



PREFEITURA MUNICIPAL DE CONGONHAS

CIDADE DOS PROFETAS

CONTRATO DE PRESTAÇÃO DE SERVIÇOS Nº PMC/050/2022

PMC/16224/2009

PRC/227/2021

Pregão Presencial PMC/113/2021

Termo de contrato de prestação de serviços de suporte técnico especialista em Microsoft Office365 e Microsoft Windows Server ADM Active Directory e solução integrada de segurança que possibilite a visibilidade e controle de tráfego, filtragem de conteúdo web, filtro de dados, VPN, servidores web dedicado na nuvem para hospedagem do site e solução de rede wireless como serviço gerenciado e controlador na nuvem, que fazem entre si, a Prefeitura Municipal de Congonhas, pessoa jurídica de direito público, com sede administrativa na Praça Presidente Kubitschek, nº 135 Centro, inscrita no CNPJ sob o nº 16.752.446/0001-02, representada neste ato pelo Prefeito Municipal, Sr. Cláudio Antônio de Souza, que por força do Decreto nº 5.936 de 07 de fevereiro de 2014 passa a integrar o presente contrato a Secretária Municipal de Planejamento e Gestão, Lucimara Aparecida Junqueira, doravante denominada CONTRATANTE, e a empresa **NETSOL LTDA-EPP**, CNPJ nº. 03.675.909/0001-38, localizada na Rua Domingos Vieira, nº 587, sala 1908, Bairro Santa Efigênia, Belo Horizonte- MG, CEP.30150-242, neste ato representada pelo Sr. Erasmio Borja Sobrinho, CPF nº 436.752.806-59, C.I. nº M-751.735, e pelo Sr. Geraldo Eduardo Gonçalves Júnior, CPF nº 685.741.936-15 e C.I. nº M-3.133.308, SSP/MG, doravante denominada CONTRATADA, perante as testemunhas abaixo assinadas, firmam o presente contrato, decorrente do processo licitatório nº. PRC/227/2021, Pregão Presencial nº 113/2021, Processo Administrativo nº PMC/16224/2009, e que se regerá pelas Leis nº 10.520/02 e 8.666/93 e posteriores alterações, atendidas as cláusulas e condições que se enunciam a seguir:

CLAUSULA I - DO OBJETO

1.1. Contratação de empresa especializada para a prestação de serviço de suporte técnico especialista em Microsoft Office365 e Microsoft Windows Server ADM Active Directory e solução integrada de segurança que possibilite a visibilidade e controle de tráfego, filtragem de conteúdo web, filtro de dados, VPN, servidores web dedicado na nuvem para hospedagem do site e solução de rede wireless como serviço gerenciado e controlador na nuvem, durante o período de 24 (vinte e quatro) meses, conforme especificações constantes no Termo de Referência, que integra o presente Edital.

CLÁUSULA II - DAS SANÇÕES



PREFEITURA MUNICIPAL DE CONGONHAS

CIDADE DOS PROFETAS

2.1. Serão aplicadas ao FORNECEDOR, garantido o contraditório e a ampla defesa, as seguintes penalidades:

2.1.1. Na hipótese de o FORNECEDOR não entregar o objeto contratado no prazo estabelecido neste Termo de Referência, caracterizar-se-á atraso, e será aplicada multa sobre o valor da contratação de:

- a) 1% (*um por cento*) até o 5º (*quinto*) dia de atraso;
- b) 2% (*dois por cento*) a partir do 6º (*sexto*) dia, aplicável até o 10º (*décimo*) dia de atraso.

2.2. O Município de Congonhas a partir do 10º (*décimo*) dia de atraso, poderá recusar a execução do objeto contratado, ocasião na qual será cobrada a multa relativa à recusa e não mais a multa diária por atraso, ante a imaculabilidade da cobrança.

- a) Em caso de recusa do objeto contratado aplicar-se-á multa de 10% (*dez*) sobre o valor da contratação.

2.3. Caso o FORNECEDOR não atenda aos demais prazos e obrigações constantes no Edital, neste Termo de Referência e no instrumento contratual, aplicar-se-á:

- b) Multa de 0,2% (*zero vírgula dois por cento*) por dia, limitada a 10% (*dez por cento*) sobre o valor da contratação.

2.4. A multa aplicada em razão de atraso injustificado não impede que a Administração rescinda a contratação e aplique outras sanções previstas em lei.

2.5. Nas hipóteses de rescisão unilateral, deve ser aplicada multa de 10% (*dez por cento*) sobre o valor da contratação.

2.6. Não deve haver cumulação entre a multa prevista neste artigo e a multa específica prevista para outra inexecução que enseje em rescisão. Nessa hipótese, deve ser aplicada a multa de maior valor.

2.7. As multas descritas serão descontadas de pagamentos a serem efetuados ou da garantia, quando houver, ou ainda cobradas administrativamente e, na impossibilidade, judicialmente.

2.8. O Município de Congonhas poderá suspender os pagamentos devidos até a conclusão dos processos de aplicação das penalidades.

CLAUSULA III – DO PREÇO, DO PAGAMENTO E REAJUSTE

3.1. O preço da prestação de serviços licitado será o mesmo apresentado no mapa de julgamento da licitante vencedora, constante do Pregão Presencial nº. PMC/113/2021.

3.2. O valor global do presente contrato é de **R\$ 846.360,00** (oitocentos e quarenta e seis mil, trezentos e sessenta reais).

3.3 O pagamento será realizado no prazo máximo de até 30 (trinta) dias, contados a partir do recebimento da Nota Fiscal ou Fatura, através de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

3.4. Considera-se ocorrido o recebimento da nota fiscal ou fatura no momento em que o órgão contratante atestar a execução do objeto do contrato.



PREFEITURA MUNICIPAL DE CONGONHAS

CIDADE DOS PROFETAS

3.5. A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao CEIS ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 29 da Lei nº 8.666, de 1993.

3.6. Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a Contratada 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 a Contratante.

3.7. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

3.8. Antes de cada pagamento à contratada, será realizada consulta ao CEIS para verificar a manutenção das condições de habilitação exigidas no edital.

3.9. Constatando-se, junto ao CEIS, a situação de irregularidade da contratada, 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 da contratante.

3.10. Persistindo a irregularidade, a contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à contratada a ampla defesa.

3.11. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a contratada não regularize sua situação fiscal.

3.12. Será rescindido o contrato em execução com a contratada inadimplente no SICAF, salvo por motivo de economicidade, segurança nacional ou outro de interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da contratante.

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

3.14. A Contratada 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.

3.15. O preço pelos serviços prestados poderá ser reajustado a cada 12 meses, a contar da data da proposta da CONTRATADA, considerando seu valor básico o atualizado até esta data, devendo ser utilizado como índice de reajuste o INPC, ou de qualquer outro índice que venha a substituí-lo, observando sempre as datas-base dos reajustes concedidos.

3.16. Os novos valores contratuais decorrentes das repactuações terão suas vigências iniciadas observando-se a assinatura do termo aditivo.



PREFEITURA MUNICIPAL DE CONGONHAS

CIDADE DOS PROFETAS

3.17. O reajuste iniciará a partir do 1º dia do 2º ano da vigência do contrato, não sendo conhecido o índice do mês de reajuste, poderá ser utilizado o índice do mês anterior.

3.18. De acordo com o decreto nº 5.832/2013, aplica-se-ão as seguintes regras a contratada:

3.18.1. O reajuste deverá ser concedido mediante a requerimento da parte da CONTRATADA, em observância as regras do respectivo contrato e instrumento convocatório;

3.18.2. Não será aplicado o reajuste após prorrogação contratual, se na celebração deste aditivo se parte CONTRATADA foi omissa no exercício do seu direito;

3.18.3. Inaplicável o reajuste referente a contrato expirado;

CLÁUSULA IV – DAS ESPECIFICAÇÕES DOS SERVIÇOS

A. SUPORTE TÉCNICO DO MICROSOFT OFFICE 365

A.1. O serviço de suporte técnico à solução fornecida e implementada, deverá ser iniciada em até 30 dias corridos contados do recebimento da Ordem de Serviço.

A.2. Correção de problemas e esclarecimento de dúvidas sobre configuração, funcionamento e utilização da solução ofertada.

A.3. Manutenção e atualização da solução ofertada.

A.4. O serviço de suporte será prestado pela CONTRATADA conforme a necessidade da CONTRATANTE durante a vigência do contrato, período integral (24x7x365), sem limite de quantidade de atendimentos.

A.5. Os serviços serão solicitados pela equipe técnica da DTIN – Diretoria de Tecnologia da Informação mediante abertura de atendimento junto à CONTRATADA, via chamada telefônica local ou gratuita, e-mail ou sítio na Internet.

A.6. A CONTRATADA após registrado atendimento deverá enviar para o e-mail dtin@congonhas.mg.gov.br com o número do registro do atendimento para acompanhamento.

A.7. No caso de indisponibilidade do e-mail a CONTRATADA deverá informar o número do registro do atendimento no telefone 31 3731-1300 ramais 1196.

A.8. O tempo máximo de resposta inicial para atendimento registrado deverá ser de 60 (sessenta) minutos.

A.9. Os atendimentos poderão ser realizados remotamente (via Internet, telefone ou e-mail) ou presencialmente, se necessário.

A.10. Todos chamados deverão ser tratados em língua portuguesa do Brasil.

A.11. CARACTERÍSTICAS

A.11.1. A CONTRATADA deverá instalar, configurar e parametrizar toda a solução.

A.11.2. A CONTRATADA deverá dar o treinamento técnico de toda a solução para a equipe de TI da CONTRATANTE.

A.11.3. A CONTRATANTE poderá durante o período do contrato solicitar novos treinamentos sempre que julgar necessário, sem nenhum custo adicional.



PREFEITURA MUNICIPAL DE CONGONHAS

CIDADE DOS PROFETAS

- A.11.4. O pagamento do serviço contratado será efetuado mensalmente durante o período de vigência do contrato.
- A.11.5. Em caso de utilização de softwares proprietários, as licenças em nome do fornecedor deverão ser apresentadas após a instalação.
- A.11.6. Geração de relatórios em tempo real das atividades de correio eletrônico.
- A.11.7. Permitir a configuração de múltiplos domínios.
- A.11.8. Monitorar o funcionamento da solução com software de monitoramento ativo, de modo a antecipar problemas como disco lotado, alta carga de processamento e serviço indisponível.

A.12. TIPOS DE SERVIÇOS

- A.12.1. Entende-se por suporte/manutenção o serviço de ajustes, correções e configurações nos softwares, sem custo adicional para CONTRATANTE, sob as condições abaixo especificadas:
- A.12.2. Manutenção Preventiva - A manutenção preventiva corresponde às verificações e ajustes necessários ao correto funcionamento de toda a solução, atendendo questões que não alterem a estrutura do sistema.
- A.12.3. Manutenção Corretiva - Manutenção de toda a solução para correção de erros nas funcionalidades e consultoria.
- A.12.4. Manutenção Evolutiva (ou upgrade) - Aplicação de novas atualizações e versões, acompanhando a evolução das ferramentas no que se refere a novas funcionalidades implementadas por seus desenvolvedores, bem como correções que visam sanar eventuais falhas de segurança.

B. AMBIENTE TECNOLÓGICO

- B.1. As atividades desenvolvidas pela CONTRATADA deverão ocorrer no ambiente computacional de produção alocados no datacenter da CONTRATADA.
- B.2. Para alterações significativas deve se ter um plano para testes feitos em segundo ambiente dito de homologação que deverá ser criado nesta oportunidade, garantindo-se a continuidade dos serviços.
- B.3. Os servidores físicos deverão ser baseados em estrutura Intel 64 bits.

C. SOLUÇÃO DE SEGURANÇA BASEADA EM APPLIANCE NEXT GENERATION FIREWALL

- C.1. Prestação de serviços de solução integrada de segurança que possibilite a visibilidade e controle de tráfego, filtragem de conteúdo Web, prevenção contra ameaças de rede modernas, filtro de dados, VPN e controle granular de banda de rede, compreendendo fornecimento de equipamento e software integrados Appliance, na modalidade locação; licenciamento, garantia de atualização e funcionamento, com suporte técnico, durante o período de 24 (vinte e quatro) meses, conforme especificações e condições estabelecidas neste Edital.

C.2. REQUISITOS TÉCNICOS



PREFEITURA MUNICIPAL DE CONGONHAS

CIDADE DOS PROFETAS

- C.2.1. Não serão permitidas soluções baseadas em sistemas operacionais abertos como FreeBSD, Debian ou mesmo Linux.
- C.2.2. Desempenho em modo Threat Prevention (Proteção Anti-Malware, IPS e Controle de Aplicação habilitados) mínimo de 3.0 Gbps ou superior.
- C.2.3. Desempenho em modo de Inspeção (decriptografia e criptografia) de tráfego criptografado (SSL/TLS) mínimo de 800 Mbps. Os desempenhos solicitados devem ser comprovados por documento de domínio público do fabricante. Não serão aceitas declarações ou cartas de fabricantes para atendimento deste item.
- C.2.4. Desempenho mínimo de 3.3 Gbps de IPS.
- C.2.5. Suporte mínimo de 500.000 conexões simultâneas/concorrentes no modo DPI.
- C.2.6. Suporte mínimo de 20.000 novas conexões por segundo.
- C.2.7. Deve suportar expansão de armazenamento interno para até 256Gb.
- C.2.8. Deve possuir fonte de alimentação com chaveamento automático de 100-240 VAC.
- C.2.9. Deve possuir 16 interfaces 1 GbE padrão RJ-45.
- C.2.10. Deve possuir 3 interfaces 10GbE SFP+;
- C.2.11. Deve possuir 1 do tipo 1 GbE RJ-45 dedicada para gerenciamento do equipamento.
- C.2.12. Deve possuir 1 interface USB 3.0 com suporte a tecnologias LTE 3G/4G e 5G.
- C.2.13. A VPN Client-to-Site IPsec deve ser licenciada para, no mínimo, 5 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 200 usuários simultâneos, com aquisição de licença complementar.
- C.2.14. A VPN SSL deve ser licenciada para, no mínimo, 2 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 100 usuários simultâneos, com aquisição de licença complementar.
- C.2.15. Deve suportar 250 túneis de VPN tipo Site-to-Site padrão IPSEC simultâneos.
- C.2.16. Deve suportar, no mínimo, 2.1 Gbps de desempenho de VPN IPSEC.
- C.2.17. Os desempenhos apontados devem ser comprovados por documento de domínio público do fabricante. A ausência de tais documentos comprobatórios reservará ao órgão o direito de aferir a performance dos equipamentos em bancada, assim como atendimento de todas as funcionalidades especificadas neste edital. Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, o fornecedor será considerado inabilitado. Todos os custos oriundos do teste de bancada serão custeados pelo fornecedor/vendedor do certame.
- C.2.18. O fornecimento dos produtos e seus licenciamentos devem ser entregues através de empresa credenciada e autorizada pelo fabricante. Isto deve ser comprovado através de carta de reconhecimento assinada pelo representante legal do fabricante no Brasil.
- C.2.19. O Equipamento deverá ser homologado pela ANATEL.
- C.2.20. Não serão aceitas cartas ou declarações de fabricantes para atendimento aos valores de desempenho solicitados.
- C.2.21. O licenciamento para todos os serviços de Next Generation Firewall deverá ser de no mínimo 24 meses.
- C.2.22. A garantia do hardware deverá ser de 24 meses.

C.3. CARACTERÍSTICAS GERAIS



PREFEITURA MUNICIPAL DE CONGONHAS

CIDADE DOS PROFETAS

C.3.1. A solução deve consistir em plataforma de proteção de rede baseada em appliance com funcionalidades de Next Generation Firewall. O termo Next Generation Firewall doravante será empregado como NGFW ou simplesmente FIREWALL.

C.3.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, prevenção de ataques zero-day, filtro de URL, identificação de usuários e controle granular de permissões.

C.3.3. Para proteção do ambiente contra-ataques, o dispositivo de proteção deve possuir módulos de IPS, Antivírus e Anti-Spyware (para bloqueio de arquivos maliciosos), integrados ao próprio appliance de NGFW.

C.3.4. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7.

C.3.5. Define-se o termo “appliance” como sendo um equipamento dotado de processamento, memória e outros recursos tecnológicos exclusivos para um determinado serviço.

C.3.6. Não serão aceitas soluções baseadas em PC's (personal computers) de uso geral, assim como, soluções de “appliance” que utilizam hardware e software de fabricantes diferentes.

C.4. CARACTERÍSTICAS DIVERSAS

C.4.1. Deve implementar controle do tráfego para os protocolos TCP, UDP, ICMP, e serviços como FTP, DNS, P2P entre outros, baseados nos endereços de origem e destino.

C.4.2. Implementar recurso de NAT (network address translation) tipo one-to-one, one-to-many, many-to-many, many-to-one, porta TCP de conexão (NAPT) e NAT Traversal em VPN IPsec (NAT-T) e NAT dentro do tunel IPsec.

C.4.3. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico.

C.4.4. Deve possuir proteção anti-spoofing.

C.4.5. Suportar protocolos de roteamento RIP, RIPng, OSPF, OSPFv3 e BGP;

C.4.6. Suportar Equal Cost Multi-Path (ECMP) no mínimo para roteamento estático e protocolo OSPF.

C.4.7. Suporte a Policy-Based Routing (PBR), com a capacidade de roteamento no mínimo, mas não limitada a: endereço de origem, endereço de destino, serviço e aplicação.

C.4.8. A solução deverá implementar tecnologia de SD-WAN (Software Defined WAN).

C.4.9. Capacidade de agregar no mínimo 4 (quatro) circuitos WAN distintos em um único canal lógico onde seja possível criar controles de caminho automático baseado em políticas, com habilidade de selecionar o melhor caminho, no mínimo, através dos seguintes parâmetros simultâneos:

C.4.9.1. Latência;

C.4.9.2. Jitter;

C.4.9.3. Perda de pacotes.

C.4.10. O administrador da solução deverá ter a capacidade de configurar o canal lógico de SD-WAN para encaminhar tráfego simultaneamente por todos os links pertencentes a esse canal lógico.



PREFEITURA MUNICIPAL DE CONGONHAS

CIDADE DOS PROFETAS

- C.4.11.A comutação do SD-WAN deve ocorrer de maneira dinâmica e automática baseada nas políticas previamente aplicadas.
- C.4.12.A solução de SD-WAN deve permitir encaminhamento de tráfego com base em assinaturas de aplicações conhecidas (DPI), como Office 365, Facebook e Youtube, bem como aplicações associadas como Facebook Messenger e Office 365 Outlook.
- C.4.13.Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede.
- C.4.14.Deve suportar modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas.
- C.4.15.Implementar proxy transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das máquinas clientes.
- C.4.16.Possuir servidor de DHCP (Dynamic Host Configuration Protocol) interno com capacidade de alocação de endereçamento IP para as estações conectadas às interfaces do firewall e via VPN.
- C.4.17.Deve suportar DHCP relay.
- C.4.18.Possibilitar a aplicação de regras de firewall e IPS por IP e grupo de usuários, permitindo a definição de regras para determinado horário ou período (dia da semana e hora) com matriz de horários que possibilite o bloqueio de serviços em horários específicos, tendo o início e fim das conexões vinculadas a essa matriz de horários.
- C.4.19.Deve permitir a utilização de regras de Anti-Vírus, Anti-Spyware, IPS e filtro de conteúdo web por segmentos de rede. Todos os serviços devem ser suportados no mesmo segmento de rede, VLAN ou zona de segurança.
- C.4.20.Possuir capacidade de inspecionar e bloquear em tempo real aplicativos e transferências de arquivos de softwares p2p (peer-to-peer) incluindo, no mínimo, Kazaa, Limewire, Morpheus e Napster e de comunicadores instantâneos (instant messengers) incluindo, no mínimo, ICQ, WhatsApp, Google Talk, Skype e IRC, para usuários da rede, individualmente ou em grupo.
- C.4.21.Deve ter suporte a proteção e identificação de hosts possivelmente infectados com “botnets”. A solução ofertada deve permitir ao administrador a possibilidade de apenas registrar e identificar as máquinas possivelmente contaminadas, além de ter a possibilidade de habilitar e analisar todas as conexões que passam por este dispositivo de segurança, bem como ativar tal funcionalidade especificando análise por regra de firewall, permitindo assim maior granularidade da gestão e do recurso.
- C.4.22.Possuir assinaturas específicas, ou implementar mecanismo interno no appliance, para mitigação de ataques DoS (denial-of-service) e DDoS devidamente licenciados.
- C.4.23.Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc.
- C.4.24.Detectar e bloquear a origem de portscans.
- C.4.25.Deve permitir o bloqueio de ataques.
- C.4.26.Deve permitir o bloqueio de exploits conhecidos.
- C.4.27.O gateway Anti-Vírus deve suportar a análise de pelo menos os protocolos HTTP, FTP, IMAP, e SMTP.
- C.4.28.Deve ter a capacidade de analisar tráfegos criptografados HTTPS/SSL, que deverá ser decriptografado de forma transparente à aplicação.
- C.4.29.Implementar DSCP (Differentiated Services Code Points).



PREFEITURA MUNICIPAL DE CONGONHAS

CIDADE DOS PROFETAS

C.4.30. Possuir mecanismo de forma a possibilitar o funcionamento transparente dos protocolos FTP, SIP, RTP, RTSP e H323, mesmo quando acessados por máquinas através de conversão de endereços. Este suporte deve funcionar tanto para acessos de dentro para fora quanto de fora para dentro da rede.

C.4.31. Implementar controle e gerenciamento de banda para a tecnologia VoIP (Voice OverIP) sobre diferentes segmentos de rede com inspeção profunda de segurança sobre este serviço.

C.4.32. Implementar mecanismo de sincronismo de horário através do protocolo NTP.

C.4.33. Possuir suporte ao protocolo SNMP versões 2 e 3.

C.4.34. Possuir suporte a log via syslog.

C.4.35. Possuir suporte aos protocolos de roteamento RIP, OSPF e BGP. As configurações de RIP e OSPF devem ser configuradas através da interface gráfica.

C.4.36. O fabricante ou o produto deve possuir certificado ICSA (International Computer Security Association) para FIREWALL, ou CC (Common Criteria). Será aceito certificado equivalente ao ICSA, emitido por órgãos nacionais com competência para tal, desde que nos moldes deste, ou seja, certificado baseado na versão ou release atual do firewall, com manutenção recorrente deste certificado a cada mudança de versão, ou após determinado período de tempo, e baseado em normas nacionais e internacionais de segurança da informação.

C.4.37. Visando estabelecer efetividade de segurança dos firewalls de nova geração e assegurar que o fornecedor tenha uma solução já testada e comprovada por um órgão independente de mercado, o fabricante da solução deverá ser avaliado e certificado pelo NetSecOPEN, além de ser avaliado e citado pelo Gartner MQ (Magic Quadrant for Network Firewalls) nos relatórios de 2019 ou mais recentes.

C.4.38. Reconhecer aplicações como, no mínimo, peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos e e-mail.

C.4.39. Para tráfego criptografado SSL/TLS, deve de-criptografar pacotes possibilitando a leitura de payload dos pacotes para checagem de assinaturas de aplicações conhecidas pelo fabricante.

C.4.40. Controle, inspeção e de-criptografia de SSL/TLS por política para tráfego de entrada (Inbound) ou Saída (Outbound) com suporte a no mínimo, SSLv23, SSLv3, TLS 1.0, TLS 1.1, TLS 1.2 e TLS 1.3

C.5. CARACTERÍSTICAS DE VPN

C.5.1. Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo site-to-site, com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC.

C.5.2. Suportar algoritmos de criptografia 3DES, AES 128 e AES 256.

C.5.3. Suportar algoritmos Hash no mínimo SHA-1, SHA-256 e SHA-384.

C.5.4. Diffie-Hellman: Grupo 2 (1024 bits), Grupo 5 (1536 bits) e Grupo 14 (2048 bits).

C.5.5. Deverá suportar algoritmo Internet Key Exchange (IKE)v1 e v2.

C.5.6. Autenticação via de tuneis IPsec via certificado digital para VPNs Site-to-Site e Client-to-Site.



PREFEITURA MUNICIPAL DE CONGONHAS

CIDADE DOS PROFETAS

C.5.7. A solução deve suportar VPNs L2TP, incluindo suporte para Apple iOS e Android.

C.5.8. Solução deve suportar VPNs baseadas em políticas, e VPNs baseadas em roteamento estático e/ou dinâmico.

C.5.9. Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo Site-to-Site com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC.

C.5.10. Solução deve incluir a capacidade de estabelecer VPNs com outros firewalls que utilizam IP públicos dinâmicos.

C.5.11. Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do circuito primário.

C.5.12. Permitir criação de políticas de roteamento estático utilizando IPs de origem, destino, serviços e a própria VPN como parte encaminhadora deste tráfego, sendo este visto pela regra de roteamento como uma interface simples de rede para encaminhamento do tráfego.

C.5.13. Suportar a criação de túneis IP sobre IP (IPSEC Tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet.

C.5.14. Implementar os esquemas de troca de chaves manual, IKE e IKEv2 por Pré-Shared Key, certificados digitais e XAUTH client authentication.

C.5.15. Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do primário.

C.5.16. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

C.6. ALTA DISPONIBILIDADE

C.6.1. Devem ser fornecidos 02 (dois) appliances de NGFW com gerenciamento unificado, novos e sem uso anterior, funcionando em alta disponibilidade. O modelo ofertado deverá estar em linha de produção, sem previsão de encerramento de fabricação, na data de entrega da proposta. O software deverá ser fornecido em sua versão mais atualizada.

C.6.2. A solução deve ser entregue operando em alta disponibilidade no modo Ativo/Standby, com as implementações de Failover.

C.6.3. Não serão permitidas soluções de cluster (HA) que façam com que os equipamentos se reiniciem após qualquer modificação de parâmetro/configuração realizada pelo administrador.

C.6.4. A solução deve ter capacidade de fazer monitoramento físico das interfaces dos membros do cluster.

C.6.5. A solução deve operar em alta disponibilidade implementando monitoramento lógico de um host na rede, e possibilitar failover.

C.6.6. A solução deve permitir o uso de endereço MAC virtual para evitar problemas de expiração de tabela ARP em caso de Failover.

C.6.7. A solução deve possibilitar a sincronização de todas as configurações realizadas na caixa principal do cluster incluído, mas não limitado a objetos, regras, rotas, VPNs e políticas de segurança.



PREFEITURA MUNICIPAL DE CONGONHAS

CIDADE DOS PROFETAS

C.6.8. A solução deve permitir visualizar no equipamento principal, o status da comunicação entre os parceiros do cluster, status de sincronização das configurações, status atual do equipamento redundante.

C.7. CONTROLE DE AMEAÇAS

C.7.1. Para as ameaças de dia-zero, a solução deve ter a habilidade de prevenir o ataque antes de qualquer assinatura ser criada. Deve possuir módulo de Anti-Vírus e Anti-Bot integrado ao próprio appliance de segurança.

C.7.2. A solução de Anti-Virus integrada deve ter capacidade de analisar arquivos maiores que 1Gbps.

C.7.3. A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliances através de assinaturas.

C.7.4. Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego.

C.7.5. Implementar funcionalidade de detecção e bloqueio de “call-backs”.

C.7.6. A solução deverá ser capaz de detectar e bloquear comportamento suspeito ou anormal da rede.

C.7.7. A solução Anti-bot deve possuir mecanismo de detecção que inclua reputação de endereço IP.

C.7.8. Implementar interface gráfica WEB segura, utilizando o protocolo HTTPS.

C.7.9. Implementar interface CLI segura através do protocolo SSH.

C.7.10. Possuir Anti-Vírus em tempo real, para ambiente de gateway internet integrado à plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, IMAP, POP3, FTP, CIFS e TCP Stream.

C.7.11. A solução deve permitir criar regras de exceção de acordo com a proteção.

C.7.12. Deve possuir visualização na própria interface de gerenciamento referente aos top incidentes através de hosts, ou incidentes referentes a vírus e Bots;

C.7.13. Permitir o bloqueio de malwares (vírus, worms, spyware e etc).

C.7.14. A solução deve ser capaz de proteger contra-ataques a DNS.

C.7.15. A solução deverá ser gerenciada a partir de uma console centralizada com políticas granulares.

C.7.16. A solução deve ser capaz de prevenir acesso a websites maliciosos.

C.7.17. A solução deve ser capaz de realizar inspeção de tráfego SSL/TLS e SSH.

C.7.18. A solução deverá receber atualizações de um serviço baseado em cloud.

C.7.19. A solução deverá ser capaz de bloquear a entrada de arquivos maliciosos.

C.7.20. A solução Anti-Vírus deverá suportar análise de arquivos que trafegam dentro do protocolo CIFS.

C.7.21. A solução deve suportar funcionalidade de Geo-IP, ou seja, a capacidade de identificar, isolar e controlar tráfego baseado na localização (origem e/ou destino), incluindo a capacidade de configuração de listas customizadas para esta mesma finalidade

C.7.22. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS integrados no próprio appliance de firewall, onde sua console de gerência deverá residir na mesma console centralizada dos appliances de segurança, com suporte a pelo menos 3.000 assinaturas;



PREFEITURA MUNICIPAL DE CONGONHAS

CIDADE DOS PROFETAS

- C.7.23.A solução de IPS deverá possuir os seguintes mecanismos de detecção: assinaturas e trabalhar em conjunto com o controle de aplicações;
- C.7.24.A solução de IPS deve fazer a inspeção de todo o pacote, independentemente do tamanho;
- C.7.25.A solução de IPS deve fazer a inspeção de todo o tráfego de forma bidirecional, analisando qualquer tamanho de pacote sem degradar a performance do equipamento solicitada neste edital;
- C.7.26.Possuir capacidade de remontagem de pacotes para identificação de ataques;
- C.7.27.O mecanismo de inspeção deve receber e implementar em tempo real atualizações para os ataques emergentes sem a necessidade de reiniciar o appliance;
- C.7.28.Para cada proteção de segurança, deve ser possível consultar informações no site do fabricante.
- C.7.29.A ferramenta de log deve possuir a capacidade de criar uma regra de exceção a partir do log visualizado na gerência centralizada;
- C.7.30.As regras de exceção devem possuir: origem, destino e serviço;
- C.7.31.A solução deve ser capaz de inspecionar tráfego HTTPS.
- C.7.32.Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;
- C.7.33.Detecção de anomalias;
- C.7.34.A solução de IPS deve possuir política capaz de definir o modo de operação (bloqueio ou detecção);
- C.7.35.O módulo de IPS deve possuir assinaturas voltadas para ambientes de servidores de SMTP, Web e DNS;
- C.7.36.O mecanismo de inspeção deve receber e implementar em tempo real atualizações de novas assinaturas sem a necessidade de reiniciar o appliance;
- C.7.37.Para cada proteção, ou para todas as proteções suportadas, deve incluir a opção de adicionar exceções baseado na origem e destino;
- C.7.38.A solução deve ser capaz de detectar e bloquear ataques nas camadas de rede e aplicação, protegendo pelo menos os seguintes serviços: Aplicações web, serviços de e-mail, DNS, FTP, SQL Injection, ataques a sistemas operacionais e VOIP;
- C.7.39.Deve incluir proteção contra worms;
- C.7.40.Deve incluir uma tela de visualização situacional a fim de monitorar graficamente a quantidade de alertas de diferentes severidades e a evolução ao longo do tempo dispondo o sumário quantitativo das ameaças analisadas.
- C.7.41.A solução deve possuir esquema de atualização de assinaturas através de um click;
- C.7.42.Atualização de modo offline, onde poder ser baixado na base do fabricante e posteriormente fazer o upload do arquivo na solução;
- C.7.43.A solução deve suportar importar certificados de servidor para inspeções de tráfego seguro HTTP (HTTPS) de entrada. Depois de importar esses certificados, a solução deve permitir o IPS para Inspeção segura HTTP(HTTPS);
- C.7.44.A solução deverá ser capaz de inspecionar e proteger apenas hosts internos;
- C.7.45.A solução deverá possuir proteções para sistemas SCADA;
- C.7.46.Solução deverá permitir que o administrador bloqueie facilmente o tráfego de entrada e/ou saída com base em países, sem a necessidade de gerir manualmente os ranges de endereços IP dos países que deseja bloquear.



PREFEITURA MUNICIPAL DE CONGONHAS

CIDADE DOS PROFETAS

C.8. PROTEÇÃO CONTRA ATAQUES AVANÇADOS

C.8.1. A solução deverá prover as funcionalidades de inspeção de tráfego de entrada e saída de malwares não conhecidos ou do tipo APT, com filtro de ameaças avançadas e análise de execução em tempo real, e inspeção de tráfego de saída de “call-backs”.

C.8.2. Suportar os protocolos HTTP assim como inspeção de tráfego criptografado através de HTTPS.

C.8.3. A solução deve ser capaz de inspecionar o tráfego criptografado SSL/TLS e SSH.

C.8.4. Identificar e bloquear a existência de malware em comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle.

C.8.5. Implementar mecanismo de bloqueio de vazamento não intencional de dados oriundos de máquinas existentes no ambiente LAN em tempo real.

C.8.6. Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar arquivo PDF com até 10Mb.

C.8.7. Implementar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows e Android.

C.8.8. Conter ameaças de dia zero permitindo ao usuário final o recebimento dos arquivos livres de malware.

C.8.9. A tecnologia de máquina virtual deverá suportar diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas.

C.8.10. A solução deve possuir nuvem de inteligência proprietária do fabricante, onde este seja responsável por atualizar toda a base de segurança dos appliance através de assinaturas.

C.8.11. Implementar a visualização dos resultados das análises de malwares de dia zero nos diferentes sistemas operacionais dos ambientes controlados (sandbox) suportados.

C.8.12. Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e quaisquer outros mecanismos de redirecionamento de tráfego;

C.8.13. Conter ameaças avançadas de dia zero.

C.8.14. Toda análise deverá ser realizada de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador.

C.8.15. Implementar mecanismo do tipo múltiplas fases para verificação de malware e/ou códigos maliciosos;

C.8.16. Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real. Não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos.

C.8.17. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx) e Android APKs no ambiente controlado.

C.8.18. Implementar a análise de arquivos executáveis, DLLs e ZIP no ambiente controlado.

C.8.19. Possuir Anti-Vírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, POP3, FTP, IMAP e CIFS.

C.8.20. Mitigar ameaças de dia zero de forma transparente para o usuário final.



PREFEITURA MUNICIPAL DE CONGONHAS

CIDADE DOS PROFETAS

- C.8.21. Mitigar ameaças de dia zero através de tecnologias de emulação e código de registro.
- C.8.22. Implementar mecanismo de pesquisa por diferentes intervalos de tempo.
- C.8.23. Mitigar ameaças de dia zero via tráfego de internet.
- C.8.24. Permitir a contenção de ameaças de dia zero sem a alteração da infra-estrutura de segurança.
- C.8.25. Mitigar ameaças de dia zero que possam burlar o sistema operacional emulado.
- C.8.26. A solução deve permitir a criação de listas brancas (whitelist) baseadas no MD5 do arquivo.
- C.8.27. Mitigar ameaças de dia zero antes da execução e evasão de qualquer código malicioso.
- C.8.28. Conter e mitigar exploits avançados.
- C.8.29. A análise em nuvem local deve prover informações sobre as ações do malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo malware, gerar assinaturas de Anti-Vírus e Anti-Spyware automaticamente, definir URLs não confiáveis utilizadas pelo novo malware e prover informações sobre o usuário infectado (seu endereço IP e seu login de rede).
- C.8.30. Suporte a submissão manual de arquivos para análise através do serviço de Sandbox.

C.9. CARACTERÍSTICAS DE FILTRO DE CONTEÚDO WEB

- C.9.1. Possuir filtro de conteúdo integrado ao NGFW para classificação de páginas web com, no mínimo, 50 (cinquenta) categorias distintas, com mecanismo de atualização e consulta automáticas.
- C.9.2. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs, através da integração com serviços de diretório, Active Directory e base de dados local.
- C.9.3. Devem ser fornecidas licenças de filtro de conteúdo para cada equipamento e quantidade de usuários ilimitada, provendo atualização automática e em tempo real através da categorização contínua de novos sites da Internet, sem custo adicional, por todo o período de vigência da garantia e do contrato de manutenção e suporte técnico.
- C.9.4. Permitir a customização de página de bloqueio.
- C.9.5. Controle de conteúdo filtrado por categorias de sites com base de dados continuamente atualizada pelo fabricante.
- C.9.6. Deve permitir submissão de novos sites para categorização.
- C.9.7. Permitir a classificação dinâmica de sites web, URLs e domínios.
- C.9.8. Permitir a associação de grupos de usuários a diferentes regras de filtragem de sites web, definindo quais categorias deverão ser bloqueadas ou permitidas para cada grupo de usuários, podendo ainda adicionar ou retirar acesso a domínios específicos da Internet.
- C.9.9. Permitir a definição de quais zonas de segurança terão aplicadas as regras de filtragem de web.
- C.9.10. Permitir aplicar a política de filtro de conteúdo baseada em horário do dia, bem como dia da semana.



PREFEITURA MUNICIPAL DE CONGONHAS

CIDADE DOS PROFETAS

C.10. CARACTERÍSTICAS DE AUTENTICAÇÃO

C.10.1. Prover autenticação de usuários para os serviços Telnet, FTP, HTTP e HTTPS, utilizando as bases de dados de usuários e grupos de servidores Windows e Unix, de forma simultânea.

C.10.2. Permitir a autenticação dos usuários utilizando servidores LDAP, AD, RADIUS, Tacacs+, Single Sign On e API.

C.10.3. Permitir o cadastro manual dos usuários e grupos diretamente no NGFW por meio da interface de gerência remota do equipamento.

C.10.4. Permitir a integração com qualquer autoridade certificadora emissora de certificados X.509 que siga o padrão de PKI descrito na RFC 2459, inclusive verificando os certificados expirados/revogados, emitidos periodicamente pelas autoridades certificadoras, os quais devem ser obtidos automaticamente pelo NGFW.

C.10.5. Permitir o controle de acesso por usuário, para plataformas Microsoft Windows de forma transparente, para todos os serviços suportados, de forma que ao efetuar o login na rede, um determinado usuário tenha seu perfil de acesso automaticamente configurado sem a instalação de softwares adicionais nas estações de trabalho e sem configuração adicional no browser.

C.10.6. Deve 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 NGFW.

C.10.7. Permitir aos usuários o uso de seu perfil independentemente do endereço IP da máquina que o usuário esteja utilizando.

C.10.8. Permitir a atribuição de perfil por faixa de endereço IP nos casos em que a autenticação não seja requerida.

C.10.9. Suportar a criação de túneis seguros sobre IP (IPSEC tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet

C.11. CARACTERÍSTICAS DE ADMINISTRAÇÃO

C.11.1. Permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o NGFW, cada um responsável por determinadas tarefas da administração.

C.11.2. Possuir mecanismo para aplicar remotamente, pela interface gráfica, correções e atualizações para o NGFW.

C.11.3. Possuir mecanismo para realizar remotamente, através de interface gráfica, cópias de segurança (backup) e restauração de configurações e sistema operacional.

C.11.4. Possuir mecanismo para agendamento realização das cópias de segurança(backups) de configuração.

C.11.5. Possuir mecanismo para exportar as configurações através de FTP, HTTPs ou SFTP.

C.11.6. A solução deve permitir ao administrador aplicar ajustes rápidos das melhores práticas de segurança no dispositivo com apenas um clique, possibilitando implementar as melhores práticas recomendadas pelo fabricante.



PREFEITURA MUNICIPAL DE CONGONHAS

CIDADE DOS PROFETAS

- C.11.7. Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do NGFW e a remoção de qualquer uma destas sessões ou conexões.
- C.11.8. Permitir a visualização, em forma gráfica, do percentual do uso de CPU e quantidade de tráfego de rede em todas as interfaces do NGFW em tempo real.
- C.11.9. Permitir a visualização, em tempo real, dos serviços com maior tráfego e os endereços IP mais acessados.
- C.11.10. Deve suportar minimamente dois tipos de negação de tráfego nas políticas de firewall: Descarte sem notificação do bloqueio ao usuário (discard), descarte com notificação do bloqueio ao usuário (drop), descarte com opção de envio de "ICMP Unreachable" para máquina de origem do tráfego, "TCP-Reset" para o cliente, "TCP-Reset" para o servidor ou para os dois lados da conexão.
- C.11.11. Ser capaz de visualizar, de forma direta no appliance e em tempo real, as aplicações mais utilizadas, os usuários que mais estão utilizando estes recursos informando sua sessão, total de pacotes enviados, total de bytes enviados e média de utilização em Kbps, URLs acessadas e ameaças identificadas.
- C.11.12. Ser capaz de visualizar, de forma direta no appliance e em tempo real estado do processamento do produto e volume/desempenho de dados utilizado pela rede de computadores conectada ao equipamento.
- C.11.13. Possibilitar a geração de relatório de ameaças com avaliação e gerenciamento de riscos e informações detalhadas sobre o ambiente, ajudando a identificar explorações de vulnerabilidades, intrusões e outras ameaças. Deve permitir a emissão deste relatório em formato PDF.
- C.11.14. Ser capaz de visualizar, de forma direta no appliance e em tempo real, a largura de banda utilizada por política, por protocolo TCP/UDP IPV4 e IPV6.
- C.11.15. Ser capaz de visualizar, de forma direta no appliance e em tempo real, as conexões estabelecidas, com possibilidade de aplicar filtros na visualização.
- C.11.16. Possibilitar a geração de pelo menos os seguintes tipos de relatório, mostrados em formato HTML: máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas, ou categorias Web mais acessadas (considerando a existência do filtro de conteúdo Web).
- C.11.17. Permitir habilitar auditoria de configurações no equipamento, possibilitando o rastreamento das configurações aplicadas no produto.
- C.11.18. Ser capaz de implementar a funcionalidade de "Zero-Touch", permitindo que o equipamento se provisione autônoma e automaticamente no sistema de gestão centralizada.
- C.11.19. A solução deve possuir mecanismo de gerenciamento através de aplicativo móvel, com disponibilidade para os sistemas operacionais IOS e Android.
- C.11.20. O aplicativo móvel deve possibilitar conexão ao dispositivo via protocolo HTTPS e conexão USB.
- C.11.21. O gerenciamento via aplicativo móvel deve permitir visualização de status de consumo de banda, CPU, conexões ativas dos dispositivos e topologia do NGFW.
- C.11.22. O aplicativo móvel deve permitir visualização de status das ameaças observadas e bloqueadas pelas funcionalidades de segurança de NGFW.
- C.11.23. O aplicativo móvel deve permitir visualização dos últimos logs gerados no NGFW.



PREFEITURA MUNICIPAL DE CONGONHAS

CIDADE DOS PROFETAS

- C.11.24. O aplicativo móvel deve permitir diagnósticos simples na solução, como testes ICMP e verificação DNS.
- C.11.25. O aplicativo móvel deve permitir configurar interfaces, objetos e políticas de acesso, além de exportar configurações.
- C.11.26. O recurso de Alta Disponibilidade deverá ser suportado em modo Bridge.
- C.11.27. Possuir Mecanismo de IPS / IDS, com suporte a pelo menos 5.000 assinaturas de ataques, aplicações ou serviços, completamente integrados ao Firewall.
- C.11.28. Possuir interface orientada a linha de comando para a administração do firewall a partir do console ou conexão SSH suportando está múltiplas sessões simultâneas.
- C.11.29. Implementar proxy transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das máquinas clientes.
- C.11.30. Capacidade para realizar filtragens/inspeções dentro de portas TCP conhecidas por exemplo porta 80 http, buscando por aplicações que potencialmente expõe o ambiente como: P2P, Kazaa, Morpheus, BitTorrent ou messengers.
- C.11.31. Suportar recurso de autenticação única para todo o ambiente de rede, ou seja, utilizando a plataforma de autenticação atual que pode ser de LDAP ou AD. O perfil de cada usuário deverá ser obtido automaticamente através de regras no Firewall DPI (Deep Packet Inspection) sem a necessidade de uma nova autenticação como por exemplo, para os serviços de navegação a Internet atuando assim de forma toda transparente ao usuário. Serviços como FTP, HTTP, HTTPS devem apenas consultar uma base de dados de usuários e grupos de servidores 2003/2008/2012 com AD.
- C.11.32. Os Throughputs devem ser comprovados por documento de domínio público do fabricante. A ausência de tais documentos comprobatórios reservará ao órgão o direito de aferir a performance dos equipamentos em bancada, assim como atendimento de todas as funcionalidades especificadas neste edital. Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, o fornecedor será considerado inabilitados. Todos os custos oriundos do teste de bancada serão por conta do fornecedor.

C.12. CERTIFICAÇÕES

- C.13. O equipamento deve comprovar através de documento do portfólio de forma pública o desempenho de todas as funcionalidades habilitadas em modo DPI ou, e através de comprovação técnica atestada por simulador de tráfego. Os custos relativos ao simulador de tráfego, caso utilizado, correrão por conta da CONTRATADA.
- C.14. O Fabricante deve comprovar participação no MAPP da Microsoft, a comprovação deverá ser feita no através do link <http://technet.microsoft.com/en-us/security/dn568129>.
- C.15. O fabricante da solução deverá ser avaliado pela VPNC para interoperabilidade de VPN entre outros fabricantes através do link <http://www.vpnc.org/>.
- C.16. A performance mínima da plataforma de segurança, considerando as funcionalidades de firewall de aplicação, IPS, gateway antivírus e análise profunda de pacotes, operando todas simultaneamente, também deverá ser comprovada através de documento do portfólio ou comprovação técnica atestada por simulador de tráfego. Os



PREFEITURA MUNICIPAL DE CONGONHAS

CIDADE DOS PROFETAS

custos relativos ao simulador de tráfego, caso utilizado, correrão por conta da CONTRATADA.

C.17. O fabricante da solução deverá ser avaliado pela NSS Labs (Network Security Services) no desempenho do Next Generation Firewall Comparative Analysis mais recente, ou por outra empresa de análise compatível.

C.18. AUTENTICAÇÃO

C.19. Prover autenticação de usuários para os serviços Telnet, FTP, HTTP, HTTPS e Gopher, utilizando as bases de dados de usuários e grupos de servidores NT e Unix, de forma simultânea.

C.20. Permitir a utilização de LDAP, AD e RADIUS.

C.21. Permitir o cadastro manual dos usuários e grupos diretamente na interface de gerência remota do Firewall, caso onde se dispensa um autenticador remoto para o mesmo.

C.22. Permitir a integração com qualquer autoridade certificadora emissora de certificados X509 que seguir o padrão de PKI descrito na RFC 2459, inclusive verificando as CRLs emitidas periodicamente pelas autoridades, que devem ser obtidas automaticamente pelo firewall via protocolos HTTP e LDAP.

C.23. Permitir o controle de acesso por usuário, para plataformas Windows Me, NT, 2000, XP, Windows 7, Windows 8 e Windows 10 de forma transparente, para todos os serviços suportados, de forma que ao efetuar o logon na rede, um determinado usuário tenha seu perfil de acesso automaticamente configurado.

C.24. Possuir perfis de acesso hierárquicos.

C.25. Permitir a restrição de atribuição de perfil de acesso à usuário ou grupo independente ao endereço IP da máquina que o usuário esteja utilizando.

C.26. Suportar padrão IPSEC, de acordo com as RFCs 2401 a 2412, de modo a estabelecer canais de criptografia com outros produtos que também suportem tal padrão.

C.27. Suportar a criação de túneis IP sobre IP (IPSEC Tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet.

C.28. FILTRO WWW

C.29. Possuir módulo integrado ao mesmo Firewall DPI (Deep Packet Inspection) para classificação de páginas web com no mínimo 56 categorias distintas, com mecanismo de atualização automática.

C.30. Deverão ser fornecidas licenças de Filtro de Conteúdo durante a vigência do contrato.

C.31. Controle de conteúdo filtrado por categorias de filtragem com base de dados continuamente atualizada e extensível.

C.32. Capacidade de submissão instantânea de novos sites e palavras chaves.

C.33. Permitir a classificação dinâmica de sites Web, URLs e domínios.

C.34. Suporte à filtragem para, no mínimo, 56 categorias e com, pelo menos, as seguintes categorias: violência, nudismo, roupas íntimas/banho, pornografia, armas, ódio / racismo, cultos / ocultismo, drogas / drogas ilegais, crimes / comportamento ilegal, educação sexual, jogos, álcool / tabagismo, conteúdo adulto, conteúdo questionável, artes



PREFEITURA MUNICIPAL DE CONGONHAS

CIDADE DOS PROFETAS

e entretenimento, bancos / e-trading, chat, negócios e economia, tecnologia de computadores e Internet, e-mail pessoal, jogos de azar, hacking, humor, busca de empregos, newsgroups, encontros pessoais, restaurantes / jantar, portais de busca, shopping e portais de compras, MP3, download de software, viagens e WEB hosting.

C.35. O administrador de política de segurança poderá definir grupos de usuários e diferentes políticas de filtragem de sites WEB, personalizando quais categorias deverão ser bloqueadas ou permitidas para cada grupo de usuários, podendo ainda adicionar ou retirar acesso a domínios específicos da Internet.

C.36. O administrador de política de segurança poderá personalizar quais zonas de segurança, em cada um dos firewalls da rede, terão aplicadas as políticas de filtragem de WEB, e de maneira centralizada.

C.37. O administrador poderá adicionar filtros por palavra-chave de modo específico e individual em cada um dos firewalls da rede, de forma centralizada.

C.38. A política de Filtros de conteúdo deverá ser baseada em horário do dia e dia da semana.

C.39. Suportar recurso de autenticação única para todo o ambiente de rede, ou seja, utilizando a plataforma de autenticação atual que pode ser de LDAP ou AD; o perfil de cada usuário deverá ser obtido automaticamente para o controle das políticas de Filtro de Conteúdo sem a necessidade de uma nova autenticação.

C.40. Possibilitar a filtragem da linguagem Javascript e de applets Java e Active-X em páginas WWW, para o protocolo HTTP.

C.41. Deverá ser fornecida todas as atualizações de software assim como a atualização da base de conhecimento (URLs categorizadas), sem custo adicional, pelo período de vigência do contrato.

C.42. ADMINISTRAÇÃO

C.43. Permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o firewall, cada um responsável por determinadas tarefas da administração.

C.44. Fornecer interface gráfica que permita a realização de cópias de segurança (backups) e sua posterior restauração remotamente, sem necessidade de se reinicializar o sistema.

C.45. Possuir mecanismo para possibilitar a aplicação de correções e atualizações para o firewall remotamente através da interface gráfica.

C.46. Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do firewall e a remoção de qualquer uma destas sessões ou conexões.

C.47. Permitir a geração de gráficos em tempo real, representando os serviços mais utilizados e as máquinas mais acessadas em um dado momento.

C.48. Permitir a visualização de estatísticas do uso de CPU, memória da máquina onde o firewall está rodando e tráfego de rede em todas as interfaces do Firewall através da interface gráfica remota, em tempo real e em forma tabular e gráfica.

C.49. Permitir a conexão simultânea de vários administradores, sendo um deles com poderes de alteração de configurações e os demais apenas de visualização das mesmas.



PREFEITURA MUNICIPAL DE CONGONHAS

CIDADE DOS PROFETAS

Permitir que o segundo ao se conectar possa enviar uma mensagem ao primeiro através da interface de administração.

C.50. Possibilitar a geração de pelo menos os seguintes tipos de relatório, mostrados em formato HTML: máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas, ou categorias Web mais acessadas (em caso de existência de um filtro de conteúdo Web), maiores emissores e receptores de e-mail.

C.51. Possibilitar a geração de pelo menos os seguintes tipos de relatório com cruzamento de informações, mostrados em formato HTML: máquinas acessadas X serviços bloqueados, usuários X URLs acessadas, usuários X categorias Web bloqueadas (em caso de utilização de um filtro de conteúdo Web).

C.52. Possibilitar a geração dos relatórios sob demanda e através de agendamento diário, semanal e mensal. No caso de agendamento, os relatórios deverão ser publicados de forma automática em pelo menos três servidores web diferentes, através do protocolo FTP.

C.53. LOG

C.54. Possibilitar o registro de toda a comunicação realizada através do firewall, e de todas as tentativas de abertura de sessões ou conexões que forem recusadas pelo mesmo.

C.55. Prover mecanismo de consulta às informações registradas integrado à interface de administração.

C.56. Possibilitar o armazenamento de seus registros (log e/ou eventos) na mesma plataforma de gerenciamento.

C.57. Possibilitar a recuperação dos registros de log e/ou eventos armazenados em máquina remota, através de protocolo criptografado, de forma transparente através da interface gráfica.

C.58. Possibilitar a análise dos seus registros (log e/ou eventos) por pelo menos um programa analisador de log disponível no mercado.

C.59. Possuir sistema de respostas automáticas que possibilite alertar imediatamente o administrador através de e-mails, janelas de alerta na interface gráfica, execução de programas e envio de Traps SNMP.

C.60. Possuir mecanismo que permita inspecionar o tráfego de rede em tempo real (sniffer) via interface gráfica, podendo opcionalmente exportar os dados visualizados para arquivo formato PCAP e permitindo a filtragem dos pacotes por protocolo, endereço IP origem e/ou destino e porta IP origem e/ou destino, usando uma linguagem textual.

C.61. Permitir a visualização do tráfego de rede em tempo real tanto nas interfaces de rede do Firewall quando nos pontos internos do mesmo: anterior e posterior à filtragem de pacotes, onde o efeito do NAT (tradução de endereços) é eliminado.

D. TREINAMENTO

D.1. A CONTRATADA deverá capacitar tecnicamente a equipe que irá gerenciar a solução na CONTRATANTE em todas as funcionalidades exigidas.

D.2. O treinamento deverá ser ministrado por técnico certificado da empresa fabricante do equipamento.



PREFEITURA MUNICIPAL DE CONGONHAS

CIDADE DOS PROFETAS

D.3. A CONTRATANTE poderá durante o tempo do contrato solicitar novos treinamentos sempre que julgar necessário, sem nenhum custo adicional.

D.4. Todo material necessário para o treinamento, caso necessário, deverá ser fornecido pela CONTRATADA.

E. RELATÓRIOS

E.1. A solução deverá possuir sistema de relatório próprio fornecido pelo fabricante na plataforma Windows, VMware ou Cloud.

E.2. Caso a solução de relatórios seja fornecida em nuvem, o armazenamento deverá ser de no mínimo 3 meses de dados.

E.3. Fornecer gerência remota do sistema de relatórios, com interface gráfica nativa.

E.4. A interface gráfica deverá possuir mecanismo que permita a gerência e emissão de relatórios de forma remota de múltiplos firewalls.

E.5. Possibilitar a geração de pelo menos os seguintes tipos de relatório, mostrados em formato HTML, PDF e CSV: máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas, ou categorias Web mais acessadas (em caso de existência de um filtro de conteúdo Web), maiores emissores e receptores de e-mail, detecção de intrusos, intrusos bloqueados e alvos, para vírus e spywares bloqueados, alvos e detectados.

E.6. Possibilitar a geração de pelo menos os seguintes tipos de relatório com cruzamento de informações, mostrados em formato HTML: máquinas acessadas X serviços bloqueados, usuários X URLs acessadas, usuários X categorias Web bloqueadas (em caso de utilização de um filtro de conteúdo Web).

E.7. Possibilitar o registro de toda a comunicação realizada através do firewall, e de todas as tentativas de abertura de sessões ou conexões que forem recusadas pelo mesmo.

E.8. Possibilitar o armazenamento de seus registros (log e/ou eventos) na mesma plataforma de gerenciamento.

E.9. Possibilitar a recuperação dos registros de log e/ou eventos armazenados em máquina remota, através de protocolo criptografado, de forma transparente através da interface gráfica.

E.10. Possibilitar a análise dos seus registros (log e/ou eventos) por pelo menos um programa analisador de log disponível no mercado.

E.11. Possuir sistema de respostas automáticas que possibilite alertar imediatamente o administrador através de e-mails, janelas de alerta na interface gráfica, execução de programas e envio de Traps SNMP.

F. SUPORTE ESPECIALISTA SOLUÇÃO DE ACTIVE DIRECTORY (AD)

F.1. Instalação, configuração de um Active Directory (AD) em um Servidor Windows.

F.2. INSTALAÇÃO DE SERVIDORES

F.2.1. Instalação de Service Pack e fixes que se façam necessários no servidor Windows;

F.2.2. Configuração do servidor, observando critérios de segurança e performance;



PREFEITURA MUNICIPAL DE CONGONHAS

CIDADE DOS PROFETAS

F.2.3. Criação e Configuração de Active Directory, seguindo padronização de segurança;

F.2.4. Promoção dos servidores para Controladores de Domínio (Domain Controllers).

F.3. ACTIVE DIRECTORY

F.3.1. Criação de estrutura do Active Directory, contemplando Unidades Organizacionais (OU's) de forma a atender às necessidades do cliente, no que se refere às futuras aplicações de políticas através de GPO;

F.3.2. Configuração de replicação das configurações entre os Domain Controllers;

F.3.3. Cadastramento de usuários com scripts contendo instruções básicas de login;

F.3.4. Criação de subnet referente ao(s) site(s) do cliente;

F.3.5. Testes de replicações entre servidores Domain Controllers da rede (dois sentidos).

F.4. DNS

F.4.1. Instalação do serviço DNS nos servidores Domain Controllers da rede corporativa;

F.4.2. Criação e configuração de zona integrada ao Active Directory;

F.4.3. Criação de Zona reversa para domínio criado.

F.5. GROUP POLICY OBJECTS (GPO)

F.5.1. É altamente aconselhável a abordagem de GPO's em domínios com Active Directory, visto que os benefícios são inúmeros, no sentido de proporcionar segurança e padronização do ambiente computacional de uma empresa.

F.5.2. O objetivo principal da GPO é manter o ambiente computacional da empresa de forma mais homogênea possível, através da utilização de templates já previamente definidos, possibilitando uma administração mais segura e eficaz dos computadores constantes em rede.

F.5.3. Ativação de Acesso Remoto às estações de trabalho, através de ferramenta nativa;

F.5.4. Padronização de armazenamento da pasta Meus Documentos, utilizando a opção FOLDER REDIRECTORY;

F.5.5. Mensagem de aviso referente à utilização de recursos da rede corporativa;

F.5.6. Padronização de papel de parede nas estações de trabalho da rede corporativa;

F.5.7. Padronização de proteção de tela nas estações de trabalho da rede corporativa;

F.5.8. Padronização de usuários com direitos administrativos nas estações de trabalho;

F.5.9. Configuração do serviço de Atualizações Automáticas para servidor WSUS;

F.5.10. Padronização das seguintes configurações do Internet Explorer:

F.5.11. Definição de página inicial;

F.5.12. Limpeza de Temporary Internet Files após fechamento do mesmo;

F.5.13. Limpeza das configurações de detecção automática de proxy;

F.5.14. Desativar armazenamento automático de senhas no Internet Explorer;

F.5.15. Definição de Políticas de senhas para Usuários e Administradores da rede;

F.5.16. Padronização da senha do usuário ADMINISTRADOR nas estações de trabalho;



PREFEITURA MUNICIPAL DE CONGONHAS

CIDADE DOS PROFETAS

F.6. SERVIDOR DHCP

F.6.1. Permitir a configuração automática das interfaces de rede dos equipamentos da prefeitura, facilitando e tornando mais segura a configuração de rede destes (computadores, smartphones, impressoras, cameras, etc).

F.6.2. Permitir fixar os IP's de acordo com o mac address (endereço único da interface de rede) de cada dispositivo.

F.6.3. Servidor de envio de e-mails (SMTP) com capacidade sup 200 e-mails por dia com anexo.

G. TERMO DE REFERÊNCIA SCAN DE VULNERABILIDADES

G.1.1. A contratada deverá a cada 6 meses realizar a Varredura de Vulnerabilidades com objetivo de identificar vulnerabilidades que criminosos digitais possam utilizar para causar prejuízos à prefeitura. O criminoso digital pode ser identificado como um agente malicioso que tem conhecimento avançado das tecnologias para espionar, roubar e causar interrupção nos negócios. Ele pode ser um concorrente, funcionário mal-intencionado, cliente ganancioso ou até mesmo um cidadão de outro país que quer utilizar sua rede para ter ganhos financeiros na internet.

G.1.2. Itens a serem verificados:

- o Identificar vulnerabilidades que hackers possam utilizar;
- o Identificar principais alvos (pessoas, servidores e clientes);
- o Identificar falhas no sistema que pode ser explorada por criminosos;
- o Identificar fraudes que podem estar acontecendo;
- o Identificar vazamentos ou roubo de informações;
- o Bloquear ataques futuros e ataques em andamento;
- o Mapear os riscos e avaliar maturidade de segurança cibernética da empresa;

G.1.3. Ao final a contratada deverá fornecer dois relatórios:

o Sumário Executivo: quantidade de vulnerabilidades encontradas, gravidade das vulnerabilidades, maturidade de segurança cibernética da empresa, atual nível de risco cibernético e possíveis sugestões diante do cenário encontrado;

o Relatório Técnico: vulnerabilidades encontradas, descrição da vulnerabilidade, solução para correção, classificação de risco, informações adicionais e referências;

G.1.4. Importante: trechos mais técnicos do relatório final podem estar no idioma inglês.

G.1.5. A contratada deverá utilizar pelo menos uma ferramenta comercial de mercado, não sendo aceitos testes utilizando apenas ferramentas gratuitas.

H. SERVIDOR DEDICADO NA NUVEM PARA HOSPEDAGEM DE SITES



PREFEITURA MUNICIPAL DE CONGONHAS

CIDADE DOS PROFETAS

H.1. Contratação de um Servidor Dedicado na nuvem para hospedagem de site da Prefeitura de Congonhas e hospedagem de um Servidor de mensagens instantânea privativo e gerenciamento de DNS.

H.2. REQUERIMENTOS

H.2.1. Sistema Operacional Ubuntu 16.04 LTS.

H.2.2. Servidor Web Apache 2.4 com módulos: MOD-Rewrite, Open SSL, CSPAM, MOD Security.

H.2.3. Linguagem HTML, PHP Versão 8, Perl 5.24.

H.2.4. Banco de dados MySQL 8.0, Postgre 13.4.

H.2.5. Espaço 1 TB com disco SSD.

H.2.6. Memória 16GB.

H.2.7. Processador 4 cores.

H.2.8. Certificado SSL para página Web sem custo de certificação para o Município.

H.2.9. Fazer a hospedagem de domínios virtuais pretendentes ao Município de Congonhas e seus subdomínios na internet.

H.2.10. As páginas podem ser criadas em HTML, APACHE, Java, Perl e PHP.

H.2.11. Permite a atualização das páginas web do site por FTP de forma rápida e segura. Também pode ser usado para troca de arquivos entre empresas.

H.2.12. Possibilitar dar nomes válidos na Internet (DNS) e publicado domínio do Município.

H.2.13. Permiti a criação de bases de dados que podem ser consultadas através de comandos SQL.

H.2.14. Banda de 100 MB.

H.2.15. Oferecer Hospedagem WordPress gerenciada que estão incluídos a instalação e configuração do WordPress.

H.2.16. Antivírus e AntiSpam.

H.2.17. Monitoramento 24x7.

H.2.18. Proteção contra ataques WordPress.

H.2.19. Backups diários e atualização automática do WordPress, temas e plugins.

I. SOLUÇÃO DE REDE WIRELLES COMO SERVIÇO GERENCIADO E CONTROLADOR NA NUVEM

I.1. Fornecimento de 15 equipamentos wireless na modalidade de locação para a rede sem fio local, a serem utilizados na Prefeitura de Congonhas, incluindo manutenção e assistência técnica durante o período de 24 meses, tudo em conformidade com as disposições abaixo.

I.2. ACCESS POINT

I.2.1. Os access points fornecidos devem ter um controlador wireless que seja compatível com o appliance UTM. Este controlador deve ser capaz de administrar todos



PREFEITURA MUNICIPAL DE CONGONHAS

CIDADE DOS PROFETAS

os access points e mostrar todos os dispositivos conectados, aplicando regras de segurança para as redes wireless e exibindo as seguintes informações:

- I.2.1.1. Listagem de access point wireless.
- I.2.1.2. Informações detalhadas de cada access point wireless.
- I.2.1.3. Utilização de rede.
- I.2.1.4. Listagem de clientes wireless.
- I.2.1.5. Bloqueio ou limitação de velocidade a dispositivos conectados.
- I.2.1.6. Criação de mapa mostrando a posição de cada access point neste mapa.
- I.2.2. Devem ser fornecidos access points wireless que atendam no mínimo as seguintes características:
 - I.2.2.1. Deverá fornecer cobertura total e com qualidade no ambiente físico do CONTRATANTE;
 - I.2.2.2. Deverá possuir e acompanhar componentes que permita sua fixação em teto e/ou parede;
 - I.2.2.3. Deverá atender simultaneamente aos padrões Wi-Fi Standards 802.11 a/b/g/n/ac com cada access point possuindo pelo menos um rádio de 2.4GHz MIMO e rádio de 5GHz MIMO;
 - I.2.2.4. Deverá operar para conexão à rede local com uma interface gigabit, com conector RJ-45 Fêmea;
 - I.2.2.5. Deverá permitir sua energização, pela interface de rede descrita no item anterior, através de um único injetor PoE (Power over Ethernet), fornecido junto com cada access point;
 - I.2.2.6. Deverá possuir LEDs indicativos do estado de operação;
 - I.2.2.7. Deverá possuir antenas internas (no mínimo 2X2 MIMO), em conformidade com o padrão Wi-Fi Standards 802.11 a/b/g/n/ac;
 - I.2.2.8. Deverá selecionar automaticamente o canal de transmissão;
 - I.2.2.9. Deverá possuir suporte a pelo menos 04 (quatro) SSIDs;
 - I.2.2.10. Deverá permitir habilitar e desabilitar a divulgação do SSID;
 - I.2.2.11. Deverá implementar Fast Roaming ou funcionalidade similar de forma a garantir o roaming sem perda de conexão e com integridade de sessão, dando suporte a aplicações em tempo real;
 - I.2.2.12. Deverá permitir o protocolo de autenticação Radius para acesso wireless a rede corporativa;
 - I.2.2.13. Deverá ter filtros de acesso à rede baseados em endereços MAC;
 - I.2.2.14. Deverá fornecer acesso a internet para a rede wireless visitante através de HotSpot com autenticação via voucher e/ou redes sociais;
 - I.2.2.15. Deverá suportar customização do portal de access point wireless (Hotspot) para atender as necessidades do CONTRATANTE;
 - I.2.2.16. Deverá suportar acesso wireless a celulares, tablets e outros.
 - I.2.2.17. Permitir que a administração de WLAN seja feita através da interface Ethernet ou através da interface WLAN usando web ou aplicativo para Android/iOS;
 - I.2.2.18. Permitir desabilitar a administração via WLAN;
 - I.2.2.19. Permitir a seleção do país de instalação do ponto de acesso;
 - I.2.2.20. Realizar atualização de sistema operacional do ponto de acesso utilizando o controlador;



PREFEITURA MUNICIPAL DE CONGONHAS

CIDADE DOS PROFETAS

I.2.2.21. Permitir conexão SSH ao access point;

CLÁUSULA V – DAS OBRIGAÇÕES DA CONTRATADA

5.1 O prazo de entrega dos produtos (*hardware e software*) deverá ser de, no máximo, 30 (trinta) dias corridos após o recebimento da nota de empenho com autorização de serviços.

5.2 As despesas de deslocamento, hospedagem e alimentação do(s) técnico(s), a partir da sede da CONTRATADA, serão por conta da CONTRATADA.

5.3 Executar os serviços conforme especificações deste Termo de Referência e de sua proposta, com os recursos necessários ao perfeito cumprimento das cláusulas contratuais.

5.4 Utilizar empregados habilitados e com conhecimentos dos serviços a serem executados, de conformidade com as normas e determinações em vigor.

5.5. Apresentar à CONTRATANTE, quando for o caso, a relação nominal dos empregados que adentrarão o órgão para a execução do serviço, os quais devem estar devidamente identificados por meio de crachá.

5.6. Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas na legislação específica, cuja inadimplência não transfere responsabilidade à Administração.

5.7 Instruir seus empregados quanto à necessidade de acatar as orientações da Administração, inclusive quanto ao cumprimento das Normas Internas, quando for o caso.

5.8 Não permitir a utilização do trabalho do menor.

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

5.10 Não transferir a terceiros, por qualquer forma, nem mesmo parcialmente, as obrigações assumidas, nem subcontratar qualquer das prestações a que está obrigada, exceto nas condições autorizadas no Termo de Referência ou na minuta de contrato.

5.11 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 ao objeto da licitação, exceto quando ocorrer algum dos eventos arrolados nos incisos do § 1º do art. 57 da Lei nº 8.666, de 1993.

5.12 Suporte técnico para instalação, configuração, migração, atualizações, manutenções (*preventivas, corretivas, evolutivas - ou de upgrade - da solução, sem custos*), gerenciamento e resolução de problemas para toda a plataforma CONTRATADA para as caixas postais com serviço de certificação digital.

5.13 Prestar atendimento 8X5 nos dias úteis.

5.14 Prestar atendimento em regime de plantão nos feriados e finais de semana das 8:00 as 24:00hs.

5.15 A CONTRATADA deverá instalar, ativar e migrar, o serviço no prazo máximo de 10 dias, contados a partir da assinatura do contrato.



PREFEITURA MUNICIPAL DE CONGONHAS

CIDADE DOS PROFETAS

5.16 Conforme a severidade da manutenção, deve-se estabelecer prioridades nas entregas e o respeito aos prazos de atendimento e solução do problema, conforme tabela de indicadores.

5.17 No caso de aumento dos requisitos de infraestrutura, deverá ser feita uma especificação desta necessidade, bem como um detalhamento dos riscos deste processo.

5.18 Para as alterações em que existam mudanças em tela ou de procedimentos, deve-se prever um repasse "hands-on" ou em outra modalidade a ser acordada, para transferência de tecnologia contemplando instalação, configuração, gerenciamento e resolução de problemas de todos os componentes.

5.19 A CONTRATADA deverá entregar à CONTRATANTE relatório mensal de nível de serviço.

5.20 Nos casos de manutenção corretiva em que houver a necessidade de prazo maior que 24 horas ou dependência de terceiros, esta deverá acordada (*documentada para registro*) e deverá ser acompanhada de cronograma de solução.

5.21 Para toda manutenção corretiva deverá ser fornecido um relatório do diagnóstico do problema e quais medidas corretivas foram adotadas pela CONTRATANTE.

5.22 A equipe ou pessoa que prestará os serviços de suporte deve estar nos quadros da CONTRATADA.

5.23 A CONTRATADA deve possuir Service Desk próprio permitindo abertura e acompanhamento de chamados técnicos, com atendimento em língua portuguesa e através de atendimento eletrônico via web.

5.24 Chamados técnicos ilimitados.

5.25 Suporte remoto para incidentes graves, em até 4 horas úteis.

5.26 Os prazos de atendimento e resolução de manutenção devem seguir os descritos nos indicadores abaixo:

5.26.1 Indicadores

Os chamados devem ser categorizados e atendidos de acordo com a prioridade:

PRIORIDADE	TMR	TMPR
CRÍTICA	15 minutos	4 horas
ALTA	15 minutos	6 horas
MÉDIA	15 minutos	7 horas
BAIXA	15 minutos	8 horas
PLANEJADA	15 minutos	-

Legenda:

Sigla	Significado	Detalhamento
TMR	Tempo Médio de Resposta	Via telefone em até 3 toques Via Web em até 15 minutos



PREFEITURA MUNICIPAL DE CONGONHAS

CIDADE DOS PROFETAS

TMPR	Tempo Médio Para	Tempo para restabelecer/reinstalar um serviço depois de uma falha.
------	------------------	--

5.27 Conforme a complexidade da manutenção solicitada deverá ser acordada entre as partes o prazo para a solução avaliando-se a sua extensão e complexidade na solução.

5.28. SUPORTE REMOTO CONTINUADO

5.28.1. A CONTRATADA deve possuir Central de Atendimento, do tipo (0800) ou número local (DDD 31), para abertura dos chamados de garantia, comprometendo-se a manter registros dos mesmos constando a descrição do problema. A CONTRATADA também deve oferecer canais de comunicação e ferramentas adicionais de suporte online como “chat”, “e-mail” e página de suporte técnico na internet com disponibilidade de atualizações e “hotfixes” de drivers, BIOS, firmware, sistemas operacionais e ferramentas de troubleshooting, no mínimo.

5.28.2. Prestar atendimento 8X5 nos dias úteis.

5.28.3. Prestar atendimento em regime de plantão nos feriados e finais de semana das 8:00 as 24:00hs.

5.28.4. A CONTRATADA deve possuir Service Desk próprio permitindo abertura e acompanhamento de chamados técnicos, com atendimento em língua portuguesa e através de atendimento eletrônico via web.

5.28.5. Durante o prazo do contrato celebrado entre as partes a CONTRATADA dará garantia total sem ônus para o CONTRATANTE, a parte ou peça defeituosa, após a conclusão do respectivo analista de atendimento de que há a necessidade de substituir uma peça ou recolocá-la no sistema, salvo se quando o defeito for provocado por uso inadequado dos equipamentos.

5.28.6. Casos em que se tornará obrigatório a substituição de peças ou equipamentos do fabricante, a CONTRATADA será responsável pela retirada, remessa, recolocação e reconfiguração do equipamento, arcando com todas as despesas inerentes ao processo de substituição.

5.28.7. Os Serviços de suporte consistem na disponibilidade do Grupo de especialistas da CONTRATADA via telefone, para prestação de serviços de Suporte Técnico Remoto e aberturas de chamados de 1º, 2º e 3º nível e contempla:

5.28.7.1. Atividade técnica programada, para a realização de Manutenções e correções dos patches de segurança UpGrade e UpDate do ambiente de segurança.

5.28.7.2. Realizar o acompanhamento das atualizações UpDate & Upgrade no período e verificação.

5.28.7.3. Correção de anomalias nos equipamentos Segurança.

5.28.7.4. Solucionar dúvidas quanto à operação dos módulos do Segurança.

5.28.7.5 Atualizações e correções de novos “patches” e versões para os equipamentos.

5.29. SEGURANÇA

5.29.1. Suporte Técnico e Substituição ao Hardware que apresentar problema.



PREFEITURA MUNICIPAL DE CONGONHAS

CIDADE DOS PROFETAS

5.29.1.1. A garantia de funcionamento do hardware será fornecida pelo CONTRATANTE, que deverá possuir equipamento backup para substituição imediata.

5.29.2. O atendimento será em regime 8X5, na modalidade on-site, e serão prestados pelo Fabricante ou empresa fornecedora da solução.

5.29.3. O prazo máximo para que se inicie o atendimento técnico será de 04 (*quatro*) horas corridas, contado a partir do momento em que for realizado o chamado técnico devidamente formalizado. Entende-se por início do atendimento técnico inclusive contato telefônico para identificação do tipo de ocorrência afim de preparação de peças adequadas e demais procedimentos técnicos.

5.29.4. O prazo máximo para que seja realizado o reparo do equipamento será de até 24 (*vinte e quatro*) horas corridas para as principais capitais da federação do Brasil, contado a partir do início do atendimento do chamado. Para as demais em até 5 dias úteis.

5.29.5. A manutenção corretiva, que se fará sempre que necessária ou solicitada pela CONTRATANTE, compreende o diagnóstico, assistência técnica e solução de problemas, bem como a substituição de componentes que apresentarem defeitos ou avarias, ou seja, quaisquer serviços que se fizerem necessários para deixar os equipamentos em perfeito estado de funcionamento.

5.29.6. Na manutenção corretiva, após a sua realização, deverão ser feitos testes com os equipamentos, acompanhando o seu funcionamento, pelo técnico em conjunto com o usuário, havendo a obrigatoriedade da assinatura de ambos no documento, ao final dos trabalhos.

5.29.7. Na substituição de algum componente ou periférico, devido à manutenção, este deverá ser compatível com os softwares envolvidos, e com as demais partes do equipamento

5.30. INSTALAÇÃO E MIGRAÇÃO

5.30.1. Todo o serviço de instalação e migração da solução atual da Prefeitura de Congonhas será de responsabilidade da CONTRATADA, que deverá realizar visita técnica para propor um cronograma de migração.

5.30.2. A CONTRATADA e a CONTRATANTE deverão elaborar um checklist que será executado após a migração, que será feita em data proposta pela Prefeitura de Congonhas.

5.31. OBRIGAÇÕES ESPECÍFICAS REFERENTE A POLÍTICA ANTICORRUPÇÃO.

5.31.1. A CONTRATADA se obriga, sob as penas previstas no CONTRATO e na legislação aplicável, a observar e cumprir rigorosamente todas as leis cabíveis na política de combate a corrupção, especialmente a Lei 12.846/2013, de 1º de agosto de 2013, bem como as normas e exigências constantes das políticas internas da CONTRATANTE.



PREFEITURA MUNICIPAL DE CONGONHAS

CIDADE DOS PROFETAS

5.31.2. A CONTRATADA declara que, direta ou indiretamente, não ofereceu, prometeu, pagou ou autorizou o pagamento em dinheiro, deu ou concordou em dar presentes ou qualquer objeto de valor e, durante a vigência do Contrato, não irá ofertar, prometer, pagar ou autorizar o pagamento em dinheiro, dar ou concordar em dar presentes ou qualquer objeto de valor a qualquer pessoa ou entidade, pública ou privada, com o objetivo de beneficiar ilicitamente a CONTRATANTE e/ou seus negócios.

5.31.3. A CONTRATADA declara que, direta ou indiretamente, não irá receber, transferir, manter, usar ou esconder recursos que decorram de qualquer atividade ilícita, bem como não irá contratar como empregado ou de alguma forma manter relacionamento profissional com pessoas físicas ou jurídicas envolvidas em atividades criminosas, em especial pessoas investigadas pelos delitos previstos nas leis anticorrupção, de lavagem de dinheiro, tráfico de drogas e terrorismo.

5.31.4. A CONTRATADA se obriga a notificar prontamente, por escrito, à CONTRATANTE a respeito de qualquer suspeita ou violação do disposto nas leis anticorrupção e ainda de participação em práticas de suborno ou corrupção, assim como o descumprimento de qualquer declaração apresentada no processo licitatório originário do contrato.

5.31.5. A CONTRATADA declara e garante que: (I) os atuais representantes de sua empresa não são servidores públicos municipais sob qualquer forma de investidura; e que (II) informará por escrito, no prazo de 3 (três) dias úteis, qualquer nomeação de seus representantes como servidores públicos municipais sob qualquer forma de investidura.

5.31.5.1. A CONTRATADA, nos termos do descrito no item (II) poderá a seu exclusivo critério rescindir o CONTRATO com o Município, não sendo aplicáveis quaisquer multas ou penalidades às partes.

5.31.6. O não cumprimento pela CONTRATADA das leis anticorrupção e/ou no **disposto no Anexo IX** será considerado uma infração grave ao CONTRATO e conferirá à CONTRATANTE o direito de, agindo de boa fé, declarar a suspensão imediata do CONTRATO e, garantindo o direito ao contraditório e a ampla defesa, sua rescisão sem quaisquer ônus ou penalidade à CONTRATANTE, sendo a CONTRATADA responsável por eventuais perdas e danos.

5.31.7. A CONTRATADA se obriga a cumprir e fazer respeitar as regras de conduta da CONTRATANTE para execução do futuro contrato, em especial nas questões relacionadas ao sigilo das informações relativas ao presente CONTRATO e tratar como matéria sigilosa todos os assuntos de interesse da CONTRATANTE que, direta ou indiretamente, tenha ou vier a ter conhecimento, obrigando-se a deles não utilizar em benefício próprio ou divulgar, de forma a não permitir ou deixar que qualquer pessoa deles se utilize, sob pena de rescisão do presente CONTRATO, de pleno direito.



PREFEITURA MUNICIPAL DE CONGONHAS

CIDADE DOS PROFETAS

CLÁUSULA VI – DAS OBRIGAÇÕES DO CONTRATANTE

6.1. Além das obrigações resultantes da observância da Lei n.º 8.666/93 e alterações posteriores, a CONTRATANTE deverá:

- 6.1.1. receber o objeto no prazo e condições estabelecidas no Edital e seus anexos;
- 6.1.2. verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento definitivo;
- 6.1.3. comunicar à Contratada, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido;
- 6.1.4. acompanhar e fiscalizar o cumprimento das obrigações da Contratada, através de comissão/servidor especialmente designado, a saber: Wanderson Ferreira Leão, matrícula 20143618, Diretor de Tecnologia da Informação e Clever da Conceição Júnior, matrícula 20143625, Chefe de Departamento de Tecnologia da Informação.
- 6.1.5. efetuar o pagamento à Contratada no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos no Edital e seus anexos;
- 6.1.6. a Administração não responderá por quaisquer compromissos assumidos pela Contratada com terceiros, ainda que vinculados à execução do presente Termo de Contrato, bem como por qualquer dano causado a terceiros em decorrência de ato da Contratada, de seus empregados, prepostos ou subordinados.

CLÁUSULA VII – DA DOTAÇÃO ORÇAMENTÁRIA

7.1. A despesa decorrente da contratação do objeto desta licitação correrá à conta das seguintes Dotações Orçamentárias:

Órgão: 11 – Secretaria Municipal de Planejamento e Gestão

Unidade: 02 – Gestão Administrativa

Atividade: 2.031 – Informatização das Atividades Administrativas

339040 – Serviços de Tecnologia da Informação e Comunicação

CLÁUSULA VIII - DO TERMO CONTRATUAL

8.1. As obrigações decorrentes deste Contrato serão formalizadas através de Ordem de Serviço e Nota de Empenho, em estrita observância aos princípios gerais do direito e às normas contempladas em nossa legislação vigente.

8.2. A recusa da adjudicatária em assinar o Contrato, a dar quitação em Nota de Empenho e retirar a ordem de serviço equivalente, caracteriza descumprimento de obrigações, passíveis das sanções previstas no art. 81 e seguintes da Lei 8.666/93 com as alterações posteriores. Neste caso, a critério do Município, poderá ser celebrado contrato com o ofertante do menor preço por lote, subsequente, ou promover nova licitação.



PREFEITURA MUNICIPAL DE CONGONHAS

CIDADE DOS PROFETAS

8.3. O instrumento contratual poderá ser alterado com fundamento nas disposições previstas no art. 65 da Lei 8.666/93 e com alterações posteriores.

CLÁUSULA IX – DA RESCISÃO

10.1. A rescisão contratual poderá ser:

10.1.1. Determinada por ato unilateral e escrito da Administração, nos casos enumerados nos incisos I a XII e XVII do art. 78 da Lei Federal nº 8.666/93;

10.1.2. Amigável, por acordo entre as partes, mediante autorização escrita e fundamentada da autoridade competente, reduzida a termo no processo licitatório, desde que haja conveniência da Administração.

10.2. A inexecução total ou parcial do Contrato enseja sua rescisão pela Administração, com as consequências previstas na Lei 8666/93.

10.3. Constituem motivos para rescisão do contrato os previstos no art. 78 da Lei Federal nº 8.666/93.

10.3.1. Em caso de rescisão prevista nos incisos XII a XVII do art. 78 da Lei Federal nº 8.666/93, sem que haja culpa da Contratada, será esta ressarcida dos prejuízos regulamentares comprovados, quando os houver sofrido.

10.3.2. A rescisão contratual de que trata o inciso I do art. 79 acarreta as consequências previstas no art. 80, incisos I a IV, ambos da Lei Federal nº 8.666/93.

CLAUSULA XI - DO PRAZO DE VIGÊNCIA

11.1. O Contrato entre a terá vigência de 24 (*vinete e quatro*) meses, podendo ser prorrogado por períodos sucessivos de 24 (*vinete e quatro*) meses, até máximo de 48 (*quarenta e oito*) meses.

CLÁUSULA XII – GESTÃO E FISCALIZAÇÃO DO CONTRATO

12.1. O gestor do Contrato será o Secretário de Administração e a fiscalização e acompanhamento ao cumprimento das obrigações da Contratada, através de comissão/servidor especialmente designado, a saber: Wanderson Ferreira Leão, matrícula 20143618, Diretor de Tecnologia da Informação e Clever da Conceição Júnior, matrícula 20143625, Chefe de Departamento de Tecnologia da Informação.

CLÁUSULA XIII – DA VINCULAÇÃO AO EDITAL

13.1. O presente contrato fica vinculado ao Edital do Processo Licitatório nº. PRC/227/2021, Pregão Presencial nº. PMC/113/2021, Processo Administrativo nº PMC/16224/2009 e ao Termo de Referência, que passam a fazer parte integrante deste contrato, independentemente de transcrição.



PREFEITURA MUNICIPAL DE CONGONHAS
CIDADE DOS PROFETAS

CLÁUSULA XIV – DO FORO

14.1. Fica eleito o foro da comarca de Congonhas - MG para dirimir dúvidas e decidir pendências jurídicas provenientes deste contrato.

E por estarem as partes justas e contratadas, assinam o presente contrato lavrado em 02 (duas) vias de igual teor e forma, juntamente com 02 (duas) testemunhas.

Congonhas, 04 de maio de 2022

LUCIMARA APARECIDA JUNQUEIRA:02612195610
610

Assinado de forma digital por
LUCIMARA APARECIDA
JUNQUEIRA:02612195610
Dados: 2022.05.09 13:47:16
-03'00'

Lucimara Aparecida Junqueira
Secretária Municipal de Planejamento e Gestão

Assinado de forma digital por
BORJA SOBRINHO:43675280659
Motivo: Estou aprovando este
documento
Dados: 2022.05.09 10:30:22 -03'00'

Erasmo Borja Sobrinho
Netsol Ltda-EPP

Assinado de forma digital por
GERALDO EDUARDO GONCALVES
JUNIOR:68574193615
Dados: 2022.05.07 09:12:19 -03'00'

Geraldo Eduardo Gonçalves Júnior
Netsol Ltda-EPP

TESTEMUNHAS:

1ª

2ª

