contratante.

9. CLÁUSULA NONA – GARANTIA DE EXECUÇÃO

9.1. Não haverá exigência de garantia contratual da execução.

10. CLÁUSULA DÉCIMA – INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

10.1. Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o Contratado que:
a) der causa à inexecução parcial do contrato;
b) der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;
c) der causa à inexecução total do contrato;
d) deixar de entregar a documentação exigida para o certame;
e) não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;
f) não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;
g) ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;
h) apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a dispensa eletrônica ou execução do contrato;
i) fraudar a contratação ou praticar ato fraudulento na execução do contrato;
j) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
k) praticar atos ilícitos com vistas a frustrar os objetivos da contratação;
l) praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

10.2. Serão aplicadas ao responsável pelas infrações administrativas acima descritas as seguintes sanções:
I - Advertência, quando o Contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §2º, da Lei);
II - Impedimento de licitar e contratar, quando praticadas as condutas descritas nas alíneas b, c, d, e, f e g do subitem acima deste Contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §4º, da Lei);
III - Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nas alíneas h, i, j, k e l do subitem acima deste Contrato, bem como nas alíneas b, c, d, e, f e g, que justifiquem a imposição de penalidade mais grave (art. 156, §5º, da Lei)

IV - Multa: 1. moratória de 0,5% (zero vírgula cinco por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 90 (noventa) dias;

11. CLÁUSULA DÉCIMA PRIMEIRA – DA EXTINÇÃO CONTRATUAL

11.1. O contrato se extingue quando cumpridas as obrigações de ambas as partes, ainda que isso ocorra antes do prazo estipulado para tanto.

11.2. Se as obrigações não forem cumpridas no prazo estipulado, a vigência ficará prorrogada até a conclusão do objeto, caso em que deverá a Administração providenciar a readequação do cronograma físico-financeiro.

11.3. Quando a não conclusão do contrato referida no item anterior decorrer de culpa do contratado:

a. ficará ele constituído em mora, sendo-lhe aplicáveis as respectivas sanções administrativas; e

b. poderá a Administração optar pela extinção do contrato e, nesse caso, adotará as medidas admitidas em lei para a continuidade da execução contratual.

12. CLÁUSULA DÉCIMA SEGUNDA – DOTAÇÃO ORÇAMENTÁRIA

12.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento deste exercício, na dotação abaixo discriminada:

20.03.00 Secretaria Municipal de Administração

20.03.10 Gestão Secretaria Municipal de Administração,

Classificação Funcional: 04.122.0019.2.0135

Natureza da Despesa: 3.3.90.40.99

Recurso: 1.500.0000.0000

13. CLÁUSULA DÉCIMA TERCEIRA – DOS CASOS OMISSOS

13.1. Os casos omissos serão decididos pelo CONTRATANTE, segundo as disposições contidas na Lei nº 14.133, de 2021 e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

14. CLÁUSULA DÉCIMA QUARTA – ALTERAÇÕES

14.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 14.133, de 2021.

14.2. O CONTRATADO é obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessária, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

14.3. As supressões resultantes de acordo celebradas entre as partes contratantes poderão exceder o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do termo de contrato.

14.4. Registros que não caracterizam alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do art. 136 da Lei nº 14.133, de 2021.

15. CLÁUSULA DÉCIMA QUINTA – PUBLICAÇÃO

15.1. 1.1. Incumbirá à CONTRATANTE providenciar a publicação deste instrumento nos termos e condições previstas na Lei nº 14.133/21.

16. CLÁUSULA DÉCIMA SEXTA - DA FISCALIZAÇÃO DOS SERVIÇOS

16.1 – A fiscalização e o acompanhamento da execução do objeto do contrato, com fundamento no artigo 117 da Lei Federal nº 14.133/2021 será feita pelo **CONTRATANTE**, através da Secretaria Municipal de Turismo, na pessoa do Srº Anderson Cabrini de Paula-Matrícula: 8330, Cargo: Gerente de TI, E-Mail: gti@conceiçcaodabarra.es.gov.br, Telefone: 27- 9.9877-7743, deverão exercê-los de modo amplo, irrestrito e permanente em todas as fases de execução das obrigações, inclusive quanto ao desempenho da Contratada, sem prejuízo do dever deste de fiscalizar os seus empregados, prepostos ou subordinados.

17. CLÁUSULA DÉCIMA SÉTIMA – FORO

17.1. É eleito o Foro da cidade de Conceição da Barra-ES, para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não possam ser compostos pela conciliação, conforme art. 92, §1º da Lei nº 14.133/21.

E, por estarem de acordo, depois de lido e achado conforme, foi o presente contrato assinado pelas partes.

Conceição da Barra – ES, 13 de Maio de 2025.

JOSÉ ERIVAN TAVARES DE MORAES
Prefeito Municipal
Contratante

gov.br
Documento assinado digitalmente
ANDRE LUIZ MONJARDIM DA SILVA FILHO
Data: 21/05/2025 09:12:23-0300
Verifique em https://validar.iti.gov.br

SISINFRA TECNOLOGIA LTDA
CNPJ-MF sob o nº 30.634.546/0001-74
Contratado

Fiscal do Contrato: Anderson Cabrini de Paula
Matrícula: 8330
Telefone: 27- 9.9877-7743
E-mail: gti@conceiçcaodabarra.es.gov.br
Cargo/Função: Gerente de Transporte
Secretaria Municipal de Infraestrutura

ANEXO I

Descrição do Produto/Serviços:

Item	Material	Un.	Marca	Modelo	Média C.	Qtde	Pr. Unit.	Pr. Total
01	2.19.01.0034-2	SV			0,000	06,0000	5.550,0000	33.300,00

DETALHAMENTO DOS SERVIÇOS DESCRITOS NOS ITENS 1,2,3,4,5 E 6 Item 1 – Otimização do TI OTIMIZAÇÃO DO TI 1. VMWare VCenter. Descrição: Um problema no banco de dados utilizado no sistema VMWare VCenter não permite a abertura dos consoles de gerenciamento, não permitindo a configuração dos diversos recursos oferecidos pela plataforma de virtualização. Solução: 1.1- Instalação de novo Servidor Virtual que suportará a plataforma de Gerenciamento VCenter. 1.2- Instalação de novo banco de dados que suportará a plataforma de virtualização. 1.3- Reinstalação e Atualização dos 3 Hosts de Virtualização. 1.4- Reconfiguração dos Hosts de VMWare. 2. Serviço Active Directory. Descrição: Erros no banco de dados e nos serviços do Active Directory impedem o funcionamento de outros serviços. A falta de definição de Sites do Active Directory como Educação, Secretaria de Saúde e outras unidades aumentam o tráfego desnecessário da rede e criam o mal funcionamento dos serviços essenciais da rede. Solução: 2.1- Criação de novo Servidor Mestre de Operações do Active Directory. 2.2- Desfragmentação do Banco de Dados do Active Directory. 2.3- Configurar servidores adicionais e Sites do Active Directory - PMCB, Saúde, Educação, CAA Sede e CAA de Braço do Rio. 2.4- Configuração de Logs e alertas. 3. Serviço de Arquivos Descrição: Com o aumento do número de arquivos e as ameaças de perda é necessário a implantação de sistema de gerenciamento profissional com réplica de dados, triagem e detecção de duplicatas. Solução: 3.1- instalação e configuração do Serviço de FSRM 3.2- Configuração dos Serviços de Log e de Auditoria. 3.3- Configuração de Servidores de Arquivo 3.4- Configuração do DFS. 3.5- Configuração do DFSR. 3.6- Configuração de Triagem de Arquivos. 3.7- Configuração do RMS. 4. Proteção contra a execução de aplicativos não autorizados. Descrição: Devido ao grande aumento de ameaças do tipo malwares, scripts maliciosos e códigos que podem comprometer todo o parque de computadores é importante a criação de uma política de autorização de aplicativos. Solução: 4.1- Planejamento de Estratégia de Diretiva de Segurança Appiocker. 4.2- Configuração e implantação da diretiva de segurança APPLOCKER. 5 - Serviço de e-mail Descrição: Com o aumento das ameaças relacionadas a interceptação de mensagens e ataques aos serviços de Email faz-se necessário a implantação do Serviço de E-mail internamente. Solução: 5.1 - Preparação da Floresta do Active Directory. 5.2- implementação do Servidor de Hub Transporte 5.3- implementação do Servidor do Servidor CAS 5.4- Implementação do Servidor Mailbox. 5.5- Implementação das Políticas de Anti-spam. 5.6- implementação de Política de Backup e Restauração. 5.7- implementação de Política de Segurança. 5.8- Configuração de todos os registros necessários para o correto recebimento e envio de e-mails. 5.9- Instalação e configuração do OWA. 5.10- Instalação e configuração dos serviços e protocolos MAPI, POP3 e IMAPI para conexão com cliente. 5.11- Configuração do Framework SPF. 5.12- Implantação de Rede de Perímetro. 5.13- implantação de 2 Servidores de DNS para Zona Pública em Rede de Perímetro. 5.14- implantação de Zona Reversa em Rede de Perímetro. 5.15- implantação do Servidor Edge Transport em Rede de Perímetro. 5.16- instalação de Certificados digitais que permitam a autenticação segura e criptografia de dados enviados e recebidos pelo sistema de e-mails. 5.17- Configuração do serviço RMS. 5.18- Criação de grupos de e-mails. 5.19- Criação de Caixas de Correio. 5.20- Criação de Caixas de Correio de Recursos. 6. Configuração do Serviço de Implantação. Descrição: O serviço de Implantação é fundamental para a conformidade e segurança dos desktops e servidores da rede. 6.1- Implementação do Servidor de Implantação. 6.2- Criação e Teste das Imagens de Implantação. 6.3- Criação de política de Atualização off-line de imagens de servidores e desktops. 7. Servidor de Banco de Dados. Descrição: Devido a importância dos dados existentes nos sistemas da prefeitura, é importante que se tenha várias formas de proteção e formas de acesso redundantes a estes dados. 7.1- Implementação de Servidor de Réplica de Dados do SQL Server. 7.2- Efetuar Manutenção do Servidor de Banco de Dados SQL Server que Hospeda os Dados dos Sistemas SMAR. 7.3- Reconfigurar política de segurança para os servidores 7.4- Configuração das Políticas de Backup/Restauração. 8. Configuração de Servidor de Certificados Digitais. Descrição: A criação do Servidor de Certificados Digitais é de fundamental importância para a implementação dos demais Serviços de Segurança que serão configurados na Rede. 8.1 - Instalação e Configuração do AD CS 8.2- Configuração de Política de Segurança para o Servidor. 8.3- Configuração de estratégia de Backup/Restauração de Servidor. 9. Área de Trabalho Remota. Descrição: Devido ao grande número de usuário com a necessidade de utilização remota dos aplicativos da prefeitura é necessária a configuração, de maneira profissional dos serviços de Virtualização de Área de Trabalho Remota (tipo apresentação) e Remote APP. 9.1 - Configuração de Portal de Área de Trabalho Remota. Esse Serviço permite o acesso seguro, contabilizado e controlado dos Serviços de Terminais. 9.2- Configuração de dois Hosts de Virtualização de Desktops. 9.3- Configuração do portai de Remote Apps. 9.4- Configuração dos Aplicativos Remotos. 9.5- Configuração dos Certificados Digitais. 9.6- Configuração dos Clientes de Acesso a Virtualização de Desktops. 9.7- Configuração de política de impressão nos serviços de virtualização de desktops. 10. Configuração do Serviço de NAP e NPS (Network Policy Services). Descrição: A Configuração dos Serviços de Política de Rede se tornam indispensáveis para a autorização de dispositivos e usuários com acesso à rede. Essa política tem o objetivo de impedir, através do protocolo IEEE 802.1x, o acesso físico não autorizado na rede com e sem fio, além da VPN. Além disso, com a política NAP, são implantadas as políticas de conformidade para

o acesso aos servidores e desktops da rede. 10.1- implantação do Serviço de NPS. 10.2- Configuração dos Clientes de RADIUS, Comutadores com fio e sem fio, servidores de VPN para autenticação de todos os dispositivos através de certificado digitai. 10.3- Configuração dos Dispositivos clientes. 10.4- implantação do NAP. 10.5- Criação das Políticas de Conformidades. 10.6- implementação das Políticas de Restrição. 10.7- Configuração da rede de Quarentena. 10.8- Configuração de Políticas de IPSec para comunicação segura entre os dispositivos. 11. Configuração do Serviço de Direct Access Descrição: Com o serviço Direct Access os dispositivos móveis podem ter acesso remoto aos serviços da rede de maneira segura e automática, sem a interação do usuário. 11.1- implementação do Serviço de Direct Access. 11.2- Criação de Política de Grupo para implantação do Direct Access. 11.3- Configuração do IPV6 para serviços acessados por clientes remotos. 12. Configuração do Serviço de Gerenciamento de Atualizações (WSUS) Descrição: A Falta de atualizações de software pode comprometer toda a segurança do ambiente computacional. O Windows System Update Server gerencia toda as atualizações de software do ambiente Microsoft. 12.1- Criação de estratégia de Atualização. 12.2- Implementação de configuração de diretivas. 12.3- Criação de Grupos de Servidores. 12.4- Criação de Grupos de Clientes. 12.5- Configuração das aprovações de atualização. 12.6- Criação de Ambiente e estratégia de homologação de atualizações. 13. Criação e Configuração de Estratégia de Gerenciamento de impressoras. Descrição: Devido ao grande número de Dispositivos de Impressão será necessário criar estratégia de Configuração de impressoras baseadas em departamento. 13.1- Criação de Grupos de impressoras. 13.2- Configuração de Diretivas de Grupo para Mapeamento de impressoras. 14. Configuração do Microsoft System Center. Dado o Tamanho da rede e o número de dispositivos, torna-se Indispensável um sistema de gerenciamento que abordará as seguintes características: System Center: 1. Configuration Manager (Gerenciamento de Hardware e Software). 2. APP Controller (Gerencia de Aplicativos) 3. End Point Protect (Anti-Mal ware). 4. DataProtection (Gestão de Backup/Restauração) 5. Portal de Auto-Atendimento (Suporte Técnico). 6. Virtual Machine Manager (Virtualização). 7. Service Manager (Gerenciamento de Chamados do Ti SLA) 15.Implementação da infraestrutura de Redes. Configuração da infraestrutura de Redes da Prefeitura. 15.1 Planejamento e implantação das Camadas Core e Acesso da rede da Prefeitura, interligando os demais setores. 15.2 Instalação e configuração dos Comutadores na camada Core e interligando aos Comutadores de Acesso da infraestrutura atual. 15.3 Configuração da separação de serviços e setores em VLANs nos Comutadores Core e Comutadores de Acesso. 15.4 Configuração do roteamento entre as sub-redes e VLANs. Item 2 – Suporte Técnico Continuado. Execução continuada de atividades do processo de tratamento de incidentes e solicitação de serviços com suporte técnico remoto e presencial (Service Desk) a infraestrutura de tecnologia da informação, nos moldes das boas práticas descritas nas bibliotecas ITIL, abrangendo, o gerenciamento de incidentes, atividade que inclui: detecção e registro dos incidentes, classificação e suporte inicial, investigação e diagnóstico, resolução e recuperação, acompanhamento e monitoramento do atendimento de incidente até seu fechamento; Prestação de serviços de assistência técnica em TI, ao parque de equipamentos, atualmente instalado ou que venha a ser instalado, compreendo a manutenção corretiva de equipamentos (servidores, equipamentos ativos de rede como: switches, concentradores ópticos, cabeamentos e roteadores): ORGANIZAÇÃO DO ATENDIMENTO Descrição Geral A gerência e tratamento dos incidentes e solicitações do usuário serão apoiados por ferramenta adequada chamada de SGSD (Sistema de Gestão de Service Desk) que atribuirá para cada incidente ou solicitação um identificador (chamado ticket) e será usado para armazenar todo o histórico do tratamento dado ao incidente ou solicitação. Essa ferramenta, fornecida pela PMCB, é usada para a contabilização dos serviços com vista à gerência dos ANS, e é responsabilidade da CONTRATADA manter seus registros atualizados em tempo real. O SGSD equivale ao Sistema de Controle de Ordem de Serviço e o ticket a sua numeração. Os microcomputadores instalados na central de atendimento deverão estar interligados em rede local, com acesso a todas as facilidades necessárias ao atendimento: Internet, serviço de correio eletrônico, sistema específico para gestão de service desk,dentre outros necessários. Os chamados serão recebidos principalmente por meio de ligações telefônicas, mas podem ser considerados outros meios de recepção, tais como: correio eletrônico, Chat, dentre outros. O acesso ao SGSD e base de conhecimento será disponibiliza na infraestrutura de rede local da PMCB com recursos de segurança implementados e interligando a PMCB à central de atendimento. A CONTRATADA terá que manter continuamente atualizada base de conhecimento, suportada por sistema gerenciador de banco de dados, a qual conterá roteiros de atendimentos, scripts para permitir atendimento imediato dos chamados recebidos. Fluxo de atendimento O tratamento dos incidentes será realizado em níveis de atendimento. Os níveis são grupo de técnicos com conhecimento e ferramentas gradualmente mais especializadas para atender aos incidentes. O Primeiro Nível é o Tele-suporte (Service Desk) que deve prover um ponto central de contato. O Service Desk registra e acompanha todos os incidentes, solicitações de serviços e acesso, e prover ao usuário uma interface de acesso a outros processos e atividades do Serviço de Operações. O Segundo Nível consiste no Atendimento Presencial no ambiente do usuário, que é sempre acionado quando o primeiro nível não conseguir resolver o incidente ou solicitação, pelo tele-suporte. Quando a CONTRATADA identificar que a solução do incidente ou solicitação depender de serviços especializados do PMCB, essa deve escalonar o tratamento para um Terceiro Nível. O Terceiro Nível consiste em equipes de especialistas nos diversos Serviços de Operação da PMCB, como a Equipe de Suporte a Banco de Dados e outros de nível especializado. Os serviços de equipes de especialistas não são objeto desse contrato, entretanto a CONTRATADA deve solicitar o serviço registrando no SGSD ou através de outro meio definido pela PMCB, aguardar o resultado e verificação de sua efetividade para então proceder o

fechamento do atendimento. O fechamento do ticket inclui duas etapas: o registro dos detalhes da solução implementada e a comunicação da solução ao usuário. O usuário terá a oportunidade de em até dois dias aceitar ou rejeitar a solução. Caso o usuário aceite, será convidado a fazer sua avaliação de satisfação. Caso rejeite a solução, ela deve ser reaberta e continuar seu tratamento pela CONTRATADA. Os atendimentos resolvidos a mais de dois dias úteis, comunicados ao solicitante e não avaliados pelo mesmo podem ser "fechados sem avaliação". Catálogo de Serviços e ANS Escopo: O suporte Técnico especializado realizado pela contratada tem seu escopo delimitado ao Datacenter da Prefeitura Municipal de Conceição da Barra. Todos os Servidores e Serviços providos pelo datacenter serão de responsabilidade da Contratada, inclusive os chamados relacionados a terceiros como fabricantes de hardware e desenvolvedores de software deverão ser acompanhados pela mesma. O serviço foi dividido em seis categorias: Esclarecimento de Dúvidas – abrangendo as atividades de apoio ao usuário na utilização dos itens de configuração disponíveis para apoiar seu trabalho. Manutenção de Acesso – Serviços que visam a configuração das permissões de acesso a recursos do ambiente da rede de computadores ou de sistema corporativos disponíveis para o usuário. Ambiente de Trabalho – Serviços que mantêm em perfeito funcionamento os itens de configuração disponíveis ao usuário. Equipamento – abrangendo a instalação, manutenção e configuração dos diversos equipamentos disponíveis no ambiente de TI da PMCB. Serviço Geral – Outros serviços que necessitam de expertise em TI, normalmente utilizados esporadicamente para apoiar atividades temporárias. Serviços Administrativos são as atividades que a CONTRATADA deve executar para cumprir exigências do contrato bem como de seu gerenciamento. Política de Severidade O atendimento deverá atender a política de severidade de acordo com a tabela a seguir: Severidade Descrição Tempo de Atendimento A O problema afeta todo o funcionamento da organização. 2 Horas B O problema afeta um usuário ou setor e impede seu funcionamento. 4 Horas C O problema afeta parte do funcionamento de um usuário, ou setor ou um esclarecimento de dúvida ou melhoria. 24 Horas Demais especificações do SUPORTE TÉCNICO Serviço de Suporte Técnico de Segundo Nível (Avançado): Como as equipes de TI estão ligadas a diversos projetos e a execução de uma demanda de serviços crescente, torna-se necessária a aquisição de Suporte técnico específico relacionado a problemas da Infraestrutura de Redes e Servidor: - Suporte Técnico a Infraestrutura de Servidores de Virtualização VMWare. - Suporte na Infraestrutura de Active Directory e demais servidores como AD CS RMS. - Suporte a infraestrutura do System Center - Suporte a Infraestrutura de Redes incluindo os Serviços NPS e NAP. - Suporte aos Serviços WDS com criação e atualização de Imagens de Instalação, - Suporte a Infraestrutura de Firewall UTM. - Visita presencial semanal à Prefeitura Municipal de Conceição da Barra A dinâmica de suporte técnico deverá seguir o Acordo de Nível de Serviço (SLA) de acordo com a severidade do chamado conforme a seguir: Severidade A - O problema afeta totalmente o desempenho das tarefas: Resposta ao chamado em 2 Horas úteis. Severidade B - O problema afeta parte das tarefas: Resposta em até 8 Horas úteis. Severidade C - Solicitação de Melhoria: Reposta em até 24 horas úteis. Item 3 - Configuração do Firewall. Descrição: FIREWALL NEXT GENERATION 1- A Contratada deverá fornecer solução de firewall next generation com devido hardware e licença para todo o período de vigência do contrato. A solução deverá atender aos requisitos a seguir: 1.1.- O hardware e software que executem as funcionalidades de proteção de rede, deverão ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico. 1.1.2- Com os seguintes recursos: 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 a internet 1.1.3- Com as funcionalidades de reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões. 1.1.4- Deverá permitir autenticação centralizada, tanto da rede cabeada como da rede sem fio, integrando-se ao AD existente 1.1.5- Os equipamentos deverão ser próprios para montagem em rack 19 polegadas, incluindo kit tipo trilho ou bandeja para adaptação se necessário e todos acessórios (como cabo de energia, conectores, etc.) necessários para sua instalação 1.1.6- Deverá possuir um throughput mínimo de 600 Mbps com as seguintes funcionalidades habilitadas simultaneamente (para todas as assinaturas que a plataforma de segurança possuir, devidamente ativadas e atuantes): controle de aplicações, IPS, Antimalware, Antivírus e Antispyware e URL filtering. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito; 1.1.7- Os throughputs deverão ser comprovados por documento de domínio publico do fabricante; 1.1.8- Suporte a no mínimo, 700.000 de conexões simultâneas; 1.1.9- Suporte a no mínimo, 35.000 novas conexões por segundo; .1.10- Deverá possuir, no mínimo, 10 interfaces de rede 1 Gbps Ethernet RJ45, incluindo a interface de gerenciamento; 1.1.11- Deverá possuir, no mínimo, 1 (uma) interface do tipo console ou similar; 1.1.12- Deverá suportar 200 (duzentos) clientes de VPN SSL simultâneos; 1.1.13- Deveá suportar 200 (duzentos) túneis de VPN IPSEC simultâneos; 1.1.14- Deverá suportar, no mínimo, 10 sistemas virtuais lógicos (Contextos) no firewall físico; 1.1.15- Os contextos virtuais deverão suportar as funcionalidades nativas do gateway de proteção incluindo: Firewall, IPS, Antivírus, Anti-Spyware, Filtro de URL, Filtro de Dados VPN, Controle de Aplicações, QOS, NAT e Identificação de usuáios; 1.1.16- 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 ou qualquer outra forma de lista de descontinuidade; 1.1.17- Suportar sub-interfaces ethernet lógicas 1.1.18- Suporte a 4094 VLAN Tags 802.1q; 1.1.19- Agregação de links 802.3ad e LACP; 1.1.20- DHCP Server e DHCP Relay; 1.1.21- O firewall deverá ter a capacidade de testar o funcionamento de rotas estáticas e rota default com a definição de um endereço IP de destino que deverá estar comunicável através de uma rota. Caso haja falha na comunicação o firewall deverá ter a capacidade de usar

rota alternativa para estabelecer a comunicação 1.1.22- Suporte a criação de objetos de rede que possam ser referenciados nas regras de firewall; 1.1.23- Deverá os registros de logs para sistemas de monitoração externos, simultaneamente. Deverá haver a opção de enviar logs via protocolo TCP e SSL; 1.1.24- Deverá permitir configurar certificado caso necessário para autenticação no sistema de monitoramento externo de logs; 1.1.25- Deverá implementar Proteção anti-spoofing; 1.1.26- Deverá suportar a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: 1.1.27- As funcionalidades de firewall, IDS/IPS, identificação de usuários, controle de aplicações, VPN IPSec e SSL, QOS, decriptografia SSL e SSH, DHCP server, DHCP relay, NAT, suporte a VLAN e protocolos de roteamento dinamico deverão 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; 1.1.28- Deverá suportar controles e criação de políticas por zona de segurança, porta/protocolo e aplicações, categorias de aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações usuários, grupos de usuários, endereço IP e redes; 1.1.29- Deverá 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; 1.1.30- Deverá permitir autenticação segura através de certificado nas fontes externas de endereços IP, domínios e URLs; 1.1.31- Deverá permitir consultar e criar exceção para objetos das listas externas a partir da interface de gerenciamento do próprio firewall; 1.1.32- Deverá permitir controle, inspeção e decriptografia de SSL por política para tráfego de entrada (Inbound) e saída (Outbound); 1.1.33- Deverá permitir offload de certificado em inspeção de conexões SSL de entrada (Inbound); 1.1.34- Deverá permitir Controle de inspeção e decriptografia de SSH por política; 1.1.35- Deverá suportar objetos e regras IPV6; 1.1.36- Deverá permitir no mínimo três tipos de negação de tráfego nas políticas de firewall: Drop sem notificação do bloqueio ao usuário, Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego, TCP-Reset para o cliente TCP-Reset para o server ou para os dois lados da conexão; 1.1.37- Deverá suportar a atribuição de agendamento as políticas com o objetivo de habilitar e desabilitar políticas em horários pré definidos automaticamente 1.1.38- Deverá suportar objetos e regras IPV6; 1.1.39- Deverá permitir a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos; 1.1.40- Deverá permitir a inspeção do payload do 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 deverá determinar se uma aplicação esta utilizando a porta default ou não, incluindo, mas não limitado a RDP na porta 80 ao invés de 3389; 1.1.41- Para tráfego criptografado SSL, deverá decriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante; 1.1.42- Deverá atualizar a base de assinaturas de aplicações automaticamente; 1.1.43- Deverá reconhecer aplicações em IPv6; 1.1.44- Deverá permitir limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem; 1.1.45- Deverá permitir adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras; 1.1.46- Deverá permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão; 1.1.47- Para proteção do ambiente contra ataques, a solução deverá possuir modulo de IPS, Antivírus e AntiSpyware integrados no próprio appliance de Firewall; 1.1.48- Deverá ser capaz de identificar e bloquear as seguintes ameaças: vírus, trojans, spywares, ransomwares e demais tipos de malwares; 1.1.49- Deverá permitir a inclusão de assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware); 1.1.50- As funcionalidades de IPS, Antivírus e Anti-Spyware deverão 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; 1.1.51- Deverá permitir o bloqueio de vulnerabilidades; 1.1.52- Deverá permitir o bloqueio de exploits conhecidos; 1.1.53- Deverá incluir proteção contra ataques de negação de serviços (DoS); 1.1.54- Deverá possuir os seguintes mecanismos de inspeção de IPS: . Analise de padrões de estado de conexões; . Analise de decodificação de protocolo; . Análise para detecção de anomalias de protocolo; . Análise heurística; . IP Defragmentation; . Remontagem de pacotes de TCP; . Bloqueio de pacotes malformados; 1.1.55- Deverá ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPfloof, etc; 1.1.56- Deverá detectar e bloquear a origem de port scans com possibilidade de criar exceções para endereços IPs de ferramentas de monitoramento da organização; 1.1.57- Deverá bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões; 1.1.58- Deverá suportar os seguintes mecanismos de inspeção contra ameaças de rede: análise de padrões de estado de conexões, análise de decodificacão de protocolo, análise para detecção de anomalias de protocolo, análise heurística, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados; 1.1.59- Deverá possuir assinaturas específicas para a mitigação de ataques DoS e DDoS; 1.1.60- Deverá possuir assinaturas para bloqueio de ataques de buffer overflow; 1.1.61- Deverá permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3; 1.1.62- Deverá permitir Inspeção profunda de pacotes; 1.1.63- A contratada deverá apresentar relatório trimestral sobre tentativas de invasão e bloqueio de ataques ocorridos. Item 4 – Backup Configuração do Serviço de Estratégia de Backup. ?Configuração de backup em nuvem para os sistemas de banco de dados. ?Configuração de Unidade de Backup Asustor NAS, para backup de todos os dados ?Configuração de Réplica de Servidores Virtuais. ?Configuração de

servidores Críticos. Item 5 – Microsoft System Centrer Configuração do Microsoft System Center. Dado o Tamanho da rede e o número de dispositivos, torna-se indispensável um sistema de gerenciamento que abordará o seguinte características: System Center: ?System Center Configuration Manager. ?System Center DataProtection. ?System Center Operation Manager 6 . Capacitação Técnica: 6.1 A empresa deverá definir um gerente para o contrato e o corpo técnico para execução dos Serviços que já deverão estar contratados em regime de CLT há no mínimo 6 meses ou comprovação da disponibilidade do profissional mediante contrato de prestação de serviços. 6.2 A empresa deverá apresentar atestado de Capacidade Técnica emitido por empresa pública ou privada com serviços realizados de acordo com escopo relacionado neste termo de referência, com devidas permissões para visitas e validação da veracidade das informações relacionadas. 6.3 Gestor de Contrato. Gestor do contrato com que tenha no mínimo curso superior. 6.4 Corpo Técnico A contratada deverá dispor em seu corpo técnico profissionais com as seguintes certificações: VCP - VMWare Certified Professional MCSA - Microsoft Certified Solutions Ass Microsoft 365 Certified: Messaging Administrator Associate Microsoft Certified: Azure Fundamentals MCTS - Microsoft Certified Technology Specialist Network Infrastructure MCTS - Microsoft Certified Technology Specialist Active Directory Certificação Técnica do Fabricante do Firewall Next Generation O gestor ou qualquer membro do corpo técnico deverá ser substituído a qualquer momento, mesmo sem justificativa, caso o gestor de TI da PMCB solicite com um prazo de 72 horas. 180 (cento e oitenta dias), ou até que se conclua o procedimento licitatório.

Valor Total: R$ 33.300,00 (Trinta e Três Mil Trezentos Reais).

Anexo II
Termo de Referência

1. OBJETIVO
Contratação de serviços especializados na área de tecnologia da informação.

1.1 DEFINIÇÃO DO OBJETO
Presente Termo de Referência, tem por objeto a contratação de serviços especializados na área de Tecnologia da Informação - TI, visando o atendimento das necessidades da *PREFEITURA MUNICIPAL DE CONCEIÇÃO DA BARRA*, para: Manutenção, ampliação e recuperação da Infraestrutura atual do Datacenter.
Execução Continuada de atividades de suporte técnico e tratamento de incidentes e solicitação de serviços com suporte técnico e assistência técnica em TI, ao parque de equipamentos atualmente instalado ou que venha a ser instalado compreendendo a manutenção corretiva de equipamentos (servidores, equipamentos ativos de rede como: switches, concentradores ópticos, cabeamentos e roteadores);

2. FUNDAMENTAÇÃO
A presente contratação tem por objetivo dar continuidade ao atendimento e suporte a infraestrutura dos serviços de tecnologia da informação da PMCB.
O atendimento a PMCB tem como tarefa principal manter os ANS (Acordo de Níveis de Serviço) oferecidos nos serviços de atendimento, assistência técnica e manutenção da infraestrutura de Tecnologia da Informação.

3. NECESSIDADES DA CONTRATAÇÃO
A maioria dos colaboradores da PMCB utiliza equipamentos e recursos de tecnologia da informação para execução das atividades e processos necessários ao funcionamento da Instituição.
O atendimento e a assistência técnica aos usuários de soluções de TI, bem como a manutenção dos equipamentos de informática são atividades essenciais para a continuidade das atividades institucionais.
Assim, buscando melhorar a qualidade dos serviços prestados pela PMCB, mediante o pronto atendimento às demandas da sociedade e do público interno em geral, torna-se imprescindível a manutenção de sua infraestrutura de tecnologia da informação, de forma a apoiar, tempestivamente os usuários no processo de trabalho do Órgão e suas atribuições.

3.1 BENEFÍCIOS DIRETOS

Esta contratação busca alcançar os seguintes resultados:

a) Reduzir o tempo de restauração da operação normal dos serviços com o mínimo de impacto nos processos de negócios da PMCB, dentro dos ANS e prioridades acordados;
b) Oferecer atendimento de qualidade aos usuários de TI, deixando transparente que há efetivo gerenciamento dos incidentes;
c) Oferecer aos usuários de TI a manutenção dos equipamentos de informática, de acordo com as políticas de Tecnologia da Informação da PMCB;
d) Criação de uma base histórica dos reais tratamentos de incidentes e solicitações à área de TI da PMCB.

4. DETALHAMENTO DOS SERVIÇOS DESCRITOS

4.1 Item 1 — Otimização do TI

OTIMIZAÇÃO DO TI
1. VMWare VCenter.
Descrição:
Um problema no banco de dados utilizado no sistema VMWare VCenter não permite a abertura dos consoles de gerenciamento, não permitindo a configuração dos diversos recursos oferecidos pela plataforma de virtualização.
Solução:
4.1.1- Instalação de novo Servidor Virtual que suportará a plataforma de Gerenciamento VCenter.
4.1.2- Instalação de novo banco de dados que suportará a plataforma de virtualização.
4.1.3- Reinstalação e Atualização dos 3 Hosts de Virtualização.
4.1.4- Reconfiguração dos Hosts de VMWare.

4.2. Serviço Active Directory.

Descrição:
Erros no banco de dados e nos serviços do Active Directory impedem o funcionamento de outros serviços. A falta de definição de Sites do Active Directory como Educação, Secretaria de Saúde e outras unidades aumentam o tráfego desnecessário da rede e criam o mal funcionamento dos serviços essenciais da rede.
Solução:
4.2.1- Criação de novo Servidor Mestre de Operações do Active Directory.
4.2.2- Desfragmentação do Banco de Dados do Active Directory.
4.2.3- Configurar servidores adicionais e Sites do Active Directory - PMCB, Saúde, Educação, CAA Sede e CAA de Braço do Rio.
4.2.4- Configuração de Logs e alertas.

4.3. Serviço de Arquivos

Descrição:
Com o aumento do número de arquivos e as ameaças de perda é necessário a implantação de sistema de gerenciamento profissional com réplica de dados, triagem e detecção de duplicatas.
Solução:
4.3.1- Instalação e configuração do Serviço de FSRM
4.3.2- Configuração dos Serviços de Log e de Auditoria.
4.3.3- Configuração de Servidores de Arquivo
4.3.4- Configuração do DFS.
4.3.5- Configuração do DFSR.

4.3.6- Configuração de Triagem de Arquivos.
4.3.7- Configuração do RMS.

4.4. Proteção contra a execução de aplicativos não autorizados.
Descrição:
Devido ao grande aumento de ameaças do tipo malwares, scripts maliciosos e códigos que podem comprometer todo o parque de computadores é importante a criação de uma política de autorização de aplicativos.
Solução:
4.4.1- Planejamento de Estratégia de Diretiva de Segurança Appiocker.
4.4.2- Configuração e implantação da diretiva de segurança APPLOCKER.

4.5. Configuração do Serviço de Implantação.
Descrição:
O serviço de Implantação é fundamental para a conformidade e segurança dos desktops e servidores da rede.
4.5.1- Implementação do Servidor de Implantação.
4.5.2- Criação e Teste das Imagens de Implantação.
4.5.3- Criação de política de Atualização off-line de imagens de servidores e desktops.

4.6. Configuração de Servidor de Certificados Digitais.
Descrição:
A criação do Servidor de Certificados Digitais é de fundamental importância para a implementação dos demais Serviços de Segurança que serão configurados na Rede.
4.6.1 - Instalação e Configuração do AD CS
4.6.2- Configuração de Política de Segurança para o Servidor.
4.6.3- Configuração de estratégia de Backup/Restauração de Servidor.

4.7. Configuração do Serviço de NAP e NPS (Network Policy Services).
Descrição:
A Configuração dos Serviços de Política de Rede se tornam indispensáveis para a autorização de dispositivos e usuários com acesso à rede. Essa política tem o objetivo de impedir, através do protocolo IEEE 802.1x, o acesso físico não autorizado na rede com e sem fio, além da VPN. Além disso, com a política NAP, são implantadas as políticas de conformidade para o acesso aos servidores e desktops da rede.
4.7.1- implantação do Serviço de NPS.
4.7.2- Configuração dos Clientes de RADIUS, Comutadores com fio e sem fio, servidores de VPN para autenticação de todos os dispositivos através de certificado digitai.
4.7.3- Configuração dos Dispositivos clientes.
4.7.4- implantação do NAP.
4.7.5- Criação das Políticas de Conformidades.
4.7.6- implementação das Políticas de Restrição.
4.7.7- Configuração da rede de Quarentena.
4.7.8- Configuração de Políticas de IPSec para comunicação segura entre os dispositivos.

4.8. Configuração do Serviço de Gerenciamento de Atualizações (WSUS)
Descrição:
A Falta de atualizações de software pode comprometer toda a segurança do ambiente computacional. O Windows System Update Server gerencia toda as atualizações de software do ambiente Microsoft.
4.8.1- Criação de estratégia de Atualização.

4.8.2- Implementação de configuração de diretivas.
4.8.3- Criação de Grupos de Servidores.
4.8.4- Criação de Grupos de Clientes.
4.8.5- Configuração das aprovações de atualização.
4.8.6- Criação de Ambiente e estratégia de homologação de atualizações.

4.9. Criação e Configuração de Estratégia de Gerenciamento de impressoras.
Descrição:
Devido ao grande número de Dispositivos de Impressão será necessário criar estratégia de Configuração de impressoras baseadas em departamento.
4.9.1- Criação de Grupos de impressoras.
4.9.2- Configuração de Diretivas de Grupo para Mapeamento de impressoras.

4.10. Configuração do Microsoft System Center.
Dado o Tamanho da rede e o número de dispositivos, torna-se Indispensável um sistema de gerenciamento que abordará as seguintes características:
System Center:
4.10.1. Configuration Manager (Gerenciamento de Hardware e Software).
4.10.2. APP Controller (Gerencia de Aplicativos)
4.10.3. End Point Protect (Anti-Mal ware).
4.10.4. DataProtection (Gestão de Backup/Restauração)
4.10.5. Portal de Auto-Atendimento (Suporte Técnico).
4.10.6. Virtual Machine Manager (Virtualização).
4.10.7. Service Manager (Gerenciamento de Chamados do Ti SLA)

4.11. Implementação da infraestrutura de Redes.
Configuração da infraestrutura de Redes da Prefeitura.
4.11.1 Planejamento e implantação das Camadas Core e Acesso da rede da Prefeitura, interligando os demais setores.
4.11.2 Instalação e configuração dos Comutadores na camada Core e interligando aos Comutadores de Acesso da infraestrutura atual.
4.11.3 Configuração da separação de serviços e setores em VLANs nos Comutadores Core e Comutadores de Acesso.
4.11.4 Configuração do roteamento entre as sub-redes e VLANs.

4.12 <u>Item 2 — Suporte Técnico Continuado.</u>
Execução continuada de atividades do processo de tratamento de incidentes e solicitação de serviços com suporte técnico remoto e presencial (Service Desk) a infraestrutura de tecnologia da informação, nos moldes das boas práticas descritas nas bibliotecas ITIL, abrangendo, o gerenciamento de incidentes, atividade que inclui: detecção e registro dos incidentes, classificação e suporte inicial, investigação e diagnóstico, resolução e recuperação, acompanhamento e monitoramento do atendimento de incidente até seu fechamento;Prestação de serviços de assistência técnica em TI, ao parque de equipamentos, atualmente instalado ou que venha a ser instalado, compreendo a manutenção corretiva de equipamentos (servidores, equipamentos ativos de rede como: switches, concentradores ópticos, cabeamentos e roteadores);

4.12.1 Organização do Atendimento
Descrição Geral
A gerência e tratamento dos incidentes e solicitações do usuário serão apoiados por ferramenta adequada chamada de SGSD (Sistema de Gestão de Service Desk) que

atribuirá para cada incidente ou solicitação um identificador (chamado ticket) e será usado para armazenar todo o histórico do tratamento dado ao incidente ou solicitação. Essa ferramenta, fornecida pela PMCB, é usada para a contabilização dos serviços com vista à gerência dos ANS, e é responsabilidade da CONTRATADA manter seus registros atualizados em tempo real.

O SGSD equivale ao Sistema de Controle de Ordem de Serviço e o ticket a sua numeração.Os microcomputadores instalados na central de atendimento deverão estar interligados em rede local, com acesso a todas as facilidades necessárias ao atendimento: Internet, serviço de correio eletrônico, sistema específico para gestão de service desk,dentre outros necessários.

Os chamados serão recebidos principalmente por meio de ligações telefônicas, mas podem ser considerados outros meios de recepção, tais como: correio eletrônico, Chat, dentre outros.

O acesso ao SGSD e base de conhecimento será disponibiliza na infraestrutura de rede local da PMCB com recursos de segurança implementados e interligando a PMCB à central de atendimento.

A CONTRATADA terá que manter continuamente atualizada base de conhecimento, suportada por sistema gerenciador de banco de dados, a qual conterá roteiros de atendimentos, scripts para permitir atendimento imediato dos chamados recebidos.

4.12.2 Fluxo de atendimento

O tratamento dos incidentes será realizado em níveis de atendimento. Os níveis são grupo de técnicos com conhecimento e ferramentas gradualmente mais especializadas para atender aos incidentes.

O Primeiro Nível é o Tele-suporte (Service Desk) que deve prover um ponto central de contato.

O Service Desk registra e acompanha todos os incidentes, solicitações de serviços e acesso, e prover ao usuário uma interface de acesso a outros processos e atividades do Serviço de Operações.

O Segundo Nível consiste no Atendimento Presencial no ambiente do usuário, que é sempre acionado quando o primeiro nível não conseguir resolver o incidente ou solicitação, pelo tele-suporte.

Quando a CONTRATADA identificar que a solução do incidente ou solicitação depender de serviços especializados do PMCB, essa deve escalonar o tratamento para um Terceiro Nível.

O Terceiro Nível consiste em equipes de especialistas nos diversos Serviços de Operação da PMCB, como a Equipe de Suporte a Banco de Dados e outros de nível especializado.

Os serviços de equipes de especialistas não são objeto desse contrato, entretanto a CONTRATADA deve solicitar o serviço registrando no SGSD ou através de outro meio definido pela PMCB, aguardar o resultado e verificação de sua efetividade para então proceder o fechamento do atendimento.

O fechamento do ticket inclui duas etapas: o registro dos detalhes da solução implementada e a comunicação da solução ao usuário.

O usuário terá a oportunidade de em até dois dias aceitar ou rejeitar a solução.

Caso o usuário aceite, será convidado a fazer sua avaliação de satisfação.

Caso rejeite a solução, ela deve ser reaberta e continuar seu tratamento pela CONTRATADA.

Os atendimentos resolvidos a mais de dois dias úteis, comunicados ao solicitante e não avaliados pelo mesmo podem ser "fechados sem avaliação".

4.12.3 Catálogo de Serviços e ANS

Escopo: O suporte Técnico especializado realizado pela contratada tem seu escopo delimitado ao Datacenter da Prefeitura Municipal de Conceição da Barra. Todos os Servidores e Serviços providos pelo datacenter serão de responsabilidade da Contratada, inclusive os chamados relacionados a terceiros como fabricantes de hardware e desenvolvedores de software deverão ser acompanhados pela mesma.

4.12.4 O serviço foi dividido em sete categorias:

Esclarecimento de Dúvidas — abrangendo as atividades de apoio ao usuário na utilização dos itens de configuração disponíveis para apoiar seu trabalho.

Manutenção de Acesso — Serviços que visam a configuração das permissões de acesso a recursos do ambiente da rede de computadores ou de sistema corporativos disponíveis para o usuário.

Ambiente de Trabalho — Serviços que mantêm em perfeito funcionamento os itens de configuração disponíveis ao usuário.

Equipamento — abrangendo a instalação, manutenção e configuração dos diversos equipamentos disponíveis no ambiente de TI da PMCB.

Serviço Geral — Outros serviços que necessitam de expertise em TI, normalmente utilizados esporadicamente para apoiar atividades temporárias.

Serviços Administrativos são as atividades que a CONTRATADA deve executar para cumprir exigências do contrato bem como de seu gerenciamento.

Política de Severidade

O atendimento deverá atender a política de severidade de acordo com a tabela a seguir:

Severidade	Descrição	Tempo de Atendimento
A	O problema afeta todo o funcionamento da organização.	2 Horas
B	O problema afeta um usuário ou setor e impede seu funcionamento.	4 Horas
C	O problema afeta parte do funcionamento de um usuário, ou setor ou um esclarecimento de dúvida ou melhoria.	24 Horas

4.12.5 Demais especificações do SUPORTE TÉCNICO

Serviço de Suporte Técnico de Segundo Nível (Avançado):

Como as equipes de TI estão ligadas a diversos projetos e a execução de uma demanda de serviços crescente, torna-se necessária a aquisição de Suporte técnico específico relacionado a problemas da Infraestrutura de Redes e Servidor:

- Suporte Técnico a Infraestrutura de Servidores de Virtualização VMWare.
- Suporte na Infraestrutura de Active Directory e demais servidores como AD CS RMS.
- Suporte a infraestrutura do System Center
- Suporte a Infraestrutura de Redes incluindo os Serviços NPS e NAP.
- Suporte aos Serviços WDS com criação e atualização de Imagens de Instalação,
- Suporte a Infraestrutura de Firewall UTM.
- Visita presencial semanal à Prefeitura Municipal de Conceição da Barra, se faz necessário.

A dinâmica de suporte técnico deverá seguir o Acordo de Nível de Serviço (SLA) de acordo com a severidade do chamado conforme a seguir:

Severidade A - O problema afeta totalmente o desempenho das tarefas: Resposta ao chamado em 2 Horas úteis.

Severidade B - O problema afeta parte das tarefas: Resposta em até 8 Horas úteis.

Severidade C - Solicitação de Melhoria: Reposta em até 24 horas úteis.

4.13 Item 3 - Configuração do Firewall.

Descrição:

FIREWALL NEXT GENERATION

4.13.1- A Contratada deverá fornecer solução de firewall next generation com devido hardware e licença para todo o período de vigência do contrato. A solução deverá atender aos requisitos a seguir:

4.13.1.1 - O hardware e software que executem as funcionalidades de proteção de rede, deverão ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico.

4.13.1.2- Com os seguintes recursos: 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 a internet.

4.13.1.3- Com as funcionalidades de reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões.

4.13.1.4- Deverá permitir autenticação centralizada, tanto da rede cabeada como da rede sem fio, integrando-se ao AD existente.

4.13.1.5- Os equipamentos deverão ser próprios para montagem em rack 19 polegadas, incluindo kit tipo trilho ou bandeja para adaptação se necessário e todos acessórios (como cabo de energia, conectores, etc.) necessários para sua instalação.

4.13.1.6- Deverá possuir um throughput mínimo de 600 Mbps com as seguintes funcionalidades habilitadas simultaneamente (para todas as assinaturas que a plataforma de segurança possuir, devidamente ativadas e atuantes): controle de aplicações, IPS,Antimalware, Antivírus e Antispyware e URL filtering. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito;

4.13.1.7- Os throughputs deverão ser comprovados por documento de domínio publico do fabricante;

4.13.1.8- Suporte a no mínimo, 700.000 de conexões simultâneas;

4.13.1.9- Suporte a no mínimo, 35.000 novas conexões por segundo;

4.13.1.10- Deverá possuir, no mínimo, 10 interfaces de rede 1 Gbps Ethernet RJ45, incluindo a interface de gerenciamento;

4.13.1.11- Deverá possuir, no mínimo, 1 (uma) interface do tipo console ou similar;

4.13.1.12- Deverá suportar 200 (duzentos) clientes de VPN SSL simultâneos;

4.13.1.13- Deveá suportar 200 (duzentos) túneis de VPN IPSEC simultâneos;

4.13.1.14- Deverá suportar, no mínimo, 10 sistemas virtuais lógicos (Contextos) no firewall físico;

4.13.1.15- Os contextos virtuais deverão suportar as funcionalidades nativas do gateway de proteção incluindo: Firewall, IPS, Antivírus, Anti-Spyware, Filtro de URL, Filtro de Dados VPN, Controle de Aplicaçães, QOS, NAT e Identificação de usuáios;

4.13.1.16- 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 ou qualquer outra forma de lista de descontinuidade;

4.13.1.17- Suportar sub-interfaces ethernet lógicas

4.13.1.18- Suporte a 4094 VLAN Tags 802.1q;

4.13.1.19- Agregação de links 802.3ad e LACP;

4.13.1.20- DHCP Server e DHCP Relay;

4.13.1.21- O firewall deverá ter a capacidade de testar o funcionamento de rotas estáticas e rota default com a definição de um endereço IP de destino que deverá estar comunicável através de uma rota. Caso haja falha na comunicação o firewall deverá ter a capacidade de usar rota alternativa para estabelecer a comunicação.

4.13.1.22- Suporte a criação de objetos de rede que possam ser referenciados nas regras de firewall;

4.13.1.23- Deverá os registros de logs para sistemas de monitoração externos, simultaneamente. Deverá haver a opção de enviar logs via protocolo TCP e SSL;

4.13.1.24- Deverá permitir configurar certificado caso necessário para autenticação no sistema de monitoramento externo de logs;

4.13.1.25- Deverá implementar Proteção anti-spoofing;

4.13.1.26- Deverá suportar a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo:

4.13.1.27- As funcionalidades de firewall, IDS/IPS, identificação de usuários, controle de aplicações, VPN IPSec e SSL, QOS, decriptografia SSL e SSH, DHCP server, DHCP relay, NAT, suporte a VLAN e protocolos de roteamento dinamico deverão 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;

4.13.1.28- Deverá suportar controles e criação de políticas por zona de segurança, porta/protocolo e aplicações, categorias de aplicaçães, grupos estáticos de aplicações, grupos dinâmicos de aplicações usuários, grupos de usuários, endereço IP e redes;

4.13.1.29- Deverá 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;

4.13.1.30- Deverá permitir autenticação segura através de certificado nas fontes externas de endereços IP, domínios e URLs;

4.13.1.31- Deverá permitir consultar e criar exceção para objetos das listas externas a partir da interface de gerenciamento do próprio firewall;

4.13.1.32- Deverá permitir controle, inspeção e decriptografia de SSL por política para tráfego de entrada (Inbound) e saída (Outbound);

4.13.1.33- Deverá permitir offload de certificado em inspeção de conexões SSL de entrada (Inbound);

4.13.1.34- Deverá permitir Controle de inspeção e decriptografia de SSH por política;

4.13.1.35- Deverá suportar objetos e regras IPV6;

4.13.1.36- Deverá permitir no mínimo três tipos de negação de tráfego nas políticas de firewall: Drop sem notificação do bloqueio ao usuário, Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego, TCP-Reset para o cliente TCP-Reset para o server ou para os dois lados da conexão;

4.13.1.37- Deverá suportar a atribuição de agendamento as políticas com o objetivo de habilitar e desabilitar políticas em horários pré definidos automaticamente

4.13.1.38- Deverá suportar objetos e regras IPV6;

4.13.1.39- Deverá permitir a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;

4.13.1.40- Deverá permitir a inspeção do payload do 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 deverá determinar se uma aplicação esta utilizando a porta default ou não, incluindo, mas não limitado a RDP na porta 80 ao invés de 3389;

4.13.1.41- Para tráfego criptografado SSL, deverá decriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

4.13.1.42- Deverá atualizar a base de assinaturas de aplicações automaticamente;

4.13.1.43- Deverá reconhecer aplicações em IPv6;

4.13.1.44- Deverá permitir limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem;

4.13.1.45- Deverá permitir adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

4.13.1.46- Deverá permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;

4.13.1.47- Para proteção do ambiente contra ataques, a solução deverá possuir modulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de Firewall;

4.13.1.48- Deverá ser capaz de identificar e bloquear as seguintes ameaças: vírus, trojans, spywares, ransomwares e demais tipos de malwares;

4.13.1.49- Deverá permitir a inclusão de assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

4.13.1.50- As funcionalidades de IPS, Antivírus e Anti-Spyware deverão 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;

4.13.1.51- Deverá permitir o bloqueio de vulnerabilidades;

4.13.1.52- Deverá permitir o bloqueio de exploits conhecidos;

4.13.1.53- Deverá incluir proteção contra ataques de negação de serviços (DoS);

4.13.1.54- Deverá possuir os seguintes mecanismos de inspeção de IPS:

. Analise de padrões de estado de conexões;
. Analise de decodificação de protocolo;
. Análise para detecção de anomalias de protocolo;
. Análise heurística;
. IP Defragmentation;
. Remontagem de pacotes de TCP;
. Bloqueio de pacotes malformados;

4.13.1.55- Deverá ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPfloof, etc;

4.13.1.56- Deverá detectar e bloquear a origem de port scans com possibilidade de criar exceções para endereços IPs de ferramentas de monitoramento da organização;

4.13.1.57- Deverá bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;

4.13.1.58- Deverá suportar os seguintes mecanismos de inspeção contra ameaças de rede: análise de padrões de estado de conexões, análise de decodificacão

de protocolo, análise para detecção de anomalias de protocolo, análise heurística, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

4.13.1.59- Deverá possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

4.13.1.60- Deverá possuir assinaturas para bloqueio de ataques de buffer overflow;

4.13.1.61- Deverá permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

4.13.1.62- Deverá permitir Inspeção profunda de pacotes;

4.13.1.63- A contratada deverá apresentar relatório trimestral sobre tentativas de invasão e bloqueio de ataques ocorridos.

4.14 Item 4 — Backup

4.14.1 Configuração do Serviço de Estratégia de Backup.

- Configuração de backup em nuvem ambiente VMware.
- Configuração de Unidade de Backup Asustor NAS, para backup de todos os dados
- Configuração de Réplica de Servidores Virtuais.
- Configuração de servidores Críticos.

4.15 Item 5 — Microsoft System Centrer

4.15.1 Configuração do Microsoft System Center.

Dado o Tamanho da rede e o número de dispositivos, torna-se indispensável um sistema de gerenciamento que abordará o seguinte características:

System Center:

- System Center Configuration Manager.
- System Center DataProtection.
- System Center Operation Manager

5 - DA FORMA E CRITÉRIOS DE PAGAMENTO

O pagamento deverá ser efetuado após a conclusão, aprovação do Gestor (Fiscal) da CONTRANTANTE e emissão de nota Fiscal.

O pagamento será efetuado mensalmente, após o atesto do Gestor (Fiscal) do Contrato na Nota Fiscal/Fatura, relativo ao mês no período e mediante a apresentação da Nota Fiscal/Fatura. O prazo de pagamento será de 10 (dez) dias a contar do atesto da Nota fiscal/Fatura.

6 - FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

6.1. Forma de seleção e critério de julgamento da proposta:

6.1.1. O fornecedor será selecionado por meio da realização de procedimento de licitação, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo [MENOR PREÇO] OU [MAIOR DESCONTO] (a ser definido pelo Setor de Licitação).

6.2. Exigências de habilitação:

Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos:

6.2.1. Habilitação jurídica

6.2.1.1. Pessoa física: cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional;

6.2.1.2. Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

6.2.1.3. Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio https://www.gov.br/empresas-e-negocios/pt-br/empreendedor;

6.2.1.4. Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

6.2.1.5. Sociedade empresária estrangeira: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020;

6.2.1.6. Sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

6.2.1.7. Filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz;

6.2.1.8. Sociedade cooperativa: ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro 1971.

6.2.1.9. Agricultor familiar: Declaração de Aptidão ao Pronaf – DAP ou DAP-P válida, ou, ainda, outros documentos definidos pela Secretaria Especial de Agricultura Familiar e do Desenvolvimento Agrário, nos termos do art. 2º, §3º do Decreto nº 22.802, de 28 de novembro de 2023.

6.2.1.10. Produtor Rural: matrícula no Cadastro Específico do INSS – CEI, que comprove a qualificação como produtor rural pessoa física, nos termos da Instrução Normativa RFB n. 2110, de 17 de outubro de 2022.

6.2.1.11. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

6.3.1 Habilitação fiscal, social e trabalhista

6.3.1.1 Prova de inscrição no Cadastro Nacional de Pessoa Jurídica (CNPJ), ou no Cadastro de Pessoas Físicas, conforme o caso;

6.3.1.2 Prova de inscrição no cadastro de contribuintes estadual e/ou municipal, se houver, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

6.3.1.3 Prova de regularidade para com as Fazendas federal, estadual/distrital e Municipal do domicílio ou sede do licitante, ou outra equivalente, na forma da lei; 7.3.1.4. Prova de regularidade relativa à Seguridade Social e ao Fundo de Garantia por Tempo de Serviço (FGTS), demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei.

6.3.1.5. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante apresentação de certidão negativa ou positiva com efeito de negativa, nos

termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei no 5.452, de 1o de maio de 1943.

6.3.1.6. Declaração expressa de que o licitante não emprega trabalhador menor nas situações previstas no inciso XXXIII do art. 7º da Constituição da República.

6.3.1.7. Os documentos referidos acima poderão ser substituídos ou supridos, no todo ou em parte, por outros meios hábeis a comprovar a regularidade do licitante, inclusive por meio eletrônico.

6.4.1 Qualificação Econômico-Financeira

6.4.1.1 Certidão negativa de feitos sobre falência expedida pelo distribuidor da sede do licitante.

6.4.1.1.1 Na hipótese em que a certidão for positiva, caso a empresa se encontre em recuperação judicial ou extrajudicial, deve o licitante apresentar comprovante da homologação/deferimento, pelo juízo competente, do plano de recuperação em vigor.

6.4.1.2. Cálculo dos Índices de Liquidez Geral (LG) e Liquidez Corrente (LC), superiores a 1 (um), comprovados mediante a apresentação de balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais e obtidos pela aplicação das seguintes fórmulas: I - Liquidez Geral (LG) = (Ativo Circulante + Realizável a

Longo Prazo)/(Passivo Circulante + Passivo Não Circulante); II - Liquidez Corrente (LC) = (Ativo Circulante)/(Passivo Circulante).

6.4.1.2.1. Caso a empresa licitante apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG) e Liquidez Corrente (LC), será exigido para fins de habilitação de 10% do valor da proposta.

6.4.1.3. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura.

6.4.1.4. O balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos.

6.4.1.5. Os documentos referidos acima deverão ser exigidos com base no limite definido pela Receita Federal do Brasil para transmissão da Escrituração Contábil Digital - ECD ao SPED.

6.4.1.6. Reserva-se ao pregoeiro o direito de efetuar os cálculos dos índices, caso estes não sejam apresentados.

6.5.1 Qualificação Técnica

6.5.1.1 Comprovação de aptidão para a prestação de serviço(s) similar(es) com o objeto desta contratação, por meio da apresentação de certidões ou atestados emitidos por pessoas jurídicas de direito público ou privado.

6.6.1 Dos critérios de aceitabilidade da proposta

6.6.1.1 A proposta de preços deverá conter:

6.6.1.1.1 Razão social, n.º do CNPJ, endereço, telefone e endereço eletrônico do licitante;

6.6.1.1.2. Modalidade e número da licitação;

6.6.1.2. Especificação do objeto licitado, sendo obrigatório constar a marca;

6.6.1.3. No caso da marca possuir mais de um modelo, o licitante deverá informá-lo.

6.6.1.4. Valor global do grupo/lote, discriminando o valor unitário e total do(s) item(ns) que o compõe;

6.6.1.4.1. O(s) valor(es) unitário(s) e total(is) deve(m) ser apresentado(s) em moeda corrente nacional e em algarismo com no máximo 02 (duas) casas decimais.

6.6.1.4.2. O valor global deve ser apresentado em moeda corrente nacional, em algarismo e por extenso, com no máximo 02 (duas) casas decimais.

6.6.1.4.2.1. Quando a divisão do valor total/global pela quantidade licitada resultar em valor com mais de 2 (duas) casas decimais, o valor unitário deverá ser adequado ao limite de duas casas decimais. O valor global de cada grupo/lote obtido após a adequação deverá ser igual ou inferior ao valor arrematado.

7. DO PRAZO DE CONTRATO

O serviço terá o prazo de contrato de 12 (doze) meses, podendo ser prorrogado de acordo com a necessidade da Administração.

8. FISCAL DO CONTRATO.

Fiscal do contrato: Anderson Cabrini de Paula, Mat. 8330.

9.0. DEMAIS PRESCRIÇÕES:

9.1 Capacitação Técnica:

9.1.1 A empresa deverá definir um gerente para o contrato e o corpo técnico para execução dos Serviços que já deverão estar contratados em regime de CLT há no mínimo 6 meses **ou comprovação da disponibilidade do profissional mediante contrato de prestação de serviços**.

9.1.2 A empresa deverá apresentar atestado de Capacidade Técnica emitido por empresa pública ou privada com serviços realizados de acordo com escopo relacionado neste termo de referência, com devidas permissões para visitas e validação da veracidade das informações relacionadas.

9.2 Corpo Técnico

A contratada deverá dispor em seu corpo técnico profissionais com as seguintes certificações:

VCP - VMWare Certified Professional
MCSA - Microsoft Certified Solutions Associate Windows Server 2016.
Microsoft 365 Certified: Messaging Administrator Associate
Microsoft Certified: Azure Fundamentals
MCTS - Microsoft Certified Technology Specialist Network Infrastructure
MCTS - Microsoft Certified Technology Specialist Active Directory
Certificação Técnica do Fabricante do Firewall Next Generation

10. DAS DISPOSIÇÕES FINAIS:

10.1. A contratada deverá atender às exigências contidas neste Termo de Referência e nos demais procedimentos inerentes a está aquisição.

10.2. Os casos omissos serão analisados pelos representantes legais das partes, com o intuito de solucionar o impasse, sem que haja prejuízo para nenhuma delas, tendo por base o que dispõem as legislações vigentes aplicáveis à espécie.