ANEXO I

TERMO DE REFERÊNCIA

1. UNIDADE SOLICITANTE

1.1. Setor de TI

2. OBJETO

2.1. Contratação de empresa para prestação de serviços de gerenciamento da infraestrutura de TI, incluindo os Serviços de Next Generation Firewall (NGFW), manutenção corretiva e preventiva de servidores, gerenciamento eficiente da rede com e sem fio, execução regular de backups com armazenamento de dados em nuvem, para atender às demandas da Câmara Municipal de Carapicuíba, pelo período de 1 (um) ano, conforme especificações constantes neste Anexo I - Termo de Referência.

2.2. À luz das definições contidas nos incisos XIII e XV do artigo 6º da Lei 14.133/2021, o objeto em questão se classifica como serviços comuns e contínuos.

3. JUSTIFICATIVA E OBJETIVO DA CONTRATAÇÃO

3.1. A crescente digitalização dos processos legislativos, administrativos e de atendimento ao cidadão exige da Câmara Municipal de Carapicuíba uma infraestrutura tecnológica cada vez mais segura, estável e eficiente. Neste contexto, a contratação de uma empresa especializada torna-se fundamental para garantir a continuidade das operações institucionais, a integridade das informações públicas e o cumprimento das normas legais e boas práticas em tecnologia da informação.

3.2. A demanda contempla três eixos essenciais:

3.2.1. Segurança da Informação: Diante do aumento dos riscos cibernéticos, como vazamentos de dados, ataques de ransomware e acessos indevidos, é imprescindível a implementação de políticas de segurança robustas. A empresa contratada deverá atuar com o serviço de firewall, protegendo o perímetro e a confidencialidade das informações legislativas e administrativas.

3.2.2. Suporte Técnico Especializado: A atuação contínua e qualificada no suporte aos equipamentos Câmara, é essencial para garantir o bom funcionamento dos equipamentos, redes e servidores utilizados no cotidiano institucional. A contratação visa assegurar agilidade no atendimento de demandas técnicas, prevenindo falhas operacionais e promovendo maior eficiência nos serviços públicos.

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850

3.2.3. Gestão de Backup Local e em Nuvem: A manutenção de cópias de segurança atualizadas, tanto em servidores locais quanto em ambientes de nuvem, é um requisito essencial para a proteção dos dados institucionais. A empresa deverá garantir a integridade e a disponibilidade das informações, além de estabelecer rotinas automáticas de backup e mecanismos eficazes de recuperação em caso de perda de dados.

3.3. A solução de Next Generation Firewall (NGFW) como serviço tem como objetivo proporcionar uma solução completa de segurança perimetral, aliada à gestão integrada da infraestrutura de rede e à proteção dos dados institucionais. A solução contempla a disponibilização e operação contínua de um firewall de próxima geração, com funcionalidades avançadas como inspeção profunda de pacotes, prevenção contra intrusões (IPS), controle de aplicações, filtragem de conteúdo, integração com VPNs e mecanismos de defesa contra ameaças conhecidas e desconhecidas. Todo o ambiente será gerenciado em regime de serviço (as a service), incluindo atualizações, licenciamento, monitoramento e manutenção proativa.

3.4. O serviço inclui suporte técnico e monitoramento 24x7 por meio de um Centro de Operações de Rede (NOC), responsável pela visualização, notificação e análise de incidentes de segurança em tempo real, garantindo resposta rápida a qualquer anomalia identificada no ambiente. Também está contemplado o suporte técnico 24x7 para a solução de antivírus corporativo, abrangendo ações de mitigação, atualização de assinaturas, investigação de alertas e suporte especializado em caso de incidentes relacionados a malware, spyware, ransomware, entre outras ameaças.

3.5. Além disso, será prestado suporte técnico completo para todos os access points e switches gerenciáveis da rede, incluindo atendimento remoto e/ou presencial, conforme a necessidade, para diagnóstico de falhas, substituição de equipamentos com defeito, aplicação de atualizações e ajustes de configuração que assegurem o pleno funcionamento e o desempenho adequado da infraestrutura de rede.

3.6. Por fim, o serviço contempla o gerenciamento de backup como serviço (Backup as a Service - BaaS), com armazenamento em nuvem de cópias de segurança dos dados críticos e a manutenção de uma segunda cópia local, garantindo a disponibilidade, integridade e rápida recuperação das informações em caso de falha, exclusão acidental ou evento de indisponibilidade. O gerenciamento incluí políticas de retenção, monitoramento dos jobs de backup, relatórios periódicos e suporte para recuperação de dados sempre que necessário.

3.7. Essa abordagem integrada permite à instituição contar com um ambiente de TI mais seguro, estável e continuamente monitorado, com suporte especializado e alta disponibilidade de serviços essenciais à sua operação.

3.8. A contratação está alinhada às diretrizes da Lei Geral de Proteção de Dados (LGPD), às normas de governança em TI e às necessidades específicas da Câmara Municipal de Carapicuíba, que carece de equipe técnica própria para atender plenamente essas demandas com a complexidade e a responsabilidade exigidas.

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850

3.9. Dessa forma, justifica-se plenamente a contratação de empresa especializada, visando não apenas a modernização e segurança da infraestrutura tecnológica da Câmara, mas também a proteção do interesse público, a transparência institucional e a eficiência dos serviços prestados à população.

3.10. A justificativa da necessidade da contratação encontra-se pormenorizada no Estudo Técnico Preliminar que será disponibilizado após a homologação do processo licitatórios, nos termos do §3° do art. 54 da Lei 14.133/2021.

4. QUANTITATIVOS E ESPECIFICAÇÕES

	ITEM	DESCRIÇÃO	QNT MESES
LOTE 01	01	Serviços de Next Generation Firewall (NGFW)	12
	02	Serviço de Backup	12
	03	Suporte Técnico e Monitoramento	12
	04	Serviço de Instalação e Configuração	01

4.1. Os equipamentos e soluções a serem utilizados na execução dos serviços de segurança da informação deverão atender aos mais rigorosos requisitos de segurança da informação, compatibilidade eletromagnética e eficiência energética. Deverão, ainda, apresentar baixo nível de ruído em operação, visando garantir um ambiente de trabalho adequado. Os dispositivos deverão ser capazes de realizar inspeção profunda de pacotes (DPI), controle de aplicações, detecção e prevenção de intrusões (IDS/IPS), gerenciamento centralizado e políticas de segurança customizáveis, assegurando total compatibilidade com a infraestrutura de rede existente e atendendo às exigências da legislação vigente, em especial a Lei Geral de Proteção de Dados (LGPD).

4.2. Deverão ser apresentados pela licitante proponente, após ser declarada vencedora, para fins de avaliação de conformidade e aceitabilidade da proposta, para fins de formalização e conferência final, sempre que solicitado pela Administração (inclusive por diligência e no prazo por ela definido), todos os catálogos, datasheets/folhetos técnicos, manuais e demais documentos técnicos dos equipamentos, softwares e serviços ofertados, emitidos pelo fabricante/desenvolvedor ou representante oficial, contendo de forma objetiva as especificações técnicas e a descrição detalhada dos recursos utilizados (equipamentos, softwares, componentes, acessórios e demais itens que compõem a solução), de modo a permitir a consistente avaliação da conformidade dos itens com as exigências do Termo de Referência.

5. DESCRIÇÃO TÉCNICA DA SOLUÇÃO

5.1. ITEM 1: Serviços de Next Generation Firewall (NGFW):

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850

5.1.1. Fornecer e substituir, em caso de necessidade, as peças defeituosas de todos os equipamentos e efetuar os necessários ajustes sem ônus para o Contratante desde que os danos causados não sejam decorrentes do mau uso, imperícia ou imprudência.
5.1.2. Os equipamentos devem ser iguais e suportar no mínimo as seguintes configurações e ser configuradas de acordo com ambiente:
5.1.3. Especificações Gerais:
5.1.4. Os equipamentos a serem utilizados deverá fornecer logs e relatórios embarcados, com armazenamento histórico mínimo de 12 meses, contendo no mínimo os itens abaixo:

- Dashboard com informações do sistema:
- Informações de CPU
- Informações do uso da rede.
- Informações de memória.
- Informações de atividades de navegação.
- Permitir visualizar número políticas ativas.
- Visualizar número de usuários conectados remotamente.
- Visualizar número de usuários conectados localmente.

5.1.5. Relatórios com informações sobre as conexões de origem e destino por países.
5.1.6. Relatórios informando as conexões dos hosts.
5.1.7. Visualizar relatórios por período, permitindo o agendamento e o envio destes relatórios por e-mail.
5.1.8. Permitir exportar relatórios para as seguintes extensões/plataformas:

- PDF
- HTML
- Excel

5.1.9. Permitir visualizar relatório de políticas ativas associado ao ID da política criada.
5.1.10. Possuir pelo menos, 1 (um) slot para adição de módulo de portas;
5.1.11. Deverá possuir Pinos de montagem para externo fonte de energia.
5.1.12. Possuir no máximo as seguintes dimensões 438 x 44 x 405 mm.
5.1.13. Ter o peso máximo após desembalado de 9 kg.
5.1.14. Possuir os seguintes certificados CB, CE, UKCA, UL, FCC, ISED, VCCI, KC, RCM, NOM, Anatel, CCC, BSMI, TEC e SDPPI.
5.1.15. Possuir ao menos uma porta para gerenciamento de conexão RJ45 e uma conexão Micro-USB.
5.1.16. Relatório que informe o uso IPSEC por host e usuário.
5.1.17. Relatório que informe o uso L2TP por host e usuário.
5.1.18. Relatório que informe o uso PPTP por usuários.
5.1.19. Relatório abordando eventos de VPN.
5.1.20. Proporcionar sistema de logs em tempo real, com no mínimo as seguintes informações:

- Logs do sistema;
- Logs das políticas de segurança;
- Logs de autenticação;

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850

- Logs de administração do firewall NGFW.
- Permitir ocultar os relatórios usuários e IPs cadastrados.

5.1.21. A solução firewall deverá possuir no mínimo as seguintes configurações tanto quanto de software como de hardware:

5.1.22. Modalidade de configuração, alta disponibilidade e dois equipamentos configurados como ativo/ativo.

5.1.23. Possuir no mínimo 8 interfaces 10/100/1000 base-T.

5.1.24. Possuir no mínimo 2 interfaces SFP Fibra.

5.1.25. Deve possuir no mínimo 1 portas que suportem by-pass.

5.1.26. A solução proposta deve corresponder aos seguintes critérios:

- Suportar no mínimo 134.700 novas conexões por segundo;
- Suportar no mínimo 6.500.000 conexões simultâneas;
- Possuir no mínimo 30 Gbps de rendimento (throughput) do Firewall;
- No mínimo 6.000 Mbps de rendimento (throughput) de IPS;
- Deverá possuir no mínimo 5.000 Mbps de taxa de transferência de Threat Protection.
- Latência do Firewall máxima (UDP de 64 bytes) 6 µs.
- IPsec VPN throughput deverá suportar no mínimo 17.000 Mbps.
- Quantidade mínima de túneis simultâneos VPN IPsec 5.000.
- Quantidade mínima de Túneis simultâneos SSL VPN 2.500
- Inspeção SSL/TLS de 1.100 Mbps no mínimo.
- Deve possuir um interruptor de alimentação.
- Conexões SSL/TLS simultâneas 18.432.

5.1.27. A solução proposta deve suportar a configuração de políticas baseadas em usuários para segurança e gerenciamento de internet.

5.1.28. A solução proposta deve fornecer os relatórios diretamente no Firewall NGFW, baseados em usuário, não só baseado em endereço IP.

5.1.29. A solução proposta deve possuir no mínimo 120 GB de espaço em disco SSD SATA-III para o armazenamento local de eventos e relatórios.

5.1.30. Deverá ter disponível pelo menos 2 conexões USB 3.0.

5.1.31. Não deverá possuir limitação na quantidade de VPN via Software.

5.1.32. Deverá possuir um display LCD, multifuncional e na parte frontal do firewall.

5.1.33. Número irrestrito de usuários/IP conectados.

5.1.34. O equipamento deve ter no máximo 1 (um) U de altura para montagem em rack.

5.1.35. A solução proposta deve suportar administração via comunicação segura (HTTPS, SSH) e console.

5.1.36. A solução proposta deve ser capaz de importar e exportar cópias de segurança (backup) das configurações, incluindo os objetos de usuário.

5.1.37. O backup pode ser realizado localmente, enviado pela ferramenta para um ou mais e-mails pré-definidos, deve-se também ser feito sob demanda, ou seja, agendar para que este backup seja realizado, por dia, semana, mês e ano.

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850

5.1.38. A solução proposta deve suportar implementações em modo Router (camada 3) e transparente (camada 2) individualmente ou simultâneos.
5.1.39. A solução proposta deve suportar integrações com Active Directory, LDAP, Radius, eDirectory, TACACS+ e Banco de Dados Local para autenticação do usuário.
5.1.40. A solução proposta deve suportar em modo automático e transparente "Single Sign On" na autenticação dos usuários do active directory e eDirectory.
5.1.41. Suporte à autenticação do Chromebook.
5.1.42. Os tipos de autenticação devem ser, modo transparente, por autenticação NTLM e cliente de autenticação nas máquinas.
5.1.43. Fornecer clientes de autenticação para Windows, MacOS X, Linux 32/64.
5.1.44. Certificados de autenticação para iOS e Android.
5.1.45. A solução proposta deve ter gráficos de utilização de banda em modos diários, semanais, mensais ou anuais para os links de forma consolidada ou individual.
5.1.46. A solução proposta deve suportar Parent Proxy com suporte a IP / FQDN.
5.1.47. A solução proposta deve suportar NTP.
5.1.48. A solução proposta deverá suportar a funcionalidade de unir usuário/ip/mac para mapear nome de usuário com o endereço IP e endereço MAC por motivo de segurança.
5.1.49. A solução proposta deve ter suporte multilíngue para console de administração web.
5.1.50. A solução proposta deverá suportar fazer um rollback de versão.
5.1.51. A solução proposta deve suportar a criação de usuário baseada em ACL para fins de administração.
5.1.52. A solução proposta deve suportar instalação de LAN by-pass no caso do firewall NGFW estar configurado no modo transparente.
5.1.53. A solução proposta deve suportar cliente PPPOE e deve ser capaz de atualizar automaticamente todas as configurações necessárias, sempre que o PPPoE mudar.
5.1.54. A solução proposta deve suportar SNMP v1, v2c.
5.1.55. A solução proposta deve suportar SSL/TLS para integração com o Active Directory ou LDAP.
5.1.56. A solução proposta deve ser baseada em Firmware ao contrário de Software e deve ser capaz de armazenar duas versões de Firmware ao mesmo tempo para facilitar o retorno "rollback" da cópia de segurança.
5.1.57. A solução proposta deve fornecer uma interface gráfica de administração flexível e granular baseado em perfis de acesso.
5.1.58. A solução proposta deve fornecer suporte a múltiplos servidores de autenticação para diferentes funcionalidades (Exemplo: Firewall um tipo de autenticação, VPN outro tipo de autenticação).
5.1.59. A solução proposta deve ter suporte a ambiente de terminais (Microsoft) suportando autenticação de usuário de diferentes sessões originando do mesmo endereço IP.
5.1.60. A solução proposta deve suportar:
5.1.61. Serviço de DHCP/DHCPv6;
5.1.62. Serviço de DHCP/DHCPv6 Relay Agent;
5.1.63. A solução proposta deve trabalhar como DNS/DNSv6 Proxy.
5.1.64. Gráficos, relatórios e ferramentas avançadas de apoio para troubleshooting.
5.1.65. Permitir exportar informações de troubleshooting para arquivo PCAP.

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850

5.1.66. Reutilização de definições de objetos de rede, hosts, serviços, período, usuários, grupos, clientes e servers.
5.1.67. Portal de acesso exclusivo para usuários poderem realizar atividades administrativas que envolve apenas funcionalidades específicas a ele.
5.1.68. Controle de acesso e dispositivos por zoneamento.
5.1.69. Integrar com ferramenta de gerenciamento centralizado disponibilizado pelo próprio fabricante.
5.1.70. Traps SNMP ou e-mail para notificações do sistema.
5.1.71. Suportar envio de informações via Netflow e possuir informações via SNMP;

5.1.2. ESPECIFICAÇÕES DE BALANCEAMENTO DE CARGA E REDUNDÂNCIA PARA MÚLTIPLOS PROVEDORES DE INTERNET

5.1.2.1. A solução proposta deve suportar o balanceamento de carga e redundância (Failover) para no mínimo 2 (dois) links de Internet.
5.1.2.2. Possuir pelo menos, 1 (um) slot para adição de módulo de portas.
5.1.2.3. Deverá possuir Pinos de montagem para externo fonte de energia.
5.1.2.4. Possuir no máximo as seguintes dimensões 438 x 44 x 405 mm.
5.1.2.5. Ter o peso máximo após desembalado de 9 kg.
5.1.2.6. Possuir os seguintes certificados CB, CE, UKCA, UL, FCC, ISED, VCCI, KC, RCM, NOM, Anatel, CCC, BSMI, TEC e SDPPI.
5.1.2.7. Possuir ao menos uma porta para gerenciamento de conexão RJ45 e uma conexão Micro-USB.
5.1.2.8. A solução proposta deve suportar o roteamento explícito com base em origem, destino, nome de usuário e aplicação.
5.1.2.9. A solução proposta deve suportar algoritmo "Round Robin" para balanceamento de carga.
5.1.2.10. A solução proposta deve fornecer opções de condições em caso de falha "Failover" do link de Internet através dos protocolos ICMP, TCP e UDP.l
5.1.2.11. A solução proposta deve enviar e-mail de alerta ao administrador sobre a mudança do status de gateway.
5.1.2.12. A solução proposta deve ter ativo/ativo utilizando algoritmo de "Round Robin".
5.1.2.13. A solução proposta deve fornecer o gerenciamento para múltiplos links de Internet, bem como tráfego IPv4 e IPv6.

5.1.3. ESPECIFICAÇÕES DE ALTA DISPONIBILIDADE

5.1.3.1. A solução proposta deve suportar Alta Disponibilidade (High Availability) no modelo ativo/ativo.
5.1.3.2. A solução proposta deve notificar os administradores sobre o estado (status) dos gateways, mantendo a Alta Disponibilidade.
5.1.3.3. O tráfego entre os equipamentos em Alta Disponibilidade deverá ser criptografado.
5.1.3.4. A solução deverá detectar falha em caso de Link de Internet, Hardware e Sessão.

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850

5.1.4. A solução proposta deve suportar sincronização automática e manual entre os firewalls NGFWs em "cluster".
5.1.5. A solução deve suportar Alta Disponibilidade (HA) em "Bridge Mode" e Mixed Mode" (Gateway + Bridge).

5.1.4. ESPECIFICAÇÕES DO FIREWALL E ROTEAMENTO

5.1.4.1. A solução deve ser Standalone Firewall NGFW e com Sistema Operacional fortalecido "Hardening" para aumentar a segurança.
5.1.4.2. A solução proposta deve suportar "Stateful Inspection" baseado no usuário "one-to-one", NAT Dinâmico e PAT.
5.1.4.3. A solução proposta deve usar a "Identidade do Usuário" como critério de Origem/Destino, IP/Subnet/Grupo e Porta de Destino na regra do Firewall.
5.1.4.4. A solução proposta deve unificar as políticas de ameaças de forma granular como Antivírus/AntiSpam, IPS, Filtro de Conteúdo, Políticas de Largura de Banda e Política de Balanceamento de Carga, baseado na mesma regra do Firewall para facilitar de uso.
5.1.4.5. A solução proposta deve suportar arquitetura de segurança baseado em Zonas.
5.1.4.6. A solução proposta deve ter predefinido aplicações baseadas na "porta/assinatura" e suporte à criação de aplicativo personalizado baseado na "porta/número de protocolo".
5.1.4.7. A solução proposta deve suportar balanceamento de carga de entrada (Inbound NAT) com diferentes métodos de balanceamento como First Alive, Round Robin, Random, Sticky IP e Failover conforme a saúde (Health Check) do servidor por monitoramento (probe) TCP ou ICMP.
5.1.4.8. A solução proposta deve suportar 802.1q (suporte a marcação de VLAN).
5.1.4.9. A solução proposta deve suportar roteamento dinâmico como RIP1, RIP2, OSPF, BGP4.
5.1.4.10. A solução proposta deve possuir uma forma de criar roteamento Estático/Dinâmico via shell.
5.1.4.11. O sistema proposto deve prover mensagem de alertas no Dashboard (Painel de Bordo) quando eventos como, por exemplo: nova firmware disponível para download ou a licença irá expirar em breve.
5.1.4.12. O sistema proposto deve prover Regras de Firewall através de endereço MAC (MAC Address).
5.1.4.13. A solução proposta deve suportar IPv6.
5.1.4.14. A solução proposta deve suportar implementações de IPv6 Dual Stack.
5.1.4.15. A solução proposta deve suportar tuneis 6in4,6to4,4in6,6rd.
5.1.4.16. A solução proposta deve suportar toda a configuração de IPv6 através da Interface Gráfica.
5.1.4.17. A solução proposta deve suportar DNSv6.
5.1.4.18. A solução proposta deve oferecer proteção DoS contra ataques IPv6.
5.1.4.19. A solução proposta deve oferecer prevenção contra Spoof em IPv6.
5.1.4.20. A solução proposta deve suportar 802.3ad para Link Aggregation.
5.1.4.21. A solução proposta deve suportar 3G UMTS e 4G modem via interface USB para VPN e Link Backup "Plano de Continuidade" - Balanceamento de Carga.

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850

5.1.4.22. A solução proposta deve suportar gerenciamento de banda baseado em aplicação, que permite administradores criarem políticas de banda de utilização de link baseado por aplicação.
5.1.4.23. Flood protection, DoS, DDoS e Portscan.
5.1.4.24. Bloqueio de Países baseados em GeoIP.
5.1.4.25. Suporte a Upstream proxy.
5.1.4.26. Suporte a VLAN DHCP e tagging.
5.1.4.27. Suporte a Multiple bridge.
5.1.4.28. Funcionalidades do portal do usuário.
5.1.4.29. Autenticação de dois fatores (OTP) para IPSEC e SSL VPN, portal do usuário, e administração web (GUI).
5.1.4.30. Download dos clientes de autenticação disponibilizados pela ferramenta.
5.1.4.31. Download do cliente VPN SSL em plataformas Windows.
5.1.4.32. Download das configurações SSL em outras plataformas.
5.1.4.33. Informações de hotspot.
5.1.4.34. Autonomia de troca de senha do usuário.
5.1.4.35. Visualização do uso de internet do usuário conectado.
5.1.4.36. Acesso a mensagens em quarentena.
5.1.4.37. Opções base de VPN.
5.1.4.38. Site-to-site VPN: SSL, IPSec, 256-bit AES/3DES, PFS, RSA, X.509 certificates, pre-shared key.
5.1.4.39. L2TP e PPTP.
5.1.4.40. VPN SSL, IPSEC.
5.1.4.41. Proporcionar através do portal do usuário uma forma de conexão via HTML5 de acesso remoto com suporte aos protocolos, RDP, HTTP, HTTPS, SSH, Telnet e VNC.

5.1.5. FUNCIONALIDADES BASE DE QOS E QUOTAS

5.1.5.1. QoS aplicado a redes e usuários de download/upload em tráfegos baseados em serviços.
5.1.5.2. Otimização em tempo real do protocolo VoIP.
5.1.5.3. Suporte a marcação DSCP.
5.1.5.4. Regras associadas por usuário.
5.1.5.5. Criar regras que limitem e garantam upload e download.
5.1.5.6. Permitir criar regra de QoS individualmente e compartilhada.

5.1.6. FILTRAGEM E SEGURANÇA WEB

5.1.6.1. Proporcionar transparência total de autenticação no proxy, provendo segurança antimalware e filtragem web.
5.1.6.2. Possuir uma base de dados com mais de 1.000.000 (um milhão) de URLs reconhecidas e categorizadas, agregadas a pelo menos 75 categorias oferecidas pela solução.
5.1.6.3. Realizar autenticação dos usuários nos modos transparente e padrão.
5.1.6.4. As autenticações devem ser feitas via NTLM.
5.1.6.5. Possuir sistema de quotas aplicado por usuários e grupos.

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850

5.1.6.6. Permitir criar políticas por horário aplicado a usuários e grupos.
5.1.6.7. Possuir sistema de malware scanning que realize as seguintes ações:

- Bloquear toda forma de vírus
- Bloquear malwares web
- Prevenir infecção de malwares, trojans e spyware em tráfegos HTTPS, HTTP, FTP e e-mails baseados em acesso web (via navegador).

5.1.6.8. Prover proteção em tempo real de todos os acessos web.
5.1.6.9. A proteção em tempo real deve consultar constantemente a base de dados na nuvem do fabricante que deverá manter-se atualizada prevenindo novas ameaças.
5.1.6.10. Prover pelo menos duas engines diferentes de antimalware para auxiliar na detecção de ataques e ameaças realizadas durante os acessos web realizados pelos usuários.
5.1.6.11. Fornecer Pharming Protection.
5.1.6.12. Possuir pelo menos dois modos diferentes de escaneamento durante o acesso do usuário.
5.1.6.13. Permitir criação de regras customizadas baseadas em usuário e hosts.
5.1.6.14. Permitir criar exceções de URLs, usuários e hosts para que não sejam verificados pelo proxy.
5.1.6.15. Validação de certificado.
5.1.6.16. Prover cache de navegação, contribuindo na agilidade dos acessos à internet
5.1.6.17. Realizar filtragem por tipo de arquivo, mime-type, extensão e tipo de conteúdo (exemplo: Activex, applets, cookies, etc.)
5.1.6.18. Prover funcionalidade que força o uso das principais ferramentas de pesquisa segura (SafeSearch): Google, Bing e Yahoo.
5.1.6.19. Permitir alterar a mensagem de bloqueio apresentada pela solução para os usuários finais.
5.1.6.20. Permitir alterar a imagem de bloqueio que é apresentado para o usuário quando feito um acesso não permitido.
5.1.6.21. Permitir a customização da página HTML que apresenta as mensagens e alertas para os usuários finais.
5.1.6.22. Especificar um tamanho em Kbytes de arquivos que não devem ser escaneados pela proteção web.
5.1.6.23. Range aceitável de 1 a 25600KB.
5.1.6.24. Bloquear tráfego que não segue os padrões do protocolo HTTP.
5.1.6.25. Permitir criar exceções de sites baseados em URL Regex, tanto para HTTP quanto para HTTPS.
5.1.6.26. Nas exceções, permitir definir operadores "AND" e "OR".
5.1.6.27. Permitir definir nas exceções a opção de não realizar escaneamento HTTPS.
5.1.6.28. Permitir definir nas exceções a opção de não realizar escaneamento contra malware.
5.1.6.29. Permitir definir nas exceções a opção de não realizar escaneamento de critérios especificado por políticas.
5.1.6.30. Permitir criar regras de exceções por endereços IPs de origem.
5.1.6.31. Permitir criar regras de exceções por endereços IPs de destino.
5.1.6.32. Permitir criar exceções por grupo de usuários.

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850

5.1.6.33. Permitir criar exceções por categorias de sites.
5.1.6.34. Permitir a criação de agrupamento de categorias feitas pelo administrador do equipamento.
5.1.6.35. Ter grupos de categorias pré-configuradas na solução apresentando nomes sugestivos para tais agrupamentos, por exemplo: "Criminal Activities, Finance & Investing, Games and Gambling", entre outras.
5.1.6.36. Permitir editar grupos de categorias pré-estabelecidos pela solução.
5.1.6.37. Deve ter sistema que permita a criação de novas categorias com as seguintes especificações:

- Nome da regra;
- Permitir criar uma descrição para identificação da regra.
- Ter a possibilidade de classificação de pelo menos: Produtivo ou Não produtivo;
- Permitir aplicar Traffic shaping diretamente na categoria.
- Na especificação das URLs e domínios que farão parte da regra, deve-se permitir cadastrar por domínio e palavra-chave.
- Deve permitir importar uma base com domínios e palavras chaves na hora da criação da categoria, a base com informações de domínios e palavras chaves deverá aceitar pelo menos as seguintes extensões: .tar, .gz, .bz, .bz2, e .txt.
- Permitir importar a base citada no item anterior de forma externa, ou seja, especificar uma URL externa que contenha as informações com a lista domínios que poderá ser mantida pelo administrador ou um terceiro.

5.1.6.38. Ter função para criar grupos de URLs.
5.1.6.39. A base de sites e categorias devem ser atualizadas automaticamente pelo fabricante.
5.1.6.40. Permitir ao administrador especificar um certificado autoritário próprio para ser utilizado no escaneamento HTTPS.
5.1.6.41. Deve permitir que em uma mesma política sejam aplicadas ações diferentes de acordo com o usuário autenticado.
5.1.6.42. Nas configurações das políticas deve-se existir pelo menos as opções de: Liberar categoria/URL, bloquear e Alarmar o usuário quando feito acesso a uma categoria não desejada pelo administrador.
5.1.6.43. Forçar filtragem diretamente nas imagens apresentadas pelos buscadores, ajudando na redução dos riscos de exposição de conteúdo inapropriado nas imagens.
5.1.6.44. Permitir criar cotas de navegação com os seguintes requisitos:
5.1.6.45. Tipo do ciclo, especificando se o limite será por duração de acesso à internet ou se será especificado uma data limite para o acesso.

5.1.7. CONTROLE E SEGURANÇA DE APLICAÇÕES

5.1.7.1. Prover controle para mais de 2500 aplicações diferentes.
5.1.7.2. Controlar aplicações baseadas em categorias, característica (Ex: Banda e produtividade consumida), tecnologia (Ex: P2P) e risco.
5.1.7.3. Permitir criar regras de controle por usuário e hosts.

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850

5.1.7.4.Permitir realizar traffic shaping por aplicação e grupo de aplicações.
5.1.7.5.Possibilitar que as regras criadas baseadas em aplicação permitam:

- Bloquear o tráfego para as aplicações
- Liberar o tráfego para as aplicações
- Criar categorização das aplicações por risco:
- Risco muito baixo
- Risco baixo
- Risco médio
- Risco alto
- Risco muito alto

5.1.7.6.Permitir visualizar as aplicações por suas características, por exemplo: aplicações que utilizam banda excessiva, consideradas vulneráveis, que geram perda de produtividade, entre outras.
5.1.7.7.Permitir selecionar pela tecnologia, por exemplo: p2p, client server, protocolos de redes, entre outros.
5.1.7.8.Permitir granularidade na hora da criação da regra baseada em aplicação, como por exemplo: Permitir bloquear anexo dentro de um post do Facebook, bloquear o like do Facebook, permitir acesso ao youtube, mas bloquear o upload de vídeos, e etc.
5.1.7.9.Permitir agendar um horário e data específica para a aplicação das regras de controle de aplicativos, podendo ser executadas apenas uma vez como também de forma recursiva.

5.1.8. PROTEÇÃO DE REDE

5.1.8.1.Prover funcionalidade de Intrusion Prevention System (IPS).
5.1.8.2.Proporcionar alta performance na inspeção dos pacotes.
5.1.8.3.Possuir mais de 6500 assinaturas conhecidas.
5.1.8.4.Suportar a customização de assinaturas, permitindo o administrador agregar novas sempre que desejado.
5.1.8.5.Proporcionar flexibilização na criação das regras de IPS, ou seja, permitir que as regras possam ser aplicadas tanto para usuários quanto para redes, permitindo total customização.
5.1.8.6.Possuir funcionalidade Anti-DoS.
5.1.8.7.Deve-se permitir customizar os valores das seguintes funcionalidades de DoS:

- SYN Flood
- UDP Flood
- TCP Flood
- ICMP Flood
- IP Flood

5.1.8.8.Possuir templates pré-configurados pelo fabricante havendo sugestões de fluxo dos pacotes, exemplo: LAN to DMZ, WAN to LAN, LAN to WAN, WAN to DMZ e etc.
5.1.8.9.Possuir proteção contra spoofing.

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850

5.1.8.10. Poder restringir IPs não confiáveis, somente aqueles que possuírem MAC address cadastrados como confiáveis.
5.1.8.11. Possuir funcionalidade para o administrador poder criar by-pass de DoS.
5.1.8.12. Permitir ao administrador clonar templates existentes para ter como base na hora da criação de sua política customizada.

5.1.9. POSSUIR PROTEÇÃO AVANÇADA CONTRA AMEAÇAS PERSISTENTES (APT)

5.1.9.1. Detectar e bloquear tráfego de pacotes suspeitos e maliciosos que trafegam pela rede onde tentam realizar comunicação com servidores de comando externo(C&C), usando técnicas de multicamadas, DNS, AFC, Firewall e outros.
5.1.9.2. Possuir logs e relatórios que informem todos os eventos de APT.
5.1.9.3. Permitir que o administrador possa configurar entre apenas logar os eventos ou logar e bloquear as conexões consideradas ameaças persistentes.
5.1.9.4. Em casos de falso positivo, permitir o administrador criar exceções para o fluxo considerado como APT.
5.1.9.5. Proteção para E-mails
5.1.9.6. Possuir suporte para escaneamento dos protocolos SMTP, POP3 e IMAP.
5.1.9.7. Possuir serviço de reputação para monitoramento dos fluxos dos e-mails, sendo assim, o AntiSpam deverá bloquear e-mails considerados com má reputação na internet e pelo fabricante.
5.1.9.8. Bloquear SPAN e MALWARES durante a transação SMTP.
5.1.9.9. Possuir duas engines de antivírus para duplo escaneamento.
5.1.9.10. Ter proteção em tempo real, sendo que a solução deverá realizar consultas na nuvem para verificar a integridade e segurança dos e-mails que passam pela solução e assim tomar ações automáticas de segurança, caso necessário.
5.1.9.11. Os updates das assinaturas e proteção deverão ser realizados de forma automática pelo fabricante.
5.1.9.12. Possuir funcionalidade que permite detectar arquivos por suas extensões e bloqueá-los caso estejam em anexo.
5.1.9.13. Usar conteúdo pré-definido pela solução para que seja possível criar regras baseadas neste conteúdo ou customizá-los de acordo com o desejado.
5.1.9.14. Ter suporte a criptografia TLS para SMTP, POP e IMAP.
5.1.9.15. As ações dos e-mails considerados SPAM devem ser:
- Drop
- Warn
- Quarantine

5.1.9.16. Poder definir um prefixo no subject de cada e-mail considerado SPAM, como por exemplo: SPAM Marketing etc. etc. etc.
5.1.9.17. Permitir visualizar os e-mails que se encontram na fila para serem enviadas.
5.1.9.18. Possuir funcionalidade que permita a adição de um banner no final dos E-mails analisados pela solução.

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850

5.1.9.19. Possuir funcionalidade de allowlist e blocklist.
5.1.9.20. Possuir funcionalidade que rejeite e-mails com HELO inválido e/ou que não possuam RDNS.
5.1.9.21. Permitir que o escaneamento seja feito tanto para e-mails de entrada quanto para os de saída.
5.1.9.22. Prover ambiente de Sandbox na nuvem provido pelo próprio fabricante.
5.1.9.23. Realizar inspeções de executáveis e documentos que possuam conteúdo executáveis.
5.1.9.24. Possuir suporte aos principais executáveis Windows como: .exe, .com e .dll
5.1.9.25. Possuir suporte aos principais documentos do Word como: .doc, .docx, .docm e .rft.
5.1.9.26. Realizar análise em documentos PDF.
5.1.9.27. Realizar análise de qualquer tipo de conteúdo que possua os seguintes tipos de arquivos: ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet.
5.1.9.28. Suporte a mais de 20 tipos de arquivos e extensões.
5.1.9.29. Realizar análises dinâmicas de malwares e ameaças, rodando estes arquivos em ambientes reais e em produção, todos providos na nuvem pelo fabricante.
5.1.9.30. Relatórios detalhados das ameaças bem como visibilidade dos alertas na dashboard da solução.
5.1.9.31. O tempo em média das análises devem ser menores do que 120 segundos.
5.1.9.32. Suportar a análise de links de download em tempo real.
5.1.9.33. Permitir escolher pelo menos duas regiões para as quais os arquivos para análise devem ser enviados.
5.1.9.34. Possuir uma opção que permita a solução identificar automaticamente o caminho com menor latência para envio dos arquivos para análise.
5.1.9.35. Permitir o administrador criar exceções para aqueles eventos que serão considerados falsos positivos.
5.1.9.36. O firewall NGFW deve oferecer relatórios locais referente a todos os eventos registrados pela funcionalidade de Sandbox.
5.1.9.37. A solução deverá prover uma ferramenta distribuída pelo mesmo fabricante para gerenciamento centralizado de ambos os firewalls NGFWs adquiridos pela Contratante.
5.1.9.38. A solução de gerenciamento deverá permitir que o administrador da ferramenta possa criar políticas de gerenciamento para um ou mais equipamentos e aplicá-los todos de uma única vez.
5.1.9.39. As políticas de configurações devem ter no mínimo as seguintes opções:

- Proteção e políticas de acesso web
- Controle de aplicativos
- IPS
- VPN
- E-mail
- Firewall

5.1.9.40. A solução deverá oferecer funcionalidade que permita o administrador criar templates de configuração, para que o administrador possa aproveitar as mesmas regras para novos firewalls NGFWs.

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850

5.1.9.41. Deverá haver na dashboard da solução, indicadores que permitam o administrador avaliar a saúde do equipamento de uma maneira fácil para visualização.
5.1.9.42. Possuir múltiplas formas de customização de warning thresholds.
5.1.9.43. Possuir flexibilização na hora da criação de grupos de firewall NGFWs gerenciados, sendo possível diferenciá-los como por exemplo: Região, modelo ou outro parâmetro.
5.1.9.44. Deverá possuir funcionalidade que permita o administrador delegar funções para diferentes técnicos, com diferentes funções.
5.1.9.45. Possuir logs de todas as alterações para que seja possível realizar o rollback das alterações realizadas caso necessário.

5.1.10. ANÁLISE E MONITORAMENTO POR INTELIGENCIA ARTIFICIAL

5.1.10.1. Cada firewall deverá ser composto por software integrado através de API's de comunicação para a utilização de inteligência artificial para análise de e ações proativas com o foco nas melhores práticas destacadas pelo fabricante.
5.1.10.2. As ações do software de inteligência artificial deverão tomar ações automáticas e supervisionadas.
5.1.10.3. O serviço de firewall deverá ter disponível API's de comunicação para integração com inteligência artificial voltada a cibersegurança.
5.1.10.4. A inteligência artificial deverá atender todos os equipamentos de firewall e ter compatibilidade com a estrutura ATIVO/ATIVO nos firewalls.
5.1.10.5. A inteligência artificial deverá monitorar todas as ações e regras de firewall para levantamento dos dados referentes as configurações executadas medindo o seu nível de efetividade.
5.1.10.6. Integrar-se aos sistemas de logs do firewall para coletar, analisar e correlacionar eventos de segurança.
5.1.10.7. A criação de logs deverá ser em tempo real.
5.1.10.8. Atuar como uma plataforma centralizada para gerenciar várias instâncias de firewalls, oferecendo visibilidade de toda a infraestrutura de segurança.
5.1.10.9. Em resposta a eventos ou ameaças detectadas, a solução pode disparar ações automáticas no firewall, como bloqueio de IPs, isolamento de dispositivos, ou alterações nas regras de firewall para mitigar riscos.
5.1.10.10. Deverá ajudar a configurar e gerenciar as políticas de segurança no firewall, permitindo ajustes em tempo real de acordo com as necessidades da organização.
5.1.10.11. Através da integração com o firewall, a solução deverá oferecer um painel de monitoramento em tempo real, com relatórios detalhados sobre o tráfego de rede, ataques detectados e atividades suspeitas.
5.1.10.12. Deverá identificar vulnerabilidades de segurança em dispositivos na rede e sugerir ou aplicar correções baseadas nas configurações do firewall.
5.1.10.13. Quando integrada com a proteção de firewall deverá entregar uma abordagem de segurança mais robusta, correlacionando eventos e tomando medidas mais eficazes para a proteção da rede em tempo real.
5.1.10.14. Integração com as funcionalidades de prevenção de intrusões (IPS) e proteção contra malware, para uma resposta rápida a ameaças emergentes.

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850

5.1.10.15. A solução de análise e proteção de inteligência artificial deverá monitorar e proteger todos os servidores tanto virtuais como físicos.
5.1.10.16. A solução de análise e proteção de inteligência artificial deverá monitorar e proteger todos os storages, NAS e dispositivos de armazenamento externo.

5.2. ITEM 2: SERVIÇO DE BACKUP:

5.2.1. O licenciamento da solução deverá cobrir a solução de Armazenamento e Compartilhamento de arquivos em Windows, presente neste documento, pelo período do contrato.
5.2.2. Após a conclusão do contrato, deverão ser excluídos todos os dados armazenados em nuvem, com as devidas evidências apresentadas e aprovadas pela CONTRATANTE.
5.2.3. Condições Gerais:
5.2.4. A solução deverá incluir funcionalidades de proteção (backup) e replicação integradas em uma única solução, incluindo retorno (rollback) de réplicas e replicação desde e até a infraestrutura virtualizada.
5.2.5. A solução não deverá necessitar de instalação de agentes para poder realizar suas tarefas de proteção, recuperação e replicação das máquinas virtuais.
5.2.6. Deverá garantir, no mínimo, a proteção de máquinas virtuais e seus dados, gerenciadas através das soluções de virtualização VMware ou Hyper-V, conforme CONTRATADA
5.2.7. Deverá proteger o ambiente, sem interromper a atividade das máquinas virtuais e sem prejudicar sua performance, facilitando as tarefas de proteção (backup) e migrações em conjunto.
5.2.8. Deverá ter a capacidade de testar a consistência do backup e replicação (S.O., aplicação, VM), emitindo relatório de auditoria para garantir a capacidade de recuperação.
5.2.9. Deverá prover a duplicação e compressão das máquinas virtuais diretamente e durante a operação de backup.
5.2.10. Deverá ser capaz de proteger, de forma indistinta uma máquina virtual completa ou discos virtuais específicos de uma máquina virtual.
5.2.11. Deverá ser fornecida com ferramenta de gestão de arquivos para os administradores de máquinas virtuais no console do operador.
5.2.12. Deverá ter a capacidade de integração através de API's dos fabricantes de infraestrutura virtualizada para a proteção de dados.
5.2.13. Deverá ter a capacidade de realizar proteção (backup) incremental e replicação diferencial, aproveitando a tecnologia de "rastreio de blocos modificados" (CBT - changedblock tracking), reduzindo ao mínimo necessário, o tempo de backup e possibilitando proteção (backup e replicação).
5.2.14. Deverá oferecer múltiplas estratégias e opções de transporte de dados para as áreas de proteção (backup) a saber:
- Diretamente através de Storage Area Network (SAN);
- Diretamente do storage, através do hypervisor I/O (Virtual Appliance);
- Mediante uso da rede local (LAN);
- Diretamente do snapshot do storage onde os dados das VMs estejam armazenados; (para Netapp, HPE 3Par ou EMC VNX)

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850

5.2.15. Deverá proporcionar um controle centralizado de implementação distribuída, para isso deverá incluir uma console web, integrada ou não, que possibilite uma visão consolidada de sua arquitetura distribuída e conjunto de múltiplos servidores de proteção (backup), relatórios centralizados, alertas consolidados e restauração de autosserviço de máquinas virtuais no nível de sistema de arquivos (granular), com delegação de permissões sobre máquinas virtuais individuais.

5.2.16. Deverá poder manter um backup sintético, eliminando assim a necessidade de realizar backups completos (full) periódicos, incremental permanente, o que permitirá economizar tempo e espaço.

5.2.17. Deverá contar com tecnologia de deduplicação também para o ambiente de máquinas virtuais para gerar economia de espaço de armazenamento no repositório de backups sem a necessidade de hardware de terceiros (appliancededuplicadora).

5.2.18. Deverá proporcionar proteção quase contínua de dados (near-CDP), permitindo a minimização dos Objetivos de Pontos de Recuperação (RPO).

5.2.19. Deverá prover/devolver o serviço aos usuários através da inicialização da máquina virtual que falhou, diretamente do arquivo de backup, armazenado no repositório de backup de segurança, sem necessidade, inclusive de "hidratação" dos dados gravado no repositório do backup, os quais obrigatoriamente deverão estar "deduplicados" e também "comprimidos".

5.2.20. Deverá permitir a recuperação de mais de uma máquina virtual e/ou ponto de restauração simultâneo, permitindo assim, ter múltiplos pontos de tempo de uma ou mais máquinas virtuais.

5.2.21. Todo serviço de migração das máquinas virtuais do repositório de backup até o armazenamento na produção restabelecida, não deverá afetar a disponibilidade e acesso pelo usuário, sem paradas.

5.2.22. Deverá prover acesso ao conteúdo das máquinas virtuais, para recuperação de arquivos, pastas ou anexos, diretamente do ambiente protegido (repositório de backup) ou replicados, sem a necessidade de recuperar completamente o backup e inicializar

5.2.23. Deverá permitir realizar buscas rápidas mediante os índices dos arquivos que sejam controlados por um sistema operacional Windows, quando este seja o sistema operacional executado dentro da máquina virtual da qual se tenha realizado o backup.

5.2.24. Deverá assegurar a consistência de aplicações transacionais de forma automática por meio da integração com Microsoft VSS, dentro de sistemas operacionais Windows.

5.2.25. Deverá permitir realizar a truncagem de logs transacionais (transaction logs) para máquinas virtuais com Microsoft Exchange, SQL Server e Oracle.

5.2.26. Deverá permitir notificações por correio eletrônico, SNMP ou através dos atributos da máquina virtual do resultado da execução de seus trabalhos.

5.2.27. Deverá permitir recuperar no nível de objetos de qualquer aplicação virtualizada, em qualquer sistema operacional, utilizando as ferramentas de gestão das aplicações existentes.

5.2.28. Deverá incluir ferramentas de recuperação, mediante as quais os administradores de servidores de correio eletrônico, tais como Microsoft Exchange 2010 sp1, 2013 e superiores, possam recuperar objetos individuais, tais como contatos, mensagens,

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850

compromissos, anexos, entre outros, sem a necessidade de recuperar os arquivos da máquina virtual como um todo ou reiniciar a mesma.

5.2.29. Deverá incluir ferramentas de recuperação, mediante as quais os administradores dos servidores de serviços de diretório, tais como Microsoft Active Directory, possam recuperar objetos individuais, tais como usuários, grupos, contas, Objetos de Política de Grupo (GPOs), registros do Microsoft DNS integrados ao Active Directory entre outros, sem a necessidade de recuperar os arquivos das máquinas virtuais como um todo ou reiniciar a mesma.

5.2.30. Deverá incluir ferramentas de recuperação, mediante as quais os administradores dos servidores de banco de dados, tais como Microsoft SQL Server, possam recuperar objetos individuais, tais como bases, tabelas, registros, entre outros, sem a necessidade de recuperar os arquivos das máquinas virtuais como um todo ou reiniciar a mesma.

5.2.31. Deverá oferecer visibilidade instantânea, capacidades avançadas de busca e recuperação rápida de elementos individuais para Microsoft Sharepoint, desde a versão 2010, sem a necessidade de agentes. (recuperação granular).

5.2.32. Deverá incluir ferramentas de recuperação de elementos individuais para Microsoft Exchange 2010-SP1 em diante, sem que seja necessário inicializar a máquina virtual a partir do backup e que possa ser extraído a frio (ex. mensagens, tarefas, contatos, etc.) e sem requerer infraestrutura intermediária (staging), fazer busca rápidas no servidor de e-mail

5.2.33. Deverá oferecer testes automatizados de recuperação para todas as máquinas virtuais protegidas, gerando confiabilidade de 100% na execução correta das máquinas virtuais e de suas aplicações (DNS Server, Controlador de domínio, Servidor de e-mail, etc.).

5.2.34. Deverá permitir criar uma cópia da máquina virtual de produção, para criação de ambiente de homologação, teste, QA, etc; em qualquer estado anterior para a resolução de problemas, provas de procedimentos, capacitação, entre outros. Deverá ser possível executar uma ou várias máquinas virtuais a partir do arquivo de backup, em um ambiente isolado, sem a necessidade de espaço de armazenamento adicional e sem modificar os arquivos de backup (read-only).

5.2.35. Deverá oferecer arquivamento em fita, suportando VTL (Virtual Tape Libraries), biblioteca de fitas e drives LTO3 ou superior, possibilitando a gravação paralela em múltiplos drives, além da criação de pools de mídia globais e pools de mídia GFS.

5.2.36. Deverá oferecer trabalhos de cópia de backup com implementação de políticas de retenção.

5.2.37. Deverá ser fornecida com a funcionalidade de acelerar a rede "WAN" para geração de cópia ou replicação das máquinas virtuais, sem utilização de agentes, nem configurações de rede especiais.

5.2.38. Deverá incluir suporte para VMware vCloudDirector com visibilidade integrada da infraestrutura vCD no console de backup, fazendo backup de meta-dados e dos atributos associados com vApps e VMs, permitindo a recuperação diretamente ao vCD.

5.2.39. Deverá incluir um plug-in para VMware vSphere Web Client, afim de permitir o monitoramento da infraestrutura de backup diretamente do vSphere Web Client, com visibilidade detalhada e geral do estado dos trabalhos e recursos de backup.

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850

5.2.40. Deverá operar em ambientes virtualizados através das soluções da VMware e Hyper-V, incluido: VMware vSphere 5.5 e/ou Microsoft Hyper-V 2012-R2 e superiores.

5.2.41. Deverá garantir a recuperação granular e consistente, sem necessidade de agentes adicionais para o ambiente virtualizado através das soluções acima, principalmente para os seguintes softwares:

- Microsoft Active Directory Server 2008 R2 em diante;
- Microsoft Exchange Server 2010-SP1 em diante;
- Microsoft SQL Server 2008 SP4 em diante;
- Microsoft Sharepoint 2010 em diante;
- Oracle Database 11g, 12c, 18c, 19c e 21c.

5.2.42. Deverá ser capaz de realizar réplicas em outros sites ou infraestruturas a partir dos backups realizados.

5.2.43. Deverá regular de forma dinâmica e parametrizável, a exigência sobre os sistemas protegidos, de forma tal, que se possa definir limites de utilização de performance em discos para diminuir o impacto na infraestrutura de produção, durante as atividades de backup.

5.2.44. Deverá permitir um método de fácil de recuperação, desde ambientes de contingência, com as ações pré-configuradas para evitar ações manuais em caso de desastre, similar a um botão de emergência.

5.2.45. Deverá oferecer a possibilidade de armazenar os arquivos de backup de forma criptografada, com algoritmo mínimo de 256 bits, ativando e desativando tal operação, assim como assegurar o trânsito da informação através desse cenário, mesmo que impacte a performance da gravação.

5.2.46. Deverá permitir a criação de níveis de delegação de tarefas (perfis) de recuperação no nível de elementos da aplicação, inclusive para outros usuários, de forma a diminuir a carga de atividades executadas pelo administrador da plataforma.

5.2.47. Deverá dispor de funcionalidades integradas que permitam a seleção de um repositório de backup que esteja alojado em um provedor de serviços na nuvem (backup ou replicação na nuvem - cloud providers).

5.2.48. Deve suportar múltiplas operações dos componentes/servidores participantes da estrutura de backup, permitindo atividades de backup e recuperação simultâneas;

5.2.49. Deve suportar repositório de backup com aumento de escala ilimitado para o armazenamento de dados com suporte aos seguintes sistemas de armazenamento:

- Microsoft Windows;
- Linux;
- Pastas compartilhadas;
- Appliances de duplicadoras.
- Suportar servidores proxy de backup virtuais ou físicos para backup de máquinas virtuais;
- Deve estar homologado para o Oracle Database 11g e 12g nos sistemas operacionais Windows ou Linux sem a necessidade de instalação de agentes;

5.2.50. Deve possuir a funcionalidade de recuperar dados para servidores diferentes do equipamento de origem;

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850

5.2.51. Deve ser ofertada a versão mais atual do software de backup, liberada oficialmente pelo fabricante do software. Caso haja necessidade, por razões de compatibilidade com os demais componentes de hardware e software do ambiente de backup, a Contratante se reserva o direito de utilizar a versão do software imediatamente anterior à versão mais atual, sem nenhum ônus adicional para a Contratante.
5.2.52. Repositório de Armazenamento em Nuvem Privada
5.2.53. Esse serviço deverá cobrir a solução de Armazenamento e Compartilhamento de arquivos em Windows, presente neste documento, pelo período do contrato;
5.2.54. Será de responsabilidade da Contratada implementar e configurar o software de transferência de backup local para o repositório na nuvem.
5.2.55. A ferramenta deve estar hospedada em Data Center com certificação Tier III ou ISO27001 ou SOC 2 Type 2;
5.2.56. Deverá conter um espaço mínimo líquido de 4 TB de armazenamento em nuvem;
5.2.57. Deverá conter um espaço mínimo líquido de 4 TB de armazenamento em nuvem incluindo na imutabilidade totalmente desligada/apartada do ambiente de armazenamento em nuvem.
5.2.58. O licenciamento da estrutura de backup é totalmente de responsabilidade da Contratada e deverá ser dimensionada para atender totalmente os dados da Contratante.
5.2.59. A solução deverá conter compactação e/ou aceleração WAN, para menor carga de utilização dos links de internet da Contratante;
5.2.60. O licenciamento e operação do ambiente em nuvem é de total responsabilidade da Contratada;
5.2.61. O armazenamento de dados da Contratante deverá estar localizado no estado de São Paulo, mantendo assim uma menor latência na comunicação e transferência de dados;
5.2.62. A Contratada deverá garantir a segurança da informação dos dados e estrutura em nuvem que irá hospedar os dados de backup da Contratante. Se responsabilizando por qualquer dano causado a eles;
5.2.63. Os backups deverão estar criptografados com um mínimo de 256 bits;
5.2.64. As instalações físicas do data center deverão ter os seguintes itens:

- Sistema de piso elevado, com vias independentes de cabos de energia, lógicos e óticos;
- Deverá possuir vias de energia elétrica e lógica em alta disponibilidade;
- Sistema de proteção contra descargas eletromagnéticas, descargas atmosféricas e aterramento.

5.2.65. A estrutura de energia elétrica do data center deverá atender aos seguintes requisitos:
5.2.66. Alimentação elétrica redundante;
5.2.67. Total independência no fornecimento de energia na eventualidade de falha na subestação que atende ao data center;
5.2.68. Solução de grupo gerador redundante e independente (n+1), com acionamento automático na eventualidade de interrupção no fornecimento de energia e com capacidade mínima de funcionamento por 72 horas com combustível local:

- Mínimo de 2KVAs nominais;
- Alimentação elétrica redundante e independente para os equipamentos da solução.
- O data center que aloca os backups da Contratante deverá atender os seguintes requisitos de climatização:

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850

- Sistema de climatização com controles de temperatura, umidade relativa do ar e filtros de poeira;
- Sistema de climatização redundante (n+1), refrigerado por formas diferentes;
- Temperatura constante de 20ºC +/- 2ºC e umidade relativa do ar constante de 50% +/- 10%.

5.2.69. O data center que aloca os backups da Contratante deverá atender os seguintes requisitos de proteção contra incêndio:

- Dispositivos tradicionais de prevenção e combate a incêndio (brigada de incêndio, extintores manuais e detectores de fumaça);
- Sistema automático de extinção de incêndios, baseado em agentes gasosos não poluentes, com ação baseada na quebra das moléculas de Oxigênio, do tipo FM200 e/ou FE227, ou equivalente, não nocivos aos equipamentos e seres humanos e que atenda a padrões internacionais;
- Sistema de detecção de incêndio por sensores termovelocimétricos para a sala dos servidores do data center, tipo VESDA, ou equivalente; possuir dispositivos de detecção precoce de incêndio pela análise do superaquecimento de cabos ou hardwares que sejam de maior sensibilidade que os tradicionais detectores de fumaça;
- Possuir sistema de detecção de incêndio por sensores termovelocimétricos para os ambientes de servidores e de armazenamento de dados;
- Possuir os componentes de segurança necessários para garantir a preservação dos dados em casos de incêndio e execução de plano de recuperação de catástrofes.

5.2.70. O data center que aloca os backups da Contratante deverá possuir os seguintes requisitos de segurança física:

- Disponibilidade de pessoas dedicadas, treinadas e responsáveis pela segurança de acesso ao prédio e aos equipamentos;
- Mecanismos efetivos de controle de entrada e saída de pessoas que acessem e façam uso do IDC, bem como de registros passíveis de posterior pesquisa;
- Capacidade de cadastro remoto de usuários para acesso ao data center;
- Deverá possuir a capacidade de cadastro de novo usuário local com permissão do administrador;
- Acesso ao local através de leitura biométrica;
- Possuir alerta por SMS e e-mail em tempo real de acesso ao ambiente;
- Arquivar as imagens gravadas pelas câmeras de vídeo de segurança por pelo menos 30 (trinta) dias;
- O Datacenter deverá possuir vigilância patrimonial 24 horas por dia, 7 dias por semana, 365 dias por ano, permitindo apenas a entrada de pessoas autorizadas e devidamente identificadas;
- Possuir metodologia para classificação e controle de ativos e de acessos ao ambiente do Datacenter;
- Acondicionar equipamentos e mídias geradas no ambiente do Datacenter, livres de riscos físicos;
- Possuir rígido controle de acessos aos equipamentos do Datacenter, mesmo por pessoas credenciadas pela Contratante;

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850

- Disponibilizar mecanismos efetivos de controle de entrada e saída de pessoas, que acessam ou façam uso do Datacenter, com leitores biométricos ou cartões magnéticos individuais;
- Possuir travas eletrônicas que, de acordo com a política de segurança estabelecida para o Datacenter, a dívida em regiões com níveis de restrição diferenciados;
- Possuir sistema de detectores de movimento no ambiente.

5.3. ITEM 3: SUPORTE TÉCNICO E MONITORAMENTO:

5.3.1. A Contratada deverá administrar, suportar, monitorar os serviços de segurança, backup e suporte técnico nos equipamentos descritos nesse documento:

PATRIMONIO	EQUIPAMENTO
3328	Servidor
3330	Servidor
3329	Switch 24 portas L2
4227	Switch 24 portas L2
4236	Controladora WiFi
4237	Access Point
4238	Access Point
4239	Access Point
4233	Switch 24 portas L2
4234	Switch 24 portas L2
4232	Switch 24 portas L2
4231	Switch 24 portas L2
4229	Switch 24 portas L2
4228	Switch 24 portas L2
4230	Switch 24 portas L2

5.3.2. A Contratada será responsável pela administração tanto do monitoramento, como do suporte técnico dos equipamentos de Firewall, Switch, WiFi, Servidores, Backup local, backup em nuvem, Antivírus e monitoramento pelo NOC.

5.3.3. A Contratante poderá abrir chamados de manutenção através de chamada telefônica para número com DDD (11), central de atendimento via navegador (WEB) ou correio eletrônico sem a necessidade prévia consulta e/ou qualquer liberação por parte da Contratada;

5.3.4. O atendimento técnico remoto e presencial deverá ocorrer 24 horas por dia, 7 dias por semana;

5.3.5. Não deve haver limites para aberturas de chamados, sejam dúvidas, configurações ou resolução de problemas de hardware e/ou software;

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850

5.3.6. Toda falha e indisponibilidade no ambiente ocasionado por falhas físicas nos equipamentos (hardware) serão de plena responsabilidade da Contratada seguindo exatamente as orientações da garantia/suporte técnico do fabricante quando houver necessidade;

5.3.7. A equipe de suporte técnico deverá buscar, no escopo de serviços, prevenir a ocorrência de problemas e seus incidentes resultantes, eliminando incidentes recorrentes correlacionando-os e identificando a causa-raiz e sua solução, além de minimizar o impacto dos incidentes que não podem ser prevenidos;

5.3.8. Será de responsabilidade da Contratada manter o pleno funcionamento das políticas de segurança da solução.

5.3.9. Deverá monitorar diariamente, os relatórios de segurança gerados ao concluir as tarefas, caso apresente algum erro ou anomalia na execução na tarefa, será de responsabilidade da Contratada efetuar correção ou ajuste técnico para a normalização dele, garantindo o pleno funcionamento da solução.

5.3.10. A Contratada deverá ser responsável por executar as restaurações do ambiente.

5.3.11. A empresa Contratada se responsabilizará pelas despesas com material de escritório, reprodução de documentos (cópias, etc) e materiais diversos, que forem necessários à execução dos serviços de manutenção dos serviços e pelos seus profissionais;

5.3.12. A Contratada deverá realizar atendimentos remotos à equipe de tecnologia da informação da Contratante, a partir de solicitações recebidas dos técnicos ou gestores de contrato da Contratante via sistema de atendimento, telefone ou correio eletrônico;

5.3.13. Todos os atendimentos deverão estar registrados em central de atendimento técnico e gestão de chamados;

5.3.14. Correlacionar incidentes a fim de identificar sua causa-raiz, solucioná-la e prevenir novas ocorrências;

5.3.15. Manter o ambiente de segurança sempre atualizado em com as melhores práticas aplicadas;

5.3.16. A Contratada deverá garantir que os profissionais designados para atendimento técnico serão capacitados;

5.3.17. Análise de logs e relatórios de auditoria para detectar atividades suspeitas ou violações de segurança.

5.3.18. A garantia de tempo de resposta será realizada conforme critérios de prioridades a seguir:

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850

CLASSE	DESCRIÇÃO	INÍCIO DO ATENDIMENTO EM ATÉ	TEMPO MÁXIMO DE SOLUÇÃO
1	Serviço indisponível	15 Minutos	4 Horas
2	Suporte técnico de maior impacto	1 Hora	8 Horas Úteis
3	Suporte técnico com menor impacto	4 Horas	2 Dias Úteis
4	Manutenção preventiva	Programada	Programada

5.3.19. O acordo de nível de serviço para suporte técnico deverá obedecer ao seguinte escopo:

PRIORIDADE	DESCRIÇÃO
1 (Crítico)	O serviço está fora de operação ou há um impacto crítico nas operações.
2 (Alta)	O serviço está degradado, ou aspectos significativos das operações que sofreram impactos negativos pelo desempenho inadequado.
3 (Média)	Serviço funcionando com pequenos problemas sem impacto direto na operação.
4 (Baixa)	O desempenho operacional do serviço está prejudicado, não causando quebra de funcionamento ou de operação.

5.3.20. As horas para primeiro atendimento e resolução de incidentes são horas corridas e serão contabilizadas dentro do horário de atendimento descrito neste **TERMO DE REFERÊNCIA**.

5.3.21. No caso de um problema ser relacionado a correção por parte do fabricante do Hardware ou Software utilizado, será considerado o SLA do fabricante em questão.

5.3.22. Caso seja identificado que o Serviço de segurança (firewall) se encontre indisponível por causa de soluções de terceiros, link de internet, indisponibilidade de switch, energia elétrica, roteadores, firewall, problemas de hardware/infraestrutura de TI ou qualquer serviço que interligue as unidades, será de responsabilidade da Contratada em realizar a detecção e resolução do problema respeitando o SLA do fabricante ou prestador de serviço caso tenha a necessidade.

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850

5.3.23. A Contratada deverá disponibilizar e gerenciar os atendimentos técnicos da Contratante através de portal de gerenciamento de atendimentos com acesso através de navegador web;
5.3.24. Mesmo os chamados sendo abertos através de ligação telefônica ou correio eletrônico, os chamados deverão ser registrados na central;
5.3.25. A solução deverá ser aderente aos processos do ITIL para gerenciamento de incidentes e requisições;
5.3.26. A Contratada deverá emitir relatórios mensais abrangendo, no mínimo, requisições, incidentes, informações de atendimentos e soluções conforme linha de atendimento com especificações e detalhes de cada atendimento;
5.3.27. A Contratante deverá ser avisada através de e-mail sobre a abertura e solução de qualquer tipo de solicitação através do portal WEB, telefone e e-mail;
5.3.28. O sistema operacional e servidor responsável por suportar a console de gerenciamento de atendimentos e informações ficam sob responsabilidade da Contratada, sendo essa responsável por sua atualização e manutenção;
5.3.29. A solução deverá conter a possibilidade de criação de regras de negócio, para automação no atendimento técnico especializado;
5.3.30. O sistema de gerenciamento de chamados deverá ter histórico de alterações do chamado bem como solução, para eventuais processos de auditoria;
5.3.31. A Contratada deverá garantir que a solução de atendimento e informações conte com uma área de cadastro de contatos, para consulta pela Contratante;
5.3.32. Deverá ser possível anexar documentos de qualquer tipo na abertura e gerenciamento de atendimentos técnicos;
5.3.33. Os atendimentos técnicos deverão ser organizados por categoria, que serão acordados junto a Contratante;
5.3.34. O sistema de atendimento deverá contar com a função de aprovação dos atendimentos técnicos, sendo possível o envio de tal aprovação para gestores e responsáveis pelos devidos atendimentos junto a Contratante;
5.3.35. Deverá ser possível o envio de notificação de abertura e solução de atendimentos para um grupo de e-mails;
5.3.36. A solução de atendimento técnico deverá permitir que o chamado possa ser exportado para o formato ".PDF";
5.3.37. A solução deverá contar com perfis de usuários, sendo possível a criação de acessos somente leitura;
5.3.38. Deverá ser possível a criação de grupos de usuários na solução;
5.3.39. A solução disponibilizada pela Contratada deverá ter a possibilidade da criação de várias entidades dentro de um mesmo banco de dados da solução.
5.3.40. Relatórios Mensais, durante o período do contrato
5.3.41. Relatório de Chamados:

- Categoria do chamado;
- Usuário;
- Ativos relacionados;

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850

- Data de abertura e fechamento;
- Status;

5.3.42. O suporte técnico deverá ter os seguintes canais de atendimento: Suporte Telefônico, E-mail e Sistema online de chamados, todos em português do Brasil;

5.3.43. A Contratada deverá sempre disponibilizar versões mais recentes dos softwares sem ônus financeiro;

5.3.44. **MONITORAMENTO**

5.3.45. O Monitoramento deverá ser disponibilizado para as unidades destacadas na tabela inicial deste Termo de Referência.

5.3.46. O serviço de monitoramento deverá ser composto de tecnologia que seja totalmente apartada do ambiente computacional e de servidores da Contratante.

5.3.47. A Contratada deverá disponibilizar um switch de 8 portas ou superior, para configurar as conexões de rede necessárias para o monitoramento do ambiente sem a necessidade de utilizar os switches da Contratante.

- Capacidade de comutação: 20 Gbps.
- Tabela de endereços MAC no mínimo de: 8.000 mil.
- Memória interna de no mínimo: 256 MB.
- Memória Flash: 32 MB
- Buffer de pacote mínimo de: 512 kb.
- Suportar até 256 VLANS simultaneamente e 4.000 mil Ids de VLAN.
- Interface das 8 portas em 10/100/1000 BASE-T ou superior.
- SFP de 1GB no mínimo de: 2 Interfaces.
- Interruptor de liga e desliga com entrada DC-in
- Deverá ser bivolt (100V-240V)
- LEDs para representar o status na localidade frontal do hardware.

5.3.48. A Contratante não vai disponibilizar hardware ou software para que a Contratada realize o monitoramento.

5.3.49. A Contratante não será responsável por armazenar hardware ou software para a substituição.

5.3.50. A fonte de carregamento e gerenciamento de energia deverá ser conectada através da porta tipo-C.

5.3.51. A Contratante não disponibilizará recursos computacionais para a instalação do sistema de monitoramento.

5.3.52. O recurso tecnológico poderá consumir até uma tomada do rack com o tipo padrão NBR 14136 de três pinos.

5.3.53. O recuso tecnológico deverá ser acompanhado com uma fonte de 100/240 VA, padrão NBR 14136 de três pinos, com botão que tenha a possibilidade de ligar e desligar o recurso energético da fonte, deverá entregar 5V de 3000mA e o fio de conexão com a fonte de energia não deverá ser superior a 100cm.

5.3.54. Deverá possuir uma entrada do tipo RJ-45 com a velocidade de Gigabite 10/100/1000.

5.3.55. Deverá possuir 2 entradas USB 2.0.

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850

5.3.56. Deverá possuir 2 entradas de USB 3.0.
5.3.57. Deverá possuir 2 entradas Micro HDMI 2.0.
5.3.58. A entrada Micro HDMI deverá possuir o suporte de resolução em 4Kp60.
5.3.59. Deverá possuir uma entrada A/V habilitado para TV out.
5.3.60. Deverá possuir 1 entrada categorizada como tipo-C.
5.3.61. O recurso tecnológico de monitoramento deverá ter suporte para sistema operacional Linux.
5.3.62. O recurso tecnológico deverá ser um dispositivo para que monitore toda a infraestrutura Contratada pela Contratante neste termo de referência.
5.3.63. A comunicação com o datacenter deverá ser feita através do protocolo de comunicação TCP.
5.3.64. O recurso tecnológico deverá possuir um cooler para que ele consiga realizar a dissipação de calor assim evitando qualquer tipo de impacto no serviço de monitoramento.
5.3.65. O recurso tecnológico deverá dispor de 4 borrachas de proteção na parte inferior;
5.3.66. O recurso tecnológico deverá possuir furação para que a dissipação de calor seja mais eficiente;
5.3.67. O recurso tecnológico deverá possuir o armazenamento em MicroSD de no mínimo 64gb;
5.3.68. A Contratada ficará responsável em realizar a entrega do recurso tecnológico juntamente com as respectivas licenças do sistema operacional e softwares de segurança como licença contra-ataques cibernéticos, backup do sistema operacional e até mesmo monitoramento do sistema tecnológico.
5.3.69. Requisitos técnicos da solução de segurança com inteligência artificial para detecção e resposta estendida a incidentes na camada de proteção nos servidores deverá ser totalmente compatível com a estrutura em cloud.
5.3.70. A contratação da prestação do serviço e a disponibilização da ferramenta devem atender integralmente aos normativos exarados pelos órgãos fiscalizadores e de controle correlatos, em especial do que trata a Lei 13.709/2018 (Lei Geral de Proteção de Dados).
5.3.71. A plataforma deve contar com agentes da Inteligência Artificial para auxiliar em toda a etapa da investigação.
5.3.72. A plataforma deve disponibilizar comunicação direta por texto com os agentes da Inteligência Artificial.
5.3.73. A plataforma deve disponibilizar durante a navegação, interação com a Inteligência Artificial e acesso aos dados investigados.
5.3.74. A plataforma deve utilizar diferentes agentes da Inteligência Artificial para investigação de endpoints, alertas e Inteligência de ameaças.
5.3.75. A inteligência Artificial deve ser capaz de buscar todos os endpoints cadastrados, alertas abertos e vulnerabilidades identificadas na interação por texto e o resultado deve ser retornado em tela.
5.3.76. Os agentes de Inteligência devem ser capazes de correlacionar todos os dados coletados, analisar e fornecer um parecer investigativo sobre quais ações foram e/ou devem ser realizadas.

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850

5.3.77. Deve usar um modelo matemático gerado a partir de aprendizado de máquina para comparar diferentes características de um arquivo executável, de forma estática, para determinar se ele é malicioso.
5.3.78. A plataforma deve ser capaz de detectar vazamento de dados sobre a Contratante, apresentando o tipo de dado vazado e as datas que ocorreram.
5.3.79. A plataforma através dos agentes da Inteligência Artificial deve ser capaz de reclassificar a pontuação de risco da ameaça de acordo com a técnica explorada e a classificação do ativo;
5.3.80. A plataforma deve ser capaz de se integrar a aplicações e equipamentos da Contratante para enriquecer a detecção e resposta estendida em tempo real;
5.3.81. A proteção deve estar disponível para os sistemas operacionais Windows, Linux e MacOS.
5.3.82. Prevenção de ameaças baseada em comportamento para análise dinâmica de processos em execução.
5.3.83. Prevenção de exploração por técnicas conhecidas de exploits.
5.3.84. Prevenção de exploração baseada em kernel.
5.3.85. Prevenção de ameaças com base em inteligência de ameaças, como hash de arquivos.
5.3.86. Integração automatizada com um serviço de prevenção de malware, baseado em nuvem do próprio fabricante.
5.3.87. A solução deve prover, integrada à gerência de administração da solução, capacidades de emulação de execução de arquivos, sem instalação de componentes adicionais ou softwares de terceiros.
5.3.88. A solução deve ser compatível, no mínimo, com o seguinte sistema operacionais e distribuições:
5.3.89. Linux;
5.3.90. A solução deve incluir na análise de execução, no mínimo, as seguintes características:

- Táticas e técnicas de acordo com o modelo de ameaças MITRE ATT&CK;
- Caraterísticas comportamentais suspeitas;
- Detalhes do arquivo como nome, hash, tamanho, tipo;
- Atividade de rede incluindo conexões, endereços IP de destino, domínios, portas;
- Leitura e escrita de arquivos em disco;
- Leitura e alteração de chaves de registro;

5.3.91. Detalhes de processos iniciados durante a execução.
5.3.92. Atualizações transparentes do mecanismo de detecção de ameaças.
5.3.93. Proteção contra malware, ransomware e ataques sem arquivo.
5.3.94. Identificação e prevenção de tentativas de escalonamento de privilégios ao nível de Kernel. Essa proteção deve poder ser usada em agentes instalados em endpoints com Sistemas Operacionais Windows, Mac e Linux.
5.3.95. Deve permitir gerar alertas das soluções integradas.
5.3.96. Deve permitir a consulta de eventos de forma integrada.
5.3.97. Os usuários locais da solução devem ter uma política de senha que permita, no mínimo as seguintes configurações, alteração no primeiro login e identificação de complexidade de senha.

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850

5.3.98. A solução deve ter a capacidade de detectar metodologias e padrões de ataques, mesmo sem a presença de arquivos de malware (malware operando apenas na memória\fileless).
5.3.99. No caso de detecção de um incidente, a solução deve permitir a execução de rotinas automatizadas para rapidamente responder aos eventos gerados pelos dispositivos.
5.3.100. A solução deve disponibilizar o rastreio de detecção de possíveis movimentações laterais, criando um mapa visual das ocorrências.
5.3.101. A solução deve disponibilizar o rastreio de processos suspeitos, aos quais podem receber classificações através dos indicadores de comprometimentos mapeados pela rede de inteligência do fabricante.
5.3.102. A solução deve disponibilizar o rastreio de tentativas de roubo de credenciais e\ou tentativa de acessos indevidos a recursos chave do sistema operacional.
5.3.103. Permitir a visualização automática de contexto adicional sobre alertas, fornecendo um fluxo de trabalho automatizado que coleta e analisa artefatos, destacando rapidamente índices de comprometimento já conhecidos.
5.3.104. Gerenciamento unificado e centralizado de todas as funções na mesma console de, bem como a instalação e atualização dos agentes.
5.3.105. Detecção de comprometimento: vírus, malware, backdoors, hosts em comunicação com sistemas infectados por botnet, serviços da Web vinculados a conteúdo malicioso.
5.3.106. Frequência de atualização, personalizável por dia, semana ou mês.
5.3.107. Varredura em tempo real de arquivos (gravação, renomeio e leitura) e de processos em memória.
5.3.108. Monitoramento em tempo real para captura de malwares que são executados em memória sem a necessidade de escrever em arquivo.
5.3.109. Capacidade de finalizar processos perigosos que possam causar instabilidade ou risco ao sistema através de análise comportamental, realizado por inteligência artificial.
5.3.110. Solução única para proteção contra malwares e ransomware, com a capacidade de coletar dados de sistemas operacionais e de rede para detecção de eventos maliciosos, sem a obrigatoriedade de criação e ativação de regras manualmente.
5.3.111. A solução deve permitir instalação silenciosa do agente, em sistemas operacionais Windows, através de pacotes MSI e executável EXE.
5.3.112. A solução deverá ser capaz também de analisar ameaças, sem o uso de assinaturas, fazendo esta análise por comportamento.
5.3.113. A solução deve prover formas de segregar os equipamentos por grupo facilitando assim a aplicação de políticas granulares e outras configurações.
5.3.114. A solução deve suportar nativamente a integração com terceiros, sem a necessidade de instalação de recursos adicionais para receber eventos de múltiplas fontes de origem.
5.3.115. A solução deve disponibilizar, informações sobre o número de dispositivos que possuem o agente instalado e a versão do agente.
5.3.116. A solução deve ser capaz de monitorar email e domínio para identificar vazamento de dados.
5.3.117. Requisitos de detecção e resposta do agente.
5.3.118. A solução não deve ter limitação para recebimento de eventos.
5.3.119. A comunicação entre agente e plataforma deve acontecer através do protocolo TCP porta 443;

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850

5.3.120. O agente deve permitir a sua instalação em sistema operacional Linux Ubuntu 24.04 ou superiores.
5.3.121. A solução deve utilizar criptografia para conexão entre agente e plataforma, no mínimo, TLS 1.3 com AES 256.
5.3.122. A solução deve utilizar criptografia nos dados enviados para a plataforma de gerenciamento, no mínimo, AES 256.
5.3.123. A solução deve utilizar algoritmos de aprendizado de máquina para identificar padrões e comportamentos suspeitos.
5.3.124. A solução deverá ser capaz de bloquear tanto ameaças conhecidas como também as desconhecidas.
5.3.125. O agente deve detectar e proteger o dispositivo mesmo offline.
5.3.126. O agente deve receber atualizações de forma automática.
5.3.127. O agente deve receber as novas assinaturas de segurança em tempo real.
5.3.128. A solução deve utilizar detecção de ameaças por meio de dados e padrões baseados em comportamentos, que se utilizam de motores baseados em aprendizado de máquina para averiguação de arquivos.
5.3.129. O agente deve possuir a funcionalidade de inteligência contra malware.
5.3.130. O agente deve possuir a funcionalidade de inteligência contra ransomware.
5.3.131. O agente deve possuir a funcionalidade de bloqueio de indicadores de comprometimento.
5.3.132. O agente deve disponibilizar na sua interface, os seguintes dados:
5.3.133. Nome do usuário logado.
5.3.134. Nome do host.
5.3.135. Informações de sistema operacional (Build, Plataforma).
5.3.136. Estado do equipamento (Online ou Offline).
5.3.137. Última data comunicação com a console de gerenciamento.
5.3.138. Informações relacionadas à rede (IP, DNS, DHCP).
5.3.139. A solução deve possuir capacidade de ser instalada sem requerer nenhuma licença adicional de sistema operacional ou qualquer outra não fornecida pela contratada.
5.3.140. A solução deve operar em tempo real, monitorando e bloqueando as ameaças.
5.3.141. A solução deve detectar e bloquear tentativas de exploração por malware conhecido ou desconhecido, usando técnicas de análise de comportamento na interação entre componentes.
5.3.142. A solução deve fornecer a capacidade de executar análises de estações de trabalho/servidores sem a necessidade de interagir com o usuário. Essa capacidade deve ser centralizada e transparente para o usuário.
5.3.143. A solução deve fornecer suporte para estações de trabalho que não estão conectadas à rede interna, como computadores na Internet, sem perder a capacidade de proteger e atualizar.
5.3.144. Deve incluir recursos para detecção de malware conhecido, incluindo a capacidade de operar em conjunto com outras ferramentas de proteção a estações de trabalho.
5.3.145. A solução deve ser capaz de fazer análise avançada e utilizar algoritmos de aprendizado de máquina, mesmo que sem conexão ao servidor de gerenciamento.

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850

5.3.146. Consulta APIs: Capacidade de extrair dados de segurança e eventos para integração, utilizando os protocolos SSH, HTTP, SNMP e Syslog em todos os itens fornecidos dentro da solução proposta.
5.3.147. A solução deve disponibilizar um agente instalável e compatível com sistemas operacional, Windows, Linux e MacOS. Com a capacidade de detectar, coletar e enviar a plataforma, comportamentos maliciosos de aplicações que estão sendo executadas no sistema operacional.
5.3.148. A solução deve disponibilizar um coletor com capacidade de executar consultas de coleta de eventos e detecção de ação maliciosas em suas integrações, mesmo se houver indisponibilidade de conectividade.
5.3.149. Atualizações regulares e automáticas de binários e base de dados de segurança.
5.3.150. O agente deve ser compatível com o sistema operacional Linux Ubuntu 24.04 ou superiores.
5.3.151. A solução deve suportar a integração baseada em agente e autenticação.
5.3.152. A solução deve permitir o recebimento de eventos por múltiplos coletores.
5.3.153. A solução deve identificar os eventos por integração e agente.
5.3.154. A solução deve permitir a classificação de severidade, quando cadastrado o dispositivo.
5.3.155. **QUANTO A ARMAZENAMENTO**
5.3.156. A solução deve prover no mínimo 2TB de armazenamento para retenção dos eventos coletados e normalizados pela solução, sem custo adicional ou necessidade de fornecimento de hardware para armazenamento pela Contratante.
5.3.157. O evento armazenado pela solução, bem como hardware necessário para tal, é de responsabilidade da Contratada em armazenar em datacenter.
5.3.158. Solução deve ter a capacidade de permitir que o Contratante modifique o período de armazenamento de eventos de Windows, Linux e Firewall de forma independente e através de plataforma gráfica disponibilizada pela solução proposta pela Contratada.
5.3.159. **QUANTO A RELATÓRIOS E DASHBOARDS**
5.3.160. Visualização de Dados
5.3.161. Painéis de controle para visualização em tempo real de incidentes e status de segurança.
5.3.162. Relatórios sobre incidentes, tendências de segurança e desempenho do sistema, exportando em formatos pdf, csv e html.
5.3.163. A solução deve ter capacidade de enviar relatórios através dos protocolos SMTP, HTTP, SFTP e ter integração com soluções de colaboração.

5.3.164. **RELÁTORIOS**

5.3.165. Deverá ser fornecido relatórios mensais de chamados e monitoramento de recursos dos componentes do serviço, com:
5.3.166. Relatório de Chamados (referente ao serviço descrito nesse lote):

- Categoria do chamado;
- Usuário;
- Ativos relacionados;

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850

- Data de abertura e fechamento;
- Status;
- Relatório de Monitoramento de recursos (referente ao serviço descrito nesse lote):
- Disponibilidade;
- Consumo de hardware (CPU, memória, disco, consumo de banda);
- Alertas e erros;

5.3.167. **MANUTENÇÃO PREVENTIVA DA SOLUÇÃO DE INTELIGENCIA ARTIFICIAL**

5.3.168. A manutenção preventiva será destinada a atualizar os componentes de software (atualização tecnológica), conforme definições nesse documento, e a realizar quaisquer operações que evitem uma parada total ou parcial solução de TI.

5.3.169. A Contratante, através de sua equipe técnica, observará o desempenho do sistema contratado e, caso necessário, solicitará à Contratada uma manutenção preventiva para viabilizar o melhor desempenho da solução.

5.3.170. A manutenção preventiva está inclusa no suporte técnico da solução, sendo prestada pela Contratada sem qualquer ônus adicional para a Contratante.

5.3.171. Durante a manutenção preventiva, a Contratada deverá analisar a solução, sua condição atual de funcionamento, seus logs de sistema e sugerir mudanças para uma melhor prática de utilização da ferramenta.

5.3.172. Durante o período de suporte técnico deverá ser realizada a atualização de qualquer outro software constituinte da solução para as versões mais recentes, sem ônus adicional para a Contratante.

5.3.173. A manutenção corretiva será destinada a remover erros ou falhas apresentadas pelos componentes de software da solução contratada.

5.3.174. Como erro ou falha entende-se a geração de resultado diferente do previsto. Para a resolução desses erros, é necessária a intervenção técnica especializada ou mesmo até a substituição de seus componentes por parte da Contratada.

5.3.175. A manutenção corretiva após o diagnóstico (determinação da origem da falha) deverá ser realizada por meio de ajustes, consertos ou substituição dos elementos que apresentam problemas, restabelecendo a solução suas condições normais de funcionamento ou operação, conforme as especificações do fabricante.

5.3.176. Entende-se como diagnóstico à compilação e análise de informações para definição da causa de um problema.

5.3.177. Entende-se como Recuperação da Disponibilidade a execução de atividades que permitem restabelecer o funcionamento da solução.

5.3.178. A comprovação de isenção de responsabilidade se dará pela apresentação de relatório técnico circunstanciado dos elementos da solução contratada, e pelas demais informações consideradas necessárias pela Contratada para embasar a justificativa.

5.3.179. Tomar todas as providências necessárias para que seus funcionários, representantes e/ou contratados observem os regulamentos, normas e instruções de segurança da informação e Comunicações pela Contratante, quando estiverem executando serviços.

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850

5.3.180. A Contratada deve comprometer-se a manter informações confidenciais no mais estrito sigilo sobre todos os dados, configurações, processos, fórmulas, rotinas e quaisquer outros objetos que sejam disponibilizados, pela Contratante, à CONTRATADA, para a realização dos trabalhos. Compromete-se a não copiar, não usar em seu próprio benefício, nem revelar ou mostrar a terceiros, nem divulgar tais informações, no território brasileiro ou no exterior, sob pena prevista em lei. Só os representantes e prepostos, devidamente autorizados entre as partes, cuja avaliação das informações confidenciais seja necessária e apropriada, para os propósitos especificados em contrato, terão acesso às mesmas.

5.3.181. Prestar os esclarecimentos necessários a Contratante, bem como informações concernentes à natureza e andamento dos serviços executados, ou em execução.

5.3.182. Requisitos sociais, ambientais e culturais

5.3.183. Sistema e todos os seus módulos deve ser desenvolvido/disponibilizados de forma compatível para as características do Brasil quanto a aspectos de interface gráfica, linguagem, legislação, costumes, apresentação, funcionalidades, telas e relatórios. Deve também possuir manuais de usuário on-line, com possibilidade de impressão, e documentação técnica do software em idioma português do Brasil ou inglês.

5.4. ITEM 4: SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO:

5.4.1. Deverão ser instalados e configurados todos os itens físicos e lógicos seguindo os padrões e melhores práticas recomendadas na norma NBR ISO/IEC 27002 e conforme critérios definidos pela contratante, devendo a implantação inicial e o início do monitoramento e das rotinas operacionais ocorrerem em até 30 (trinta) dias, contados da assinatura do contrato, conforme disposto no item 7.1.2, mediante aprovação da contratante.

5.4.2. Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, em observância às normas legais e regulamentares aplicáveis e às recomendações aceitas pela boa técnica;

5.4.3. Prestar todos os esclarecimentos que lhe forem solicitados, atendendo prontamente a quaisquer reclamações;

5.4.4. Fornecer toda mão de obra necessária à completa execução do serviço, bem como ferramentas e equipamentos a serem utilizados na manutenção e reparos;

5.4.5. Instalação física de todos os equipamentos em Rack disponibilizado no local de instalação;

5.4.6. Os equipamentos devem ser configurados em alta disponibilidade, no modo ativo/passivo, dois equipamentos funcionando simultaneamente e em caso de falha o outro continue em operação e quando necessário deverá suportar o processo de ativo/ativo;

5.4.7. Deverá migrar ou executar configurações similares às configurações atuais implementadas no firewall, atualmente em produção na contratante. A EMPRESA, além de apontar Marca e Modelo do Firewall, deverá apresentar o projeto de migração completo do Firewall atual para o novo Firewall. Não será aceito um programa

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850

automatizado de importação de Regras, especialmente para Firewall com arquitetura diferente da tecnologia atual.

5.4.8. O projeto deve levar em conta a diferença de arquiteturas e demonstrar a preservação das políticas através das camadas.

5.4.9. Toda a estrutura de backup em nuvem deverá ser realizada através da Contratada.

5.4.10. O equipamento deve estar com firmware e/ou software na versão mais recente e estável recomendada pelo fabricante da solução;

5.4.11. A empresa deverá elaborar um plano de implementação junto a contratante, com: descrição de atividades a serem desenvolvidas, relatórios e diagramas com dados relevantes para efeito decisório, responsáveis pelas atividades, cronograma de implementação, compondo o documento denominado "Projeto Executivo" tendo a visibilidade completa do projeto e seus status evolutivos. O documento deve ser entregue para a contratante antes do início da instalação, em até 10 dias úteis a partir do 1° dia útil subsequente a assinatura do contrato. A Central de TI analisará o documento e dará o aceite em um prazo máximo de 02 dias úteis. Havendo necessidade de adequações a empresa terá um prazo máximo de 02 dias úteis para apresentar o projeto readequado, que será reavaliado pela Central de TI para aprovação, em um prazo máximo de 01 dia útil.

5.4.12. Os profissionais alocados para a instalação por parte da contratada deverão ter conhecimento pleno nas melhores práticas de configuração do produto e fabricantes;

5.4.13. As senhas configuradas no ambiente durante a instalação deverão ter requisito mínimo de 08 (oito) caracteres contendo letras maiúsculas, minúsculas e caracteres especiais;

5.4.14. Os profissionais técnicos quando em serviço na CÂMARA MUNICIPAL DE CARAPICUÍBA deverão apresentar documento de identificação com foto e identificação da empresa com os seguintes:

5.4.15. RG/CNH;

5.4.16. Estar devidamente uniformizado para identificação da Contratante.

5.4.17. A contratante deverá designar um profissional para acompanhar o processo de implementação, com a finalidade de esclarecimentos sobre o ambiente.

5.4.18. Juntamente com a proposta deverá ser apresentada documentação oficial do fabricante contendo as especificações técnicas dos produtos ofertados para verificação do responsável pela análise técnica.

6. REQUISITOS DA CONTRATAÇÃO

6.1. **Sustentabilidade:** Os critérios de sustentabilidade estão eventualmente inseridos na descrição do objeto.

6.2. **Indicação de marca:** Todas as especificações do objeto contidas na proposta, tais como marca, modelo, tipo, fabricante e procedência, vinculam a Contratada.

6.3. **Subcontratação:** Não é admitida a subcontratação do objeto contratual.

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850

6.4. **Garantia da contratação:** Não haverá exigência da garantia da contratação do art. 96 e seguintes da Lei nº 14.133/21, a fim ampliar a competitividade.

6.5. **Garantia de proposta:** Não será exigida garantia de proposta.

7. FORMA DE EXECUÇÃO DO OBJETO

7.1. Dos prazos, do local e das condições de início e execução dos serviços:

7.1.1. A execução do objeto ocorrerá nas dependências da Câmara Municipal de Carapicuiba e, quando aplicável, por meio de acesso remoto seguro conforme os parâmetros, diretrizes e autorizações do Contratante, observado o período contratual de 1 (um) ano.

7.1.2. A Contratada deverá realizar a implantação inicial (onboarding) dos serviços, com levantamento do ambiente, validação de acessos, inventário lógico da infraestrutura, definição do plano de trabalho a ser realizado e início do monitoramento e rotinas operacionais, em até 30 (trinta) dias contados da assinatura do contrato, mediante aprovação do Contratante.

7.1.3. Os serviços serão prestados para atender a Câmara Municipal de Carapicuíba, situada à Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuiba – SP, podendo envolver atividades presenciais e remotas, conforme necessidade técnica e determinação do Contratante.

7.1.4. Quando houver necessidade de atividade presencial (vistorias, intervenções técnicas, validações e apoio à operação), o atendimento ocorrerá em dias úteis, das 9h às 18h, mediante agendamento com o fiscal do contrato, sem prejuízo dos atendimentos remotos e do registro de chamados.

7.1.5. Intervenções que impliquem em alterações na infraestrutura (mudanças de configuração de rede, firewall, servidores e rotinas de backup), bem como eventuais atividades presenciais, ocorrerão conforme priorização e autorização prévia do Contratante, observadas as janelas de manutenção acordadas.

7.1.6. As despesas de deslocamento, diárias e demais custos necessários à execução dos serviços presenciais, quando demandados e autorizados, serão de responsabilidade da Contratada, salvo previsão diversa no instrumento convocatório e no contrato.

7.1.7. Após concluída a implantação inicial prevista no item 7.1.2, a Contratada deverá executar continuamente os serviços contratados, incluindo operação assistida, suporte técnico, rotinas preventivas, atendimento à incidentes e emissão de relatórios, conforme este Termo de Referência e o contrato.

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850

7.2. **Obrigações do contratante:**

7.2.1. Acompanhar, fiscalizar, conferir e avaliar o objeto do presente contrato afim de que sejam executados rigorosamente em conformidade com o estabelecido neste instrumento;

7.2.2. A fiscalização do contrato, por parte do Contratante, não exonera nem diminui a completa responsabilidade da Contratada por inobservância ou omissão a qualquer das cláusulas contratuais estabelecidas no presente ajuste;

7.2.3. Prestar informações, esclarecer e fazer abertura de chamados técnicos, quando necessário;

7.2.4. Deverá responsabilizar-se pela infraestrutura predial e física necessária ao funcionamento do ambiente (energia elétrica, aterramento, climatização, racks, cabeamento estruturado e pontos lógicos), bem como por prover acesso às áreas técnicas, quando necessário.

7.2.5. Zelar pelos ativos de TI sob sua guarda, permitindo o acesso da Contratada para fins de suporte, monitoramento e manutenção.

7.2.6. Eventuais danos decorrentes de mau uso, vandalismo, condições ambientais inadequadas ou intervenções por terceiros não autorizados serão apurados e comunicados, não se caracterizando como falha imputável à Contratada.

7.2.7. Notificar a Contratada, por escrito, de qualquer irregularidade constatada, para que seja sanada;

7.2.8. Efetuar o pagamento nas condições e nos preços pactuados;

7.2.9. Aplicar à contratada as penalidades regulamentares e contratuais.

7.3. **Obrigações da contratada:**

7.3.1. Prestar serviços especializados de gerenciamento da infraestrutura de TI do contratante, incluindo: (I) administração e suporte aos serviços de Next Generation Firewall (NGFW); (II) manutenção preventiva e corretiva de servidores (sistemas, serviços e rotinas operacionais); (III) gerenciamento e suporte da rede cabeada e sem fio; e (IV) execução e monitoramento regular das rotinas de backups, com armazenamento de dados em nuvem, durante toda a vigência contratual;

7.3.2. Rotinas de backup com execução de backups regulares, monitorar janelas, validar execução, realizar testes periódicos de restauração, manter relatórios e garantir armazenamento em nuvem com controle de acesso e trilhas de auditoria;

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850

7.3.3. Gestão do NGFW com administração de políticas de segurança, VPNs, atualizações, relatórios, e tratamento de incidentes de segurança relacionados ao perímetro;

7.3.4. Manutenção preventiva de servidores com rotinas de patching, health checks, monitoramento de recursos e ações preventivas;

7.3.5. Gestão de rede cabeada e wi-fi com monitoramento, resolução de problemas, ajustes de configuração, inventário lógico e documentação;

7.3.6. A Contratada deverá disponibilizar canais de comunicação para abertura de chamados durante a vigência do contrato (telefone, email, website), com recebimento de chamados 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, e registro com número de protocolo;

7.3.7. A Contratada deverá realizar o atendimento inicial aos chamados técnicos em até 24 (vinte e quatro) horas a partir da abertura do chamado, com diagnóstico preliminar e plano de ação. Quando o incidente demandar substituição de dispositivo de propriedade do Contratante, a Contratada deverá indicar formalmente as medidas necessárias e apoiar na recuperação dos serviços, não se incluindo no escopo o fornecimento de peças ou equipamentos, salvo previsão expressa no contrato;

7.3.8. Buscar informações complementares para correta identificação da falha/incidente e definição das ações técnicas, incluindo coleta de evidências (logs, métricas, eventos e testes), não cabendo alegação de impossibilidade do atendimento por imprecisão do chamado, desde que o Contratante forneça as informações mínimas disponíveis;

7.3.9. Executar as ações corretivas necessárias à restauração do serviço, incluindo ajustes de configuração, aplicação de correções, recomposição de serviços e validações técnicas. Quando a causa envolver defeito físico de ativo do Contratante, a Contratada deverá emitir recomendação técnica e apoiar o processo de garantia junto aos fabricantes, quando aplicável;

7.3.10. A Contratada deverá atuar para minimizar indisponibilidades e restabelecer os serviços no menor prazo possível, priorizando sempre incidentes críticos. Reincidências de falhas de mesma natureza deverão ser tratadas com análise de causa raiz e plano de ação preventivo, formalmente apresentado ao fiscal do contrato;

7.3.11. Após cada atendimento, apresentar Relatório de Atendimento Técnico (RAT) contendo: identificação do chamado, data/hora de abertura, severidade, data/hora de início e término, diagnóstico, evidências coletadas, ações executadas, responsável técnico, status (resolvido/mitigado/pendente), e recomendações. O RAT deverá ser submetido à homologação da fiscalização do contrato;

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850

7.3.12. Considera-se o atendimento concluído após validação do Contratante quanto à normalização do serviço. Caso o chamado seja reaberto por persistência do problema, a Contratada deverá dar continuidade ao atendimento sem cobrança adicional, observados os níveis de serviço e condições contratuais;

7.3.13. Manter base de registros (histórico) contendo chamados, incidentes, mudanças, rotinas executadas, tempos de resposta e resolução, e lições aprendidas, disponibilizando acesso ao Contratante para consulta por técnicos e gestores, resguardadas as credenciais e informações sensíveis;

7.3.14. Comunicar por escrito ao fiscal do contrato quando constatar indícios de mau uso, intervenção não autorizada ou sinais de vandalismo que impactem os ativos e serviços;

7.3.15. Prestar suporte técnico relacionado aos serviços contratados, incluindo administração dos dispositivos de firewall, conectividade da rede cabeada e sem fio, rotinas de backup e suporte aos servidores, conforme escopo definido neste Termo de Referência;

7.3.16. Realizar treinamento operacional para a equipe designada do Contratante, abordando rotinas de abertura e acompanhamento de chamados, leitura de relatórios, procedimentos de contingência e boas práticas de operação relacionadas a NGFW, rede e backups;

7.3.17. Realizar treinamento para acesso e uso do portal de visualização dos relatórios de backup, com orientações para solicitação de restauração (restore), quando aplicável;

7.3.18. Manter-se em compatibilidade com as obrigações assumidas no presente contrato durante toda a sua execução, conservando todas as condições de habilitação e qualificação exigidas no procedimento licitatório;

7.3.19. Indicar preposto para manter entendimentos e receber comunicações, ou transmiti-las à fiscalização do presente objeto;

7.3.20. Empregar, na execução do ajuste, bem como na manutenção e nas atividades dele decorrentes, pessoal idôneo, e habilitado;

7.3.21. Substituir, sempre que exigido pela Contratante, qualquer um de seus empregados em serviço, cuja atuação, permanência ou comportamento forem julgados prejudiciais, inconvenientes ou insatisfatórios à execução dos serviços;

7.3.22. Responsabilizar-se, direta e exclusivamente, pelos serviços objeto deste Contrato, respondendo por seus empregados, nos termos da lei, por todos os danos e prejuízos que, na execução dos serviços, venham direta ou indiretamente provocar ou causar à CONTRATANTE ou a terceiros;

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850

7.3.23. Diligenciar permanentemente no sentido de preservar e manter a Contratante à margem de todas as reivindicações, queixas e representações de qualquer natureza, referentes aos serviços;

7.3.24. Sujeitar-se a ampla e irrestrita fiscalização por parte da Contratante, no acompanhamento da execução do serviço, prestando todos os esclarecimentos que lhe forem solicitados e atendendo às reclamações formuladas;

7.3.25. Arcar com o pagamento de quaisquer tributos, multas ou ônus oriundos da contratação, pelos quais seja responsável, principalmente os de natureza fiscal e comercial;

7.3.26. A Contratada responderá integralmente pelos serviços sob sua execução e gestão, respeitadas as responsabilidades do Contratante quanto à infraestrutura predial/física e disponibilização de acessos e informações necessárias, conforme este Termo de Referência.

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

7.4. **Da vigência do contrato**

7.4.1. O prazo de vigência do contrato será de 1 (um) ano, contado a partir da data de assinatura, prorrogáveis na forma da Lei.

8. GESTÃO DO CONTRATO

8.1. Os gestores e fiscais de contratos e os respectivos substitutos serão representantes da Câmara Municipal de Carapicuíba/SP designados pela autoridade competente, com atribuições de acompanhar e fiscalizar a execução do contrato, nos termos dos art. 21 a 23, observados os requisitos estabelecidos no art. 11, do Ato da Mesa nº 7/2023, de 11 de dezembro de 2023, que regulamenta a Lei nº 14.133, de 1º de abril de 2021, no âmbito da Câmara Municipal de Carapicuíba.

8.2. A fiscalização de que trata este item não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por qualquer irregularidade ou ainda resultante de imperfeições técnicas, vícios redibitórios, não implica em corresponsabilidade do CONTRATANTE ou de seus agentes e prepostos.

9. CRITÉRIOS PARA MEDIÇÃO E PAGAMENTO

9.1. **Do recebimento dos serviços**

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850

9.1.1. O recebimento do objeto do contrato ocorrerá da seguinte forma:

9.1.1.1.Provisoriamente, pelo responsável por seu acompanhamento e fiscalização, mediante termo detalhado, elaborado mensalmente, no prazo de 5 (cinco) dias contados do recebimento da nota fiscal pertinente, quando verificado o cumprimento das exigências de caráter técnico previamente definidos no contrato;

9.1.1.2.Definitivamente, por servidor ou comissão designada pela autoridade competente, no prazo de 10 (dez) dias após o encerramento do contrato, mediante termo detalhado que comprove o atendimento das exigências contratuais.

9.1.2. Os prazos e os métodos para a realização dos recebimentos provisório e definitivo deverão ser definidos no instrumento convocatório e/ou no contrato.

9.2. **Do prazo e forma de pagamento**

9.2.1. O pagamento será realizado no prazo máximo de até 5 (cinco) dias, contados a partir do recebimento da Nota Fiscal/Fatura devidamente atestada pela competente área, por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pela Contratada, ou através de boleto bancário com vencimento mínimo de 5 (cinco) dias.

9.2.2. Constatando-se alguma irregularidade da Contratada, será providenciada sua notificação, por escrito, para que, no prazo de 05 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da Administração Contratante.

9.2.3. Não será iniciada a contagem de prazo caso os documentos fiscais apresentados ou outros necessários contenham incorreções.

9.2.4. Quando for constatada qualquer irregularidade na nota fiscal, a Contratante solicitará imediatamente a Contratada carta de correção, quando couber, ou ainda a pertinente regularização, que deverá ser encaminhada à Contabilidade da Câmara Municipal de Carapicuíba, no prazo de 3 (três) dias úteis.

9.2.5. Caso a Contratada não apresente carta de correção no prazo estipulado, o prazo para pagamento será reiniciado a partir da data da sua apresentação.

9.2.6. Todo e qualquer pagamento será efetuado direta e exclusivamente à Contratada, eximindo-se a Contratante de obrigações a terceiros por títulos colocados em cobrança, descontos, caução ou outra modalidade de circulação ou garantia, inclusive quanto a direitos emergentes desta, ficando estabelecido que, em hipótese alguma, aceitará tais títulos, os quais serão devolvidos, incontinente, à pessoa física ou jurídica que os houver apresentado.

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850

9.2.7. Nenhum pagamento será efetuado à Contratada enquanto pendente de liquidação qualquer obrigação financeira de penalidade que lhe tenha sido imposta.

9.2.8. A Câmara Municipal de Carapicuíba não se responsabilizará por quaisquer autuações fiscais e gravames futuros decorrentes de interpretações errôneas por parte do licitante vencedor quanto à aplicação de tributos e suas alíquotas, suspensões, base de cálculo, isenções etc.

9.3. **Do critério de reajuste/repactuação**

9.3.1. O critério de reajuste será definido no instrumento de contrato.

10. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

10.1. **Forma de seleção e critério de julgamento da proposta.**

10.1.1. O fornecedor será selecionado por meio da realização de procedimento de licitação, na modalidade pregão eletrônico, que culminará com a seleção da proposta de menor preço global.

10.2. **Exigências de habilitação**

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

10.2.1.1. Habilitação Jurídica

10.2.1.1.1. Registro comercial, no caso de empresa individual;

10.2.1.1.2. Ato constitutivo, estatuto social, contrato social ou sua consolidação e posteriores alterações contratuais, devidamente registradas na junta comercial e, em vigor; e no caso de sociedade por ações, acompanhado da ata de eleição de sua atual administração, registrados e publicados;

10.2.1.1.3. Inscrição do ato constitutivo, no caso de sociedades civis, acompanhada de prova da diretoria em exercício;

10.2.1.1.4. Decreto de autorização, em se tratando de empresa ou sociedade estrangeira em funcionamento no País, e ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir;

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850

10.2.1.1.5. Em se tratando de Microempreendedor Individual – MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio www.portaldoempreendedor.gov.br

10.2.1.2. Regularidade fiscal, social e trabalhista

10.2.1.2.1. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ);

10.2.1.2.2. Prova de regularidade para com a Fazenda Federal, consistente na apresentação da Certidão Conjunta de Tributos Federais e Dívida Ativa da União, a qual engloba também os tributos relativos ao INSS;

10.2.1.2.3. Prova de regularidade para com a Fazenda Estadual, consistente na apresentação de certidão que comprove regularidade fiscal junto ao Estado ou Distrito Federal;

10.2.1.2.4. Prova de regularidade para com a Fazenda Municipal da sede da empresa licitante, consistente na apresentação de certidão de regularidade de débitos municipais mobiliários;

10.2.1.2.5. Certidão que comprove a regularidade relativa ao Fundo de Garantia por Tempo de Serviço (FGTS);

10.2.1.2.6. Certidão Negativa de Débitos Trabalhistas – CNDT.

10.2.1.3. Qualificação Econômico-Financeira

10.2.1.3.1. Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - Lei nº 14.133, de 2021, art. 69, caput, inciso II);

10.2.1.3.2. Comprovação de possuir capital social mínimo ou patrimônio líquido mínimo de 10% (dez por cento) do valor estimado do objeto da contratação. A comprovação será obrigatoriamente feita pelo Ato Constitutivo, Estatuto ou Contrato Social em vigor e devidamente registrado ou pelo balanço patrimonial e demonstrações contáveis do último exercício social, já exigíveis e apresentados na forma da lei.

10.2.1.4. Qualificação Técnica

10.2.1.4.1. Para fins de comprovação de aptidão para desempenho de atividade pertinente e compatível em características, quantidades e prazos com o objeto, a licitante deverá apresentar atestado(s) de capacidade técnica, emitido(s) por pessoa jurídica de direito público ou privado, em nome da licitante, que comprove(m) a execução satisfatória de serviços compatíveis com o objeto desta contratação, sendo considerada como parcela de maior relevância e valor significativo a prestação de serviços de gerenciamento/operação de Next Generation Firewall (NGFW), assim,

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850

a licitante deverá comprovar, por meio de ao menos 01 (um) atestado, a execução de serviços de gerenciamento/operação de NGFW, contemplando, no mínimo, atividades como administração, monitoramento e suporte operacional, sem exigência de quantitativos ou período de execução mínimo.

10.2.1.4.2. Os Atestados e Declarações deverão ser apresentados em papel timbrado, original ou cópia reprográfica autenticada, assinados por autoridade ou representante de quem os expediu, com a devida identificação e cargo.

10.2.1.5. DA VEDAÇÃO À PARTICIPAÇÃO DE EMPRESAS EM CONSÓRCIO

10.2.1.5.1. Não será admitida a participação de empresas em consórcio no presente certame, com fundamento no art. 15 da Lei nº 14.133/2021, que confere à Administração Pública a faculdade de vedar ou autorizar tal modalidade de participação, mediante decisão motivada, considerando as características específicas do objeto contratual.

10.2.1.5.2. A vedação ora adotada fundamenta-se nas seguintes razões objetivas e técnicas:

a) **Ampla competitividade do mercado fornecedor.** O mercado de prestação de serviços gerenciados de Tecnologia da Informação — abrangendo Next Generation Firewall, Backup como Serviço (BaaS) e monitoramento por NOC — conta com diversas empresas especializadas com capacidade técnica e operacional para atender integralmente ao objeto deste Termo de Referência de forma individual, sem necessidade de consórcio. Trata-se de segmento consolidado, com fornecedores plenamente aptos a cumprir as exigências aqui estabelecidas, o que restou confirmado pelas pesquisas de preços realizadas pela própria Câmara Municipal de Carapicuíba na fase de planejamento desta contratação, nas quais foram identificadas diversas empresas individualmente habilitadas a prestar os serviços ora licitados, com propostas compatíveis e competitivas. A existência dessas empresas demonstra que a vedação a consórcios não reduz o universo de potenciais licitantes a ponto de comprometer a ampla disputa. Desse modo, a admissão de consórcios não se revela necessária para ampliar a competitividade do certame, porquanto a concorrência entre empresas individuais já é suficientemente robusta para garantir a obtenção da proposta mais vantajosa para a Administração.

b) **Responsabilidade técnica unificada e indivisível.** O objeto contratual compreende uma solução tecnológica integrada, cujos componentes — firewall, backup em nuvem, monitoramento NOC e suporte técnico N3 — são interdependentes e devem ser operados de forma coesa e ininterrupta por um único responsável técnico. A execução por consórcio introduziria fragmentação da responsabilidade entre os consorciados, dificultando a exigibilidade de SLAs, a gestão de incidentes e a imputação de responsabilidade em caso de falhas, em prejuízo direto à continuidade do serviço público e à segurança institucional.

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850

c) **Risco operacional na segurança da informação.** A natureza do objeto — que envolve monitoramento 24x7, acesso privilegiado a toda a infraestrutura de rede, servidores e dados institucionais, incluindo informações sensíveis sujeitas à LGPD — exige que a Contratada seja uma entidade única, com cadeia de comando clara, procedimentos internos de segurança da informação unificados e responsabilidade integral pelos dados acessados. A participação em consórcio criaria múltiplos vínculos de acesso e responsabilidade entre empresas distintas, elevando o risco operacional e de segurança de forma incompatível com as exigências do objeto e com as obrigações desta Câmara perante a Lei nº 13.709/2018 (LGPD).

10.2.1.5.3. Diante do exposto, a vedação à participação de consórcios não restringe indevidamente a competitividade do certame, mas antes resguarda a integridade técnica e operacional da solução contratada, em plena conformidade com a Lei nº 14.133/2021 e com os princípios da eficiência e da segurança na execução contratual.

11. ESTIMATIVA DE PREÇOS E PREÇOS REFERENCIAIS

11.1. O custo estimado da contratação é de R$ 511.205,15 (Quinhentos e onze mil, duzentos e cinco reais e quinze centavos).

12. RECURSO ORÇAMENTÁRIO

12.1. Dotação Orçamentária nº 3.3.90.40.99 - Outros Serviços de TI e Comunicação.

13 - OUTRAS DISPOSIÇÕES

13.1. Demais disposições estarão explicitadas no Edital e seus anexos.

14. RESPONSÁVEIS PELA ELABORAÇÃO

14.1. Servidor Milton Uemura – Setor de TI.

Travessa Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000 – Telefone: 11 3536-8850