TERMO DE REFERÊNCIA

CONTRATAÇÃO DE SERVIÇOS ESPECIALIZADOS DE SEGURANÇA DE REDES (FIREWALL DE PRÓXIMA GERAÇÃO), GESTÃO INTEGRADA E RETENÇÃO DE LOGS, PROTEÇÃO DE SERVIDORES CONTRA EXPLORAÇÃO DE VULNERABILIDADES E FIREWALL DE APLICAÇÕES WEB (WAF)

1. DO OBJETO

1.1. Definição do objeto

Contratação de empresa especializada para a prestação de serviços continuados de segurança da informação, compreendendo o fornecimento, em regime de serviço (equipamentos, licenciamento, garantia, suporte e atualização), das soluções a seguir relacionadas, doravante designadas neste Termo de Referência pelas denominações respectivamente indicadas: (i) firewall corporativo de próxima geração para o centro de processamento de dados da CODIUB, que por sua vez envolve a Administração pública direta e indireta do município de Uberaba — Item 01; (ii) firewall corporativo de próxima geração para a administração pública indireta — Item 02; (iii) ferramenta de gestão integrada dos firewalls, com armazenamento de logs e emissão de relatórios — Item 03; (iv) sistema de prevenção contra ataques a servidores mediante exploração de vulnerabilidades — Item 04; e (v) firewall específico para aplicações web (WAF — Web Application Firewall) — Item 05.

1.2. Natureza do objeto

O objeto caracteriza-se como serviço comum e de natureza continuada, cujos padrões de desempenho e qualidade podem ser objetivamente definidos por meio de especificações usuais de mercado, prestado sem interrupção ao longo da vigência contratual e essencial à continuidade das atividades finalísticas da CONTRATANTE.

1.3. Do item único e do critério de julgamento

Os componentes descritos serão contratados de forma agrupada, em item/lote único, adotando-se o critério de julgamento de MENOR PREÇO GLOBAL, em razão da interdependência técnica e operacional entre as soluções, conforme justificativa constante do Item 3.

2. DA FUNDAMENTAÇÃO E JUSTIFICATIVA DA CONTRATAÇÃO

2.1. Base legal

A presente contratação rege-se pela Lei nº 13.303, de 30 de junho de 2016 (Estatuto Jurídico das Empresas Estatais), pelo Regulamento Interno de Licitações, Contratos e Convênios da CODIUB (RILC) — Versão III, pela Lei nº 13.709, de 14 de agosto de 2018 (LGPD) e, no que couber e de

forma supletiva, pela legislação aplicável às licitações na modalidade pregão. Em caso de divergência, prevalecem as disposições da Lei nº 13.303/2016 e do RILC/CODIUB.

2.2. Contextualização e motivação da contratação

A CODIUB é responsável pela sustentação dos serviços informatizados que suportam a gestão do Município de Uberaba, disponibilizados tanto às unidades administrativas quanto, diretamente, aos munícipes. A continuidade e a disponibilidade desses serviços dependem da manutenção de uma infraestrutura de segurança da informação capaz de proteger os ativos que os hospedam contra tentativas de intrusão, indisponibilidade e vazamento de dados.

A estrutura de segurança atualmente em produção é composta por firewalls de próxima geração instalados no Município de Uberaba, por ferramenta de gestão e retenção de logs, por solução de proteção de servidores contra a exploração de vulnerabilidades e por firewall de aplicações web (WAF).

O modelo de contratação sob a forma de serviço que reúne, em um mesmo objeto, o fornecimento dos equipamentos, o licenciamento, as atualizações, o suporte e a contingência mediante equipamentos de reserva, é mantido na presente contratação.

2.3. Dos serviços de implantação e migração

Deve estar incluso a prestação de serviços técnicos especializados para planejamento, implantação, configuração, parametrização, integração, validação, documentação, transferência de conhecimento e operação assistida de todas as soluções de segurança da informação fornecidas no âmbito deste certame.

Os serviços deverão contemplar a implementação completa do ambiente contratado, garantindo o pleno funcionamento operacional das soluções, sua integração com o ambiente tecnológico da CONTRATANTE e a entrada em produção conforme os requisitos estabelecidos neste Edital.

2.4. Dos benefícios esperados

2.4.1. Continuidade e disponibilidade dos serviços informatizados municipais, mediante manutenção ininterrupta dos controles de segurança.

2.4.2. Recomposição do suporte, da garantia e das atualizações junto ao fabricante, superando a condição de fim de suporte do equipamento da CONTRATANTE.

2.4.3. Ampliação da janela de retenção de logs, fortalecendo a resposta a incidentes e a rastreabilidade.

2.4.4. Preservação do modelo de serviço, com contingência por equipamentos de reserva e previsibilidade de custos ao longo da vigência.

3. DA DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

3.1. Visão integrada da solução

A solução é composta por cinco componentes complementares e interdependentes, que atuam de forma coordenada para prover a proteção integral do ambiente:

3.1.1. Firewall de próxima geração (NGFW) responsável pela proteção perimetral do principal centro de processamento de dados;

3.1.2. Firewall de próxima geração (NGFW), responsável pela proteção perimetral das respectivas unidades;

3.1.3. Ferramenta de gestão integrada dos firewalls, com armazenamento de logs e emissão de relatórios;

3.1.4. Sistema de prevenção contra ataques a servidores mediante exploração de vulnerabilidades, que estende a proteção à camada dos servidores físicos e virtuais;

3.1.5. Firewall de aplicação web (WAF), que protege as aplicações web publicadas contra ataques à camada de aplicação (camada 7).

3.2. Da interoperabilidade e integração

Os componentes que integram a solução deverão operar de forma interoperável e integrada, de modo a assegurar a gestão centralizada, a visibilidade consolidada dos eventos e a consistência na aplicação das políticas de segurança, observados os seguintes requisitos mínimos:

3.2.1. Os firewalls de próxima geração (Itens 01 e 02) e a ferramenta de gestão integrada (Item 03) deverão ser plenamente compatíveis entre si, permitindo a administração centralizada das políticas, a coleta e o armazenamento consolidado dos registros (logs) e a emissão de relatórios unificados, a partir de console de gerência e monitoração centralizada;

3.2.2. A solução de prevenção contra ataques a servidores (Item 04) e o firewall de aplicação web (Item 05) deverão complementar a arquitetura de proteção, atuando, respectivamente, na camada dos servidores físicos e virtuais e na camada de aplicação (camada 7), com capacidade de registro, monitoração e geração de alertas que subsidiem a resposta a incidentes;

3.2.3. A integração entre os componentes poderá ser assegurada por meio de recursos nativos da própria solução ou, alternativamente, por interfaces e protocolos abertos e usuais de mercado, a exemplo de API, syslog e formatos padronizados de exportação de eventos, admitindo-se qualquer arranjo técnico que atenda integralmente aos requisitos funcionais deste Termo de Referência;

3.2.4. O atendimento aos requisitos de interoperabilidade deverá ser comprovado por meio de documentação técnica oficial do fabricante, admitida a sua disponibilização em sítio eletrônico oficial, observado o disposto no item 10;

3.2.5. Os requisitos de interoperabilidade estabelecidos neste item constituem fundamento técnico da contratação agrupada de que trata o item 3.3 e não implicam, por si, exigência de fabricante, marca ou modelo determinado, observado o disposto nos itens 2.5 e 4.5.

3.3. Da justificativa do agrupamento em item único

Nos termos do art. 32, inciso III, da Lei nº 13.303/2016, o parcelamento do objeto é a regra, salvo quando técnica ou economicamente inviável. No caso concreto, a CONTRATANTE avaliou a possibilidade de divisão do objeto e concluiu pela sua inviabilidade técnica e econômica, adotando-se a contratação agrupada em item/lote único, com julgamento pelo menor preço global, pelos seguintes fundamentos:

3.3.1. Interdependência técnica e operacional entre os componentes, nos termos do item 3.2, cuja atuação coordenada é condição para a eficácia dos controles de segurança e para a gestão centralizada do ambiente;

3.3.2. Padronização e compatibilidade funcional dos recursos, observado o requisito do item 4.1.1, evitando incompatibilidades que comprometeriam a operação, a proteção do ambiente e a própria continuidade dos serviços municipais;

3.3.3. Responsabilização única pela disponibilidade, pelo suporte, pela contingência e pela integração do conjunto, afastando a diluição de responsabilidades entre múltiplos fornecedores e a dificuldade de apuração de responsabilidade em caso de falha ou indisponibilidade;

3.3.4. Economicidade e eficiência administrativa na gestão de um único contrato e de um único ponto de contato.

3.3.5. Preservação da economia de escala e do ganho de eficiência decorrentes da contratação integrada, cuja divisão tenderia a elevar os custos unitários e a onerar a contratação, em prejuízo da obtenção da proposta mais vantajosa.

3.3.6. O agrupamento não compromete o caráter competitivo do certame, uma vez que as especificações são definidas por parâmetros de desempenho, sem indicação de marca, fabricante ou modelo, admitindo-se soluções equivalentes ou superiores de qualquer fornecedor, e há no mercado pluralidade de empresas aptas a ofertar o conjunto integralmente. A opção pelo lote único, portanto, não decorre de restrição à competição, mas da inviabilidade técnica e econômica do parcelamento, em linha com o entendimento consolidado dos órgãos de controle quanto à admissibilidade do agrupamento quando a divisão do objeto acarretar perda de economia de escala ou risco à execução integral do contrato.

4. DOS REQUISITOS DA CONTRATAÇÃO

4.1. Requisitos gerais dos equipamentos (Itens 01 e 02)

4.1.1. Os equipamentos de firewall de próxima geração (Itens 01 e 02) deverão ser novos, de

primeiro uso, e de um mesmo fabricante, exigência destinada a assegurar a padronização, a compatibilidade funcional entre as unidades e a gestão centralizada, restringindo-se aos referidos itens e não se estendendo aos demais componentes do objeto, prevalecendo esta delimitação sobre eventuais disposições em sentido diverso constantes da Item 5.

4.1.2. Na data da proposta, nenhum dos modelos ofertados poderá constar, no sítio do fabricante, em listas de fim de comercialização (end-of-sale) ou de fim de vida (end-of-life).

4.1.3. Não serão aceitas soluções baseadas em computadores de uso geral, devendo os equipamentos de que trata este item ser do tipo appliance, próprios para montagem em rack 19", ressalvado o disposto no item 4.2 quanto aos demais componentes do objeto.

4.1.4. Os equipamentos deverão ser fornecidos com todos os acessórios necessários à sua instalação e operação, incluindo kit de trilhos para adaptação a rack, quando aplicável, e cabos de alimentação, sem ônus adicional para a CONTRATANTE.

4.2. Requisitos dos componentes fornecidos como software, appliance virtual ou serviço em nuvem (Itens 03, 04 e 05)

4.2.1. Os componentes de que tratam os Itens 03, 04 e 05 poderão ser fornecidos, a critério da licitante, sob a forma de appliance dedicado (físico ou virtual), de software instalado em infraestrutura da CONTRATANTE ou de serviço em nuvem, na forma facultada pelos itens 5.3.5, 5.4.4 e 5.5.1, não se lhes aplicando as exigências de mesmo fabricante e de appliance físico previstas nos itens 4.1.1 e 4.1.3.

4.2.2. Independentemente da modalidade de fornecimento adotada, deverão ser integralmente atendidos os dimensionamentos mínimos estabelecidos na Item 5, notadamente a capacidade de armazenamento destinada à retenção de logs (Item 03), a quantidade mínima de servidores protegidos (Item 04) e a capacidade mínima de tráfego inspecionado em camada de aplicação (Item 05), correndo por conta da CONTRATADA todos os custos de licenciamento, processamento, armazenamento e demais recursos necessários, sem ônus adicional para a CONTRATANTE.

4.2.3. Na data da proposta, as versões ofertadas não poderão constar como descontinuadas ou sem suporte pelo respectivo fabricante, devendo ser mantidas atualizadas durante toda a vigência contratual, na forma do item 4.3.5.

4.2.4. Quando o fornecimento ocorrer sob a forma de serviço em nuvem, a CONTRATADA será integralmente responsável pelo provisionamento, dimensionamento, disponibilidade e segurança do ambiente, observados os níveis de serviço da Item 8, não afastando a eventual contratação de provedor de infraestrutura a responsabilidade da CONTRATADA perante a CONTRATANTE.

4.2.5. O tratamento de dados em ambiente de nuvem observará integralmente o disposto no item 4.4, devendo a CONTRATADA informar a localização e a jurisdição dos ambientes de armazenamento e processamento, bem como observar, quanto a eventual transferência internacional de dados, os requisitos dos arts. 33 a 36 da Lei nº 13.709/2018 (LGPD).

4.2.6. Ao término da vigência contratual, por qualquer motivo, a CONTRATADA deverá promover a devolução à CONTRATANTE dos registros (logs), configurações, políticas e demais dados sob sua custódia, em formato aberto e estruturado que permita a respectiva importação por terceiros, seguida da eliminação segura das cópias remanescentes, mediante comprovação formal, assegurando a continuidade dos serviços e a ausência de dependência tecnológica em relação à CONTRATADA.

4.3. Requisitos de licenciamento, garantia e atualização

O fornecimento dar-se-á sob a forma de serviço, compreendendo os equipamentos, o software, o licenciamento, a garantia, o suporte e as atualizações de todos os componentes do objeto, nas seguintes condições:

4.3.1. As soluções de que tratam os Itens 01 e 02 deverão estar licenciadas, por todo o período contratual, com perfil de proteção unificada, contemplando, no mínimo: firewall, controle de aplicações, prevenção de intrusão (IPS), antivírus/antimalware, antispam, filtro de conteúdo web, proteção de DNS, inspeção de tráfego criptografado e os demais serviços de proteção descritos nas especificações técnicas;

4.3.2. As soluções de que tratam os Itens 03, 04 e 05 deverão estar licenciadas, por todo o período contratual, nos quantitativos e capacidades mínimas estabelecidos na Item 5, a saber: a capacidade de armazenamento destinada à retenção de logs e à emissão de relatórios (Item 03); a quantidade mínima de servidores protegidos, com a totalidade dos módulos de proteção habilitados (Item 04); e a capacidade mínima de tráfego inspecionado em camada de aplicação, para todas as aplicações relacionadas (Item 05);

4.3.3. O licenciamento deverá ser descrito e comprovado por funcionalidades e por capacidades, sendo vedada a indicação de nome comercial de pacote, marca, fabricante ou modelo;

4.3.4. Os custos de licenciamento, das assinaturas dos serviços de proteção e das respectivas atualizações, relativos a todos os componentes do objeto, estão compreendidos no preço contratado, não ensejando cobrança adicional à CONTRATANTE;

4.3.5. A CONTRATADA deverá manter as soluções atualizadas durante toda a vigência, compreendendo atualizações de versão, correções de defeitos (patches) e atualização contínua das assinaturas e bases de conhecimento dos serviços de proteção;

4.3.6. A garantia deverá abranger a substituição de todos os equipamentos e componentes com mau funcionamento, pelo prazo integral da contratação;

4.3.7. As licenças deverão ser vinculadas ao contrato e à CONTRATANTE, vedado o condicionamento de sua fruição, da aplicação de atualizações ou do atendimento de suporte a qualquer pagamento adicional não previsto na proposta.

4.4. Requisitos legais e regulatórios (LGPD e sigilo)

A CONTRATADA deverá observar, na execução do objeto, a legislação de proteção de dados pessoais e de segurança da informação, obrigando-se a:

4.4.1. Atuar em conformidade com a Lei nº 13.709/2018 (LGPD) e com as determinações dos órgãos reguladores aplicáveis, em todo tratamento de dados a que tiver acesso;

4.4.2. Tratar como confidenciais todos os dados e informações a que tiver acesso, ainda que após o encerramento do vínculo contratual, ressalvadas as de domínio público;

4.4.3. Informar imediatamente à CONTRATANTE qualquer incidente de segurança, exposição ou requisição de autoridade que envolva dados sob tratamento;

4.4.4. Adotar medidas técnicas e administrativas de segurança aptas a proteger os dados pessoais de acessos não autorizados e de situações de destruição, perda, alteração, comunicação ou difusão indevidas.

4.5. Da isonomia e da comprovação técnica

4.5.1. As especificações são referenciais de desempenho mínimo, admitindo-se solução equivalente ou superior de qualquer fabricante que as atenda integralmente, sendo vedada qualquer restrição que caracterize direcionamento.

4.5.2. As funcionalidades, capacidades e demais características exigidas neste Termo de Referência deverão ser comprovadas mediante documentação técnica oficial do fabricante da solução ofertada, admitida a sua disponibilização em sítio eletrônico oficial, facultada à CONTRATANTE a realização de diligências para verificação da conformidade.

5. DAS ESPECIFICAÇÕES TÉCNICAS DO OBJETO

As denominações Item 01 a Item 05, empregadas nesta Seção e nas demais deste Termo de Referência, correspondem às definidas no item 1.1. Os requisitos funcionais comuns aos firewalls corporativos de próxima geração constam do item 5.1 e aplicam-se integralmente aos Itens 01 e 02; as capacidades, o desempenho e as interfaces mínimas específicas de cada equipamento, bem como as ressalvas aplicáveis, constam do item 5.2. As especificações dos Itens 03, 04 e 05 constam, respectivamente, dos itens 5.3, 5.4 e 5.5.

5.1. Dos requisitos comuns aos firewalls corporativos de próxima geração (Itens 01 e 02)

Os firewalls corporativos de próxima geração deverão ser instalados e configurados pela CONTRATADA, nos locais indicados pela CONTRATANTE, compondo plataformas de segurança do tipo appliance (hardware e software integrados), com funcionalidades de firewall de próxima geração (NGFW), console de gerência e monitoração. Os requisitos funcionais estabelecidos nos subitens 5.1.1 a 5.1.11 aplicam-se integralmente a ambos os equipamentos, observadas as especificações específicas e as ressalvas constantes do item 5.2.

5.1.1. Características gerais

5.1.1.1. A solução deve consistir em plataforma de proteção e balanceamento inteligente de rede baseada em appliance com funcionalidades de firewall de próxima geração (NGFW), console de gerência e monitoração.

5.1.1.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões.

5.1.1.3. Os equipamentos devem ser novos, de primeiro uso, de um mesmo fabricante. Na data da proposta, nenhum dos modelos ofertados poderá constar nas listas de fim de vida (end-of-life) ou fim de comercialização (end-of-sale) do fabricante.

5.1.1.4. Não serão aceitas soluções baseadas em computadores de uso geral. Todos os equipamentos deverão ser do mesmo fabricante, para assegurar a padronização e a compatibilidade funcional de todos os recursos.

5.1.1.5. As funcionalidades de proteção de rede que compõem a solução podem funcionar em múltiplos appliances, desde que atendam a todos os requisitos desta especificação.

5.1.1.6. A solução deverá possuir e estar licenciada por todo o período contratual com, no mínimo, as seguintes funcionalidades: firewall, traffic shaping e QoS, filtro de conteúdo web, antivírus, antispam, detecção e prevenção de intrusos (IPS), VPN IPSec, controle de aplicações, prevenção de perda de dados (DLP) e virtualização.

5.1.2. Funcionalidades de rede e firewall

5.1.2.1. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta.

5.1.2.2. Os dispositivos de proteção de rede devem possuir suporte a VLANs.

5.1.2.3. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM).

5.1.2.4. Os dispositivos de proteção de rede devem possuir suporte a DHCP Cliente, Server e Relay.

5.1.2.5. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet lógicas.

5.1.2.6. Deve possuir a funcionalidade de tradução de endereços estáticos — NAT (Network Address Translation), um para um (1-to-1), N-para-um (N-to-1), vários para um, NAT64, NAT66, NAT46 e PAT.

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

5.1.2.8. Deverá suportar sFlow ou NetFlow.

5.1.2.9. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance e que possam ser administrados por equipes distintas.

5.1.2.10. Deverá permitir limitar o uso de recursos utilizados por cada sistema virtual.

5.1.2.11. Deve suportar o protocolo padrão da indústria VXLAN.

5.1.2.12. Deve implementar o protocolo ECMP.

5.1.2.13. Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança.

5.1.2.14. Enviar log para sistemas de monitoração externos.

5.1.2.15. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL.

5.1.2.16. Deve possuir mecanismos de proteção anti-spoofing.

5.1.2.17. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP4 e OSPFv2).

5.1.2.18. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3).

5.1.2.19. Suportar OSPF graceful restart.

5.1.2.20. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede.

5.1.2.21. Deve suportar Modo Camada 2 (L2), para inspeção de dados em linha e visibilidade do tráfego.

5.1.2.22. Deve suportar Modo Camada 3 (L3), para inspeção de dados em linha e visibilidade do tráfego.

5.1.2.23. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo.

5.1.2.24. A configuração em alta disponibilidade deve sincronizar: sessões; configurações, incluindo, mas não limitado às políticas de firewall, NAT, QoS e objetos de rede; associações de segurança das VPNs; e tabelas FIB.

5.1.2.25. Deverá possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e também Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal, sem perda de conexões.

5.1.2.26. O modo de Alta Disponibilidade (HA) deve possibilitar monitoração de falha de link.

5.1.2.27. A solução deve suportar integração nativa com Let's Encrypt, para obtenção de certificados válidos, de forma automática.

5.1.2.28. A solução deve possuir conectores nativos para integração com nuvens privadas, pelo menos: VMware ESXi, Cisco ACI e Kubernetes.

5.1.2.29. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos firewalls, suportando, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via Teams e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos.

5.1.2.30. Deverá possuir integração com tokens para autenticação de dois fatores.

5.1.2.31. Deverá suportar controle por zonas de segurança.

5.1.2.32. Deverá suportar controles de políticas por porta e protocolo.

5.1.2.33. Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações.

5.1.2.34. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.

5.1.2.35. Controle de políticas por código de País (por exemplo: BR, US, UK, RU).

5.1.2.36. Controle, inspeção e descriptografia de SSL por política para tráfego de saída (outbound).

5.1.2.37. Deve decriptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3.

5.1.2.38. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada.

5.1.2.39. Suporte a objetos e regras IPv6.

5.1.2.40. Suporte a objetos e regras multicast.

5.1.2.41. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

5.1.3. Funcionalidade de controle de aplicações

5.1.3.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo.

5.1.3.2. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos.

5.1.3.3. Reconhecer pelo menos 4.000 (quatro mil) aplicações diferentes, incluindo, mas não limitado a: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos e e-mail.

5.1.3.4. Deverá possuir, pelo menos, 15 (quinze) categorias para classificação de aplicações.

5.1.3.5. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote e google-docs.

5.1.3.6. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante, independente de porta e protocolo.

5.1.3.7. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor.

5.1.3.8. Para tráfego criptografado SSL, deve decriptografar pacotes a fim de possibilitar a

leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante.

5.1.3.9. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo; a decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação.

5.1.3.10. Identificar o uso de táticas evasivas via comunicações criptografadas.

5.1.3.11. Atualizar a base de assinaturas de aplicações automaticamente.

5.1.3.12. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller nem nas estações dos usuários.

5.1.3.13. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente à possibilidade de habilitar controle de aplicações em algumas regras.

5.1.3.14. Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos.

5.1.3.15. 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.

5.1.3.16. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações.

5.1.3.17. Deve alertar o usuário quando uma aplicação for bloqueada.

5.1.3.18. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc.), possuindo granularidade de controle/políticas para os mesmos.

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

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

5.1.3.21. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc.).

5.1.3.22. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação, tecnologia, fabricante e popularidade.

5.1.3.23. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: categoria da aplicação.

5.1.3.24. Deve permitir forçar o uso de portas específicas para determinadas aplicações.

5.1.4. Funcionalidade de prevenção de intrusão e ameaças

5.1.4.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall.

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

5.1.4.3. Deve sincronizar as assinaturas de IPS, Antivírus e Anti-Spyware quando implementado em alta disponibilidade.

5.1.4.4. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir; permitir e gerar log; bloquear; e quarentenar o IP do atacante por um intervalo de tempo.

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

5.1.4.6. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança.

5.1.4.7. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura.

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

5.1.4.9. Deve permitir o bloqueio de vulnerabilidades.

5.1.4.10. Deve permitir o bloqueio de exploits conhecidos.

5.1.4.11. Deve incluir proteção contra ataques de negação de serviços.

5.1.4.12. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc.

5.1.4.13. Detectar e bloquear a origem de portscans.

5.1.4.14. Bloquear ataques efetuados por worms conhecidos.

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

5.1.4.16. Possuir assinaturas para bloqueio de ataques de buffer overflow.

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

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

5.1.4.19. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB/CIFS, SMTP e POP3.

5.1.4.20. Identificar e bloquear comunicação com botnets.

5.1.4.21. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e destino da comunicação, além da ação tomada pelo dispositivo.

5.1.4.22. Os eventos devem identificar o país de onde partiu a ameaça.

5.1.4.23. Deve incluir proteção contra vírus em conteúdo HTML e JavaScript, software espião (spyware) e worms.

5.1.4.24. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos.

5.1.4.25. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseadas em políticas do firewall, considerando usuários, grupos de usuários, origem, destino, zonas de segurança, etc., ou seja, cada política de firewall poderá ter uma configuração diferente de IPS.

5.1.4.26. A solução deve ter capacidade de enviar artefatos suspeitos para serem executados em ambiente controlado na nuvem do fabricante.

5.1.4.27. Deve suportar a captura de pacotes (PCAP) por assinatura de IPS ou controle de aplicação.

5.1.4.28. Deve permitir que, na captura de pacotes por assinaturas de IPS, seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta, assim como seu contexto, facilitando a análise forense e a identificação de falsos positivos.

5.1.5. Funcionalidade de filtro de conteúdo web e DNS

5.1.5.1. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora).

5.1.5.2. Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança.

5.1.5.3. 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.

5.1.5.4. Deve permitir que os usuários sejam identificados através de consulta em uma base do Active Directory, permitindo que sua autenticação no domínio não seja solicitada novamente para navegar através da solução.

5.1.5.5. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL.

5.1.5.6. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs.

5.1.5.7. Possuir pelo menos 80 (oitenta) categorias de URLs.

5.1.5.8. Deve possuir a função de exclusão de URLs do bloqueio.

5.1.5.9. Permitir a customização de página de bloqueio.

5.1.5.10. Deve bloquear o acesso a conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, independentemente de a opção Safe Search estar habilitada no navegador do usuário.

5.1.5.11. Deve possuir a função de proteção à resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos e de Comando e Controle (C&C) de botnets conhecidas.

5.1.5.12. Deve possuir filtro de domínio DNS baseado em categorias para inspecionar o tráfego DNS, com classificação de domínios continuamente atualizada.

5.1.6. Funcionalidade de identificação de usuários

5.1.6.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações, através da integração com serviços de diretório, autenticação via LDAP, Active Directory, eDirectory e base de dados local.

5.1.6.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários.

5.1.6.3. Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2012 R2 ou superior.

5.1.6.4. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on; essa funcionalidade não deve possuir limites licenciados de usuários.

5.1.6.5. Deve possuir integração com Radius para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários.

5.1.6.6. Deve possuir integração com LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários.

5.1.6.7. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída à internet, para que, antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal).

5.1.6.8. Deve possuir suporte à identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços.

5.1.6.9. Deve suportar o envio e recebimento de credenciais via RADIUS.

5.1.6.10. Deve implementar a criação de grupos customizados de usuários no firewall, baseados em atributos do LDAP/AD.

5.1.7. Funcionalidade de filtro de dados

5.1.7.1. Permitir identificar e, opcionalmente, prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc.) identificados sobre aplicações (HTTP, FTP, SMTP).

5.1.7.2. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos.

5.1.7.3. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos.

5.1.7.4. Permitir identificar e, opcionalmente, prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

5.1.8. Funcionalidade de geolocalização

5.1.8.1. Suportar a criação de políticas por geolocalização, permitindo que o tráfego de determinado País/Países seja bloqueado.

5.1.8.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.

5.1.9. Funcionalidade de VPN

5.1.9.1. Suportar VPN Site-to-Site e Client-To-Site.

5.1.9.2. Suportar IPSec VPN.

5.1.9.3. A VPN IPSec deve suportar 3DES.

5.1.9.4. A VPN IPSec deve suportar autenticação MD5 e SHA-1.

5.1.9.5. A VPN IPSec deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14.

5.1.9.6. A VPN IPSec deve suportar algoritmo Internet Key Exchange (IKEv1 e v2).

5.1.9.7. A VPN IPSec deve suportar AES 128, 192 e 256 (Advanced Encryption Standard).

5.1.9.8. A VPN IPSec deve suportar autenticação via certificado IKE PKI.

5.1.9.9. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet e SonicWall.

5.1.9.10. Suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6.

5.1.9.11. Deve permitir habilitar e desabilitar túneis de VPN IPSec a partir da interface gráfica da solução, facilitando o processo de troubleshooting.

5.1.9.12. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies.

5.1.9.13. Atribuição de DNS nos clientes remotos de VPN.

5.1.9.14. Deve permitir criar políticas de controle de aplicações, IPS, Antivírus, Anti-Spyware e filtro de URL para tráfego dos clientes remotos conectados na VPN.

5.1.9.15. Suportar autenticação via AD/LDAP, Secure ID, certificado e base de usuários local.

5.1.9.16. Suportar leitura e verificação de CRL (Certificate Revocation List).

5.1.9.17. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis VPN.

5.1.9.18. Deve permitir que a conexão com a VPN seja estabelecida após a autenticação do usuário na estação.

5.1.9.19. Deve permitir que a conexão com a VPN seja estabelecida sob demanda do usuário.

5.1.9.20. Deverá manter uma conexão segura com o portal durante a sessão.

5.1.9.21. O agente de VPN client-to-site deve ser compatível com, pelo menos: Windows (10 ou superior), Ubuntu Linux (22.04 ou superior), Red Hat Linux (7.4 ou superior), CentOS Stream (9 ou superior), Fedora Linux (36 ou superior) e macOS (v13 ou superior).

5.1.10. Funcionalidade de QoS, traffic shaping e priorização de tráfego

5.1.10.1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo (como YouTube e redes sociais, etc.) e ter alto consumo de largura de banda, requer-se que a solução, além de poder permitir ou negar esse tipo de aplicações, tenha a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming.

5.1.10.2. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem.

5.1.10.3. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino.

5.1.10.4. Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo.

5.1.10.5. Suportar a criação de políticas de QoS e Traffic Shaping por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus.

5.1.10.6. Suportar a criação de políticas de QoS e Traffic Shaping por porta.

5.1.10.7. O QoS deve possibilitar a definição de tráfego com banda garantida (ex.: banda mínima disponível para aplicações de negócio).

5.1.10.8. O QoS deve possibilitar a definição de tráfego com banda máxima (ex.: banda máxima permitida para aplicações do tipo best-effort/não corporativas, tais como YouTube, Facebook, entre outros).

5.1.10.9. O QoS deve possibilitar a definição de fila de prioridade.

5.1.10.10. Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype.

5.1.10.11. Suportar marcação de pacotes DiffServ, inclusive por aplicação.

5.1.10.12. Suportar modificação de valores DSCP para o DiffServ.

5.1.10.13. Suportar priorização de tráfego usando informação de ToS (Type of Service).

5.1.10.14. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping.

5.1.10.15. Deve suportar QoS (Traffic Shaping) em interfaces agregadas ou redundantes.

5.1.10.16. Deve possibilitar a definição de bandas distintas para download e upload.

5.1.11. Funcionalidade de balanceamento inteligente de links

5.1.11.1. A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação.

5.1.11.2. A solução deve ser capaz de agregar vários links em uma interface virtual.

5.1.11.3. Deve ser possível criar políticas de roteamento inteligente, mediante regras pré-estabelecidas, considerando a verificação das seguintes condições: endereços de origem, grupos de usuários, endereços de destino, serviços na Internet e aplicações de camada 7 (O365 Exchange, AWS, Dropbox, etc.).

5.1.11.4. A solução deve ser capaz de medir o status de qualidade do link baseando-se em critérios mínimos de latência, jitter e perda de pacotes, sendo possível configurar um valor limite para cada um destes itens, utilizado como gatilho para fator de decisão nas regras de tráfego de saída e balanceamento inteligente.

5.1.11.5. A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de balanceamento em condições em que a largura de banda é modificada.

5.1.11.6. A solução deve ser capaz de monitorar a qualidade e identificar falhas nos links, enviando sinais por meio de cada link para servidores ou aplicações, permitindo utilizar protocolos como Ping, HTTP, TCP ECHO, UDP ECHO, DNS, TCP Connect e TWAMP (Two-way Active Measurement Protocol); deve suportar ainda um método para mensurar a qualidade do tráfego de voz corporativo baseado em MOS (Mean Opinion Score).

5.1.11.7. A solução deve possibilitar balanceamento de tráfego entre conexões WAN, de forma que o algoritmo de balanceamento de carga possa ser configurado considerando os seguintes parâmetros: sessões, volume de tráfego, IP de origem e destino e transbordo de link (spillover).

5.1.11.8. A solução deve possibilitar a criação de regras para seleção das interfaces e suas prioridades utilizadas para encaminhar o tráfego de saída da rede, considerando os seguintes critérios:

5.1.11.8.1. Manual: deve permitir que as interfaces tenham as prioridades atribuídas manualmente.

5.1.11.8.2. Melhor Qualidade: deve permitir que as interfaces recebam uma prioridade com base na qualidade do link ao qual a interface está conectada, considerando o monitoramento de um dos seguintes parâmetros com valores customizáveis: latência, jitter, perda de pacotes ou largura de banda.

5.1.11.8.3. Menor Custo: deve permitir que as interfaces recebam uma prioridade com base no custo atribuído à interface, considerando a satisfação dos parâmetros de qualidade do link ao qual a interface está conectada.

5.1.11.8.4. Balanceamento de Carga: deve permitir que o tráfego seja distribuído entre todas as interfaces disponíveis com base em algoritmos de balanceamento de carga e

na satisfação dos parâmetros customizados de qualidade do link.

5.1.11.9. A solução de balanceamento inteligente deve suportar marcação de pacotes DSCP nas definições e regras para o tráfego balanceado.

5.1.11.10. A solução de balanceamento inteligente de links deve suportar roteamento dinâmico (OSPFv2/v3, BGPv4/BGP4+).

5.1.11.11. A solução deve realizar o reconhecimento de aplicações, em camada 7, de pelo menos 3.000 (três mil) aplicações, incluindo aplicações SaaS, em nuvem e multimídia (Vimeo, YouTube, Facebook, etc.).

5.1.11.12. Deve possibilitar a agregação de túneis IPsec, realizando balanceamento por pacote entre os mesmos.

5.1.11.13. A solução deve possibilitar a criação e uso de túneis VPN de forma dinâmica entre unidades remotas, para aplicações sensíveis; uma vez que as unidades trocam informações entre si, o tráfego deve ser encaminhado diretamente entre as unidades remotas sem passar pela unidade sede.

5.1.11.14. A solução deve permitir a duplicação de pacotes entre dois ou mais links que atendam aos parâmetros de qualidade estabelecidos, objetivando melhor experiência de uso de aplicações.

5.1.11.15. A solução deve possuir recurso para controlar e corrigir erros (FEC) na transmissão de dados, enviando dados redundantes através de túnel VPN em antecipação à perda de pacotes que pode ocorrer durante o trânsito.

5.1.11.16. A solução deve permitir a customização de intervalo de tempo em que é feita a verificação da situação de um link, assim como permitir definir a quantidade de falhas encontradas no link antes de declará-lo inativo, com o objetivo de identificar oscilações nos links que possam impactar os serviços e a experiência dos usuários.

5.1.11.17. A solução deve suportar nativamente conectores com clouds públicas.

5.1.11.18. Deve possibilitar a definição de larguras de banda distintas nas interfaces para download e upload.

5.1.11.19. A solução deve prover estatísticas em tempo real a respeito da utilização da largura de banda (upload e download) e do nível de qualidade dos links (perda de pacote, jitter e latência).

5.1.11.20. Deve implementar balanceamento de link por hash do IP de origem.

5.1.11.21. Deve implementar balanceamento de link por hash do IP de origem e destino.

5.1.11.22. Deve implementar balanceamento de link por peso; nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links, suportando o balanceamento de, no mínimo, três links.

5.1.11.23. O appliance físico deve apresentar compatibilidade com modems USB (3G/4G), capazes de funcionar como circuito ativo em relação à saída principal de Internet e,

alternativamente, como circuito standby, acionado apenas na eventualidade de falha no link principal.

5.1.11.24. Deve ser possível extrair informações de desempenho das verificações de saúde mediante REST API, permitindo a consolidação de tais informações em aplicação terceira.

5.2. Das especificações específicas de cada firewall (Itens 01 e 02)

As especificações a seguir complementam os requisitos comuns estabelecidos no item 5.1 e definem, para cada equipamento, as capacidades, o desempenho e as interfaces mínimas exigidas, bem como as ressalvas aplicáveis.

5.2.1. ITEM 01

O firewall principal deverá atender, no mínimo, às seguintes características específicas e parâmetros de desempenho:

5.2.1.1. Deve suportar, no mínimo, 145 (cento e quarenta e cinco) Gbps de throughput com a funcionalidade de firewall habilitada para tráfego IPv4, independentemente do tamanho do pacote;

5.2.1.2. Deve suportar, no mínimo, 28.000.000 (vinte e oito milhões) de conexões simultâneas;

5.2.1.3. Deve suportar, no mínimo, 580.000 (quinhentas e oitenta mil) novas conexões por segundo;

5.2.1.4. Deve suportar, no mínimo, 55 (cinquenta e cinco) Gbps de throughput de VPN IPSec;

5.2.1.5. Deve estar licenciado para ou suportar, sem o uso de licença, no mínimo, 2.000 (dois mil) túneis de VPN IPSec Site-to-Site simultâneos;

5.2.1.6. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 50.000 (cinquenta mil) túneis de clientes VPN IPSec simultâneos;

5.2.1.7. Deve suportar, no mínimo, 25 (vinte e cinco) Gbps de throughput de IPS;

5.2.1.8. Deve suportar, no mínimo, 11,5 (onze vírgula cinco) Gbps de throughput de inspeção SSL;

5.2.1.9. Deve suportar, no mínimo, 13 (treze) Gbps de throughput com as funcionalidades de controle de aplicação, IPS e antimalware habilitadas simultaneamente, com todas as assinaturas ativadas e atuantes;

5.2.1.10. Deve possuir, pelo menos, 4 (quatro) interfaces com suporte a conectores SFP28 de 25 Gigabit Ethernet;

5.2.1.11. Deve possuir, pelo menos, 4 (quatro) interfaces com suporte a conectores SFP+ de 10 Gigabit Ethernet;

5.2.1.12. Deve possuir, pelo menos, 16 (dezesseis) interfaces com suporte a conectores SFP de 1 Gigabit Ethernet;

5.2.1.13. Deve possuir, pelo menos, 8 (oito) interfaces de 5 Gigabit Ethernet com conectores RJ45;

5.2.1.14. Deve possuir 1 (uma) interface de 2,5 Gigabit Ethernet RJ45 dedicada à alta disponibilidade (HA) e 1 (uma) interface Gigabit Ethernet RJ45 dedicada ao gerenciamento;

5.2.1.15. Deve estar licenciado, sem custo adicional, para no mínimo 10 (dez) sistemas virtuais lógicos (contextos);

5.2.1.16. Deve possuir fonte de alimentação AC redundante e ser próprio para montagem em rack 19", ocupando no máximo 1 (uma) unidade de rack (1 RU).

5.2.2. ITEM 02 — DEMAIS LOCALIDADES

Ao firewall destinado aos locais indicados pela CODIUB, aplica-se integralmente os requisitos comuns estabelecidos nos subitens 5.1.1 a 5.1.11, observada a ressalva decorrente da arquitetura da plataforma destinada a esta localidade, devendo ainda atender, no mínimo, às características específicas e aos parâmetros de desempenho a seguir:

5.2.2.1. Não se aplicam a este equipamento os requisitos relativos a sistemas virtuais lógicos (contextos), a saber, os subitens 5.1.2.9 e 5.1.2.10 e a funcionalidade de virtualização do subitem 5.1.1.6, por inexistir, nesta localidade, necessidade operacional de segregação lógica administrada por equipes distintas;

5.2.2.2. Deve suportar, no mínimo, 3,9 (três vírgula nove) Gbps de throughput com a funcionalidade de firewall habilitada para tráfego IPv4, independentemente do tamanho do pacote;

5.2.2.3. Deve suportar, no mínimo, 600.000 (seiscentas mil) conexões simultâneas;

5.2.2.4. Deve suportar, no mínimo, 30.000 (trinta mil) novas conexões por segundo;

5.2.2.5. Deve suportar, no mínimo, 3,5 (três vírgula cinco) Gbps de throughput de VPN IPSec;

5.2.2.6. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 200 (duzentos) túneis de VPN IPSec Site-to-Site simultâneos;

5.2.2.7. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 250 (duzentos e cinquenta) túneis de clientes VPN IPSec simultâneos;

5.2.2.8. Deve suportar, no mínimo, 800 (oitocentos) Mbps de throughput de IPS;

5.2.2.9. Deve suportar, no mínimo, 400 (quatrocentos) Mbps de throughput de inspeção SSL;

5.2.2.10. Deve suportar, no mínimo, 500 (quinhentos) Mbps de throughput com as funcionalidades de controle de aplicação, IPS e antimalware habilitadas simultaneamente, com todas as assinaturas ativadas e atuantes;

5.2.2.11. Deve possuir, pelo menos, 4 (quatro) interfaces Gigabit Ethernet com conectores RJ45;

5.2.2.12. Deve possuir fonte de alimentação AC, admitido o formato desktop ou para montagem em rack, conforme a arquitetura da plataforma.

5.3. ITEM 03 — Ferramenta de gestão integrada de firewall, armazenamento de logs e relatoria

A ferramenta de gestão integrada de firewall, com armazenamento de logs e emissão de relatórios (Item 03), deverá atender integralmente às especificações estabelecidas nos subitens a seguir.

5.3.1. Deve ser compatível com as soluções indicadas nos Itens 01 e 02.

5.3.2. Solução de armazenamento de logs e emissão de relatórios.

5.3.3. Armazenamento mínimo de 500 GB (quinhentos gigabytes) de dados.

5.3.4. Interface gráfica de usuário (GUI) para fazer administração da solução

5.3.5. A solução pode ser fornecida nas seguintes condições:

5.3.5.1. Hardware do tipo appliance dedicado.

5.3.5.2. Solução Cloud – Com administração e armazenamento baseado em nuvem. Sem a necessidade de instalação de dispositivo local

5.3.6. Possuir comunicação entre os componentes de forma criptografada.

5.3.7. Possuir perfis administrativos com capacidade de criar ao menos 2 (dois) perfis para monitoração dos logs.

5.3.8. Possuir a visualização de log em tempo real de tráfegos de rede.

5.3.9. Permitir a visualização de logs de histórico dos acessos de tráfegos de rede.

5.3.10. Permitir a visualização dos eventos de auditoria.

5.3.11. Possuir pelo menos 20 tipos de relatórios pré-definidos na solução.

5.3.12. Permitir geração de relatórios agendados ou sob demanda nos formatos HTML e PDF.

5.3.13. Permitir o envio dos relatórios, conforme item anterior, através de e-mail para usuários pré-definidos.

5.3.14. Permitir customização dos relatórios, incluindo logotipo customizado.

5.3.15. Possuir relatórios detalhados contendo informações como: IP de origem, IP de destino, serviço, usuário, grupo e horário.

5.3.16. Possuir gerar relatórios baseado nas últimas 24 horas, 1 semana e 1 mês.

5.3.17. Possuir pelo menos os relatórios seguintes relatórios:

5.3.17.1. 10 (dez) sites web mais acessado

5.3.17.2. 10 (dez) categorias de sites web mais acessados

5.3.17.3. 10 (dez) usuários mais ativos na rede

5.3.17.4. 10 (dez) aplicativos mais acessados

5.3.17.5. Tráfego baseado em IP

5.3.17.6. Ataques baseado em origem e destino

5.3.17.7. Vírus detectado por origem e destino

5.4. ITEM 04 — Sistema de prevenção contra eventuais ataques a servidores mediante exploração de vulnerabilidades

O sistema de prevenção contra ataques a servidores mediante exploração de vulnerabilidades

(Item 04) deverá atender integralmente às especificações estabelecidas nos subitens a seguir, observada a matriz de sistemas operacionais suportados constante do subitem 5.4.2.

5.4.1. Solução de proteção avançada para no mínimo 20 servidores.

5.4.2. Compatibilidade com pelo menos os seguintes sistemas operacionais:

5.4.2.1. Microsoft Windows Server 2016.

5.4.2.2. Microsoft Windows Server 2019.

5.4.2.3. Microsoft Windows Server 2022.

5.4.2.4. Red Hat Enterprise Linux 7, 8 e 9.

5.4.2.5. CentOS 7 e CentOS Stream 8 e 9.

5.4.2.6. Oracle Linux 7, 8 e 9.

5.4.2.7. SUSE Linux Enterprise Server 12 e 15.

5.4.2.8. Ubuntu 18.04, 20.04, 22.04 e 24.04.

5.4.2.9. Debian 10, 11 e 12.

5.4.2.10. Cloud Linux 7 e 8.

5.4.2.11. Solaris 11.4 (x86, x64 ou SPARC).

5.4.2.12. Amazon Linux e Amazon Linux 2 (x64).

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

5.4.4. A console de gerenciamento deverá ser em nuvem ou on-premises, permitindo o gerenciamento das políticas de segurança através da Internet.

5.4.5. A solução deverá ser gerenciada por console Web, compatível com pelo menos os browsers Microsoft Edge, Google Chrome e Firefox.

5.4.6. Deve suportar certificado digital para gerenciamento.

5.4.7. A solução deverá permitir a integração com pelo menos as seguintes plataforma de nuvem: Vmware vCloud, Google Cloud, Microsoft Azure e Amazon Web Services (AWS).

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

5.4.9. A solução deverá permitir a entrega de agentes por pelo menos duas dentre as principais ferramentas de distribuição de software do mercado: Microsoft System Center Configuration Manager, Novel Zen Works e Puppet.

5.4.10. A console de administração deverá permitir o envio de notificações via SMTP.

5.4.11. Todos os eventos e ações realizadas na console de gerenciamento precisam ser gravados para fins de auditoria.

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

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

5.4.14. A solução precisa permitir a criação de relatórios. A criação e envio destes relatórios deverá ocorrer sob demanda, ou agendado com o envio automático do relatório via e-mail.

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

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

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

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

5.4.19. A console deve se integrar com diferentes ”Identity Providers” para que os usuários possam administrar a solução de acordo com as permissões.

5.4.20. A solução de segurança ter a capacidade de identificar ataques entre containers.

5.4.21. Os usuários devem ter a capacidade de receber determinados papéis para administração como "acesso total" e "acesso parcial", podendo ser customizado o que compõe o "acesso parcial".

5.4.22. Quando configurado o acesso parcial, este deve permitir que um usuário tenha permissões de poder gerenciar a segurança de um único computador, podendo ainda definir em quais módulos de proteção será possível ou não editar ou criar novas políticas de segurança.

5.4.23. A comunicação entre a console de gerenciamento e os agentes deverá ser criptografada.

5.4.24. Cada agente deverá ter sua própria chave para criptografia de modo que a comunicação criptografada seja feita de forma diferente para cada agente.

5.4.25. A console de gerenciamento deverá ter dashboards para facilidade de monitoração, as quais deverão ser customizadas pelo administrador em quantidade e período de monitoração.

5.4.26. Os agentes de atualização deverão buscar os updates das assinaturas e distribuí-las para os agentes. Quando ocorrer a atualização, esta deverá ocorrer de modo absolutamente seguro utilizando-se SSL/TLS com o servidor de onde ela buscará as informações.

5.4.27. Os agentes para plataforma Microsoft deverão ser instalados por pacote MSI e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente, ou de forma automatizada através de script PowerShell.

5.4.28. Os agentes para plataforma Linux deverão ser instalados por pacote RPM ou DEB e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente, ou de forma automatizada através de bash script.

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

5.4.30. A solução deve possuir a capacidade de criar políticas de forma global para todas as máquinas, por perfis e individualmente para cada host.

5.4.31. Cada perfil poderá ser atribuído para um host ou um conjunto de hosts.

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

5.4.33. A solução deverá mostrar quais máquinas estão usando determinada política.

5.4.34. Os agentes deverão ser capazes de executar rastreamento nas máquinas onde estão instalados e após isso deverão fornecer uma lista de todas as recomendações de segurança para os softwares que estejam instalados nas máquinas bem como do sistema operacional.

5.4.35. Esses rastreamentos devem ocorrer de forma periódica a ser definida pelo administrador.

5.4.36. Brechas de segurança descobertas deverão ser protegidas de forma automática e transparente, interrompendo somente o tráfego de rede malicioso.

5.4.37. O administrador do sistema de segurança deverá ter a possibilidade de não aplicar automaticamente a proteção para as vulnerabilidades escolhendo o perfil ou o host.

5.4.38. A solução deve possuir a capacidade de isolamento de placa de rede de forma que apenas uma fique funcionando de acordo com preferência do administrador.

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

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

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

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

5.4.43. Solução deverá permitir criar relatórios customizados de todas as suas funcionalidades.

5.4.44. As atualizações de assinaturas deverão ocorrer de forma agendada e automática possibilitando ser até mesmo de hora em hora.

5.4.45. Após a atualização deve ser informado o que foi modificado ou adicionado.

5.4.46. Deve ser possível baixar as assinaturas na console de gerenciamento, mas não distribuí-las aos clientes.

5.4.47. A console de gerenciamento deve apresentar a capacidade de gerar roll back de suas atualizações de regras.

5.4.48. A solução deverá ter capacidade de gerar pacote de auto diagnóstico de modo a coletar arquivos relevantes para envio ao suporte do produto.

5.4.49. Deverá ter a capacidade de colocar etiquetas para a ocorrência de determinados eventos de modo a facilitar o gerenciamento, relatórios e visualização.

5.4.50. No gerenciamento de licenças, deve ser informada quantidade contratada e quantidade

em utilização de clientes.

5.4.51. Solução deverá ter mecanismo de procura em sua console de gerenciamento de modo que seja facilitada a busca de regras.

5.4.52. Deverá possuir a capacidade de classificar eventos para que facilite a identificação e a visualização de eventos críticos em servidores críticos.

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

5.4.54. O fabricante deverá participar do programa "Microsoft Application Protection Program" para obtenção de informações de modo a permitir a criação de regras de proteção antes mesmo dos patches serem publicados pelo fabricante.

5.4.55. A console de gerenciamento deve se integrar com o Vmware vCloud, de modo a importar e sincronizar os objetos (hosts vmware e guests vm) para a console de gerenciamento da solução.

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

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

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

5.4.59. Precisa ter a capacidade de detectar e aplicar as regras necessárias dos módulos de IDS/IPS, monitoramento de integridade e inspeção de logs, para cada servidor, de forma automática e sem a intervenção do administrador.

5.4.60. A solução deve permitir desabilitar os módulos individualmente sem a necessidade de desinstalação dos recursos quando desativados.

5.4.61. Precisa ter a capacidade de desabilitar as regras não mais necessárias dos módulos de IDS/IPS, monitoramento de integridade e inspeção de logs, para cada servidor, de forma automática e sem a intervenção do administrador.

5.4.62. Funcionalidade de Antimalware conforme especificações abaixo:

5.4.62.1. A solução deve permitir a proteção contra códigos maliciosos através da instalação de agentes, permitindo rastrear ameaças em tempo real, varredura sob demanda e conforme agendamento, possibilitando a tomada de ações distintas para cada tipo de ameaça.

5.4.62.2. A solução deve possibilitar a criação de listas de exclusão, para que o processo do antivírus não execute a varredura de determinados diretórios ou arquivos do sistema operacional.

5.4.62.3. A solução deve possuir listas de exclusão separadas por módulo da proteção antimalware como exclusão das detecções por comportamento, exclusão por machine learning e exclusão por assinatura.

5.4.62.4. A solução deve possibilitar a verificação de ameaças dentro de arquivos

compactados, efetuando a limpeza apenas de arquivos maliciosos em casos de detecção.

5.4.62.5. A solução deverá possuir a funcionalidade de monitoramento de comportamento para detectar mudanças e atividades suspeitas não autorizadas.

5.4.62.6. A solução deverá oferecer escanear processos em memória em busca de malware.

5.4.62.7. O scan de arquivos comprimidos deverá analisar no mínimo 6 camadas de compressão.

5.4.62.8. O scan de arquivos comprimidos do tipo OLE deverá ser de no mínimo 20 camadas decompressão.

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

5.4.62.10. A solução deverá permitir alterar as ações pré-configuradas para cada tipo de ameaça detectada de acordo com as necessidades da empresa.

5.4.62.11. A solução deverá mostrar informação de data sobre o último scan agendado ou manual executado.

5.4.62.12. Possuir a capacidade de efetuar “download” e “restore” de arquivos comprometidos por Ransomware.

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

5.4.62.14. Deve possibilitar o controle do consumo de recursos durante as varreduras manuais e agendadas a fim de minimizar os impactos de desempenho no servidor.

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

5.4.63. Funcionalidade de Proteção contra URLs maliciosas conforme características abaixo

5.4.63.1. Deve permitir a proteção contra acesso a websites ou URLs consideradas maliciosas ou de baixa reputação.

5.4.63.2. A lista de URLs deve ser fornecida e atualizada automaticamente pelo fabricante permitindo a consulta em uma base local ou na nuvem da reputação das URLs acessadas.

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

5.4.63.4. Deve permitir a criação de listas de exclusão ou permissão, permitindo que usuários acessem ou não determinadas URLs especificadas pelo administrador do sistema.

5.4.63.5. As listas de exceção devem suportar “wildcards”.

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

5.4.63.7. Deverá ter capacidade de identificar acessos a URLs maliciosas além das portas

padrão 80 e 8080.

5.4.63.8. A solução deve permitir que o administrador solicite ao fabricante a reclassificação de uma URL através do site do fabricante para evitar falsos positivos.

5.4.63.9. Deve ser possível customizar a página de bloqueio quando é detectado acesso web malicioso.

5.4.63.10. A solução deve suportar enviar notificações por e-mail ao administrador ao invés de apresentar uma página de bloqueio através do comando “mailto:”.

5.4.64. Funcionalidade de Firewall de Host conforme características abaixo:

5.4.64.1. Operar como firewall de host, através da instalação de agente nos servidores protegidos.

5.4.64.2. Precisa ter a capacidade de controlar o tráfego baseado no Endereço MAC, frame types, tipos de protocolos, endereços IP e intervalo de portas.

5.4.64.3. Precisa ter a capacidade de controlar conexões TCP baseado nas flags TCP.

5.4.64.4. Deve ser capaz de trabalhar em modo “stateful bidirecional” para protocolo TCP.

5.4.64.5. Precisa ter a capacidade de definir configurações de “stateful firewall” distintas para interfaces de rede distintas.

5.4.64.6. A solução deverá ser capaz de reconhecer e possibilitar o bloqueio endereços IP que estejam realizando Network Scan, Port Scan, TCP Null Scan, TCP FYNSYN Scan, TCP Xmas Scan e Computer OS Fingerprint por até 30 minutos.

5.4.64.7. Precisa ter a capacidade de implementação de regras em determinados horários que podem ser customizados pelo administrador.

5.4.64.8. Precisa ter a capacidade de definição de regras para contextos específicos.

5.4.64.9. Para facilitar a criação e administração de regras de firewall, as mesmas poderão se apoiar em objetos que podem ser lista de IPs, lista de MACs, lista de portas.

5.4.64.10. Regras de firewall poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo, se está no domínio ou não).

5.4.64.11. Regras de firewall poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana.

5.4.64.12. O firewall deverá permitir liberar ou apenas logar eventos.

5.4.64.13. O firewall deverá ser passível de criação de regras através do protocolo, origem do tráfego, frame type, TCP header flags, destino e direção.

5.4.64.14. As regras de Firewall deverão ter as seguintes ações, ou equivalentes: Allow, log only, bypass, force allow, deny.

5.4.64.15. A solução, para facilidade de administração, deverá utilizar o conceito de regras implícitas para a regra ALLOW, negando o tráfego para todo o restante que não estiver liberado.

5.4.64.16. As ações também deverão ser possíveis de terem prioridades diferentes, sendo que a prioridade maior prevalece sobre a prioridade menor.

5.4.64.17. Deverá realizar pseudo stateful em tráfego UDP.

5.4.64.18. Deverá logar a atividade stateful.

5.4.64.19. Deverá permitir limitar o número de conexões entrantes e o número de conexões de saída de um determinado computador.

5.4.64.20. Deverá permitir limitar o número de meias conexões vindas de um computador.

5.4.64.21. Deverá prevenir ack storm.

5.4.64.22. Deverão existir regras default que possam ser utilizadas como modelo para a criação e adição de novas regras.

5.4.64.23. Deverá permitir criar listas de exceções para identificar os IPs autorizados a realizar varreduras de portas ou da rede.

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

5.4.65. Funcionalidade de proteção de vulnerabilidades de sistemas operacionais e aplicações.

5.4.65.1. Precisa ter a capacidade de detectar e bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do sistema operacional e demais aplicações.

5.4.65.2. Precisa ter a capacidade de varrer o servidor protegido detectando o tipo e versão do sistema operacional, detectando também as demais aplicações, recomendando e aplicando automaticamente regras IDS/IPS que blindem vulnerabilidades existentes nos sistemas operacionais e aplicações. Esta varredura deverá poder ser executada sob demanda ou agendada.

5.4.65.3. A solução deverá conter regras pré-definidas para detecções de ransonware para as principais famílias deste tipo de malware.

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

5.4.65.5. Precisa conter regras de defesa para blindagem de vulnerabilidades e ataques que explorem os seguintes sistemas operacionais: Windows 2008, 2012, 2016, 2019, 2022, Linux Red Hat, Suse, CentOS, Ubuntu, Debian, Solaris, AIX além de regras para aplicações padrão de mercado, incluindo Microsoft IIS, SQL Server, Microsoft Exchange, Oracle Database, Adobe Acrobat, Mozilla Firefox, Microsoft Edge, Google Chrome e Web Server Apache.

5.4.65.6. Precisa ter a capacidade de armazenamento do pacote capturado quando detectado um ataque.

5.4.65.7. Deverá possibilitar a criação de regras de IPS customizadas, para proteger aplicações desenvolvidas pelo cliente.

5.4.65.8. Precisa possuir a capacidade de detectar e controlar conexões de aplicações específicas incluindo Team Viewer, programas P2P e instant Messaging.

5.4.65.9. Precisa ter a capacidade de detectar e bloquear ataques em aplicações Web tais como SQL Injection e Cross Site Scripting através de configurações customizadas.

5.4.65.10. Deverá permitir customização avançada e criação de novas regras de proteção de aplicações web, protegendo contra vulnerabilidades específicas de sistemas web legados e/ou proprietários.

5.4.65.11. Regras de IDS/IPS poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo se está no domínio ou não).

5.4.65.12. Regras de IDS/IPS poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana.

5.4.65.13. Deverá ser capaz de inspecionar tráfego criptografado de entrada.

5.4.65.14. Deverá inspecionar tráfego de aplicações Web em servidores buscando identificar: SQL injection, Crossite script, tamanho de URI fora de padrão, caracteres fora de padrão para requisição de URI, Double Decoding Exploit.

5.4.65.15. As regras de blindagem contra vulnerabilidades deverão conter links com referências externas, isto quando aplicável, explicando a vulnerabilidade do fabricante ou CVE relacionado.

5.4.65.16. Deverá possibilitar a criação de regras manuais para o bloqueio de tráfego customizado. Como por exemplo, bloquear acesso a um determinado website ou bloquear acesso de uma aplicação X.

5.4.65.17. Deverá possibilitar a criação de regras manuais baseadas em padrão XML, forma de assinatura ou padrões que possuam começo e fim coincidentes.

5.4.65.18. Deverá bloquear tráfego por aplicação independente da porta que a aplicação utilize, de modo que a aplicação não consiga comunicar na rede, como por exemplo, bloqueio de tráfego de uma determinada web browser ou aplicação de backup.

5.4.65.19. Solução deve ser capaz de habilitar modo debug na coleta dos pacotes de forma a capturar o tráfego anterior e posterior ao que foi bloqueado para facilidade de análise.

5.4.65.20. As regras de IPS deverão obrigatoriamente ter descrições de seu propósito.

5.4.65.21. As regras de IPS poderão atuar detectando ou bloqueando os eventos que as violem de modo que o administrador possa optar por qual ação tomar.

5.4.65.22. As regras de IPS de vulnerabilidade deverão apresentar severidade baseada em CVEs e/ou CVSS Score.

5.4.65.23. As regras de IPS poderão ter sua capacidade de LOG desabilitado.

5.4.65.24. As regras de IPS quando disparadas poderão ter a possibilidade de emitir um alerta.

5.4.65.25. As regras devem ser atualizadas automaticamente pelo fabricante.

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

5.4.66. Funcionalidade de monitoramento de integridade.

5.4.66.1. A solução deverá permitir a implantação nas plataformas Linux, Microsoft, Solaris,

HP-UX, AIX, através da instalação de agentes.

5.4.66.2. Precisa ter a capacidade de detectar mudanças de integridade em arquivos e diretórios do sistema operacional e aplicações terceiras.

5.4.66.3. Precisa ser capaz de detectar mudanças no estado de portas em sistemas operacionais Linux.

5.4.66.4. Precisa ter a capacidade de monitorar o status de serviços e processos do sistema operacional.

5.4.66.5. Precisa ter a capacidade de monitorar mudanças efetuadas no registro do Windows.

5.4.66.6. Precisa ter a capacidade de criação de regras de monitoramento em chaves de registro, diretórios e subdiretórios e customização de XML para criação de regras avançadas.

5.4.66.7. Precisa ter a capacidade de varrer o sistema operacional e aplicações, recomendando e aplicando automaticamente regras de monitoramento de acordo com o resultado desta varredura. Esta varredura deverá poder ser executada sob demanda ou agendada.

5.4.66.8. O monitoramento poderá ser realizado em tempo real ou utilizando de scans periódicos para detectar mudanças de integridade.

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

5.4.66.10. Deverá logar e colocar em relatório todas as modificações que ocorram.

5.4.66.11. As regras de monitoramento de integridade deverão ser atualizadas pelo fabricante ou melhoradas de forma automática.

5.4.66.12. Deverá poder classificar as regras de acordo com severidade para melhor verificação nos logs e recebimento de alertas.

5.4.66.13. Deverá possibilitar escolher o diretório onde o arquivo será monitorado e incluir ou não incluir determinados tipos de arquivos dentro desse mesmo diretório.

5.4.66.14. Deve ser possível analisar os objetos monitorados e seu estado monitorado através da console de gerência.

5.4.66.15. Os eventos de mudança em arquivos/diretório devem informar qual usuário realizou a modificação, processo utilizado e qual foi a modificação.

5.4.67. Funcionalidade de inspeção de logs conforme características abaixo:

5.4.67.1. A solução deverá permitir sua implantação nas plataformas Linux, Microsoft, Solaris, HP-UX, AIX.

5.4.67.2. Precisa ter a capacidade de monitorar e inspecionar arquivos de log do sistema operacional e demais aplicações, gravando uma cópia deste log em um banco de dados externo e notificando o administrador sobre eventos suspeitos.

5.4.67.3. Precisa ter a capacidade de varrer o sistema operacional e aplicações,

recomendando e aplicando automaticamente regras de inspeção de logs de acordo com o resultado desta varredura. Esta varredura deverá poder ser executada sob demanda ou agendada.

5.4.67.4. Precisa permitir a criação de regras de inspeção de logs adicionais para auditoria de logs de aplicações terceiras.

5.4.67.5. Precisa permitir a customização de regras existentes, adicionando, removendo ou modificando regras de inspeção de logs.

5.4.67.6. Deverá rastrear e indicar/sugerir ao administrador do sistema quais softwares estão instalados e que possuem logs passíveis de inspeção.

5.4.67.7. Deverá possibilitar a criação de regras de inspeção de logs para aplicações customizadas.

5.4.67.8. Deverá ter inteligência para que a cada violação relevante no log inspecionado que possa comprometer a segurança do ambiente ou do servidor seja alertada.

5.4.67.9. Deverá ter inteligência para que a cada violação relevante no log inspecionado que seja suspeita no servidor seja alertada.

5.4.67.10. Deverá logar cada violação e colocar em relatório todas as violações relevantes que ocorram.

5.4.67.11. As regras poderão ser modificadas por severidade de ocorrência de eventos.

5.4.67.12. As regras devem se atualizar automaticamente pelo fabricante.

5.4.67.13. Permitir modificação pelo administrador em regras para adequação ao ambiente.

5.4.68. Controle de aplicações.

5.4.68.1. A solução deverá permitir sua implantação nas plataformas Linux e Microsoft Windows;

5.4.68.2. A solução, quando habilitada, deverá criar automaticamente um inventário contendo os softwares executáveis, scripts e páginas .php dos servidores.

5.4.68.3. Uma criada o inventário o administrador deverá poder monitorar ou bloquear qualquer novo software que tente se executar nas máquinas protegidas.

5.4.68.4. Deverá ser possível incluir novos softwares automaticamente, abrindo a lista de softwares permitidos de execução sem a necessidade de aprovação do administrador por um período pré-determinado (ex: 10 minutos).

5.4.68.5. Deve permitir criar uma lista global de softwares que não podem ser executados nos servidores através do controle por hash de arquivo.

5.4.68.6. O controle de aplicações deverá ser realizado através de Hash, suportando no mínimo MD5, SHA1 e SHA256.

5.4.68.7. O agrupamento dos eventos deverá ser realizado pelo menos por Hash ou por máquina.

5.4.68.8. A console deverá exibir eventos de no mínimo 30 dias.

5.5. ITEM 05 — Solução de Firewall de Aplicação Web (WAF)

A solução de firewall de aplicação web (Item 05) deverá atender integralmente às especificações estabelecidas nos subitens a seguir.

5.5.1. Prestação de serviços que forneça solução Cloud ou baseada em Appliance físico ou virtual dedicado de firewall de aplicação web

5.5.2. Tráfego de até 200 (duzentos) Mbps total, somando entrada e saída.

5.5.3. Aplicações imediatas a serem protegidas conforme certificado Wildcard para os domínios *.uberaba.mg.gov.br e *.codiub.com.br:

5.5.4. Capacidade de proteger novas aplicações que venham a ser criadas.

5.5.5. O serviço deve ser capaz de aumentar a segurança das aplicações, mitigando riscos a ataques especializados e direcionados às aplicações Web, e também permitir a inspeção do tráfego criptografado.

5.5.6. A solução deve receber o tráfego redirecionado da rede da CONTRATANTE.

5.5.7. A solução oferecida deve proteger a infraestrutura web de ataques contra a camada de aplicação (camada 7).

5.5.8. Deve possuir capacidade de operar até 200 (duzentos) Mbps de tráfego em camada 7, correspondente ao limite de throughput contratado para o serviço, somando entrada e saída.

5.5.9. Deve possuir tecnologia para mitigação de DDoS em camada 7 baseado em análise comportamental, usando o aprendizado.

5.5.10. A solução deve possuir capacidade de automaticamente capturar tráfego no formato TCP Dump relativos a ataques DoS L7, Web Scraping e força bruta permitindo uma análise mais profunda do administrador.

5.5.11. Analisar tráfego HTTP/0.9, HTTP/1.0, HTTP/1.1 e HTTP/2.

5.5.12. Restringir métodos HTTP/HTTPS permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de cookies.

5.5.13. Permitir que novas políticas fiquem apenas monitorando o tráfego, sem bloqueá-lo, indicando caso aconteça algum evento.

5.5.14. Permitir a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes.

5.5.15. A solução deve inspecionar upload de arquivos para os servidores de aplicação.

5.5.16. Remover as mensagens de erro do conteúdo que será enviado aos usuários.

5.5.17. Proteger contra-ataques automatizados, incluindo bots e web scraping, identificando comportamento não humano, navegadores operados por scripts ou qualquer outra forma que não operados por humanos.

5.5.18. Identificar, isolar e bloquear ataques sofisticados sem impactar nas transações das aplicações.

5.5.19. Identificar, isolar e bloquear ataques sofisticados para os protocolos: HTTP e HTTPS.

5.5.20. Permitir a utilização de modelo positivo de segurança para proteger contra- ataques às aplicações HTTP e HTTPS, além de proteger contra-ataques conhecidos aos protocolos HTTP e HTTPS.

5.5.21. Bloquear de imediato o tráfego ou a sessão quando detectada uma tentativa de ataque.

5.5.22. Bloquear com intermediação e interrupção da conexão.

5.5.23. Criar políticas automáticas que bloqueiam o endereço IP que realizar violações.

5.5.24. Utilizar página HTML informativa e personalizável como HTTP Response aos bloqueios.

5.5.25. Configurar políticas de bloqueio baseadas em requisição HTTP, endereço IP e usuário de aplicação.

5.5.26. Apenas transações de aplicações validadas devem ser aceitas, o restante das transações deverá ser bloqueado, utilizando bloqueio por nível de aplicação baseado no contexto da sessão do usuário, com privilégios de autorização diferentes, entradas de usuários e tempo de resposta de aplicação.

5.5.27. Identificar e armazenar o ataque acontecido com detalhes, com as seguintes informações:

5.5.27.1. Nome do ataque.

5.5.27.2. Qual campo foi atacado.

5.5.27.3. Quantas vezes esse ataque foi realizado.

5.5.27.4. Cópia da tentativa do ataque.

5.5.27.5. Horário do ataque.

5.5.27.6. Endereços IP que originaram os ataques.

5.5.28. Armazenar informações de identificação dos usuários autenticados nas aplicações.

5.5.29. Suportar request compression e response compression.

5.5.30. Assinar cookies digitalmente e editar endereços de URL (“URL Rewriting”).

5.5.31. Proteger as aplicações de banco de dados contra-ataques conhecidos, monitorar e controlar os acessos e atividades relacionadas às bases de dados.

5.5.32. Suportar aplicações que utilizem autenticação com estes métodos:

5.5.32.1. Autenticação básica.

5.5.32.2. Certificados SSL.

5.5.33. Para as soluções que utilizam SSL para transferência de dados, os certificados e pares de chaves pública/privada devem ser importados (atuar como man-in- the-middle para tráfego SSL).

5.5.34. Possuir mecanismo de aprendizado automatizado capaz de identificar todos os conteúdos das aplicações, incluindo URLs, parâmetros URLs, campos de formulários, o que se espera de cada campo (tipo de dado, tamanho de caracteres, se é um campo obrigatório e ainda se é somente-leitura), cookies, arquivos XML, ações SOAP, e elementos XML.

5.5.35. Identificar e criar perfil de utilização dos aplicativos, inclusive desenvolvidos em Javascript, CGI, ASP e PHP.

5.5.36. O perfil aprendido de forma automatizada pode ser ajustado, editado ou bloqueado.

5.5.37. Correlacionar múltiplos eventos de segurança em conjunto para distinguir de forma precisa o tráfego permitido do tráfego malicioso.

5.5.38. Identificar ataques baseados em:

5.5.38.1. Assinaturas, com atualização diária da base pelo fabricante.

5.5.38.2. Regras.

5.5.38.3. Perfis de utilização.

5.5.39. Detectar ataques de força bruta por meio dos seguintes métodos:

5.5.39.1. Aumento do tempo de resposta da aplicação monitorada.

5.5.39.2. Quantidade de transações por segundo (TPS), monitorando a quantidade de transações por segundo por endereço IP.

5.5.40. Detectar ataques do tipo força bruta em que:

5.5.40.1. O atacante solicita repetidamente o mesmo recurso.

5.5.40.2. O atacante realiza repetidas tentativas não autorizadas de acesso.

5.5.40.3. São utilizados ataques automatizados de login.

5.5.41. Detectar ataques do tipo força bruta que explorem:

5.5.41.1. Controles de acesso da aplicação (Erro 401 – Unauthorized).

5.5.41.2. Solicitações repetidas ao mesmo recurso, em qualquer parte/URL da aplicação.

5.5.41.3. Aplicações WEB que não retornam o erro 401 por meio da identificação de expressão regular no retorno/página de erro da aplicação).

5.5.41.4. Gerenciamento de sessão (muitas sessões de um único endereço IP ou a um range de IPs).

5.5.41.5. Clientes automatizados (robôs, requisições muito rápidas).

5.5.42. Possuir mecanismo para criação dinâmica de política de segurança, com aprendizado automático de padrão de utilização da aplicação, realizado sobre o fluxo de tráfego bi-direcional atravessando o equipamento.

5.5.43. Filtrar e validar funções XML específicas da aplicação.

5.5.44. Possibilitar atualização conhecidos de novas assinaturas para ataques.

5.5.45. Apresentar proteção positiva e segura contra-ataques, como:

5.5.45.1. Anonymous Proxy Vulnerabilities.

5.5.45.2. Brute Force Login.

5.5.45.3. Buffer Overflow.

5.5.45.4. Cookie Injection.

5.5.45.5. Cookie Poisoning.

5.5.45.6. Cross Site Request Forgery (CSRF).

5.5.45.7. Cross Site Scripting (XSS).

5.5.45.8. Data Destruction.

5.5.45.9. Directory Traversal.

5.5.45.10. Form Field Tampering.

5.5.45.11. HTTP Denial of Service.

5.5.45.12. HTTP parameter pollution.

5.5.45.13. HTTP hidden field manipulation.

5.5.45.14. HTTP request smuggling.

5.5.45.15. Illegal Encoding.

5.5.45.16. Known Worms.

5.5.45.17. Malicious Robots.

5.5.45.18. OS Command Injection.

5.5.45.19. Parameter Tampering.

5.5.45.20. Remote File Inclusion Attacks.

5.5.45.21. Sensitive Data Leakage (Social Security Numbers, Cardholder Data, PII, HPI).

5.5.45.22. Session Hijacking.

5.5.45.23. Site Reconnaissance.

5.5.45.24. SQL Injection.

5.5.45.25. Web Scraping.

5.5.45.26. Web server software and operating system attacks.

5.5.45.27. Web Services (XML) attacks.

5.5.46. Permitir configurar com granularidade, por aplicação protegida, restrições de métodos HTTP permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de cookies;

5.5.47. Permitir definir regras de tamanho para upload de arquivos pelo método PUT, com as seguintes restrições:

5.5.47.1. Tamanho por arquivo.

5.5.47.2. Tamanho por conjunto de arquivos.

5.5.47.3. Quantidade de arquivos.

5.5.48. Criação das políticas deve possuir as formas:

5.5.48.1. Automático por meio da observação do tráfego para a aplicação.

5.5.48.2. Automático por meio da observação do tráfego de teste.

5.5.48.3. Manual.

5.5.49. Suportar os seguintes critérios de decisão para realizar bloqueio o gerar alerta, sendo que uma política pode conter um ou mais critérios simultaneamente:

5.5.49.1. Tempo de resposta de uma página web.

5.5.49.2. Tamanho da resposta de uma página web.

5.5.49.3. User-agent (navegador)

5.5.49.4. Usuário

5.5.49.5. Horário.

5.5.49.6. IP de origem.

5.5.49.7. Assinatura de ataque.

5.5.49.8. Conteúdo do payload.

5.5.49.9. Conteúdo do cabeçalho.

5.5.49.10. Conteúdo da cookie.

5.5.49.11. Código de response.

5.5.49.12. Hostname.

5.5.49.13. Tipo de protocolo (HTTP ou HTTPS).

5.5.49.14. Parâmetro.

5.5.49.15. Número de ocorrências em determinado intervalo de tempo.

5.5.49.16. Método HTTP.

5.5.50. Permitir criação de assinaturas de ataques.

5.5.51. Reconhecer assinaturas seletivas, e filtros de ataque que devem proteger contra:

5.5.51.1. Ataques de negação de serviços automatizados.

5.5.51.2. Worms e vulnerabilidades conhecidas.

5.5.51.3. Requests em objetos restritos.

5.5.52. Prevenir contra vazamentos dos códigos dos servidores.

5.5.53. Proteger contra as 10 maiores vulnerabilidades da lista OWASP.

5.5.54. A solução oferecida deve possuir mecanismo de aprendizado automático e possuir funcionalidade de criação automática de políticas, onde a política de segurança é criada e atualizada automaticamente baseando-se no tráfego real observado à aplicação.

5.5.55. Exportar requisições que contém os ataques, nos formatos PDF e CSV.

5.5.56. Realizar localização geográfica do IP, identificando país de origem da requisição.

5.5.57. Aprender o comportamento da aplicação:

5.5.57.1. Campos, valores, cookies e URLs,

5.5.57.2. Políticas sugeridas somente devem ser aplicadas após um período configurável.

5.5.58. Inspecionar e monitorar até a camada de aplicação, todo o tráfego de dados HTTP, incluindo cabeçalhos, campos de formulários e conteúdo, além de inspecionar os requests e responses.

5.5.59. As checagens devem ser realizadas em todos os tipos de entrada de dados, como URLs, formulários, cookies, campos ocultos e parâmetros, consultas (query), métodos HTTP,

elementos XML e ações SOAP.

5.5.60. Proteger contra mensagens XML e SOAP malformadas.

5.5.61. Utilizar o campo HTTP X-Forwarded-For sem modificar seu conteúdo de origem, permitindo a diferenciação em ambientes com NAT.

5.5.62. Suportar SSL offload.

5.5.63. Emitir os seguintes relatórios:

5.5.63.1. Gráfico indicando tipo de ataque.

5.5.63.2. Gráfico indicando tipo de violação.

5.5.63.3. Gráfico indicando quais URLs foram atacadas.

5.5.63.4. Gráfico indicando severidade.

5.5.63.5. Gráfico indicando os endereços IPs de origem.

5.5.63.6. Gráfico indicando a localização geográfica dos endereços IPs de origem.

5.5.64. Permitir a seleção de período para emissão dos relatórios, sendo que devem estar disponíveis os dados dos últimos 30 (trinta) dias.

5.5.65. Permitir a geração das seguintes informações, por período:

5.5.65.1. Auditoria detalhada das alterações de configuração efetuadas, indicando usuário, ação e horário;

5.5.65.2. Informações estatísticas de quantidade de conexões completadas e bloqueadas.

5.5.65.3. Informações estatísticas de fluxo de tráfego.

5.5.65.4. Informações estatísticas de quantidade de sessões ou conexões.

6. DO MODELO DE EXECUÇÃO DO OBJETO

6.1. Da abrangência dos serviços de implantação

Os serviços de implantação abrangem a totalidade dos componentes do objeto (Itens 01 a 05), independentemente de a CONTRATADA ser ou não a atual prestadora dos serviços, contemplando a instalação, a configuração e a migração, no formato “como está” (as is), das políticas, perfis e regras em produção, observado o seguinte:

6.1.1. A CONTRATADA deverá entregar todos os componentes instalados, configurados e em pleno funcionamento, responsabilizando-se pela instalação, pelos ajustes e pela aplicação das melhores práticas em todos os itens que compõem o objeto;

6.1.2. A execução terá início a partir do recebimento da ordem de serviço, emitida pela CONTRATANTE após a assinatura do contrato, observados os marcos e prazos do item 6.3;

6.1.3. Os serviços de implantação, incluída a operação assistida, não ensejarão cobrança adicional, estando compreendidos no preço contratado.

6.2. Da migração no formato “como está” (as is)

A migração preservará as configurações vigentes, conforme as etapas mínimas:

6.2.1. Levantamento e documentação das configurações vigentes (firewalls, gestão/logs, proteção de servidores e WAF);

6.2.2. Elaboração do plano de migração, submetido à aprovação prévia da CONTRATANTE;

6.2.3. Configuração e homologação prévia em ambiente controlado;

6.2.4. Execução da janela de corte (cutover) em horário de menor impacto;

6.2.5. Plano de retorno (rollback) previamente definido, apto a restaurar os serviços à condição anterior;

6.2.6. Validação funcional e homologação final, com aceite formal.

6.2.7. A migração deverá ser conduzida sem interrupção não planejada dos serviços, vedada a redução do escopo de proteção vigente, devendo a CONTRATADA entregar à CONTRATANTE, ao final, a documentação das configurações implantadas.

6.3. Do cronograma e prazos de implantação

A CONTRATADA observará os marcos mínimos a seguir, cujos prazos serão detalhados no plano de implantação aprovado:

6.3.1. Reunião de partida (kickoff) e apresentação do plano;

6.3.2. Entrega, instalação e configuração dos equipamentos e componentes;

6.3.3. Homologação prévia das configurações migradas;

6.3.4. Execução da janela de corte (cutover) e entrada em produção;

6.3.5. Validação funcional, homologação final e recebimento definitivo.

6.3.6. A CONTRATADA deverá iniciar a prestação dos serviços no prazo de 10 (dez) dias, contados do recebimento da ordem de serviço, observando-se, quanto aos demais marcos, os prazos estabelecidos no plano de implantação aprovado pela CONTRATANTE.

6.4. Da contingência (equipamentos de reserva)

Em caso de falha ou defeito físico dos equipamentos em produção, a CONTRATADA deverá manter o ambiente operacional mediante equipamentos provisórios de reserva, até que a substituição definitiva seja concluída, sem ônus adicional para a CONTRATANTE e observados os níveis de serviço estabelecidos no item 8.2.

6.5. Do local de prestação dos serviços

As soluções deverão ser instaladas e configuradas nos endereços indicados pela CONTRATANTE, observadas as localidades de destinação dos firewalls definidas no item 5.1.

6.6. Do recebimento provisório e definitivo

6.6.1. O recebimento provisório será formalizado por termo, ao término da instalação, configuração e migração de cada componente, para efeito de posterior verificação da

conformidade;

6.6.2. A CONTRATANTE verificará minuciosamente a conformidade dos serviços e das configurações migradas com as especificações deste Termo de Referência e com a proposta, comunicando por escrito à CONTRATADA eventuais imperfeições, falhas ou irregularidades;

6.6.3. Constatada desconformidade, a CONTRATADA deverá promover a correção, o reparo ou a substituição no prazo de até 5 (cinco) dias corridos, contados do recebimento da comunicação, sem prejuízo das sanções aplicáveis;

6.6.4. O recebimento definitivo será formalizado por termo de aceite, após a validação funcional integral de todos os componentes (Itens 01 a 05) e a comprovação do pleno funcionamento das políticas e perfis migrados, momento em que se considerará concluída a implantação;

6.6.5. O recebimento provisório ou definitivo não exclui a responsabilidade da CONTRATADA pela perfeita execução do objeto, nos termos contratuais e legais.

7. DO MODELO DE GESTÃO DO CONTRATO

7.1. Da gestão e da fiscalização do contrato

A execução do contrato será acompanhada, coordenada e fiscalizada por gestor e fiscal formalmente designados pela CONTRATANTE e nomeados no instrumento contratual, aos quais competirá acompanhar, controlar e avaliar a execução, atestar a efetiva prestação dos serviços e dirimir as dúvidas que surgirem em seu curso, nos termos do Regulamento Interno de Licitações e Contratos - RILC e da legislação aplicável.

7.1.1. Compete ao gestor do contrato:

7.1.1.1. Acompanhar o cumprimento das obrigações contratuais e a manutenção, pela CONTRATADA, das condições de habilitação e qualificação exigidas na contratação;

7.1.1.2. Controlar o prazo de vigência e adotar tempestivamente as providências relativas à prorrogação, à alteração ou ao encerramento do contrato;

7.1.1.3. Consolidar as informações prestadas pela fiscalização e deliberar sobre as questões que excedam a alçada do fiscal;

7.1.1.4. Dar ciência à autoridade competente das irregularidades verificadas na execução, para as providências cabíveis.

7.1.2. Compete ao fiscal do contrato:

7.1.2.1. Anotar, em registro próprio nos autos do processo, todas as ocorrências relacionadas à execução do contrato;

7.1.2.2. Verificar se a prestação dos serviços observa o pactuado, quanto a especificações, quantitativos, capacidades e prazos;

7.1.2.3. Aferir o cumprimento dos níveis de serviço estabelecidos no item 8.2, com base nos registros de chamados e nos relatórios de que trata o item 7.3;

7.1.2.4. Esclarecer as dúvidas que estiverem sob sua alçada e comunicar formalmente ao gestor as irregularidades identificadas;

7.1.2.5. Atestar as faturas, condicionado o atesto à efetiva e regular prestação dos serviços no período.

7.1.3. A CONTRATANTE manterá atualizada a designação do gestor e do fiscal, promovendo a respectiva substituição nos autos do processo em caso de férias, afastamento, impedimento ou desligamento, sem solução de continuidade da fiscalização.

7.1.4. A responsabilidade dos agentes designados perdurará até o encerramento do contrato.

7.1.5. A fiscalização exercida pela CONTRATANTE não exclui nem reduz a responsabilidade da CONTRATADA, inclusive perante terceiros, por quaisquer irregularidades, e, na sua ocorrência, não implica corresponsabilidade da CONTRATANTE.

7.2. Do preposto da CONTRATADA

7.2.1. A CONTRATADA indicará formalmente, até o início da execução, preposto qualificado para representá-la perante a CONTRATANTE, informando nome, qualificação e meios de contato, competindo-lhe responder pelas comunicações e pelas providências relativas à execução do contrato.

7.2.2. A substituição do preposto deverá ser comunicada previamente e por escrito à CONTRATANTE.

7.3. Dos instrumentos de acompanhamento e controle

7.3.1. A CONTRATADA permitirá e oferecerá condições para a ampla e completa fiscalização dos serviços contratados, fornecendo as informações solicitadas, inclusive as de natureza técnica, e propiciando o acesso à documentação pertinente e aos serviços em execução;

7.3.2. A CONTRATANTE, por meio do gestor e do fiscal, terá acesso, a qualquer tempo, à inspeção do objeto e dos documentos relativos à execução, admitida a realização de auditoria, diretamente ou por terceiro por ela indicado;

7.3.3. A CONTRATADA disponibilizará canais formais para abertura, acompanhamento e encerramento de chamados, com registro, numeração única e manutenção de histórico, na forma do item 8.1;

7.3.4. A CONTRATADA apresentará relatório periódico de execução contendo, no mínimo, os chamados abertos e encerrados no período, os respectivos tempos de atendimento e de solução, as ocorrências relevantes e a demonstração do cumprimento dos níveis de serviço;

7.3.5. Serão realizadas reuniões de acompanhamento entre a CONTRATANTE e a CONTRATADA, em periodicidade definida pela gestão do contrato e com registro em ata,

destinadas a avaliar a qualidade dos serviços, o cumprimento dos níveis de serviço e a resolução de pendências.

8. DO SUPORTE, GARANTIA E NÍVEIS DE SERVIÇO

8.1. Do suporte técnico

A CONTRATADA prestará suporte técnico e assistência técnica, por telefone e por meio eletrônico, incluída a operação assistida do conjunto fornecido e a substituição de peças e equipamentos, durante todo o prazo de vigência contratual, observado o seguinte:

8.1.1. Entende-se por suporte a solução de falhas e de dúvidas, a operação assistida, a aplicação de patches e atualizações, os reparos de funcionalidades ou de sistema operacional e as demais demandas de ordem lógica;

8.1.2. Entende-se por assistência técnica o serviço de manutenção corretiva, de reparo e de substituição de equipamentos e peças, sem ônus adicional para a CONTRATANTE;

8.1.3. A abertura de chamados e o respectivo atendimento serão realizados em língua portuguesa, por meio de atendimento telefônico gratuito (0800) ou de número local do Município de Uberaba/MG (DDD 34), bem como por correio eletrônico ou portal web próprio, admitido número ilimitado de chamados;

8.1.4. A CONTRATADA disponibilizará sistema de help desk online para abertura e acompanhamento de chamados, devendo cada chamado ser armazenado e identificado por numeração única, com manutenção do histórico de todos os chamados abertos e encerrados, acessível à CONTRATANTE;

8.1.5. O portal de abertura de chamados deverá manter os dados da CONTRATANTE sigilosos e criptografados, inclusive em sua transmissão (SSL/HTTPS), observado o disposto no item 4.4;

8.1.6. Os chamados que exigirem a presença física de profissional da CONTRATADA nas dependências da CONTRATANTE deverão ser previamente agendados, de segunda a sexta-feira, das 08h00 às 18h00, ou em outros horários previamente acordados entre as partes, sem custo adicional ao contrato.

8.2. Dos níveis de serviço (SLA)

Os serviços observarão, no mínimo, os níveis de serviço a seguir estabelecidos, aferidos pelo fiscal do contrato na forma do item 7.1.2.3:

8.2.1. Prazo de resposta inicial, assim entendido o registro do chamado e a comunicação de seu recebimento à CONTRATANTE: até 4 (quatro) horas, em regime 8x5 (oito horas por dia, cinco dias por semana, de segunda a sexta-feira);

8.2.2. Prazo para início do atendimento técnico, assim entendido o efetivo início dos trabalhos de diagnóstico e tratamento: até 24 (vinte e quatro) horas corridas, contadas da abertura

do chamado;

8.2.3. Prazo para solução do problema: até 72 (setenta e duas) horas corridas, contadas da abertura do chamado;

8.2.4. Tempo máximo de parada total, até que seja adotada solução definitiva ou provisória que restabeleça a operação: até 16 (dezesseis) horas comerciais;

8.2.5. Prazo para substituição de produto que não atenda às especificações do objeto: até 5 (cinco) dias corridos, contados do recebimento da solicitação;

8.2.6. O descumprimento dos níveis de serviço estabelecidos neste item, apurado com base nos registros de chamados e nos relatórios de que trata o item 7.3.4, repercutirá no atesto da fatura, na forma do item 12.2.1, e sujeitará a CONTRATADA às sanções previstas no Item 15, assegurados o contraditório e a ampla defesa.

8.3. Da garantia e da contingência

8.3.1. A garantia abrange a substituição de todos os produtos com mau funcionamento, por conta e responsabilidade integral da CONTRATADA, durante todo o prazo de vigência contratual;

8.3.2. Em caso de defeito físico, a CONTRATADA manterá o ambiente operacional com equipamentos provisórios até que as peças ou os equipamentos definitivos estejam disponíveis para substituição, observado o disposto no item 6.4;

8.3.3. A CONTRATADA é responsável pela instalação, pelos ajustes e pela aplicação das melhores práticas em todos os itens que compõem o objeto, durante toda a vigência contratual.

9. DAS OBRIGAÇÕES DAS PARTES

9.1. Das obrigações da CONTRATANTE

São obrigações da CONTRATANTE, sem prejuízo das demais previstas neste Termo de Referência e no instrumento contratual:

9.1.1. Receber o objeto no prazo e nas condições estabelecidos neste Termo de Referência;

9.1.2. Verificar minuciosamente a conformidade dos serviços e dos bens recebidos com as especificações deste Termo de Referência e com a proposta, para fins de aceitação e recebimento definitivo;

9.1.3. Comunicar à CONTRATADA, por escrito, as imperfeições, falhas ou irregularidades verificadas no objeto, para que sejam corrigidas, reparadas ou substituídas;

9.1.4. Acompanhar e fiscalizar o cumprimento das obrigações da CONTRATADA, por meio do gestor e do fiscal do contrato;

9.1.5. Prestar as informações e os esclarecimentos solicitados pela CONTRATADA e proporcionar as condições necessárias à execução do objeto;

9.1.6. Efetuar o pagamento à CONTRATADA no valor correspondente à prestação dos serviços, no prazo e na forma estabelecidos na Item 12;

9.1.7. A CONTRATANTE não responderá por quaisquer compromissos assumidos pela CONTRATADA com terceiros, ainda que vinculados à execução do contrato, nem por dano causado a terceiros em decorrência de ato da CONTRATADA, de seus empregados, prepostos ou subordinados.

9.2. Das obrigações da CONTRATADA

São obrigações da CONTRATADA, sem prejuízo das demais previstas neste Termo de Referência e no instrumento contratual:

9.2.1. Prover os recursos necessários à prestação dos serviços e entregar todos os componentes instalados, configurados e em pleno funcionamento, na forma do item 6.1.1;

9.2.2. Executar os serviços em conformidade com as especificações técnicas, funcionais e de qualidade estabelecidas, observando rigorosamente os prazos fixados e as normas técnicas aplicáveis;

9.2.3. Fornecer, por todo o período contratual, os equipamentos, o software, o licenciamento, a garantia, o suporte e as atualizações de todos os componentes do objeto, na forma do item 4.3;

9.2.4. Fornecer e atualizar, sem ônus adicional, todas as licenças de software, vacinas de antivírus/antimalware e assinaturas dos serviços de proteção;

9.2.5. Manter as soluções atualizadas durante toda a vigência, compreendendo atualizações de versão, correções de defeitos e atualização contínua das assinaturas;

9.2.6. Dar ciência à CONTRATANTE, imediatamente e por escrito, de qualquer anormalidade verificada na execução dos serviços;

9.2.7. Manter preposto qualificado para representá-la perante a fiscalização, na forma do item 7.2;

9.2.8. Executar diretamente o contrato, sem transferência de responsabilidade ou subcontratação não previamente autorizada pela CONTRATANTE;

9.2.9. Responder pelos encargos trabalhistas, previdenciários, fiscais e comerciais decorrentes da execução, bem como pelas despesas de frete, transporte, tributos, seguros e demais custos indispensáveis ao cumprimento do objeto;

9.2.10. Assumir integral responsabilidade civil, administrativa e penal por quaisquer prejuízos pessoais ou materiais causados à CONTRATANTE ou a terceiros, por si, por seus empregados, prepostos ou sucessores, na execução do objeto;

9.2.11. Manter, durante toda a execução do contrato, todas as condições de habilitação e qualificação exigidas na contratação;

9.2.12. Aceitar integralmente os métodos e processos de inspeção, verificação e controle

adotados pela CONTRATANTE, cuja existência e atuação não restringem a responsabilidade da CONTRATADA quanto ao objeto contratado;

9.2.13. Abster-se de contratar, durante a vigência contratual, empregado pertencente ao quadro de pessoal da CONTRATANTE.

9.3. Da confidencialidade e da proteção de dados pessoais (LGPD)

A CONTRATADA obriga-se, por si e por seus empregados e prepostos, a atuar em conformidade com a Lei nº 13.709/2018 (LGPD) e com as demais normas de proteção de dados e de segurança da informação, observado o disposto no item 4.4 e, em especial:

9.3.1. Tratar como confidenciais todos os dados e informações a que tiver acesso em razão do contrato, ainda que após o encerramento do vínculo contratual, ressalvadas as informações comprovadamente de domínio público;

9.3.2. Informar à CONTRATANTE, imediatamente após tomar conhecimento, de qualquer incidente de segurança, exposição, descumprimento das disposições legais de proteção de dados ou requisição de autoridade que envolva dados sob tratamento;

9.3.3. Adotar medidas técnicas e administrativas de segurança aptas a proteger os dados de acessos não autorizados e de situações de destruição, perda, alteração, comunicação ou difusão indevidas;

9.3.4. Promover, ao término da vigência, a devolução e a eliminação segura dos dados sob sua custódia, na forma do item 4.2.6;

9.3.5. A inobservância das obrigações previstas neste item sujeitará a CONTRATADA à reparação dos danos, sem prejuízo das responsabilidades administrativa, civil e penal cabíveis.

10. DA QUALIFICAÇÃO TÉCNICA

Para fins de habilitação técnica, a licitante deverá apresentar a documentação a seguir relacionada, destinada a comprovar a aptidão para o desempenho de atividade pertinente e compatível com o objeto, nos termos da Lei nº 13.303/2016 e do Regulamento Interno de Licitações e Contratos - RILC:

10.1. Declaração emitida pelo fabricante das soluções ofertadas, ou por seu representante legal no País, atestando que a licitante é revenda ou parceira autorizada de seus produtos e serviços, admitida a apresentação de declaração por fabricante, quando o objeto contemplar soluções de fabricantes distintos;

10.2. Atestado, ou atestados, de capacidade técnica, emitidos por pessoa jurídica de direito público ou privado, que comprovem a prestação, pela licitante, de serviços compatíveis em características, quantidades e prazos com o objeto desta contratação, admitido o somatório de atestados;

10.3. Os atestados deverão conter a identificação do emitente, a descrição dos serviços prestados, o período de execução e os meios de contato para eventual diligência, facultada à CONTRATANTE a verificação da veracidade das informações e a realização de diligências, na forma do item 4.5.2;

10.4. A comprovação das funcionalidades, capacidades e demais características técnicas das soluções ofertadas observará o disposto no item 4.5.2, mediante documentação técnica oficial do fabricante;

10.5. As exigências de qualificação técnica limitam-se ao indispensável à garantia do cumprimento das obrigações, sendo vedada a exigência de quantitativos, prazos ou requisitos que restrinjam indevidamente a competitividade do certame;

10.6. Não serão exigidos quantitativos mínimos nos atestados de capacidade técnica, bastando que os serviços neles descritos guardem compatibilidade em características, quantidades e prazos com o objeto desta contratação, na forma do item 10.2 e observado o disposto no item 10.5.

11. DA ESTIMATIVA DE PREÇOS E DA DOTAÇÃO ORÇAMENTÁRIA

11.1. Da estimativa de preços

O valor estimado da contratação será apurado mediante pesquisa de preços realizada em conformidade com a Lei nº 13.303/2016 e com o Regulamento Interno de Licitações e Contratos - RILC, utilizando-se, sempre que possível de forma combinada, as seguintes fontes:

11.1.1. Contratações similares celebradas por órgãos e entidades da Administração Pública, obtidas por meio de portais, painéis e sistemas oficiais de compras, com preços atualizados;

11.1.2. Pesquisa publicada em mídia especializada, em sítios eletrônicos especializados ou de domínio amplo, com indicação da data e do endereço de consulta;

11.1.3. Pesquisa direta junto a, no mínimo, 3 (três) fornecedores do ramo de atividade compatível com o objeto, mediante solicitação formal de cotação, com registro da data da consulta e da resposta;

11.1.4. Contratações anteriores da própria CONTRATANTE, com os devidos ajustes e atualizações monetárias;

11.1.5. O valor estimado será calculado com base na média, na mediana ou no menor dos valores obtidos, conforme metodologia justificada pela área competente, devendo ser desconsiderados os valores manifestamente desproporcionais em relação aos demais;

11.1.6. O orçamento estimado poderá ter caráter sigiloso, nos termos do art. 34 da Lei nº 13.303/2016, hipótese em que a informação será disponibilizada aos órgãos de controle externo e interno, sem prejuízo de sua divulgação após o encerramento da fase de lances;

11.1.7. O valor estimado da contratação e a respectiva planilha de composição por item

constam dos autos do processo administrativo, observado o disposto no item 11.1.6.

11.2. Da dotação orçamentária

11.2.1. As despesas correrão à conta de recursos próprios, na conta contábil 3.1.1.1.02.0008 - Mensalidade de Licença de Software.

12. DAS CONDIÇÕES DE PAGAMENTO E DO REAJUSTE

12.1. Da medição e da apresentação da nota fiscal

12.1.1. Os serviços serão remunerados mediante parcelas mensais, correspondentes à efetiva prestação no período, iniciando-se a contagem a partir do recebimento definitivo de que trata o item 6.6.4;

12.1.2. A nota fiscal ou fatura deverá ser apresentada à CONTRATANTE até o 5º (quinto) dia do mês subsequente ao da prestação dos serviços, acompanhada do relatório de execução de que trata o item 7.3.4;

12.1.3. A nota fiscal eletrônica ou documento equivalente deverá ser encaminhada por meio eletrônico ao endereço indicado pela CONTRATANTE, devendo a CONTRATADA informar o número da conta corrente, a agência e o banco para o respectivo pagamento.

12.2. Da liquidação e das condições para o pagamento

12.2.1. O pagamento fica condicionado ao atesto da nota fiscal pelo fiscal do contrato, nos termos do item 7.1.2.5, mediante verificação da efetiva e regular prestação dos serviços e do cumprimento dos níveis de serviço estabelecidos no item 8.2;

12.2.2. O pagamento somente será liberado mediante comprovação da regularidade fiscal e trabalhista da CONTRATADA, compreendendo as certidões negativas, ou positivas com efeito de negativas, relativas aos tributos federais e à dívida ativa da União, aos tributos estaduais e municipais, ao Fundo de Garantia por Tempo de Serviço (FGTS) e aos débitos trabalhistas (CNDT);

12.2.3. O pagamento será efetuado no prazo de até 20 (vinte) dias, contados da data de entrega, aceitação e certificação da nota fiscal, mediante ordem bancária em conta corrente indicada pela CONTRATADA;

12.2.4. A nota fiscal não aprovada será devolvida à CONTRATADA para as correções necessárias, com a indicação dos motivos da rejeição, contando-se o prazo de pagamento da data de sua reapresentação, sem que a devolução caracterize atraso imputável à CONTRATANTE;

12.2.5. As multas eventualmente aplicadas serão descontadas do pagamento a que fizer jus a CONTRATADA, na forma do item 15.2.8;

12.2.6. A CONTRATANTE poderá promover a retenção preventiva dos créditos devidos, quando

necessária para evitar prejuízo decorrente do inadimplemento de obrigações trabalhistas, previdenciárias, fiscais ou comerciais resultantes da execução do contrato;

12.2.7. No preço contratado consideram-se incluídos todos os custos necessários à perfeita execução do objeto, compreendendo equipamentos, licenciamento, assinaturas, atualizações, suporte, frete, seguros, tributos, encargos e demais despesas, na forma dos itens 4.3.4 e 6.1.3;

12.2.8. As demais condições de pagamento, notadamente os encargos decorrentes de eventual atraso imputável à CONTRATANTE e as vedações relativas à cessão de crédito e ao desconto de títulos, observarão o disposto no instrumento convocatório e na minuta do contrato.

12.3. Do reajuste e do reequilíbrio econômico-financeiro

12.3.1. Os preços contratados poderão ser reajustados anualmente, mediante aplicação da variação acumulada do INPC/IBGE, ou de outro índice que venha a substituí-lo, observada a periodicidade mínima de 1 (um) ano, nos termos do art. 2º, § 1º, da Lei nº 10.192/2001, contada da data de apresentação da proposta;

12.3.2. O reajuste dependerá de solicitação da CONTRATADA e não retroagirá a períodos anteriores, operando-se a preclusão na hipótese de prorrogação contratual sem a respectiva postulação;

12.3.3. Fica assegurado o restabelecimento do equilíbrio econômico-financeiro do contrato na hipótese de fato imprevisível, ou previsível de consequências incalculáveis, que onere ou desonere substancialmente as obrigações pactuadas, mediante requerimento fundamentado e devidamente comprovado.

13. DO CRITÉRIO DE JULGAMENTO E ADJUDICAÇÃO

13.1. O julgamento observará o critério de menor preço global, correspondente à soma dos valores de todos os componentes do objeto, em coerência com o agrupamento em item único de que trata o item 3.3;

13.2. Será declarada vencedora a licitante que ofertar o menor preço global, desde que atendidas integralmente as especificações e as condições estabelecidas neste Termo de Referência;

13.3. A proposta deverá contemplar a totalidade dos Itens 01 a 05, sendo desclassificada aquela que deixar de cotar qualquer deles ou que apresente cotação parcial do objeto;

13.4. Nos preços ofertados deverão estar computados todos os custos necessários à execução do objeto, na forma do item 12.2.7, não se admitindo pleito posterior de acréscimo sob alegação de erro, omissão ou custo não previsto;

13.5. A CONTRATANTE poderá promover diligências destinadas a aferir a conformidade técnica das soluções ofertadas, podendo exigir da licitante a apresentação de documentação

técnica complementar do fabricante, na forma do item 4.5.2;

13.6. As demais regras de julgamento, notadamente as relativas à desclassificação de propostas, à aferição de inexequibilidade, aos critérios de desempate, à adjudicação e à homologação, observarão o disposto no instrumento convocatório, na Lei nº 13.303/2016 e no Regulamento Interno de Licitações e Contratos - RILC.

14. DA VIGÊNCIA CONTRATUAL

14.1. O contrato terá vigência de 60 (sessenta) meses, contados do recebimento da ordem de serviço de que trata o item 6.1.2, com fundamento no art. 71 da Lei nº 13.303/2016, prazo que se alinha ao horizonte de suporte, garantia e atualização das soluções e confere previsibilidade e continuidade à proteção do ambiente;

14.2. A vigência poderá ser prorrogada, mediante termo aditivo, nos termos da Lei nº 13.303/2016 e do Regulamento Interno de Licitações e Contratos - RILC, desde que demonstrada, nos autos, a vantajosidade da prorrogação e mantidas as condições e os preços praticados;

14.3. A manutenção das condições de habilitação e qualificação exigidas na contratação, na forma do item 9.2.11, constitui requisito para a prorrogação;

14.4. O contrato poderá ser extinto antecipadamente nas hipóteses previstas na Lei nº 13.303/2016 e no Regulamento Interno de Licitações e Contratos - RILC, assegurados o contraditório e a ampla defesa, notadamente em razão de inexecução total ou parcial das obrigações, de razões de interesse público devidamente justificadas ou de caso fortuito ou força maior regularmente comprovado;

14.5. Encerrada a vigência, por qualquer motivo, a CONTRATADA prestará à CONTRATANTE o apoio necessário à transição dos serviços, promovendo a devolução e a eliminação segura dos dados sob sua custódia, na forma dos itens 4.2.6 e 9.3.4, de modo a assegurar a continuidade da proteção do ambiente.

15. DAS SANÇÕES ADMINISTRATIVAS

Pela inexecução total ou parcial das obrigações assumidas, garantidos o contraditório e a ampla defesa, a CONTRATADA sujeita-se às sanções previstas na Lei nº 13.303/2016 e no Regulamento Interno de Licitações e Contratos - RILC, sem prejuízo das responsabilidades civil e penal cabíveis. A dosimetria das sanções, o processo administrativo sancionador, os prazos de defesa e de recurso e o registro das penalidades observarão o disposto no instrumento convocatório, na Lei nº 13.303/2016 e no Regulamento Interno de Licitações e Contratos – RILC.

15.1. Das espécies de sanções

15.1.1. Advertência, cabível quando o ato praticado, ainda que irregular, não seja suficiente para acarretar dano à CONTRATANTE, às suas instalações, a pessoas, à sua imagem ou a

terceiros;

15.1.2. Multa, na forma do item 15.2;

15.1.3. Suspensão temporária de participação em licitação e impedimento de contratar com a CONTRATANTE, por prazo não superior a 2 (dois) anos;

15.1.4. Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a autoridade que aplicou a sanção.

15.2. Das multas

As multas poderão ser aplicadas isolada ou cumulativamente com as demais sanções, observados os seguintes parâmetros:

15.2.1. Recusa injustificada em assinar o contrato ou retirar o instrumento equivalente, no prazo estabelecido: até 10% (dez por cento) sobre o valor estimado da contratação;

15.2.2. Infração a qualquer cláusula contratual, dobrada na reincidência: 2% (dois por cento) sobre o valor estimado da contratação;

15.2.3. Atraso na execução, até o 15º (décimo quinto) dia: 0,2% (dois décimos por cento) sobre o valor total do contrato, por dia de atraso;

15.2.4. Descumprimento das especificações técnicas ou atraso superior a 15 (quinze) dias: 10% (dez por cento) sobre o valor total do objeto;

15.2.5. Descumprimento dos níveis de serviço estabelecidos no item 8.2: 2% (dois por cento) sobre o valor da parcela mensal, por nível de serviço descumprido no período, sem prejuízo da repercussão no atesto da fatura, na forma do item 8.2.6;

15.2.6. Inexecução parcial: 20% (vinte por cento) sobre o valor da parcela não executada;

15.2.7. Inexecução total: 30% (trinta por cento) sobre o valor total do contrato;

15.2.8. As multas não possuem caráter compensatório e não excluem as perdas e danos resultantes, podendo os respectivos valores ser descontados dos pagamentos devidos à CONTRATADA ou cobrados judicialmente.

16. DAS DISPOSIÇÕES FINAIS

16.1. Disposições gerais

Aplicam-se à presente contratação as seguintes disposições gerais:

16.1.1. Este Termo de Referência e os demais documentos da contratação são complementares entre si, de modo que o detalhe mencionado em um e omitido em outro considera-se especificado e válido;

16.1.2. Em caso de divergência entre os documentos da contratação, prevalecerão, sucessivamente, o instrumento contratual, o edital, este Termo de Referência e a proposta da CONTRATADA;

16.1.3. As normas disciplinadoras da contratação serão interpretadas em favor da ampliação da disputa entre os interessados, preservados o interesse público, o princípio da isonomia, a finalidade e a segurança da contratação;

16.1.4. A CONTRATANTE poderá, a qualquer tempo, promover diligências destinadas a esclarecer ou complementar a instrução do processo, bem como introduzir aditamentos, modificações ou revisões, nos termos da legislação aplicável e do Regulamento Interno de Licitações e Contratos - RILC;

16.1.5. Os casos omissos serão resolvidos à luz da Lei nº 13.303/2016, do Regulamento Interno de Licitações e Contratos - RILC e das demais normas aplicáveis;

16.1.6. As matérias de natureza procedimental e contratual apenas referenciadas neste Termo de Referência, notadamente as relativas ao julgamento das propostas, às condições de pagamento, à vigência, às sanções administrativas e ao foro, deverão ser integralmente disciplinadas no instrumento convocatório e na minuta do contrato, observada a ordem de prevalência estabelecida no item 16.1.2.

Uberaba/MG, 03 de setembro de 2026.

Companhia de Desenvolvimento de Informática de Uberaba – Codiub
Luciano Rodrigo Ferreira
Diretor de TI