TERMO DE REFERÊNCIA

1. DO OBJETO

1.1. Contratação de empresa especializada para prestação de serviços continuados de Sistema Integrado de segurança, Firewall, anti-malware/anti-exploit/anti-ransomware, com Central de Gerenciamento conforme quantidades da tabela abaixo e condições e exigências estabelecidas neste Termo de Referência.

Grupo único			
Item	**Descrição**	**Qtd**	**Período**
1	Firewall (*Next-Generation* Firewall) para proteção de informação perimetral e de rede interna que inclui *stateful Firewall* para operar em alta disponibilidade (HA) em modo ativo-passivo ou ativo-ativo, conforme especificações detalhadas no item 4.2 e seus subitens. Alta disponibilidade requer no mínimo 2 equipamentos para trabalhar em redundância.	2	36 Meses
2	Fornecimento de licenças de uso de solução corporativa de *Endpoint Detection and Response/eXtended Detection and Response* (EDR/XDR) para estações de trabalho com gerência em nuvem e integração nativa com o Firewall, conforme especificações detalhadas no item 4.3 e seus subitens.	220	36 Meses
3	Fornecimento de licenças de uso de solução corporativa de *Endpoint Detection and Response/eXtended Detection and Response* (EDR/XDR) para servidores com gerência em nuvem e integração nativa com o Firewall, conforme especificações detalhadas no item 4.3 e seus subitens.	5	36 Meses
4	Treinamento oficial do fabricante para a equipe técnica, com Certificação Oficial, conforme especificações detalhadas no item 4.5 e seus subitens.	4	Único
5	Instalação, configuração e testes, conforme especificações detalhadas no item 4.5 e seus subitens.	1	Único

1.2. A contratação se dará pelo menor preço por grupo único, composto por 5 itens.

1.3. A contratação será efetivada por meio da assinatura de instrumento de contrato administrativo, cuja **vigência será de 36 meses**, prorrogável por até 10 anos, na forma dos artigos 106 e 107 da Lei n.° 14.133/2021.

1.4. Para fins de incentivo à concorrência, o orçamento desta contratação deverá ser sigiloso.

2. DA JUSTIFICATIVA

2.1. Dos motivos para a contratação

2.1.1. A contratação se justifica para o atendimento da necessidade de incrementar

a segurança, o controle e o monitoramento da infraestrutura de rede da Câmara Municipal de Londrina (CML). Dessa forma, foi realizado um Estudo de Viabilidade Técnica (ETP) para analisar os aspectos técnicos que justificam a necessidade da CML realizar a contratação desses serviços.

2.1.2. Conforme Painel de Ataques Cibernéticos do *Security Leaders*[1], que realiza levantamento dos casos mais impactantes reportados de ataques cibernéticos, os órgãos públicos seguem como os setores mais visados pelos cibercriminosos. Considerando apenas os ataques realizados e reportados à órgãos públicos, a lista a seguir mostra os locais que sofreram algum tipo de ataque, seja no Portal/Site da Instituição, ou nos sistemas de informação existentes:

- Cibercriminoso invade CNJ e publica falso mandado de prisão contra Alexandre de Moraes.
- Câmara Municipal de Curitiba (ataque a sistema terceirizado)
- Ministério Público do Estado do Amazonas (ataque ao sistema eletrônico do Diário Oficial)
- Correios (Vazamento de dados)
- Prefeitura de Poços de Caldas (ataque aos sistemas e ao Portal)
- Conselho Federal da Ordem dos Advogados do Brasil (CFOAB)
- Prefeitura de Capão da Canoa (ataque aos servidores)
- Instituto Nacional de Pesquisas Espaciais-INPE (ataque ao site)
- Universidade Federal do Delta do Parnaíba-UFDpar (ataque ao site)
- Agência Nacional de Água e Saneamento Básico-ANA (ataque aos sistemas)
- Prefeitura de Taboão da Serra (ataque ao Portal)
- Prefeitura de Araguari (exclusão de dados no sistema de gestão)
- Câmara Municipal de Salvador (ataque ao site)
- Site da Prefeitura de Suzano (ataque ao site)
- Universidade Federal da Mato Grosso do Sul (ataque ao sistemas)
- Prefeitura Municipal de Jacarezinho (ataque ao sistema)
- Prefeitura de Dourados (ataque ao site)
- Tribunal de Contas do estado do Rio de Janeiro (ataque ao sistemas)
- Perfis de redes sociais da PF e da PRF
- Prefeitura de São José dos Pinhais (ataque ao sistema administrativo)
- Prefeitura de Macapá (ataque ao Perfil oficial no Facebook)
- Hospital Universitário da USP (ataque aos sistemas)
- Secretaria de Educação e Esportes de Pernambuco (invasão no Datacenter)

[1] https://securityleaders.com.br/painel-de-incidentes-orgaos-publicos-sao-principais-alvos-dos-ciberataques/

- Sites governamentais do estado de Tocantins
- Tribunal de Justiça do Pará

2.1.3. Vale ainda destacar que esses foram apenas alguns ataques que foram reportados, porém, a grande maioria dos ataques não são reportados.

2.1.4. A Câmara Municipal de Londrina (CML) também recebe ataques frequentes ao Portal da Instituição, até o momento, sem vazamento de dados ou indisponibilidade do sistema.

2.1.5. Sendo assim, diante dos ataques constantes e da necessidade de atualização tecnológica das ferramentas de proteção de dados e de infraestrutura de Firewall da Câmara Municipal de Londrina (CML), o Departamento de Informática realizou ETP para analisar as opções disponíveis para incrementar a segurança virtual da CML diante do cenário futuro e dos novos desafios que se apresentam.

2.1.6. Além disso, convém destacar que a CML possui contrato de solução de *endpoint* finalizando em outubro de 2024. Dessa forma, conforme ETP realizado, o Departamento de Informática analisou as opções disponíveis e concluiu que a opção mais adequada é a contratação de solução que possua integração nativa dos dispositivos de *endpoint* com o Firewall.

2.1.7. A Câmara Municipal de Londrina (CML) com o objetivo de realizar adequações para atendimento a Lei Geral de Proteção de Dados Pessoais (LGPD)[2], contratou consultoria do SENAI/PR (Inexigibilidade de Licitação n. 01/2024). Entre as atividades desenvolvidas pelo SENAI, foi realizada a criação de nova Política de Segurança para a CML com o objetivo de garantir a proteção da privacidade e a segurança das informações existentes na CML.

2.1.8. Diante desse contexto, o investimento em infraestrutura de segurança é essencial para a implantação efetiva da Política de Segurança na CML, de forma a minimizar a possibilidade de ocorrência de perdas de dados e indisponibilidades dos recursos computacionais.

2.1.9. Vale ainda destacar a necessidade da CML adequar-se em relação ao cumprimento à Lei Federal nº 13.709/2018 (Lei Geral de Proteção de Dados), Lei Federal nº 12.965/2014, Decreto Federal nº 8.771/2016 que regulamenta o Marco Civil da Internet e demais legislações Federais ou Municipais relativas à matéria. Dessa forma, é necessário que exista o controle das conexões à Internet, permitindo a gestão completa das informações acessadas pelos usuários nas infraestruturas de rede disponibilizadas pela CML.

2.1.10. Para atender integralmente às necessidades da CML, optou-se pelo agrupamento

[2]Lei Nacional nº 13.709, de 14 de agosto de 2018.

dos itens em lote único, considerando que (i) é importante garantir que os equipamentos, sistemas e demais componentes sejam entregues, instalados e configurados simultaneamente para garantir o perfeito funcionamento dos equipamentos e evitar possíveis prejuízos à Casa; (ii) Diversos grupos potencializam o risco de problemas associados à entrega, como alfândega, atraso no pedido do fabricante, entre outros. Dessa forma, pretende-se reduzir os conflitos operacionais entre as possíveis contratadas, que podem resultar em atraso na implantação da infraestrutura, bem como em tempo elevado para a solução de problemas técnicos relacionados à garantia dos equipamentos; (iii) Existe a necessidade de solução integrada, e o fornecimento dos itens por fornecedores distintos pode prejudicar o atendimento à esse requisito; (iv) Finalmente, cabe ressaltar que a contratação dos equipamentos em um único item não restringe o caráter competitivo do procedimento licitatório, já que os itens possuem natureza similar e conforme pesquisas de mercado, os licitantes possuem a capacidade de fornecer a totalidade dos equipamentos especificados no item, sem prejuízo para a competitividade.

2.1.11. Além disso, para realizar a contratação desses itens, optou-se pela contratação de Infraestrutura como Serviço (IasS). Esse tipo de contratação justifica-se pelos motivos listados a seguir: (i) **Economia** em relação à aquisição de todos os equipamentos e sistemas necessários; (ii) **Escalabilidade**, que permite que os recursos sejam incrementados facilmente, caso seja necessário; (iii) Agilidade e facilidade na realização de **manutenções e Gerenciamento dos equipamentos e sistemas.**

2.2. Justificativa do quantitativo

2.2.1. A opção de contratação pelo período de 36 (trinta e seis) meses, prorrogáveis por até 10 anos, justifica-se por tratar de sistema essencial para manter a segurança e o controle da infraestrutura de rede da Câmara Municipal de Londrina. Sendo assim, considerando-se o caráter continuado do serviço, a opção pela vigência inicial de 36 (trinta e seis) meses possibilita obtenção de melhores condições comerciais para a contratação.

2.2.2. Além disso, a implantação da infraestrutura necessária para a execução do projeto envolve aquisição de equipamentos específicos que possuem custo alto, necessidade de realização de adequações e treinamento para equipe técnica e para os usuários comuns. Dessa forma, a contratação por período menor pode resultar em desvantagem econômica para a CML, já que o investimento necessário para implantação e operacionalização do projeto é relativamente alto.

2.3. Critérios de desenvolvimento sustentável adotados

2.3.1. Os serviços prestados deverão pautar-se sempre no uso racional de recursos e equipamentos, de forma a evitar e prevenir o desperdício de insumos e materiais consumidos, bem como a geração excessiva de resíduos.

2.3.2. Com relação aos equipamentos disponibilizados na prestação dos serviços, somente será admitida a oferta de bens de informática e/ou automação que não contenham substâncias perigosas em concentração acima da recomendada na diretiva RoHS (Restriction of Certain Hazardous Substances), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr (VI)), cádmio (Cd), bifenil polibromados (PBBs), éteres difenil-polibromados (PBDEs).

2.4. Do plano anual de contratação

2.4.1. Este Termo de Referência está em conformidade com o planejamento do Departamento de Informática apresentado para composição do Plano Anual de Contratações.

3. DOS REQUISITOS DA CONTRATAÇÃO

3.1. A **proposta** encaminhada pela empresa deverá especificar marca e modelo de todos os equipamentos, softwares e licenças que compõem a solução apresentada, **acompanhada de catálogos e documentação técnica** que comprovem a adequação às especificações descritas neste Termo de Referência, especialmente:

3.1.1. Apresentação de **planilha** contendo, ponto a ponto, a comprovação das especificações dos equipamentos e sistemas solicitados nos itens 4.2 e 4.3, juntamente com datasheets, links do fabricante, documentos oficiais, etc, a fim de checar a veracidade desta comprovação.

3.2. Como requisito de **qualificação técnica** será exigido do licitante melhor classificado a apresentação dos itens listados a seguir:

3.2.1. A apresentação de **atestado de capacidade técnica**, expedido por pessoa jurídica de direito público ou privado, devidamente assinado, comprovando, no mínimo:

3.2.1.1. O fornecimento de solução de Firewall (Next-Generation Firewall), com as especificações técnicas, além da instalação e configuração de solução similar à ofertada.

3.2.1.2. O fornecimento pelo menos 110 endpoints com integração nativa ao Firewall.

3.3. Como **Qualificação Técnico-Profissional**, será exigido do vencedor:

3.3.1. A comprovação de que possui em seu quadro de funcionários, pelo menos, 1 (um) funcionário com certificação profissional na solução ofertada, podendo ser feita mediante

registro em Carteira de Trabalho e Previdência Social ou apresentação de Contrato Social ou Contrato de Prestação de Serviços.

4. DAS ESPECIFICAÇÕES TÉCNICAS DOS EQUIPAMENTOS

4.1. Requisitos Gerais: os requisitos listados neste item referem-se aos itens 1 e 2 do presente Termo de Referência.

4.1.1. Para os itens que representem bens materiais, a Contratada deverá fornecer produtos novos, sem uso anterior.

4.1.2. O hardware e o software fornecidos não podem constar, no momento da apresentação da proposta, em listas de *end-of-sale*, *end-of-support*, *end-of-engineering-support* ou *end-of-life* do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante.

4.1.3. Caso o hardware durante a execução do contrato entre em listas de *end-of-sale*, *end-of-support*, *end-of-engineering-support* ou *end-of-life* do fabricante, a Contratada/fabricante terá que manter a garantia e o suporte dos equipamentos durante o período do contrato. Após o fim da vigência inicial de 60 (sessenta) meses, em caso de renovação pelo mesmo período, a Contratada deverá realizar a substituição de todos os equipamentos para os modelos e padrões vigentes na época da renovação.

4.1.4. Todos os equipamentos de rede deverão possuir certificado de homologação expedido pela Agência Nacional de Telecomunicações (ANATEL).

4.1.5. Todos os acessórios (cabos, conectores, *patch cords*, braçadeiras, parafusos e demais componentes) necessários para o perfeito funcionamento das soluções propostas nos itens 1 e 2 deste Termo de Referência deverão ser fornecidos pela Contratada.

4.1.6. Todas as licenças necessárias para garantir o perfeito funcionamento das soluções solicitadas nos itens 1, 2 e 3 deste Termo de Referência deverão ser fornecidas pela Contratada.

4.2. FIREWALL (*NEXT-GENERATION FIREWALL*): Next-Generation Firewall (NGFW) para proteção de informação perimetral e de rede interna que inclui *stateful* firewall com capacidade para operar em alta disponibilidade (HA) em modo ativo-passivo ou ativo-ativo para controle de tráfego de dados por identificação de usuários e por camada 7, com controle de aplicação, administração de largura de banda (QoS), VPN IPsec e SSL, IPS, prevenção contra ameaças de vírus, *malwares*, Filtro de URL, criptografia de email, inspeção de tráfego criptografado e proteção de firewall de aplicação Web. Deverá ser fornecido um console de

gerenciamento dos equipamentos e centralização de logs em nuvem.

4.2.1. **Características Gerais:**

4.2.2. A solução deve consistir de *appliance* de proteção de rede com funcionalidades de *Next Generation Firewall* (NGFW), e console de gerência, monitoração e logs.

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

4.2.3.1. As funcionalidades de proteção de rede que compõem a plataforma de segurança, podem funcionar em múltiplos *appliances* desde que obedeçam a todos os requisitos desta especificação.

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

4.2.3.3. Os softwares fornecidos na solução deverão estar atualizados na versão mais recente.

4.2.4. Uma interface completa de comando de linha (*CLI command-line-interface*) deverá ser acessível através da interface gráfica e via porta serial.

4.2.4.1. A atualização de software deverá enviar avisos de atualização automáticos.

4.2.4.2. O sistema de objetos deverá permitir a definição de redes, serviços, *hosts* períodos de tempos, usuários e grupos, clientes e servidores.

4.2.4.3. O *backup* e o restabelecimento de configuração deverão ser feitos localmente, via FTP ou email com frequência diária, semanal ou mensal, podendo também ser realizado por demanda.

4.2.4.4. O firewall deverá ser *stateful*, com inspeção profunda de pacotes.

4.2.4.5. Deve possuir suporte aos roteamentos estáticos, dinâmico (RIP, BGP e OSPF, OSPFv3) e multicast (PIM-SM e IGMP) e deve suportar roteamento BGP com uso de IPv6.

4.2.4.6. A solução deverá permitir configurar os serviços de DNS, Dynamic DNS, DHCP e NTP.

4.2.4.7. O *traffic shapping* (QoS) deverá ser baseado em rede ou usuário.

4.2.4.8. A solução deve permitir o tráfego de cotas baseados por usuários para upload/download e pelo tráfego total, sendo cíclicas ou não-cíclicas.

4.2.4.9. Deve possuir otimização em tempo real de voz sobre IP.

4.2.4.10. Para cada *appliance* físico que compõe a plataforma de segurança, entende-se o hardware, software e as licenças necessárias para o seu funcionamento.

4.2.4.11. Não serão aceitos equipamentos servidores e sistema operacional de uso

genérico adaptados para serem utilizados como Firewall.

4.2.4.12. Deve possuir processadores próprios e para fins específicos, desenvolvidos exclusivamente pelo fabricante da solução, com a finalidade de processar tráfegos de redes e acelerar o processamento destes pacotes de redes, permitindo o uso de diversas funcionalidades de segurança ao mesmo tempo sem diminuir a performance do equipamento.

4.2.4.13. Por alta disponibilidade (HA) entende-se que a solução deverá ser composta ao menos por dois *appliances*, licenciados para funcionamento em redundância, em modo ativo-passivo, ou ativo-ativo e deve possibilitar a monitoração de falha de link.

4.2.4.14. A solução deverá contemplar a totalidade das capacidades exigidas, sendo permitido o uso de mais de um equipamento (sempre em modo de alta disponibilidade HA) para complementar a solução, caso o fabricante não possua todas as funções em um único equipamento.

4.2.4.15. Caso a solução ofertada ofereça link dedicado para gerenciamento de HA, deverá suportar interfaces LAG e VLAN para o link HA dedicado e interfaces VLAN para links monitorados.

4.2.4.16. Cada *appliance* deverá ser capaz de executar a totalidade das capacidades exigidas para cada função, não sendo aceitos somatórias para atingir os limites mínimos.

4.2.5. **Características de Hardware e Desempenho**

4.2.5.1. Deve possibilitar montagem em rack padrão 19", acompanhado de todos os acessórios para perfeita fixação.

4.2.5.2. Deve possuir fontes de alimentação redundantes, internas ao equipamento, 100-240 VAC.

4.2.5.3. Deverá possuir armazenamento interno de no mínimo 120 (cento e vinte) GB SSD para sistema operacional, quarentena local, logs e relatórios.

4.2.5.4. Possuir processador de Fluxo do tipo NPU para aceleração de pacotes.

4.2.5.5. Possuir no mínimo 8 (oito) interfaces de rede 1000Base-TX.

4.2.5.6. Possuir no mínimo 2 (duas) interfaces 10GbE SFP+.

4.2.5.7. Deve ser compatível com módulos do mesmo fabricante com no mínimo as seguintes opções: GbE RJ45, GbE SFP fiber e 10 GbE SFP+ fiber.

4.2.5.8. Deve suportar até 16 (Dezesseis) interfaces em sua capacidade máxima de expansão usando os módulos do mesmo fabricante;

4.2.5.9. Deve possuir no mínimo 1 (uma) interface do tipo console ou similar.

4.2.5.10. Performance mínima de 27.000 Mbps de *throughput* para firewall.

4.2.5.11. Performance mínima de 5.000 Mbps de *throughput* de IPS.
4.2.5.12. Performance mínima de 3.500 Mbps de *throughput* para controle de NGFW.
4.2.5.13. Performance mínima de 1.500 Mbps de *throughput* de *Threat Protection*.
4.2.5.14. Performance mínima de 13.000 Mbps de *throughput* de IPsec VPN.
4.2.5.15. Suporte a, no mínimo, 3.000.000 de conexões simultâneas.
4.2.5.16. Suporte a, no mínimo, 145.000 novas conexões por segundo.
4.2.5.17. Possuir o número irrestrito quanto ao máximo de usuários licenciados.

4.2.6. **LAN, VLAN, WAN e SD-WAN**

4.2.6.1. Deve suportar no mínimo 6 (seis) conexões do tipo WAN.
4.2.6.2. O balanceamento de link WAN deve permitir múltiplas conexões de links Internet, checagem automática do estado de links, *failover* automático e balanceamento por peso.
4.2.6.3. Deve possuir tecnologia de conectividade SD-WAN.
4.2.6.4. A funcionalidade SD-WAN deve suportar conectividade com o Secure SD-WAN oferecido no serviço Microsoft Azure Virtual WAN.
4.2.6.5. Deve suportar perfis de SD-WAN para balancear a carga das conexões entre as interfaces.
4.2.6.6. Deve possuir métodos de balanceamento: round-robin e persistência de sessão com no mínimo as seguintes opções: conexão, IP de origem e IP de destino.
4.2.6.7. Deve suportar a configuração de nível mínimo de qualidade (latência, jitter e perda de pacotes) para que determinado link seja escolhido pelo SDWAN.
4.2.6.8. Deve suportar o uso de links de interfaces físicas, sub-interfaces lógicas de VLAN e túneis IPSec.
4.2.6.9. Deve gerar log de eventos que registrem alterações no estado dos links do SD-WAN, monitorados pela checagem de saúde.
4.2.6.10.
4.2.6.11. A solução de SD-WAN deve ser capaz de apresentar de forma gráfica, todos os dados de análise da saúde dos links, contendo gráficos que apresentam no mínimo os critérios de Latência, Jitter e Packet Loss. Os gráficos devem ser apresentados em tempo real e possibilitar a visualização histórica de pelo menos 24 horas, 48 horas, 1 semana e 1 mês.
4.2.6.12. A solução deve possuir funcionalidade de criação da malha SD-WAN em diversos firewalls em um único concentrador. Esta funcionalidade deve facilitar a configuração do SD-WAN de múltiplos firewalls, criando automaticamente todas as

informações necessárias para que o SD-WAN aconteça, mas não se limitando a: criação de rotas, regras de firewall, objetos e túneis VPNs necessárias;

4.2.6.13. A mesma console do concentrador de SD-WAN deve monitorar os links de cada dispositivo implementado, garantindo uma visualização única de todos os dispositivos implementados.

4.2.6.14. Deve possibilitar o roteamento baseado em VPNs.

4.2.6.15. Deve suportar criar políticas de roteamento, permitindo pelo menos as seguintes condições: Interface de entrada do pacote, IPs de origem e destino, Portas de destino, usuário e aplicação em camada 7.

4.2.6.16. Deve ser possível escolher um gateway primário e um gateway de backup para as políticas de roteamento.

4.2.6.17. Deve suportar a definição de VLANs no firewall conforme padrão IEEE 802.1q e tagging de VLAN.

4.2.6.18. Deve suportar Extended VLAN.

4.2.6.19. A solução deverá permitir *port-aggregation* de interfaces de firewall suportando o protocolo 802.3ad, para escolhas entre aumento de *throughput* e alta disponibilidade de interfaces.

4.2.6.20. Deve permitir a configuração de *jumbo frames* nas interfaces de rede.

4.2.6.21. Deve permitir a criação de um grupo de portas layer2.

4.2.6.22. A Solução física deverá apresentar compatibilidade com modens USB (3G/4G), onde apenas seja acionado na eventualidade de falha no link principal.

4.2.6.23. Deve implementar o protocolo de negociação *Link Aggregation Control Protocol* (LACP).

4.2.7. **Controle por Políticas**

4.2.7.1. Deve suportar pelo menos os controles por: porta e protocolos TCP/UDP, origem/destino e identificação de usuários.

4.2.7.2. O controle de políticas deverá monitorar as políticas de redes, usuários, grupos e tempo, bem como identificar as regras não-utilizadas, desabilitadas, modificadas e novas políticas.

4.2.7.3. As políticas deverão ter controle de tempo de acesso por usuário e grupo, sendo aplicadas por zonas, redes e por tipos de serviços.

4.2.7.4. Deve possibilitar pelo menos o controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.

4.2.7.5. Deve permitir o controle de políticas por países via localização por IP,

suporte a objetos e regras IPv6 e suporte a regras *multicast*.

4.2.8. **Prevenção de Ameaças**

4.2.8.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus, *Anti-Malware* e Firewall de Proteção Web (WAF) integrados no próprio *appliance* de Firewall ou entregue em múltiplos *appliances* desde que obedeçam a todos os requisitos desta especificação.

4.2.8.2. Deve realizar a inspeção profunda de pacotes para prevenção de intrusão (IPS) e deve incluir assinaturas de prevenção de intrusão (IPS).

4.2.8.3. As assinaturas de prevenção de intrusão (IPS) devem ser customizadas.

4.2.8.4. Deve possibilitar criar regras de exceções por usuário, grupo de usuários, IP de origem ou de destino.

4.2.8.5. Deve suportar granularidade nas políticas de IPS Antivírus e *Anti-Malware*, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens, com customização completa.

4.2.8.6. A solução contratada deve realizar a emulação de *malwares* desconhecidos em ambientes de sandbox em nuvem.

4.2.8.7. Para a eficácia da análise de *malwares* Zero-Day, a solução de Sandbox deve possuir algoritmos de inteligência artificial, como algoritmos baseados em *machine learning.*

4.2.8.8. A funcionalidade de sandbox deve atuar como uma camada adicional ao motor de anti-malware, e ao fim da análise do artefato, deverá gerar um relatório contendo o resultado da análise, bem como os *screenshots* das telas dos sistemas emulados pela plataforma.

4.2.8.9. Deve permitir configuração da exclusão de tipos de arquivos para que não sejam enviados para o sandbox em nuvem.

4.2.8.10. A proteção *Anti-Malware* deverá bloquear todas as formas de vírus, web *malwares*, *trojans* e *spyware* em HTTP e HTTPS, FTP e *web-emails*.

4.2.8.11. A proteção *Anti-Malware* deverá realizar a proteção com emulação *JavaScript*.

4.2.8.12. Deve ter proteção em tempo real contra novas ameaças criadas.

4.2.8.13. Deve permitir o bloqueio de vulnerabilidades.

4.2.8.14. Deve permitir o bloqueio de *exploits* conhecidos.

4.2.8.15. Deve detectar e bloquear o tráfego de rede que busque acesso a *command and control* e servidores de controle utilizando múltiplas camadas de DNS, AFC e

firewall.

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

4.2.8.17. Deve ser imune e capaz de impedir ataques básicos como: SYN flood, ICMP flood, UDP Flood e demais ataques similares.

4.2.8.18. Deve suportar bloqueio de arquivos por tipo.

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

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

4.2.8.21. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas de segurança considerando uma das opções ou a combinação de todas elas: usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por usuários, grupos de usuários, origem, destino, zonas de segurança.

4.2.8.22. O firewall de aplicação Web (WAF) deverá ter a função de *reverse proxy*, com a função de URL *hardening* realizando *deep-linking* e prevenção dos ataques de *path* traversal ou *directory* traversal.

4.2.8.23. O firewall de aplicação Web (WAF) deverá realizar *cookie signing* com assinaturas digitais, roteamento baseado por caminho, autenticações reversas e básicas para acesso do servidor.

4.2.8.24. O firewall de aplicação Web (WAF) deve suportar a criação de politicas baseadas em Geolocalização (Geo IP)

4.2.8.25. Deve fornecer a capacidade de impedir que os usuários acessem recursos protegidos por uma política WAF de um país especificado ou de endereços IP que não podem ser associados a um país específico.

4.2.8.26. Deve permitir que o administrador do WAF defina e implante cifras mais seguras enquanto exclui cifras que eles consideram menos seguras.

4.2.8.27. Deve possuir proteção de detecção de tipo MIME, um cabeçalho usado para informar ao navegador do cliente para desativar a detecção de tipo MIME.

4.2.8.28. O firewall de aplicação Web (WAF) deverá possuir a função de balanceamento de carga de visitantes por múltiplos servidores, com a possibilidade de modificação dos parâmetros de performance do WAF e permissão e bloqueio de faixas de IP.

4.2.8.29. Deverá permitir a identificação dos IPs de origem através de proxy via *X*-

forward headers.

4.2.8.30. Alternativamente, será aceito uma solução de WAF baseada em máquina virtual do mesmo fabricante capaz de tratar 20 Mbps de tráfego HTTP para compor a solução.

4.2.8.31. Deve possuir proteção pelo menos contra os seguintes ataques, mas não limitado a: *SQL injection* e *Cross-site scripting*.

4.2.9. **Controle e Proteção de Aplicações**

4.2.9.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações por assinaturas e camada 7, utilizando portas padrões (80 e 443), portas não padrões, *port hopping* e túnel através de tráfego SSL encriptado.

4.2.9.2. Deve ser possível inspecionar os pacotes criptografados com os algoritmos SSL 2.0, SSL 3.0 e TLS 1.3.

4.2.9.3. O motor de inspeção dos pacotes criptografados deve ser configurável e permitir definir ações como não decriptografar, negar o pacote e criptografar para determinadas conexões criptografadas.

4.2.9.4. Reconhecer pelo menos 2.300 aplicações diferentes, classificadas por nível de risco, características e tecnologia, incluindo, mas não limitado a tráfego relacionado a *peer-to-peer*, redes sociais, acesso remoto, atualização de software, serviços de rede, VoIP, *streaming* de mídia, proxy e tunelamento, mensageiros instantâneos, compartilhamento de arquivos, web e-mail.

4.2.9.5. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de *payload* para checagem de assinaturas de aplicações conhecidas pelo fabricante.

4.2.9.6. Deve atualizar a base de assinaturas de aplicações automaticamente.

4.2.9.7. Deve reconhecer aplicações em IPv6.

4.2.9.8. Limitar a banda usada por aplicações (*traffic shaping*).

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

4.2.9.10. Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras.

4.2.9.11. Deve permitir o uso individual de diferentes aplicativos para usuários que

pertencem ao mesmo grupo de usuários, sem que seja necessária a mudança de grupo ou a criação de um novo grupo. Os demais usuários deste mesmo grupo que não possuírem acesso a estes aplicativos devem ter a utilização bloqueada.

4.2.10. **Controle e Proteção WEB**

4.2.10.1. Deve permitir a criação de políticas por usuários, grupos de usuários, IPs e redes.

4.2.10.2. Deve permitir especificar política de navegação Web por tempo, ou seja, a definição de regras para um determinado dia da semana e horário de início e fim, permitindo a adição de múltiplos dias e horários na mesma definição de política por tempo. Esta regra de tempo pode ser recorrente ou em uma única vez.

4.2.10.3. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via LDAP, *Active Directory*, Azure AD, Radius, E-directory e base de dados local.

4.2.10.4. Deve permitir popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório.

4.2.10.5. Deve possuir pelo menos 90 categorias de URLs, possibilitar a criação de categorias personalizadas e suportar a criação de políticas baseadas no controle por URL e categoria de URL.

4.2.10.6. Deve ser capaz de forçar o uso da opção Safe Search em sites de busca e forçar as restrições do Youtube.

4.2.10.7. Deve ser capaz de categorizar as URLs a partir de base ou cache de URLs locais ou através de consultas dinâmicas na nuvem do fabricante, independentemente do método de classificação a categorização não deve causar atraso na comunicação visível ao usuário.

4.2.10.8. Deve suportar a opção de bloqueio de categoria HTTP e liberação da categoria apenas em HTTPS.

4.2.10.9. Deve ser possível reconhecer o pacote HTTP independentemente de qual porta esteja sendo utilizada.

4.2.10.10. Deve salvar nos logs as informações adequadas para geração de relatórios indicando usuário, tempo de acesso, bytes trafegados e site acessado.

4.2.10.11. Deve permitir realizar análise flow dos pacotes, entendendo exatamente o que aconteceu com o pacote em cada checagem.

4.2.10.12. Deve ser possível realizar caching do conteúdo web.

4.2.10.13. Deve realizar filtragem por mime-type, extensão e tipos de conteúdo ativos, tais como, mas não limitado a: *ActiveX*, *applets* e *cookies*.

4.2.10.14. Deve ser possível realizar a liberação de cotas de navegação para os usuários, permitindo que os usuários tenham tempos pré determinados para acessar sites na internet. A console de gerenciamento deve possibilitar a visualização do tempo restante para cada usuário, bem como reiniciar o tempo restante com o intuito de zerar o contador.

4.2.10.15. Deve possuir capacidade de alguns usuários previamente selecionados realizarem um *bypass* temporário na política de bloqueio atual.

4.2.10.16. A solução deve permitir o *enforce* dos domínios do Google e Office365 a fim de determinar em quais domínios os usuários poderão se autenticar.

4.2.11. **Identificação de Usuários**

4.2.11.1. 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, autenticando via LDAP, *Active Directory*, Azure AD, Radius, eDirectory, TACACS+ e via base de dados local, para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários.

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

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

4.2.11.4. Deve permitir autenticação em modos: transparente, autenticação proxy (explícito, NTLM e Kerberos) e autenticação via clientes nas estações com os sistemas operacionais Windows, macOS e Linux 32/64.

4.2.11.5. Ao se utilizar da opção de proxy explícito, deve permitir a autenticação por cada conexão, a fim de garantir que usuários logados em servidores de multisessão sejam identificados corretamente pelo firewall, mesmo quando utilizando-se apenas 1(um) IP de origem.

4.2.11.6. Deve possuir a autenticação *Single sign-on* para, pelo menos, os sistemas de diretórios *Active Directory*, Azure AD e eDirectory.

4.2.11.7. Deve possuir portal do usuário para que os usuários tenham acesso ao uso de

internet pessoal, troquem senhas da base local e façam o download de softwares para as estações presentes na solução.

4.2.12. **QoS – Qualidade de Serviços**

4.2.12.1. Deve permitir controlar aplicações e tráfego cujo consumo possa ser excessivo e ter um alto consumo de largura de banda, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de limitação de largura de banda quando forem solicitadas por diferentes usuários ou aplicações.

4.2.12.2. A solução deverá suportar *Traffic Shaping* (QoS) e a criação de políticas baseadas em categoria web e aplicação por: endereço de origem; endereço de destino; usuário e grupo do LDAP/AD.

4.2.12.3. Deve possibilitar configurar o limite e a garantia de upload/download, bem como permitir priorizar o tráfego total e *bitrate* de modo individual ou compartilhado.

4.2.12.4. Deve suportar a priorização *Real-Time* de protocolos de voz (VoIP).

4.2.12.5. Deve permitir aplicar prioridade mesmo após o roteamento, utilizando o protocolo DSCP.

4.2.13. **VPN – Redes Virtuais Privadas**

4.2.13.1. Deve suportar VPN Site-to-Site e Client-to-Site.

4.2.13.2. Deve suportar Ipsec VPN, SSL VPN, L2TP e PPTP.

4.2.13.3. Suportar acesso remoto SSL, IPSec e VPN Client para Android e iPhone/iPAD.

4.2.13.4. Deve ser disponibilizado o acesso remoto ilimitado, até o limite suportado de túneis VPN pelo equipamento, sem a necessidade de aquisição de novas licenças e sem qualquer custo adicional para o licenciamento de clientes SSL.

4.2.13.5. Deve possuir o acesso via portal de usuário para o download e configuração do cliente SSL para Windows.

4.2.13.6. Deve possuir opção de VPN IPSEC com client nativo do fabricante.

4.2.13.7. Deve possuir um portal encriptado baseado em HTML5 para suporte pelo menos a: RDP, SSH, Telnet e VNC, sem a necessidade de instalação de clientes VPN nas estações de acesso.

4.2.13.8. A VPN IPsec deve suportar: DES, 3DES, GCM, Suite-B, Autenticação MD5 e SHA-1;Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; Algoritmo Internet Key Exchange (IKE); AES 128, 192 e 256 (*Advanced Encryption Standard*); SHA 256, 384 e 512; Autenticação via certificado PKI (X.509) e Pre-shared key (PSK).

4.2.13.9. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, SonicWALL, Fortinet, Huawei, Juniper, Palo Alto Networks e Sophos.

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

4.2.13.11. Deve suportar autenticação via AD/LDAP, Token e base de usuários local.

4.2.13.12. Deve permitir estabelecer um túnel SSL VPN com uma solução de autenticação via LDAP, Active Directory, Azure AD, Radius, eDirectory, TACACS+ e via base de dados local.

4.2.14. **Gerência Administrativa Centralizada**

4.2.14.1. O console de gerenciamento deve estar em nuvem.

4.2.14.2. Deve possuir solução de gerenciamento centralizado, possibilitando o gerenciamento de diversos equipamentos através de uma única console central, com administração de privilégios e funções.

4.2.14.3. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança.

4.2.14.4. Estar licenciada para gerenciar as soluções de firewall disponibilizadas.

4.2.14.5. Deve ser centralizada a gerência de todas as políticas do firewall e configurações para as soluções do firewall, sem necessidade de acesso direto aos equipamentos.

4.2.14.6. Deve permitir a criação de *Templates* para configurações.

4.2.14.7. Deve possuir indicadores do estado de equipamentos e rede.

4.2.14.8. Deve emitir alertas baseados em *thresholds* customizáveis, incluindo também alertas de expiração de subscrição, mudança de status de gateways, uso excessivo de disco, eventos ATP (*Advanced Threat Prevention*), IPS, ameaças de vírus, navegação, entre outros.

4.2.14.9. Deve permitir a criação de grupos de equipamentos por nome, modelo, firmware e regiões.

4.2.14.10. Deve ter controle de privilégios administrativos, com granularidade de funções (VPN admin, App e Web admin, IPS admin, entre outros).

4.2.14.11. Deve ter controle das alterações feitas por usuários administrativos, comparar diferentes versões de configurações e realizar o processo de r*oll back* de configurações para mudanças indesejadas.

4.2.14.12. Deve ter logs de auditoria de uso administrativo e atividades realizadas nos equipamentos.

4.2.14.13. Deve ter integração com a solução de logs e relatórios, habilitando o provisionamento automático de novos equipamentos e a sincronização dos administradores da centralização da gerência com a centralização de logs e relatórios.

4.2.14.14. Deve possibilitar o envio dos logs via syslog com conexão segura (TLS).

4.2.15. **Gerência de Logs e Relatório**

4.2.15.1. Deve possuir solução de logs e relatórios centralizados, possibilitando a consolidação total de todas as atividades da solução através de uma única console central.

4.2.15.2. Deve disponibilizar os logs pelo período mínimo estabelecido no Marco Civil da Internet, ou outra legislação equivalente.

4.2.15.3. Deve estar licenciada para gerenciar as soluções do firewall disponibilizado.

4.2.15.4. Devem ser fornecidas soluções em nuvem ou via appliances desde que obedeçam a todos os requisitos desta especificação, com armazenamento mínimo de 1 TB de dados.

4.2.15.5. Deverá prover relatórios baseados em usuários, com visibilidade sobre acesso a aplicações, navegação, eventos ATP, downloads e consumo de banda, independente em qual rede ou IP o usuário esteja se conectando.

4.2.15.6. Deve possibilitar a identificação de ataques, *malware* identificados pelos eventos ATP, usuários suspeitos, tráfegos anômalos incluindo tráfego ICMP e consumo não-usual de banda.

4.2.15.7. Deve conter relatórios pré-configurados, pelo menos de: aplicações, navegação, web server (WAF), IPS, ATP e VPN.

4.2.15.8. Deve fornecer relatórios históricos para análises de mudanças e comportamentos.

4.2.15.9. Deve possibilitar customizações dos relatórios para inserção de logotipos próprios.

4.2.15.10. Deve fornecer no mínimo relatórios de compliance HIPAA e PCI.

4.2.15.11. Deve permitir a exportação pelo menos nos formatos PDF ou CSV.

4.2.15.12. Deve fornecer relatórios sobre os acessos de procura no Google, Yahoo, Bing.

4.2.15.13. Deve fornecer relatórios de tendências.

4.2.15.14. Deve fornecer logs em tempo real, de auditoria e arquivados.

4.2.15.15. Deve possuir mecanismo de procura de logs arquivados.

4.2.15.16. Deve ter acesso baseado em Web com controles administrativos distintos.

4.2.16. **Integração com Solução de *EndPoint***

4.2.16.1. A solução de firewall deve possibilitar integração nativa com a solução de *endpoint* descrita nos itens deste Termo de Referência.

4.2.16.2. A integração deve possibilitar a criação de regras de bloqueio de *endpoints*, com determinado status, dentro do Firewall de forma automática, sem que haja intervenção por parte do time da contratante.

4.2.16.3. A integração deverá ser nativa entre o firewall e o endpoint, ou Utilizando APIs de integração da solução de firewall. Caso a integração não seja nativa, cabe a CONTRATADA: (i) Desenvolver completamente a solução de integração do Firewall e o Endpoint instalado; (ii) O Software de integração deve realizar a criação das regras do Firewall com no máximo 2 (dois) minutos após o incidente detectado no Endpoint; (iii) Possuir interface WEB, acessada por HTTP ou HTTPS, para definição dos objetos das regras a serem criadas, com no mínimo origem, destino, status do endpoint e protocolos; (iv) Deve possibilitar o envio de emails sobre as ações do software; (v) Entregar o software de integração, preferencialmente para execução em nuvem, juntamente com as devidas licenças necessárias para sistemas operacionais, banco de dados e todos os sistemas envolvidos para o perfeito funcionamento da integração; (vi) O sistema de integração não deverá enviar/receber pacotes TCP/UDP ou por qualquer outro meio de comunicação, que não sejam os objetos de Firewall deste edital ou a console do endpoint da contratante; (vii) Deve permitir backup das configurações do software de integração, possibiltando o *restore* em outra plataforma, de forma a não comprometer o ambiente; (viii) A gestão do sistema de integração será de inteira responsabilidade da contratante, de modo a garantir que sejam realizados todos os *updates*, correções de *patchs*, segurança do sistema operacional, bem como com seus softwares, alterações de versões, e assim por diante; (ix) Deve realizar manutenção/alteração total no software de integração, sem custo adicional, durante o período de vigência do suporte do Firewall; (x) Deve realizar teste de bancada, a fim de comprovar a efetividade da integração;

4.3. SOLUÇÃO DE ENDPOINT PARA ESTAÇÕES DE TRABALHO E SERVIDORES

4.3.1. **Características Gerais**

4.3.1.1. Todos os componentes que fazem parte da solução de segurança de endpoint para servidores e estações de trabalho deverão ser fornecidos pelo mesmo fabricante do Firewall. Não serão aceitas composições de produtos de fabricantes diferentes.

4.3.1.2. A console de monitoração e configuração deverá ser feita através da console

de gerenciamento descrita no item 4.2.14, deve ser baseada em web e em nuvem, e deverá conter todas as ferramentas para a monitoração e controle da proteção dos dispositivos.

4.3.1.3. A console de nuvem deve realizar o armazenamento de seus dados, garantindo conformidade e *compliance* com as leis locais como a LGPD.

4.3.1.4. Deve possuir mecanismo de comunicação via API, para integração com outras soluções de segurança, como por exemplo SIEM.

4.3.1.5. Deve possuir capacidade de realizar a integração com soluções de firewalls para criar políticas automáticas em caso de ataques em massa nos computadores e servidores.

4.3.1.6. A console deve permitir a divisão dos computadores, dentro da estrutura de gerenciamento em grupos.

4.3.1.7. Deve permitir sincronização com o *Active Directory* (AD) para gestão de usuários e grupos integrados às políticas de proteção.

4.3.1.8. Deve possuir a possibilidade de aplicar regras diferenciadas baseado em grupos ou usuários.

4.3.1.9. A instalação deve ser feita via cliente específico por download da gerência central ou também via email de configuração. O instalador deverá permitir a distribuição do cliente via *Active Directory* (AD) para múltiplas máquinas.

4.3.1.10. O console deve ser capaz de criar e editar diferentes políticas para a aplicação das proteções exigidas e aplicadas a nível de usuários, não importando em que equipamentos eles estejam acessando.

4.3.1.11. Deve fornecer atualizações do produto e das definições de vírus e proteção contra intrusos.

4.3.1.12. Deve permitir exclusões de escaneamento para determinados websites, pastas, arquivos ou aplicações, tanto a nível geral quanto específico em uma determinada política.

4.3.1.13. A console de gerenciamento deve permitir a definição de grupos de usuários com diferentes níveis de acesso às configurações, políticas e logs.

4.3.1.14. Deve possibilitar atualização incremental, remota e em tempo-real, da vacina dos Antivírus e do mecanismo de verificação (*Engine*) dos clientes.

4.3.1.15. Deve permitir o agendamento da varredura contra vírus com a possibilidade de selecionar uma máquina, grupo de máquinas ou domínio, com periodicidade definida pelo administrador.

4.3.1.16. Deve realizar atualização automática das assinaturas de ameaças (*malwares*)

e políticas de prevenção desenvolvidas pelo fabricante em tempo real ou com periodicidade definida pelo administrador.

4.3.1.17. Deve utilizar protocolos seguros padrão HTTPS para comunicação entre console de gerenciamento e clientes gerenciados.

4.3.1.18. As mensagens geradas pelo agente deverão estar no idioma em português ou permitir a sua edição.

4.3.1.19. Deve permitir a exportação dos relatórios gerenciais para pelo menos nos formatos CSV e PDF.

4.3.1.20. Recursos do relatório e monitoramento deverão ser nativos da própria central de gerenciamento, e estarem devidamente licenciados para a sua execução.

4.3.1.21. Deve permitir exibir informações como nome da máquina, versão do antivírus, sistema operacional, versão da engine, data da vacina, data da última verificação, eventos recentes e status.

4.3.1.22. Capacidade de geração de relatórios, estatísticos ou gráficos, tais como:

4.3.1.22.1. Detalhar quais usuários estão ativos, inativos ou desprotegidos, bem como detalhes dos mesmos;

4.3.1.22.2. Detalhamento dos computadores que estão ativos, inativos ou desprotegidos, bem como detalhes das varreduras e dos alertas nos computadores;

4.3.1.22.3. Detalhamento dos periféricos permitidos ou bloqueados, bem como detalhes de onde e quando cada periférico foi usado;

4.3.1.22.4. Detalhamento das principais aplicações bloqueadas e os servidores/usuários que tentaram acessá-las;

4.3.1.22.5. Detalhamento das aplicações permitidas que foram acessadas com maior frequência e os servidores/usuários que as acessam;

4.3.1.22.6. Detalhamento dos servidores/usuários que tentaram acessar aplicações bloqueadas com maior frequência e as aplicações que eles tentaram acessar;

4.3.1.22.7. Detalhamento de todas as atividades disparadas por regras de prevenção de perda de dados. Este item poderá ser atendido pela solução de NGFW.

4.3.1.23. Deverá possuir um elemento de comunicação para mensagens e notificações entre estações e a console de gerenciamento utilizando comunicação criptografada.

4.3.1.24. Deve fornecer solução de gerenciamento de arquivos armazenados em nuvem, garantindo que um arquivo que foi feito um upload (exemplo Dropbox), tenha o processo monitorado e gerenciado, bem como realizar automaticamente o escaneamento do arquivo contra *malwares*, procura das palavras chaves ou informações confidenciais.

Deve ser bloqueado o *upload* ou removida a informação confidencial antes do envio do arquivo.

4.3.1.25. As portas de comunicação deverão ser configuráveis. A comunicação deverá permitir QoS para controlar a largura de banda de rede.

4.3.1.26. A solução deverá permitir a seleção da versão do software de preferência, permitindo assim o teste da atualização sobre um grupo de computadores piloto antes de implantá-lo para toda a rede. Permitir ainda selecionar um grupo de computadores para aplicar a atualização para controlar a largura de banda de rede. A atualização da versão deverá ser transparente para os usuários finais.

4.3.1.27. O agente antivírus deverá proteger *laptops*, *desktops* e servidores em tempo real, sob demanda ou agendado para detectar, bloquear e limpar todos os vírus, *trojans*, *worms* e *spyware*. No Windows o agente também deverá detectar PUA, *adware*, comportamento suspeito, controle de aplicações e dados sensíveis. O agente ainda deve fornecer controle de dispositivos terceiros e controle de acesso a web.

4.3.1.28. Deve possuir mecanismo contra a desinstalação do *endpoint* pelo usuário e cada dispositivo deverá ter uma senha única, não sendo autorizadas soluções com senha única válida para todos os dispositivos.

4.3.1.29. Deve prover no *endpoint* a solução de HIPS (*Host Instrusion Prevention System*) para a detecção automática e proteção contra comportamentos maliciosos (análise de comportamento) e deverá ser atualizado diariamente.

4.3.1.30. Deve prover proteção automática contra web sites infectados e maliciosos, assim como prevenir o ataque de vulnerabilidades de browser via web exploits.

4.3.1.31. Deve permitir a monitoração e o controle de dispositivos removíveis nos equipamentos dos usuários, como dispositivos USB, periféricos da própria estação de trabalho e redes sem fio, estando sempre atrelado ao usuário o controle e não ao dispositivo.

4.3.1.32. O controle de dispositivos deve ser ao nível de permissão, somente leitura ou bloqueio.

4.3.1.33. Os seguintes dispositivos deverão ser, no mínimo, gerenciados: HD (*hard disks*) externos, pendrives USB, *storages* removíveis seguras, CD, DVD, Blu-ray, *floppy drives*, interfaces de rede sem fio, modems, bluetooth, infra-vermelho, MTP (*Media Transfer Protocol*) tais como Blackberry, iPhone e Android smartphone e PTP (P*icture Transfer Protocol*) como câmeras digitais.

4.3.1.34. A ferramenta de administração centralizada deverá gerenciar todos os componentes da proteção para estações de trabalho e servidores e deverá ser projetada

para a fácil administração, supervisão e elaboração de relatórios dos *endpoints* e servidores.

4.3.1.35. A Console de administração deve incluir um painel com um resumo visual em tempo real para verificação do status de segurança.

4.3.1.36. Deverá fornecer filtros pré-construídos que permitam visualizar e corrigir apenas os computadores que precisam de atenção.

4.3.1.37. Deverá exibir os equipamentos/dispositivos gerenciados de acordo com critérios da categoria, como por exemplo detalhes do estado do dispositivo, detalhes sobre a atualização, detalhes de avisos e erros, detalhes do antivírus, entre outras opções.

4.3.1.38. Uma vez que um problema seja identificado, deverá permitir corrigir os problemas remotamente, com no mínimo as opções: (i) Proteger o dispositivo com a opção de início de uma varredura; (ii) Forçar uma atualização naquele momento; (iii) Ver os detalhes dos eventos ocorridos; (iv) Executar verificação completa do sistema; (v) Forçar o cumprimento de uma nova política de segurança; (vi) Mover o computador para outro grupo; (vii) Apagar o computador da lista; (viii) Atualizar a políticas de segurança quando um computador for movido de um grupo para outro manualmente ou automaticamente; (ix) Gravar um log de auditoria seguro, que monitore a atividade na console de gerenciamento para o cumprimento de regulamentações, auditorias de segurança, análise e solução de problemas forenses.

4.3.1.39. Deverá permitir exportar o relatório de logs de auditoria pelo menos nos formatos CSV e PDF.

4.3.1.40. Deve conter vários relatórios para análise e controle dos usuários e *endpoints*. Os relatórios deverão ser divididos, no mínimo, em relatórios de: eventos, usuários, controle de aplicativos, periféricos e web, indicando todas as funções solicitadas para os *endpoints*.

4.3.1.41. Fornecer relatórios utilizando listas ou gráficos, utilizando informações presentes na console, com no mínimo os seguintes tipos: Nome do dispositivo, início da proteção, último usuário logado no dispositivo, última atualização, último escaneamento realizado, status de proteção do dispositivo e grupo a qual o dispositivo faz parte.

4.3.1.42. A console deve possuir métodos de verificação da saúde das configurações do console, possibilitando aos administradores descobrirem facilmente se existe alguma falha de configuração que pode facilitar a entrada de *malwares* e invasores no ambiente.

4.3.2. **Características Gerais da Solução de Proteção para Estações de Trabalho**

4.3.2.1. Deve possuir pré-execução do agente para verificar o comportamento

malicioso e detectar *malwares* ativos, conhecidos e desconhecidos.

4.3.2.2. O agente deve ter a capacidade de submeter o arquivo desconhecido à nuvem de inteligência do fabricante para detectar a presença de ameaças.

4.3.2.3. O agente deve realizar a atualização várias vezes por dia para manter a detecção atualizada contra as ameaças mais recentes.

4.3.2.4. A solução deve manter conexão direta com banco de dados de ameaças do fabricante para uso da rede de inteligência.

4.3.2.5. Deve realizar a verificação de todos os arquivos acessados em tempo real, mesmo durante o processo de inicialização.

4.3.2.6. Deve realizar a verificação de todos os arquivos no disco rígido em intervalos programados.

4.3.2.7. Deve realizar a limpeza do sistema automaticamente, removendo itens maliciosos detectados e aplicações potencialmente indesejáveis (PUA).

4.3.2.8. Deve proteger os navegadores Internet Explorer, Firefox, Chrome, Opera e Safari, bloqueando o acesso a sites infectados conhecidos e pela verificação dos dados baixados antes de serem executados.

4.3.2.9. Deve permitir a autorização de detecções maliciosas e excluir da varredura diretórios e arquivos específicos.

4.3.2.10. É requerida a proteção integrada, ou seja, em um único agente, contra ameaças de segurança, incluindo vírus, *spyware*, *trojans*, *worms*, *adware* e aplicativos potencialmente indesejados (PUAs).

4.3.2.11. Suportar máquinas com arquitetura 32-bits e 64-bits (Exceto para Windows 11 que não há opção de 32bits).

4.3.2.12. O cliente para instalação nas estações de trabalho deverá ser compatível com pelo menos os sistemas operacionais Windows 7, 8.1, 10, 11 e as versões mais atuais.

4.3.2.13. Possuir a funcionalidade de proteção contra a alteração das configurações do agente, impedindo aos usuários, incluindo o administrador local, reconfigurar, desativar ou desinstalar componentes da solução de proteção.

4.3.2.14. Permitir a utilização de senha de proteção para possibilitar a reconfiguração local no cliente ou desinstalação dos componentes de proteção.

4.3.3. **Características Gerais da Solução para Servidores**

4.3.3.1. A solução deverá ser capaz de proteger servidores contra *malwares*, arquivos e tráfego de rede malicioso, controle de periféricos, controle de acesso à web, controle de aplicativos em um único agente instalado nos servidores.

4.3.3.2. Deve realizar a pré-execução do agente para verificar o comportamento malicioso e detectar malwares desconhecidos.

4.3.3.3. O agente *host* deve buscar algum sinal de *malwares* ativos e detectar *malwares* conhecidos e desconhecidos.

4.3.3.4. O agente deve realizar a atualização várias vezes por dia para manter a detecção atualizada contra as ameaças mais recentes.

4.3.3.5. A solução deve manter conexão direta com banco de dados de ameaças do fabricante para uso da rede de inteligência.

4.3.3.6. Deve realizar a verificação de todos os arquivos acessados em tempo real, mesmo durante o processo de inicialização.

4.3.3.7. Deve realizar a verificação de todos os arquivos no disco rígido em intervalos programados.

4.3.3.8. Deve realizar a limpeza do sistema automaticamente, removendo itens maliciosos detectados e aplicações potencialmente indesejáveis (PUA).

4.3.3.9. Deve proteger os navegadores Internet Explorer, Firefox, Chrome, Opera e Safari, bloqueando o acesso a sites infectados conhecidos e pela verificação dos dados baixados antes de serem executados.

4.3.3.10. Deve permitir a autorização de detecções maliciosas e excluir da varredura diretórios e arquivos específicos.

4.3.3.11. É requerida a proteção integrada, ou seja, em um único agente, contra ameaças de segurança, incluindo vírus, *spyware*, *trojans*, *worms*, *adware* e aplicativos potencialmente indesejados (PUAs).

4.3.3.12. O cliente para instalação em servidores, deverá ser compatível com pelos menos os sistemas operacionais: (i) Windows Server 2012, 2016 e versões mais atualizadas; (ii) Ubuntu Server; (iii) CentOS; (iv) Debian; (v) Red Hat Enterprise; (vi) SUSE Linux Enterprise Server; (vii) Oracle Linux; (viii) Amazon Linux.

4.3.3.13. Deve suportar o uso de servidores usados para atualização em cache para diminuir a largura de banda usada nas atualizações.

4.3.3.14. Deve possuir integração com nuvem para identificar as informações dos servidores instanciados nas nuvens.

4.3.3.15. Possuir a funcionalidade de proteção contra a alteração das configurações do agente, impedindo aos usuários, incluindo o administrador local, reconfigurar, desativar ou desinstalar componentes da solução de proteção.

4.3.3.16. Permitir a utilização de senha de proteção para possibilitar a reconfiguração local no cliente ou desinstalação dos componentes de proteção.

4.3.3.17. Deve possuir funcionalidades de tecnologias conhecidas como CWPP – *Cloud Workload Protection Plataform*, ou similares, permitindo que seja possível trazer funcionalidades de próxima geração para cargas de trabalho em nuvem, bem como *containers*, e afins. Alternativamente, a solução deverá permitir a instalação do agente em máquinas virtuais disponibilizadas em nuvem pública.

4.3.3.18. A solução deve no mínimo, utilizar o modelo de sensores para containers, garantindo visibilidade e proteção de, no mínimo, estes tipos de ataques: (i) Escalação de privilégios dentro de containers; (ii) Programas utilizando técnicas de mineração de criptomoedas; (iii) Detecção de atacantes tentando destruir evidências de ambientes comprometidos (IOC – *Indicator of compromise*); (iv) Detecção de funções internas do kernel que estão sendo adulteradas em um host.

4.3.3.19. A solução deve também se integrar a tecnologias de CSPM – *Cloud Security Posture Management*, tendo como objetivo trazer funcionalidades de análises integradas de CWPP e CSPM a fim de melhorar a visibilidade e resposta a incidentes em ambientes de nuvem públicas. Alternativamente, a solução poderá ofertar APIs para permitir integrações para esta finalidade.

4.3.4. **Características da Solução de Endpoint Detection and Response (EDR)**

4.3.4.1. A solução deve ter capacidade de implementar técnicas de EDR (*Endpoint Detection and Response*), para as estações de trabalho e para os servidores, possibilitando detecção e investigação nos *endpoints* com atividades suspeitas.

4.3.4.2. Deve ter a capacidade de submeter arquivos identificados em incidentes a uma segunda consulta à nuvem de inteligência do fabricante.

4.3.4.3. Em caso de incidente a solução deve mostrar a trilha da infecção de forma visual, mostrando o início, todas as interações do *malware* e o ponto final de bloqueio.

4.3.4.4. Após a análise da nuvem de inteligência do fabricante a solução deve apresentar um relatório sobre a ameaça contendo no mínimo: (i) Detalhes do Processo, como nome, hash, hora e data da detecção e remediação; (ii) Reputação do arquivo e correlação da detecção do arquivo em outras soluções de antivírus através de bases de conhecimento como o Vírus Total; (iii) Resultado da análise do arquivo suspeito pela funcionalidade de *Machinne Learning*; (iv) Propriedades gerais do arquivo, como nome, versão, tamanho, idioma, informações de certificado.

4.3.4.5. A solução de EDR deverá ser integrada ao agente de antivírus a ser instalado com um com agente único, em estação de trabalho, servidores físicos e virtuais a fim de diminuir o impacto ao usuário final.

4.3.4.6. O gerenciamento da solução de EDR deverá ser feito a partir da mesma console de gerenciamento da solução antivírus.

4.3.4.7. Deve fornecer guias de respostas a incidentes, fornecendo visibilidade sobre o escopo de um ataque, como ele começou, o que foi impactado, e como responder.

4.3.4.8. Deve ser capaz de responder ao incidente com opção de isolamento da máquina, bloqueio e limpeza da ameaça.

4.3.4.9. Deve ser capaz realizar buscas de ameaças em todo o ambiente, sendo capaz de buscar por *hash*, nome, endereços IP, domínio ou linha de comando.

4.3.4.10. Deve ter acesso a recurso de *Data Lake* que armazene informações críticas de *endpoints* e servidores, permitindo o acesso aos dados sobre atividades mesmo quando o dispositivo correspondente está *offline* ou foi descontinuado, possibilitando o agendamento de consultas (*queries*).

4.3.4.11. Deve reter os dados no *Data Lake* por no mínimo 7 dias.

4.3.5. **Características da Solução de Extended Detection and Response (XDR)**

4.3.5.1. Além das características de EDR listadas no item 4.3.4, a solução também deverá disponibilizar para estações de trabalho e servidores, as características de XDR listadas a seguir.

4.3.5.2. Deve possuir *Data Lake* que armazene informações críticas de *endpoints* e servidores, mas também incorporando dados de outras soluções de segurança como *firewalls*, e-mail *gateways*, *public cloud* e *mobile*, permitindo o acesso aos dados sobre atividades mesmo quando o dispositivo correspondente está *offline* ou foi descontinuado.

4.3.5.3. Deve possuir recurso de pesquisa estruturada em banco de dados compatível com SQL, ou similar.

4.3.5.4. Deve disponibilizar recurso de pesquisa para comparar os indicadores de comprometimento de várias fontes de dados para identificar rapidamente um ataque suspeito.

4.3.5.5. Deve utilizar detecções de ATP e IPS do firewall para investigar *endpoints* suspeitos.

4.3.5.6. Deve disponibilizar pontos de aplicação que permitem executar ações, como colocar em quarentena um *endpoint* comprometido, bloquear o tráfego de rede ou remover *malware*.

4.3.5.7. Deve possuir sensores que forneçam telemetria de diferentes aspectos da infraestrutura de TI, capazes de identificar dispositivos não gerenciados e desprotegidos em todo ambiente da organização.

4.3.5.8. Deve possibilitar o agendamento de consultas (*queries*) cíclicas no *Data Lake* para identificação de IoCs em execuções antecipadas.

4.3.5.9. Deve reter os dados no *Data Lake* por no mínimo 30 dias.

4.3.5.10. O XDR deve permitir integração com sistemas de terceiros, no mínimo, tecnologias como Office 365 e produtos de CSPM para visibilidade e correlação de eventos em ambientes de Cloud como Azure, AWS e Google Cloud entre outros.

4.3.5.11. A console do XDR deve correlacionar os dados recebidos e armazenados no *Data Lake* e gerar evidências de ataques ou eventos suspeitos existentes dentro do ambiente.

4.3.5.12. Tais detecções e evidências devem conter todos os detalhes do evento, bem como uma análise do próprio fabricante sobre a classificação de risco de tal evento.

4.3.5.13. Deve possibilitar também que investigações sejam realizadas a partir destes eventos, coletando dados e executando consultas dentro do *Data lake* ou nos próprios dispositivos a fim de coletar mais evidências para determinar a realidade do ataque presente na console.

4.3.5.14. Deve possuir console para gerenciamento de investigações, podendo adicionar de forma automática ou manual, diversos eventos e detecções encontradas na console.

4.3.5.15. Será necessário também que exista uma trilha de auditoria para cada investigação, de tal forma que os administradores da console consigam auditar os detalhes da condução da investigação.

4.3.6. **Funcionalidades de Firewall e Detecção e Proteção de Intrusão (IDS\IPS)**

4.3.6.1. Deve possuir proteção contra exploração de *buffer overflow*.

4.3.6.2. Deve possuir atualização periódica de novas assinaturas de ataque.

4.3.6.3. Deve ter capacidade de reconhecer e bloquear automaticamente as aplicações em clientes baseando-se na impressão digital (*hash*) do arquivo ou dinamicamente através do nome da aplicação.

4.3.6.4. Deve ter capacidade de bloqueio de ataques baseado na exploração de vulnerabilidade conhecidas.

4.3.6.5. Deve possuir um sistema de prevenção de intrusão no *host* (HIPS), que monitore o código e blocos de código que podem se comportar de forma maliciosa antes de serem executados.

4.3.6.6. Ser capaz de aplicar uma análise adicional, inspecionando finalmente o comportamento de códigos durante a execução, para detectar comportamento suspeito de

aplicações, tais como *buffer overflow*.

4.3.6.7. Deve possuir técnicas de proteção, que inclui: (i) Análise dinâmica de código - técnica para detectar *malware* criptografado mais complexo; (ii) Algoritmo correspondente padrão - onde os dados de entrada são comparados com um conjunto de sequências conhecidas de código já identificado como um vírus; (iii) Emulação - uma técnica para a detecção de vírus polimórficos, ou seja, vírus que se escondem criptografando-se de maneira diferente cada vez que se espalham; (iv) Tecnologia de redução de ameaças - detecção de prováveis ameaças por uma variedade de critérios, como extensões duplas (por exemplo. jpg.txt) ou a extensão não coincida com o tipo de arquivo verdadeiro (por exemplo, um arquivo executável ou arquivo .exe com a extensão .txt); (v) Verificação de ameaças web avançadas: bloqueia ameaças verificando o conteúdo em tempo real e remontando com emulação de JavaScript e análise comportamental para identificar e parar o código malicioso de *malware* avançados.

4.3.7. **Funcionalidades de Antivírus e AntiSpyware**

4.3.7.1. Deve possuir proteção em tempo real contra vírus, *trojans*, *worms*, *rootkits*, *botnets*, *spyware*, *adwares* e outros tipos de códigos maliciosos.

4.3.7.2. Deve possuir proteção *anti-malware*, que deverá ser nativa da solução ou incorporada automaticamente por meio de *plug-ins* sem a utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante.

4.3.7.3. As configurações do *anti-spyware* deverão ser realizadas através da mesma console do antivírus.

4.3.7.4. Deve permitir a configuração de ações diferenciadas para programas potencialmente indesejados ou *malware*, com possibilidade de inclusão de arquivos em listas de exclusão (*whitelists*) para que não sejam verificados pelo produto.

4.3.7.5. Deve permitir a varredura das ameaças de maneira manual, agendada e em tempo real na máquina do usuário e nos servidores.

4.3.7.6. Deve possuir capacidade de detecção e reparo em tempo real de vírus de macro conhecidos e novos através do antivírus.

4.3.7.7. Deve possuir capacidade de remoção automática total dos danos causados por *spyware*, *adwares* e *worms*, como limpeza do registro e pontos de carregamento, com opção de finalizar o processo e terminar o serviço da ameaça no momento de detecção. A remoção automática dos danos causados deverá ser nativa do próprio antivírus ou adicionada por plugin, desde que desenvolvido ou distribuído pelo fabricante.

4.3.7.8. Deve possuir capacidade de bloquear origem de infecção através de

compartilhamento de rede com opção de bloqueio da comunicação via rede.

4.3.7.9. Deve permitir o bloqueio da verificação de vírus em recursos mapeados da rede.

4.3.7.10. Deverá detectar tráfego de rede para comandar e controlar os servidores.

4.3.7.11. Nos servidores, deverá proteger arquivos de documento contra ataques de *ransomware* e proteger que o ataque de *ransomware* seja executado remotamente.

4.3.7.12. Deverá realizar a função de Antivírus da Web (verificação de sites e downloads contra vírus).

4.3.7.13. Deverá possuir controle de acesso a sites por categoria.

4.3.7.14. Deverá proteger a navegação na web, mesmo aos usuários fora da rede, para todos os principais navegadores (IE, Firefox, Safari, Opera e Chrome), fornecendo controle da Internet independentemente do navegador utilizado, como parte da solução de proteção a estações de trabalho, incluindo a análise do conteúdo baixado pelo navegador web, de forma independente do navegador usado, ou seja, sem utilizar um *plugin*, onde não é possível ser ignorada pelos usuários, protegendo os usuários de websites infectados e categorias específicas de websites.

4.3.7.15. O Controle da Web deve controlar o acesso a sites impróprios, com no mínimo 14 categorias de sites inadequados. Deve ainda permitir a criação de lista branca de sites sempre permitidos e lista negra de sites que devem ser bloqueados sempre.

4.3.7.16. Todas as atividades de navegação na Internet bloqueadas deverão ser enviadas para a console de gerenciamento, informando detalhes do evento e a razão para o bloqueio.

4.3.7.17. Deve possuir capacidade de verificar somente arquivos novos e alterados.

4.3.7.18. Deve possuir funcionalidades específicas para prevenção contra a ação de *ransomwares*, tais como a capacidade de impedir a criptografia quando feita por aplicativos desconhecidos ou a capacidade de fazer *backup* de arquivos antes de serem criptografados para posteriormente permitir sua restauração.

4.3.8. **Funcionalidades de detecção Pró-Ativa de reconhecimento de novas ameaças**

4.3.8.1. Deve possuir funcionalidade de detecção de ameaças via técnicas de *machine learning*.

4.3.8.2. Deve possuir funcionalidade de detecção de ameaças desconhecidas que estão em memória.

4.3.8.3. Deve possuir capacidade de detecção, e bloqueio pró-ativo de *keyloggers* e outros *malwares* não conhecidos (ataques de dia zero) através da análise de

comportamento de processos em memória (heurística).

4.3.8.4. Deve possuir capacidade de detecção e bloqueio de *Trojans* e *Worms*, entre outros *malwares*, por comportamento dos processos em memória.

4.3.8.5. Deve possuir capacidade de analisar o comportamento de novos processos ao serem executados, em complemento à varredura agendada.

4.3.9. **Funcionalidades de Proteção Contra *Ransomwares* em Servidores**

4.3.9.1. Deve possuir capacidade de proteção contra *ransomware* não baseada exclusivamente na detecção por assinaturas.

4.3.9.2. Deve possuir capacidade de remediação da ação de criptografia maliciosa dos *ransomwares*.

4.3.9.3. Deve possuir capacidade de prevenção contra a ação de criptografia maliciosa executada por *ransomwares*, possibilitando ainda o bloqueio dos computadores de onde partirem tal ação.

4.3.10. **Funcionalidades de Proteção Contra *Ransomwares***

4.3.10.1. Para estações de trabalho, possuir capacidade de proteção contra *ransomware* não baseada exclusivamente na detecção por assinaturas.

4.3.10.2. Para estações de trabalho,possuir capacidade de remediação da ação de criptografia maliciosa dos *ransomwares*.

4.3.10.3. A solução deverá prevenir ameaças e interromper que elas sejam executadas em dispositivos da rede, detectando e limpando os *malwares*, além da realização de uma análise detalhada das alterações realizadas.

4.3.10.4. Deve possuir uma tecnologia *anti-exploit* baseada em comportamento, reconhecendo e bloqueando as mais comuns técnicas de *malware*, protegendo os *endpoints* de ameaças desconhecidas e vulnerabilidades zero-day.

4.3.10.5. Deve possibilitar a detecção e o bloqueio de, pelo menos, as seguintes técnicas de exploit: DEP (*Data Execution Prevention*), *Address Space Layout Randomization* (ASLR), *Bottom Up ASLR, Null Page, Anti-HeapSpraying, Dynamic Heap Spray, Import Address Table Filtering (*IAF), *Table Hijacking, Stack Pivot and Stack Exec*, SEHOP, *Stack*-based ROP (*Return-Oriented Programming*), *Control-Flow Integrity (*CFI), *Syscall, WOW64, Load Library, Shellcode, VBScript God Mode, Application Lockdown, Network Lockdown e Process Protection*.

4.3.10.6. A solução deverá trabalhar silenciosamente na máquina do usuário e deverá detectar a criptografia maliciosa de dados (*ransomware*), realizando a sua interrupção. No

caso de arquivos serem criptografados a solução deverá realizar o retorno destes arquivos ao seu estado normal. Deste modo a solução deve ser capaz de fazer a limpeza e remoção completa do *ransomware* na máquina do usuário.

4.3.10.7. Deve fornecer também uma análise detalhada das modificações realizadas pelo *ransomware*, realizando a correlação dos dados em tempo real, indicando todas as modificações feitas em registros, chaves, arquivos alvos, conexões de redes e demais componentes contaminados.

4.3.10.8. A console de monitoração e configuração deverão ser feitas através de uma central única, baseada em web e em nuvem, que deverá conter todas as ferramentas para a monitoração e controle da proteção dos dispositivos para a solução de *anti-exploit* e *anti-ransomware*.

4.3.10.9. A console deverá apresentar *Dashboard* com o resumo dos status de proteção dos computadores e usuários, bem como indicar os alertas de eventos de criticidades alta, média e informacional, bem como todas as identificações para o mapeamento instantâneo dos efeitos causados pelo *ransomware* nos *endpoints*.

4.3.11. **Funcionalidade de Controle de Aplicações e Dispositivos**

4.3.11.1. Possuir controle de aplicativos para monitorar e impedir que os usuários executem ou instalem aplicações que podem afetar a produtividade ou o desempenho da rede.

4.3.11.2. Atualizar automaticamente a lista de aplicativos que podem ser controlados, permitindo que aplicativos específicos ou categorias específicas de aplicações possam ser liberadas ou bloqueadas.

4.3.11.3. Verificar a identidade de um aplicativo de maneira genérica para detectar todas as suas versões. Permitir a solicitação de adição de novas aplicações nas listas de controle de aplicativos através de interface web.

4.3.11.4. Oferecer proteção para chaves de registro e controle de processos.

4.3.11.5. Proibir através de política a inicialização de um processo ou aplicativo baseado em nome ou no *hash* do arquivo.

4.3.11.6. Detectar aplicativo controlado quando os usuários o acessem, com as opções de permitir e alertar ou bloquear e alertar.

4.3.11.7. Deve possuir a opção de customizar uma mensagem a ser mostrada ao usuário em caso de bloqueio de execução do aplicativo.

4.3.11.8. Gerenciar o uso de dispositivos de armazenamento USB (ex: pen-drives e HDs USB). Permitir, através de regras, o bloqueio ou liberação da

leitura/escrita/execução do conteúdo desses dispositivos.

4.3.11.9. Controlar o uso de outros dispositivos periféricos, como comunicação infravermelha e modem externo.

4.3.11.10. As funcionalidades do Controle de Aplicações e Dispositivos deverão ser nativas do produto ou incorporadas automaticamente por meio de plug-ins sem utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante.

4.3.11.11. Deve possuir capacidade de bloquear execução de aplicativo que está em armazenamento externo.

4.3.11.12. A gestão desses dispositivos deverá ser feita diretamente console de gerenciamento com a possibilidade de definir políticas diferentes por grupos de *endpoints*.

4.3.11.13. Permitir a autorização de um dispositivo com no mínimo as seguintes opções: (i) dispositivos do mesmo modelo; (ii) único dispositivo com base em seu número de identificação único; (iii) acesso total; (iv) acesso somente leitura.

4.3.11.14. Deve possuir o bloqueio de pontes entre duas redes, por exemplo, um laptop conectado ao mesmo tempo na LAN e se tornar um *hotspot* Wi-Fi, ou através de um modem.

4.3.12. **Funcionalidades de Proteção e Prevenção a Perda de Dados**

4.3.12.1. Deve possuir proteção a vazamento ou perda de dados sensíveis, considerando o seu conteúdo ou o seu tipo real, além da possibilidade de avaliar a extensão do arquivo e múltiplos destinos.

4.3.12.2. Deve permitir a identificação de informações confidenciais, como números de passaportes ou outras informações pessoais identificáveis e/ou informações confidenciais mesmo que os documentos não tenham sido corretamente classificados, utilizando Lista de Controle de Conteúdo (CCL).

4.3.12.3. Deve possibilitar o bloqueio, somente registrar o evento na Console de administração, ou perguntar ao usuário se ele ou ela realmente quer transferir o arquivo identificado como sensível.

4.3.12.4. Deve possuir listas de CCLs pré-configurados com no mínimo as seguintes identificações: Números de cartões de crédito, números de contas bancárias, números de Passaportes, endereços, telefones códigos postais, lista de e-mails, informações pessoais, corporativas e financeiras, como CPF, RG, CNH, CNPJ e dados bancários, entre outras informações.

4.3.12.5. Deve possibilitar adicionar regras próprias de conteúdo. Além disso, deve

possuir um assistente fornecido para auxiliar nessa finalidade.

4.3.12.6. Deve permitir criar regras de prevenção de perda de dados por tipo verdadeiro de arquivo.

4.3.12.7. Deve possuir a capacidade de autorizar, bloquear e confirmar a movimentação de dados sensíveis e em todos os casos, gravar a operação realizada com as principais informações da operação.

4.3.12.8. Deve permitir o controle de dados para no mínimo os seguintes meios: (i)Cliente de e-mail (pelo menos Outlook Express); (ii) Navegador (pelo menos IE, Firefox e Chrome); (iii) cliente de mensagens instantâneas (ao menos Skype) e (iv) dispositivos de armazenamento (ao menos USB e CD/DVD).

4.3.12.9. As funcionalidades descritas neste item poderão ser implementadas pelo NGFW.

4.4. Instalação, Configuração e Testes do Firewall e dos *Endpoints*: A contratada deverá realizar a instalação, configuração e testes dos equipamentos e sistemas referentes aos itens 1, 2 e 3 do presente edital.

4.4.1. **Infraestrutura e Serviços de Manutenção**

4.4.1.1. A contratada será responsável pelo fornecimento de toda a infraestrutura, equipamentos, periféricos, softwares, licenciamentos, serviços de manutenção e demais componentes necessários para manter o perfeito funcionamento dos serviços contratados nos itens 1, 2 e 3 deste Termo de Referência. Sendo assim, a contratada deverá fornecer, no mínimo, os itens listados a seguir.

4.4.1.2. **Infraestrutura de tecnologia da informação e comunicação (TIC)**: A contratada fica responsável por fornecer e instalar nos racks indicados pela CML todos os equipamentos, sistemas e demais elementos de TIC necessários para o perfeito funcionamento da solução contratada e descrita neste edital.

4.4.1.3. A contratada fica responsável por qualquer item ou licenças para o perfeito funcionamento da solução proposta.

4.4.1.4. Todas as fases de planejamento, instalação e configuração deverão ser realizadas com a presença de técnicos da contratada que deverão possuir capacidade técnica necessária à execução do serviço.

4.4.1.5. A instalação e configuração deverão ser planejadas e documentadas previamente pela contratada em conjunto com a equipe de TI da Câmara Municipal de Londrina (CML), onde devem ser definidos todos os passos necessários para a

configuração e migração, incluindo o cronograma e plano de testes.

4.4.1.6. As configurações devem ser realizadas de acordo com as recomendações dos fabricantes.

4.4.1.7. O prazo máximo para instalação de todos os serviços solicitados nos itens 1 e 2 deste Termo de Referência deverá ser de no máximo 90 (noventa) dias, prorrogáveis por mais 30 dias, desde que justificados junto à Contratante.

4.4.2. **Instalação dos equipamentos no rack de 19'' da CML**

4.4.2.1. A empresa contratada deverá realizar a fixação equipamentos e demais componentes necessários no rack de 19'' da CML, sendo que todos os componentes necessários para a fixação dos equipamentos deverão ser fornecidos pela contratada.

4.4.2.2. A contratada deverá fornecer os cabos de energia e dados, conectores, adaptadores e demais componentes necessários para energizar e possibilitar a comunicação de dados entre os equipamentos.

4.4.2.3. A contratada deverá realizar a conexão e testes de comunicação entre os equipamentos instalados.

4.4.3. **Instalação dos *Endpoints* (segurança) nos Equipamentos**

4.4.3.1. A contratada deverá realizar a instalação e configuração dos *Endpoints* nos computadores *desktops*, notebooks e nos servidores indicados pela equipe de TI da Câmara Municipal de Londrina (CML).

4.4.3.2. Após a instalação dos *Endpoints*, deverá ser realizada a instalação e configuração do Console de Gerenciamento para realizar a administração dos *Endpoints* instalados na CML.

4.4.3.3. Realizar integração com o Firewall.

4.4.3.4. Realizar a atualização das bases de dados, assinaturas e demais itens que necessitem serem atualizados.

4.4.3.5. Realizar varredura completa em todos os equipamentos para verificar a possível existência de ameaças, e emitir relatório final descrevendo cada item encontrado.

4.4.4. **Instalação e Configuração da Console Centralizada de Gerenciamento**

4.4.4.1. A console de gerenciamento deverá estar instalada em nuvem.

4.4.4.2. Deve ser disponibilizado acesso HTTPS para visualização em Browser padrão, pelo menos em Firefox ou Chrome.

4.4.4.3. Deve atender a todos os requisitos listados nos itens 4.2.14 e 4.2.15.

4.4.4.4. Deve apresentar as ferramentas para administração dos *Endpoints* e do Firewall.

4.4.5. **Instalação e Configuração dos Gateways**

4.4.5.1. A Contratada deverá realizar a configuração no Firewall dos links de Internet contratados pela CML para serem utilizados como Gateway de saída tanto da rede *Ethernet* quanto da Rede WIFI da Contratante.

4.4.5.2. A CML possui 5 (cinco) links de Fibra óptica do tipo GPON de 500Mbps e 1 (um) link dedicado de 200Mbps - caso a quantidade de links se altere até a assinatura do Contrato Administrativo, eles consideram-se incluídos na contratação.

4.4.5.3. A contratada deverá configurar no Firewall o balanceamento de carga para utilização dos links, baseada em algoritmo do tipo *round-robin* ou similar. Além disso, também deverá ser realizada configuração de velocidade por QoS ou por perfil pré-definido.

4.4.5.4. O link dedicado de 200Mbps deverá ser utilizado para realizar a conexão da infraestrutura da CML com o *datacenter* em nuvem da CML.

4.4.5.5. Realizar a configuração de acesso por VPN na infraestrutura da CML.

4.4.6. **Segmentação lógica da rede e configuração de servidor DHCP**

4.4.6.1. A contratada deverá realizar a configuração do servidor DHCP que será utilizado na infraestrutura de rede da CML.

4.4.6.2. Para a segmentação da rede, a contratada deverá criar, pelo menos, as VLANs listadas a seguir:

4.4.6.2.1. Servidores de rede
4.4.6.2.2. Switches
4.4.6.2.3. Access Points
4.4.6.2.4. Telefones VoIP
4.4.6.2.5. Câmeras de segurança
4.4.6.2.6. Link Transmissão Youtube
4.4.6.2.7. Servidores efetivos
4.4.6.2.8. Servidores comissionados/Vereadores
4.4.6.2.9. Visitantes

4.4.6.3. Para a segmentação da rede WIFI, a contratada deverá criar, pelo menos, as VLANs listadas a seguir:

4.4.6.3.1. Visitantes;

4.4.6.3.2. Servidores Efetivos;
4.4.6.3.3. Servidores Comissionados;
4.4.6.3.4. Vereadores
4.4.6.3.5. Jornalistas
4.4.6.3.6. Plenário
4.4.6.3.7. Multimídia

4.4.6.4. A contratada deverá realizar a configuração das VLANs em todos os switches existentes na CML.

4.4.6.5. As regras de roteamento entre as VLANs devem ser estabelecidas em conjunto com a equipe de TI da CML, e de acordo com a Política de Segurança da CML.

4.4.7. **Definição das Regras de Acesso do Firewall**

4.4.7.1. As regras de acesso à rede *Ethernet* e à rede WIFI deverão ser configuradas em conjunto com a equipe de TI da Câmara Municipal de Londrina (CML), e de acordo com a Política de Segurança da CML.

4.4.7.2. Deverão ser criadas todas as regras necessárias para o atendimento aos requisitos estabelecidos no item 4.2. do presente Termo de Referência.

4.4.8. **Realização de Testes**

4.4.8.1. Após a instalação e configuração dos equipamentos, licenciamentos, softwares e demais componentes existentes no Termo de Referência, a contratada deverá realizar relatório de testes, demonstrando o funcionamento, pelo menos, dos tópicos listados nos itens a seguir.

4.4.8.2. Acesso e conexão ao console de gerenciamento do Firewall.
4.4.8.3. *Status* e configuração dos gateways.
4.4.8.4. Comunicação entre as VLANs.
4.4.8.5. Navegação na WEB para verificação do funcionamento das regras de acesso definidas no Firewall.
4.4.8.6. Funcionamento dos *Endpoints* nos desktops.
4.4.8.7. Funcionamento dos *Endpoints* nos servidores.
4.4.8.8. Testes de conexão por VPN.

4.5. Treinamento Oficial do Fabricante – Firewall

4.5.1. O instrutor deverá possuir certificação técnica comprovada, emitida pelo fabricante da solução, nos requisitos solicitados nos itens 4.2 e 4.3 deste Termo de Referência.

O treinamento poderá ser ministrado por mais de um instrutor.

4.5.2. O treinamento poderá ser realizado de forma *online,* ou presencial nas dependências da Câmara Municipal de Londrina.

4.5.3. O conteúdo programático do treinamento deverá envolver o conteúdo solicitado nas especificações descritas nos itens 4.2 e 4.3 deste Termo de Referência. Poderão ser disponibilizados um ou mais treinamentos para atender a esse requisito.

4.5.4. Deverão ser fornecidos os materiais didáticos completos para os participantes do curso.

4.5.5. A carga horária total de treinamentos ofertados deverá ser de no mínimo 30 horas.

4.5.6. Após o término do treinamento, deverá ser disponibilizado pela contratada um *voucher* para cada participante realizar teste de Certificação Oficial do fabricante de Firewall.

4.6. Suporte e Gestão de Chamados

4.6.1. O suporte técnico deverá ser por telefone, via chat, conexão remota ou deslocamento dos técnicos da empresa Contratada ao local da prestação dos serviços na Câmara Municipal de Londrina (CML).

4.6.2. A empresa Contratada deverá disponibilizar sistema de chamados/ticket para acompanhar o andamento dos chamados abertos.

4.6.3. O serviço será prestado em conformidade com o Acordo de Nível de Serviço (SLA):

4.6.3.1. **Os chamados considerados urgentes** deverão ser atendidos com solução paliativa em até 6 horas corridas após a abertura do chamado e em até 3 dias corridos com solução definitiva aplicada. Considerados problemas urgentes: Serviço interrompido, perda completa de todo o serviço. Exs.: Falha no Firewall que não permita conexão com a Internet ou qualquer outro tipo de problema de hardware/software que acarrete indisponibilidade do serviço para o usuário.

4.6.3.2. **Os chamados considerados de alta prioridade** deverão ser atendidos com solução paliativa no dia seguinte após abertura do chamado e em até 7 dias corridos com solução definitiva aplicada. Considerados problemas de alta prioridade: serviço degradado e ou oscilando, severa indisponibilidade do serviço. Exs.: falhas em equipamentos, conectores, cabos que acarretem indisponibilidade do serviço.

4.6.3.3. **Os chamados considerados de baixa prioridade** deverão ser atendidos com solução paliativa em até 48 horas corridas após abertura do chamado e em até 30 dias corridos com solução definitiva aplicada. Considerados problemas de baixa prioridade: serviço estável, o problema é um erro menor, contornável, sem ocasionar

perda de dados. Exs: ajustes nas regras de firewall, problemas na realização de atualizações.

4.6.4. Os atendimentos aos chamados deverão ocorrer durante o horário de expediente da Câmara Municipal de Londrina, ou com agendamento prévio.

5. MODELO DE EXECUÇÃO: CONDIÇÕES DE SOLICITAÇÃO, ENTREGA E RECEBIMENTO DO OBJETO

5.1. Após a homologação do processo de contratação a nota de empenho será encaminhada pelo Fiscal ao Contratado via e-mail ou via aplicativo de mensagens (WhatsApp), como forma de solicitação de início da execução.

5.2. O prazo para a implantação dos projetos solicitados nos itens 4.2, 4.3 e 4.4 deste Termo de Referência se dará de forma imediata e integral, em prazo não superior a 90 (noventa) dias corridos, contados a partir do envio da solicitação e da Nota de Empenho ao e-mail da empresa.

5.2.1. O prazo de entrega poderá ser prorrogado uma vez, desde que haja solicitação formal do Contratado antes do prazo de entrega terminar e que este demonstre a existência de fato posterior, que não dependa de sua vontade, mas impeça o regular cumprimento do prazo inicial de execução.

5.2.2. O pedido de prorrogação de prazo de entrega será encaminhado ao Fiscal da contratação e este apreciará a pertinência da justificativa apresentada.

5.2.3. A prorrogação do prazo de entrega não será superior a 30 (trinta) dias corridos e não eximirá o Contratado de eventual aplicação de penalidades.

5.3. Os treinamentos solicitados nos itens 4.5. deste Termo de Referência poderão ser realizados no prazo máximo de até 1 (um) ano, a depender da agenda de treinamentos disponibilizada pela Contratada.

5.4. As palestras para conscientização sobre Cibersegurança, descritas no item 4.8. deste Termo de Referência deverão ser realizadas anualmente, com agendamento prévio de pelo menos 30 dias.

5.5. A prestação mensal dos serviços iniciará após o recebimento definitivo da fase de implantação do projeto.

5.6. Os serviços deverão ser implantados na sede do órgão, localizado no Centro Cívico Bento Munhoz da Rocha Neto, Rua Parigot de Souza, nº. 145, Londrina, Paraná, CEP: 86015-903.

5.6.1. A Nota Fiscal/Fatura deverá ser entregue com os itens.

5.6.2. A Contratada arcará com os custos da entrega.

5.6.3. A Contratada se responsabilizará por danos decorrentes do transporte.

5.7. O objeto da contratação será recebido pelo Fiscal de forma:

5.7.1. Provisória, no prazo de até 5 dias, contados da data da entrega.

5.7.2. Definitiva, no prazo de 15 dias, contados do recebimento provisório.

5.8. O recebimento provisório consistirá na conferência básica da quantidade dos itens entregues em confronto com a Nota Fiscal e será dado mediante assinatura no canhoto do documento fiscal ou em protocolo de entrega.

5.8.1. O Fiscal poderá recusar o recebimento provisório em caso de incompatibilidade entre os quantitativos ou características declarados no documento fiscal e o efetivamente entregue e no caso de evidente desatendimento da solicitação.

5.9. O recebimento definitivo pressupõe a verificação da adequação do produto entregue às especificações deste Termo de Referência e à proposta do Contratado e será dado mediante ateste na Nota Fiscal ou termo de recebimento específico.

5.9.1. O prazo do recebimento definitivo ficará suspenso caso haja a necessidade da correção na entrega do objeto ou na Nota Fiscal apresentada, situação em que poderá ser dado recebimento definitivo na parcela incontroversa, em conformidade com documento fiscal específico.

5.10. Nenhuma espécie de recebimento prejudica a responsabilidade da empresa fornecedora por vícios ocultos.

5.11. Na impossibilidade de entrega da marca proposta, a Contratada poderá solicitar, via e-mail, ao Fiscal a solicitação de troca de marca, desde que:

5.11.1. Indique a motivação, devidamente comprovada, da impossibilidade de entrega da marca originalmente proposta.

5.11.2. Indique a nova marca a ser entregue, acompanhada de catálogo ou documento que comprove o pleno atendimento de todas as especificações exigidas no presente Termo de Referência;

5.11.3. Seja realizado dentro do prazo inicial de entrega dos produtos solicitados.

5.12. Após o recebimento da fase de implantação, será iniciada a execução da fase de prestação de serviços, com o envio da Nota de Empenho mensal pelo Fiscal do Contrato à Contratada.

6. MODELO DE EXECUÇÃO: CONDIÇÕES DE PAGAMENTO

6.1. Além das informações essenciais acerca da prestação realizada, a Nota Fiscal deverá ser apresentada com a descrição da prestação do serviço, com as seguintes informações:

6.1.1. Se a empresa é optante pelo Simples, se for o caso.

6.1.2. Com a indicação das retenções tributárias devidas, se for o caso, especialmente em relação ao Imposto de Renda Retido na Fonte (IRRF) quando necessário, conforme Instrução Normativa nº 1234/2012 da Receita Federal e Decreto Municipal nº 776/2023.

6.1.3. Com a informação do número e ano da Nota de Empenho a qual se refere.

6.1.4. Com a informação do número e ano do tipo de licitação.

6.1.5. Com a informação do número e ano do contrato e do aditivo, se for o caso.

6.2. O pagamento do objeto deste contrato será feito à empresa Contratada em até 7 (sete) dias úteis, contados do recebimento definitivo dos itens solicitados.

6.2.1. Havendo erro na apresentação da Nota Fiscal/Fatura ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, o prazo para pagamento ficará suspenso desde a notificação até que a Contratada providencie as medidas saneadoras.

6.2.2. Nessa hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante.

6.3. O pagamento será efetuado por meio de Ordem Bancária de Crédito, mediante depósito em conta-corrente, na agência e estabelecimento bancário indicado pela Contratada, ou por outro meio previsto na legislação vigente.

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

6.4. A Contratante não se responsabilizará por qualquer despesa que venha a ser efetuada pela Contratada, que não tenha sido especificada no Termo de Referência.

6.5. A Contratante poderá motivadamente adotar providências acauteladoras, inclusive retendo o pagamento, como forma de prevenir a ocorrência de dano de difícil ou impossível reparação.

7. MODELO DE EXECUÇÃO: OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

7.1. A Contratada se obriga a:

7.1.1. Efetuar a implantação dos serviços em perfeitas condições, no prazo e local indicado pela Administração, em estrita observância das especificações Termo de Referência e da proposta, acompanhado da respectiva nota fiscal constando detalhadamente as indicações da marca, tipo e procedência;

7.1.2. Responsabilizar-se pelos vícios e danos decorrentes do produto, de acordo com as normas do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);

7.1.3. O dever previsto no subitem anterior implica na obrigação de, a critério da Administração, substituir, reparar, corrigir, remover, ou reconstruir, às suas expensas, no prazo máximo de 7 (sete) dias corridos, os produtos com avarias ou defeitos;

7.1.4. Atender prontamente a quaisquer exigências da Administração, inerentes ao objeto do presente termo de referência;

7.1.5. Prestar todos os esclarecimentos e informações que forem solicitados de maneira clara, concisa e lógica, bem como atendendo de imediato às reclamações;

7.1.6. Comunicar à Administração, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação.

7.1.7. Não transferir a terceiros, por qualquer forma, nem mesmo parcialmente, as obrigações assumidas, nem subcontratar qualquer das prestações a que está obrigada, exceto nas condições autorizadas no Termo de Referência. Caso seja necessário, serão permitidas as subcontratações listadas nos itens a seguir:

7.1.7.1. Instalação dos equipamentos;

7.1.7.2. Suporte a chamados;

7.1.7.3. Treinamentos;

7.1.7.4. Serviços de manutenção nos equipamentos e dispositivos, desde que executada por assistência técnica autorizada pelo fabricante.

7.1.8. Responsabilizar-se pelas despesas dos tributos, encargos trabalhistas, previdenciários, fiscais, comerciais, taxas, fretes, seguros, deslocamento de pessoal, prestação de garantia e quaisquer outras que incidam ou venham a incidir na execução das obrigações assumidas.

7.1.9. Utilizar o endereço de e-mail e/ou o número de telefone em aplicativo de mensagens (WhatsApp) indicado em sua proposta ou informado no início da execução do Contrato como meio oficial de comunicação com a Contratante, devendo mantê-lo atualizado e apto a receber mensagens da Contratante.

7.1.10. Quando for o caso, a Contratada deverá entregar os Termos de Garantia dos produtos, emitidos pelos fabricantes e assinados pelo representante legal da empresa, junto ao material.

7.2. A Contratante se obriga a:

7.2.1. Verificar minuciosamente e no prazo a conformidade dos serviços implementados, com as especificações constantes do Termo de Referência e da proposta da Contratada, para fins de aceitação e recebimento definitivo;

7.2.2. Rejeitar, no todo ou em parte, objeto entregue em desacordo com as obrigações assumidas pela contratada, justificando as razões da recusa.

7.2.3. Acompanhar e fiscalizar o cumprimento das obrigações da Contratada por meio de servidor especialmente designado, nos termos do art. 117 da Lei nº 14.133/2021.

7.2.4. Proceder ao pagamento da fatura decorrente deste instrumento na forma e prazo pactuados.

7.2.5. Notificar, por escrito, a Contratada, da ocorrência de eventuais imperfeições no curso da execução do objeto, fixando prazo para a sua correção.

7.2.6. Emitir, explicitamente, decisão sobre todas as solicitações e reclamações relacionadas à execução do objeto, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do contrato, nos termos do art. 123 da Lei 14.133/2021.

8. MODELO DE GESTÃO DO CONTRATO: DA FISCALIZAÇÃO DA CONTRATAÇÃO

8.1. A fiscalização da contratação será exercida por representante da Câmara Municipal de Londrina, ao qual competirá acompanhar e orientar a execução do objeto.

8.1.1. A fiscalização será exercida pelo(a) servidor(a) Mitio Yoshida, lotado no Departamento de Informática, matrícula 4212.

8.1.2. O servidor responsável pela fiscalização poderá ser substituído por ato do Gerente do respectivo departamento ou despacho do Diretor-Geral, devendo a alteração, em qualquer caso, ser formalmente comunicada à Contratada e à Gestão do Contrato.

8.2. Ao Fiscal do contrato ficam designadas as seguintes atribuições:

8.2.1. Somente solicitar prestações da Contratada mediante o envio da Nota de Empenho correspondente.

8.2.2. Acompanhar e orientar a execução do objeto, determinando o que for necessário para a regularização das faltas ou dos defeitos observados.

8.2.3. Receber provisória e definitivamente o objeto, verificando a correção dos valores apontados na Nota Fiscal/ Fatura, antes de remetê-la ao Departamento Financeiro para pagamento.

8.2.4. Anotar em registro próprio todas as ocorrências relacionadas com a execução, indicando a data e o nome dos envolvidos

8.2.5. Controlar os saldos e quantitativos já executados e/ou já empenhados, a empenhar ou a executar, bem como os já efetivamente pagos do Contrato.

8.2.6. Comunicar ao Gestor do Contrato caso identifique faltas ou defeitos na execução aptas a causar a instauração de procedimento administrativo para aplicação de penalidade.

8.3. A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica em corresponsabilidade da Contratante ou de seus agentes e prepostos, de conformidade com o art. 120 da Lei nº 14.133/2021.

8.4. A gestora do Contrato será indicada na minuta de Contrato.

8.4.1. A Gestora do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133/2021.

9. MODELO DE GESTÃO DO CONTRATO: DAS INFRAÇÕES CONTRATUAIS E SANÇÕES ADMINISTRATIVAS

9.1. Nos termos do art. 155 da Lei 14.133/2021, a Contratada, ao descumprir quaisquer das cláusulas ou condições do presente Termo de Referência, ficará sujeita às penalidades previstas no art. 156 da referida Lei, observando-se o direito ao contraditório e à ampla defesa.

9.2. À Contratada poderão ser aplicadas as seguintes sanções:

9.2.1. Advertência por faltas leves, assim entendidas aquelas que não acarretarem prejuízos significativos ao objeto da contratação.

9.2.2. Multa:

9.2.2.1. Moratória de 0.5% (meio por cento) por dia de atraso injustificado na finalização da fase de Implantação, calculado sobre o valor da Nota de Empenho ou valor proporcional do item inadimplido, até o limite de 20% (vinte por cento). O atraso superior a 40 (quarenta) dias será considerado inexecução total do objeto da contratação ou do respectivo item inadimplido.

9.2.2.2. Multa moratória de 0,5% (meio por cento) sobre o valor mensal, por dia de atraso injustificado, limitado a 15% (quinze por cento), no descumprimento do Acordo de Nível de Serviço (SLA) definido no item 4.9.3 deste Termo de Referência.

9.2.2.3. Compensatória de até 30% (trinta por cento) sobre o valor total do empenho, em caso da não realização dos treinamentos descritos no item 4.5.

9.2.2.4. Compensatória de até 30% (trinta por cento) sobre o valor total da contratação, em caso de inexecução total do objeto, ou do valor proporcional ao item inadimplido, no caso de inexecução total de itens específicos.

9.2.3. Impedimento de licitar e contratar com a Administração direta e indireta do Município de Londrina pelo prazo de até 3 (três) anos, nos casos dos incisos II, III, IV, V, VI e VII do caput do art. 155 desta Lei, quando não se justificar a imposição de penalidade mais grave.

9.2.4. Declaração de inidoneidade para licitar ou contratar com a Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, nos casos dos incisos VIII, IX, X, XI e XII do caput do art. 155 desta Lei e nos casos citados no subitem anterior que justifiquem a imposição de sanção mais grave.

9.3. A penalidade de multa pode ser aplicada cumulativamente com as demais sanções.

9.4. A entrega de objeto em desacordo com o Termo de Referência não descaracteriza a mora, que continuará sendo contada sem interrupção até a entrega adequada do objeto.

9.5. A advertência será aplicada diretamente pelo Fiscal da contratação, sem a necessidade de instauração de processo administrativo ou de comissão para apuração de responsabilidade, cabendo recurso administrativo no prazo de 15 (quinze) dias úteis à autoridade superior (Diretor-Geral), contados a partir da notificação, pelo Fiscal, da aplicação da advertência.

9.5.1. Caso haja recurso contra a aplicação da advertência, a petição deverá ser encaminhada à Gestora para encaminhamentos processuais até a decisão do recurso pelo Diretor-Geral.

9.6. As sanções multa, impedimento de licitar e contratar com o Município de Londrina e de declaração de inidoneidade para licitar e contratar com a Administração Pública serão aplicadas mediante instauração de processo administrativo para apuração de responsabilidade, conduzido por comissão processante formada por, no mínimo, 2 (dois) agentes públicos, na seguinte forma:

9.6.1. O fiscal deverá encaminhar ao gestor relatório acerca do descumprimento contratual;

9.6.2. Recebido o relatório, o Gestor encaminhará para a Diretoria-Geral, para a instauração do processo, e para a Presidência, para designação dos servidores, escolhidos entre os lotados na Controladoria, no Departamento de Suprimentos e Patrimônio e/ou no Departamento demandante, que comporão a comissão processante, respeitada a segregação de função.

9.7. O processo administrativo tramitará da seguinte forma:

9.7.1. O interessado será notificado sobre a abertura do processo administrativo para apuração de responsabilidade para apresentação de defesa prévia no prazo de 15 (quinze) dias úteis, sendo informado que, caso tenha interesse, deve indicar, desde já, as provas que pretende produzir e que os autos estão disponíveis para consulta.

9.7.2. O pedido de produção de provas será rejeitado, mediante decisão fundamentada, nos casos em que for manifestamente protelatório ou irrelevante para o caso concreto.

9.7.3. Caso aceito o pedido de produção de provas, após a dilação probatória do processo, deverá ser concedido novo prazo de 15 (quinze) dias úteis ao interessado para alegações finais.

9.7.4. Em seguida, a comissão processante elaborará relatório e encaminhará para decisão da Diretoria-Geral em caso de arquivamento ou aplicação das penas de multa e impedimento de licitar e contratar ou para a Presidência, em caso de aplicação da pena de declaração de inidoneidade.

9.8. Na aplicação das sanções, a autoridade competente levará em consideração a gravidade da infração cometida, as peculiaridades do caso concreto, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

9.9. Da decisão que aplicar a pena de multa e de impedimento de licitar com o Município de Londrina, caberá recurso administrativo ao Presidente no prazo de 15 (quinze) dias úteis, contados da notificação.

9.9.1. O recurso será dirigido ao Diretor-Geral, que terá o prazo de 5 (cinco) dias úteis para reconsiderar sua decisão ou encaminhar o recurso à Presidência para decisão no prazo de 20 (vinte) dias úteis.

9.9.2. O recurso terá efeito suspensivo.

9.10. Da decisão que aplicar a pena de declaração de inidoneidade, caberá pedido de reconsideração ao Presidente no prazo de 15 (quinze) dias úteis, contados da notificação, que será decidido no prazo de 20 (vinte) dias úteis.

9.11. Transitada em julgado a decisão que aplicou a penalidade:

9.11.1. A interessada será notificada.

9.11.2. Será extraída portaria da decisão de aplicação da penalidade para publicação no Jornal Oficial do Município (exceto no caso de advertência), cuja data será utilizada como termo inicial da contagem dos efeitos.

9.11.3. A penalidade aplicada será registrada no SICAF e no Cadastro de Impedidos de Licitar do Tribunal de Contas do Estado do Paraná.

9.12. O prazo para pagamento da multa será de 10 (dez) dias após o recebimento da notificação para recolhimento.

9.13. A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante.

9.14. Aplica-se subsidiariamente ao procedimento de penalização previsto no presente Termo de Referência, o procedimento previsto na Lei nº 14133/2021, e analogicamente o previsto na Lei nº 9.784, de 1999.

Londrina, *datado e assinado eletronicamente*.

Câmara Municipal de Londrina
Estado do Paraná

Anderson Rafael Delattre Abe
Departamento de Informática